ESET PROTECT On-Prem

インストール、アップグレード、移行ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Digital Security
Progress. Protected.

ESET PROTECT On-PremはESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2024年/4月/17日

ヘルプ

このインストールガイドは、ESET PROTECT On-Premのインストールおよびアップグレードを支援することを目的とし、プロセスの手順を説明します。

一貫性と混乱防止のため、このガイド全体で使用される用語は、ESET PROTECT On-Premパラメーター名に基づいています。特定の関心や重要性があるトピックをハイライトするために、記号のセットを使用します。

注意は、特定の機能や一部の関連トピックへのリンクなど、有用な情報を示します。

注意が必要です。省略しないでください。通常、緊急性はありませんが、重要な情報です。

最大限の注意を持って処理すべき重大な情報。警告は、特に、危険な誤りにつながるおそれがある行為をしないようにするために示されています。警告の括弧内のテキストを読んで理解してください。極秘システム設定や危険な事項を参照しています。

含まれる場合は、トピックに関連する使用例を説明するサンプルシナリオ。例は、複雑なトピックを説明するために使用されます。

変換	意味
太字	ボックスやオプションボタンなどのインターフェース項目の名前。
斜体	提供する情報のプレースホルダー。たとえば、ファイル名またはパスは、実際のパスまたはファイル名を入力することを意味します。
Courier New	コードサンプルまたはコマンド。
ハイパーリンク	クロス参照されたトピックまたは外部Webロケーションに迅速、簡単にアクセスできます。ハイパーリンクは青でハイライトされます。下線が付く場合もあります。
%ProgramFiles%	Windowsおよびその他のインストール済みプログラムを保存するWindowsシステムディレクトリ。

- オンラインヘルプはヘルプコンテンツの一次ソースです。最新バージョンのオンラインヘルプは、作業インターネット接続があるときに、自動的に表示されます。ESET PROTECT On-Premオンラインヘルプページには、上のナビゲーションヘッダーに3つのアクティブなタブがあります。インストール/アップグレード、管理、仮想アプライアンス展開
- このガイドのトピックは複数の章とサブ章に分割されます。上の検索フィールドを使用すると、関連する情報を検索できます。

ページの上のナビゲーションバーからユーザーガイドを開くと、そのガイドの内容のみが検索されます。たとえば、管理者ガイドを開く場合、インストール/アップグレードおよびVA展開ガイドからのトピックは検索に含まれません。

- ESETナレッジベースでは、一般的な質問への回答と、さまざまな問題の推奨ソリューションが提供されます。ESET技術スペシャリストが定期的にアップデートすることで、ナレッジベースは、さまざまな問題の解決のために、最も強力なツールです。
- ESETフォーラムは、相互ヘルプのための簡単な方法です。ESET製品に関連する問題または質問を投稿できます。

インストール/アップグレード/移行

ESET PROTECT On-Premは、ネットワーク環境のクライアントワークステーション、サーバー、モバイルデバイス上のESET製品を1か所から管理できるアプリケーションです。ESET PROTECT On-Premのビルトイ

ンのタスク管理システムを使用すると、リモートコンピューターにESETセキュリティソリューションをインストールして、新しい問題や検出に迅速に対応できます。

ESET PROTECT On-Premだけでは悪意のあるコードに対する保護を提供しません。環境の保護は、ワークステーションやモバイルデバイス上のESET Endpoint Securityまたはサーバーコンピューター上のWindows用のESET Server Securityといったセキュリティソリューションがインストールされているかどうかによって決まります。

バージョン11.0以降ESET PROTECTは名前がESET PROTECT On-Premに変更されました。

ESET PROTECT On-Premは2つの主な原理に基づいて開発されています。

- **集中管理** – ネットワーク全体が、1つの場所から、設定、管理、および監視できます。
- **拡張性** – 小規模ネットワークにも大規模なエンタープライズ環境にもシステムを展開できますESET PROTECT On-Premはインフラストラクチャの拡大に対応するように設計されています。

ESET PROTECT On-Premは次世代のESETセキュリティ製品をサポートし、前の世代の製品とも互換性があります。

ESET PROTECT On-Premヘルプページには、完全なインストールおよびアップグレードガイドがあります。

- ESET PROTECT On-Premのアーキテクチャ
- インストール処理
- アップグレード手順
- 移行手順
- アンインストール手順
- ライセンス管理
- 展開処理とGPOまたはSCCMを使用したエージェント展開
- ESET PROTECT On-Premをインストールした後の最初の手順
- 管理ガイド

ESET PROTECT On-Prem 11.0の新機能

ESET LiveGuard Advanced動作レポート

EDRのお客様に、より堅牢な新しい動作レポートを提供する準備としてESET LiveGuard Advancedによって生成された動作レポートをダウンロードするオプションが追加されました。詳細を見る

製品のアップデートを確認する新しいクライアントタスク

このクライアントタスクは、新しい製品バージョンの可用性をチェックします。新しいバージョンが見つかった場合はダウンロードされ、インストールプロセスが開始されます。詳細を見る

動的グループの時間ルール

動的グループテンプレートの追加条件として、時間ルールを含めるオプションが導入されました。ルールが設定されると、コンピューターは指定された期間中にのみ動的グループに配置されます。詳細を見る

製品名の変更

製品名がESET PROTECTからESET PROTECT On-Premに変更されました。このリリースには、製品名関連のその他の変更もいくつか含まれています。

その他の改善と不具合修正

その他の改善内容については、変更ログを参照してください。

アーキテクチャ

ESET PROTECT On-Premは次世代のリモート管理システムです。

ESETセキュリティ製品の完全な展開を実行するには、次のコンポーネントをインストールする必要があります(WindowsおよびLinuxプラットフォーム)。

- ESET PROTECTサーバー
- ESET PROTECT Webコンソール
- ESET Managementエージェント

次のサポートコンポーネントは任意です。ネットワーク上のアプリケーションの最適なパフォーマンスを保証するためにインストールすることをお勧めします。

- RD Sensor
- ESET BridgeHTTPプロキシ
- Mobile Device Connector

ESET PROTECTコンポーネントは、証明書を使用して ESET PROTECTサーバーと通信します。ナレッジベース記事で、ESET PROTECT On-Premの証明書に関する詳細をお読みください。

インフラストラクチャ要素の概要

次の表では ESET PROTECTインフラストラクチャ要素と主な機能の概要について説明します。

機能	ESET PROTECTサーバー	ESET Managementエージェント	ESETセキュリティ製品	ESET BridgeHTTPプロキシ	ESETサーバー	モバイルデバイスコネクター
ESETセキュリティ製品のリモート管理(ポリシー、タスク、レポートの作成など)	✔	X	X	X	X	X

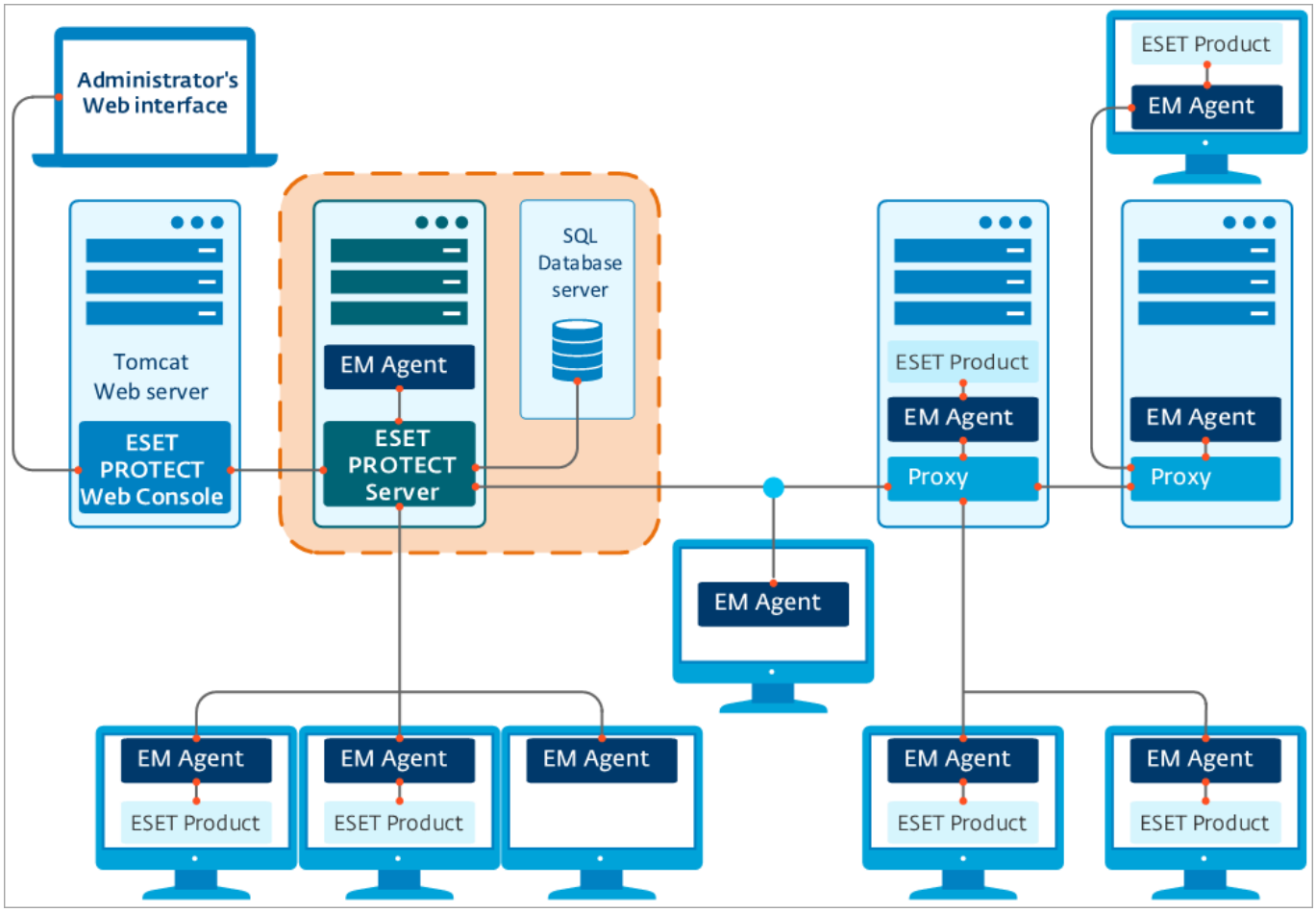
機能	ESET PROTECTサーバー	ESET Managementエージェント	ESETセキュリティ製品	ESET BridgeHTTPプロキシ	ESETサーバー	モバイルデバイスコネクター
ESETPROTECTサーバーとの通信、およびクライアントデバイスでのESETセキュリティ製品の管理	X	✔	X	X	X	✔
アップデートの提供、ライセンス検証	X	X	X	*	✔	X
アップデートのキャッシュと転送(検出エンジン、インストーラー、モジュール)	X	X	**	✔	X	X
ESET Managementエージェントと ESET PROTECTサーバーとの間のネットワークトラフィックの転送	X	X	X	✔	X	X
クライアントデバイスの保護	X	X	✔	X	X	X
モバイルデバイスのリモート管理	X	X	X	X	X	✔

* オフラインリポジトリでのみ。

** ESETセキュリティ製品はインストーラーをキャッシュに保存しません。

サーバー

ESET PROTECTサーバーは実行アプリケーションで、ESET Managementエージェントまたは[HTTPプロキシ]経由でサーバーに接続するクライアントから受信されたすべてのデータを処理します。データを正しく処理するには、ネットワークデータが保存されているデータベースサーバーへ安定した方法で接続している必要があります。パフォーマンスの強化のために、別のコンピューターにデータベースサーバーをインストールすることをお勧めします。

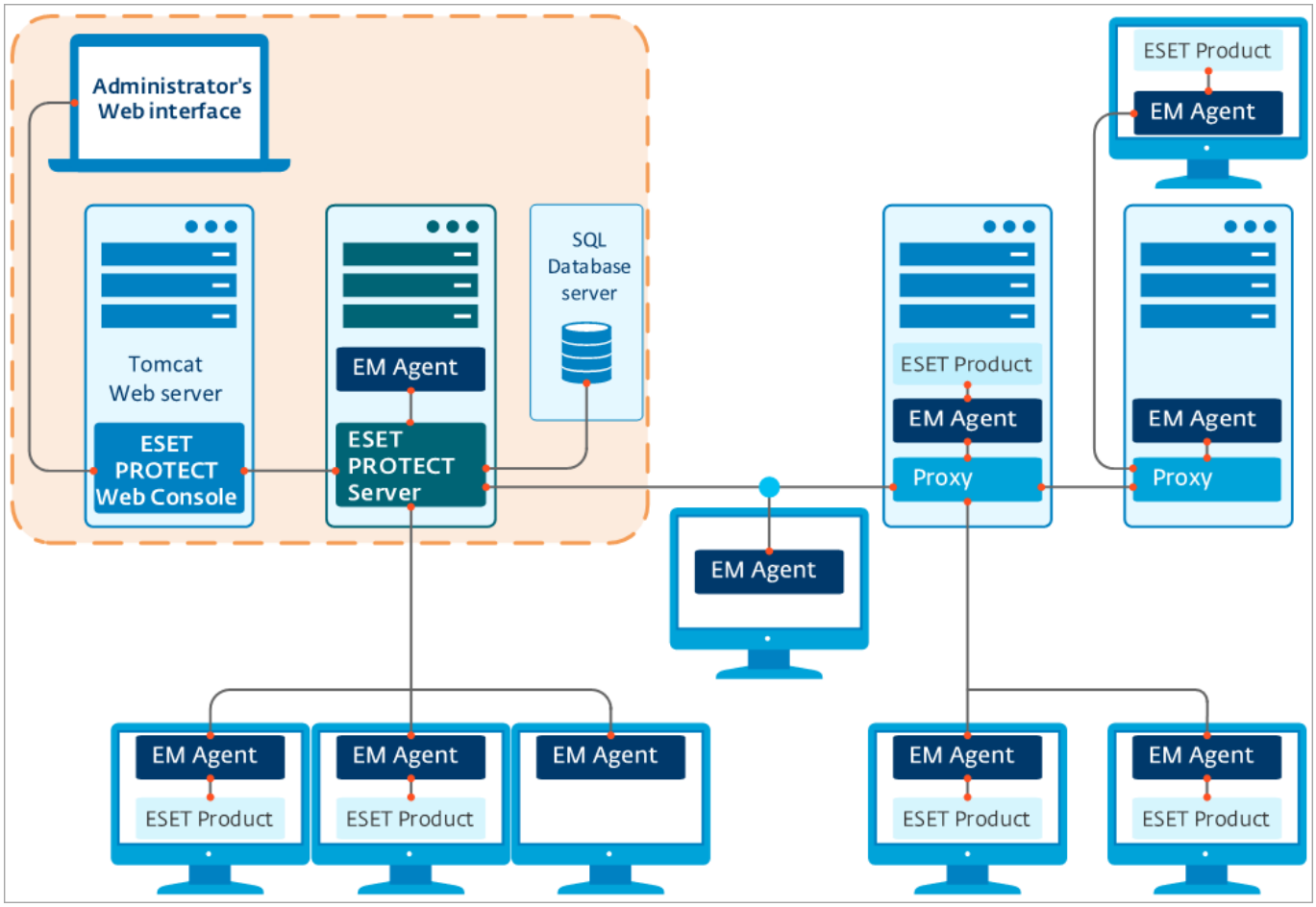


Webコンソール

ESET PROTECT Webコンソールは Webベースのユーザーインターフェースであり、現在の環境でESETセキュリティソリューションを管理できます。ネットワークのクライアントのステータスの概要を表示し、管理対象外のコンピューターにリモートでESETソリューションを展開するために使用できます。Webコンソールはブラウザを使用してアクセスします(「サポート対象のWebブラウザ」を参照)。インターネットからWebサーバーにアクセスする場合は、ほぼすべての場所とデバイスからESET PROTECT On-Premを使用できます。

Webコンソールは、HTTP Webサーバーとして Apache Tomcatを使用します。ESETインストーラーまたは仮想アプライアンスでバンドルされたTomcatを使用しているときには、WebコンソールへのTLS 1.2および1.3接続のみが許可されます。

ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。



ESET BridgeHTTPプロキシ

ESET PROTECT On-Premでは、プロキシサービスとしてESET Bridgeを使用して、次の操作を行えます。

- ダウンロードとキャッシュ:ESET PROTECT On-Premによってプッシュされたモジュールアップデート、インストールおよびアップデートパッケージ(ESET Endpoint Security MSIインストーラーなど)、ESETセキュリティ製品のアップデート(コンポーネントおよび製品アップデート)、ESET LiveGuard結果。
- ESET Managementエージェントから ESET PROTECT On-Premへ通信を転送します。

ESET Bridgeインストールおよび設定の詳細については、ESET Bridgeオンラインヘルプをお読ください。

> **Apache HTTP Proxyユーザー**
> ESET PROTECT On-Prem 10.0以降では、ESET BridgeがApache HTTP Proxyに代わります。Apache HTTP Proxyは限定サポートに達しました。Apache HTTP Proxyを使用している場合は、ESET Bridgeへの移行をお勧めします。

エージェント

エージェント(ESET Managementエージェント)はESET PROTECT On-Prem の基本的な要素です。クライアントはESET PROTECTサーバーで直接通信せず、エージェントがこの通信を容易にしています。エージェントは、クライアントから情報を収集し、ESET PROTECTサーバーに送信します。ESET PROTECTサーバーがクライアントのタスクを送信する場合、エージェントに送信され、エージェントがこのタスクをクライ

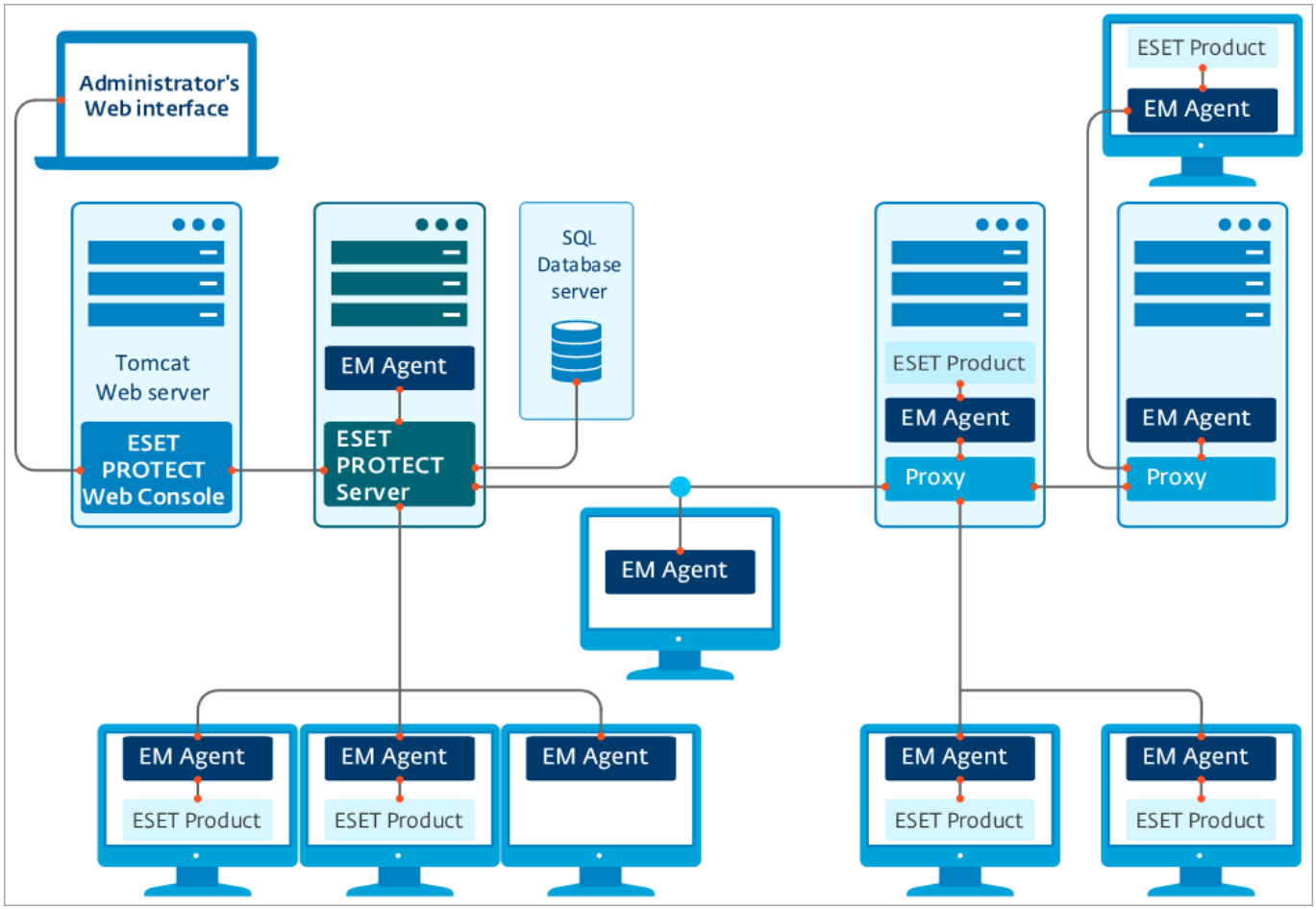
アントに送信します。ESETManagementエージェントは、新しい改善された通信プロトコルを使用します。

エンドポイント保護の実装を簡素化するために、スタンドアロンのESET Managementエージェントがインストールされ、ESET PROTECT On-Premスイートに含まれます(これはESET PROTECTサーバーおよびESET製品またはオペレーティングシステム間のすべての通信をカバーする、シンプルで、高度なモジュール性および軽量なサービスです。ESET PROTECTサーバーと直接通信せず、ESET製品がエージェント経由で通信します。ESET Managementエージェントがインストールされ、ESET PROTECTサーバーと通信ができるクライアントコンピューターは、「管理されている」として参照されます。ESETソフトウェアのインストールの有無にかかわらず、エージェントを任意のコンピューター上にインストールすることができます。

利点は次の通りです。

- 簡単設定 – 会社の標準インストールの一部としてエージェントを展開できます。
- セキュリティ管理場所 – エージェントはいくつかのセキュリティシナリオを格納する設定ができるので、検出に対する対応時間が大幅に少なくなります。
- オフラインセキュリティ管理 - ESET PROTECTサーバーに接続していない場合、エージェントはイベントに応答することができます。

エージェントとESET PROTECTサーバー間の通信プロトコルは、認証をサポートしません。ESET PROTECTサーバーへのエージェント通信の転送で使用されるプロキシソリューションと必要な認証は動作しません。
Webコンソールまたはエージェントで既定以外のポートを使用する場合は、ファイアウォールの調整が必要になることがあります。そうでない場合、インストールが失敗する可能性があります。



Rogue Detection Sensor

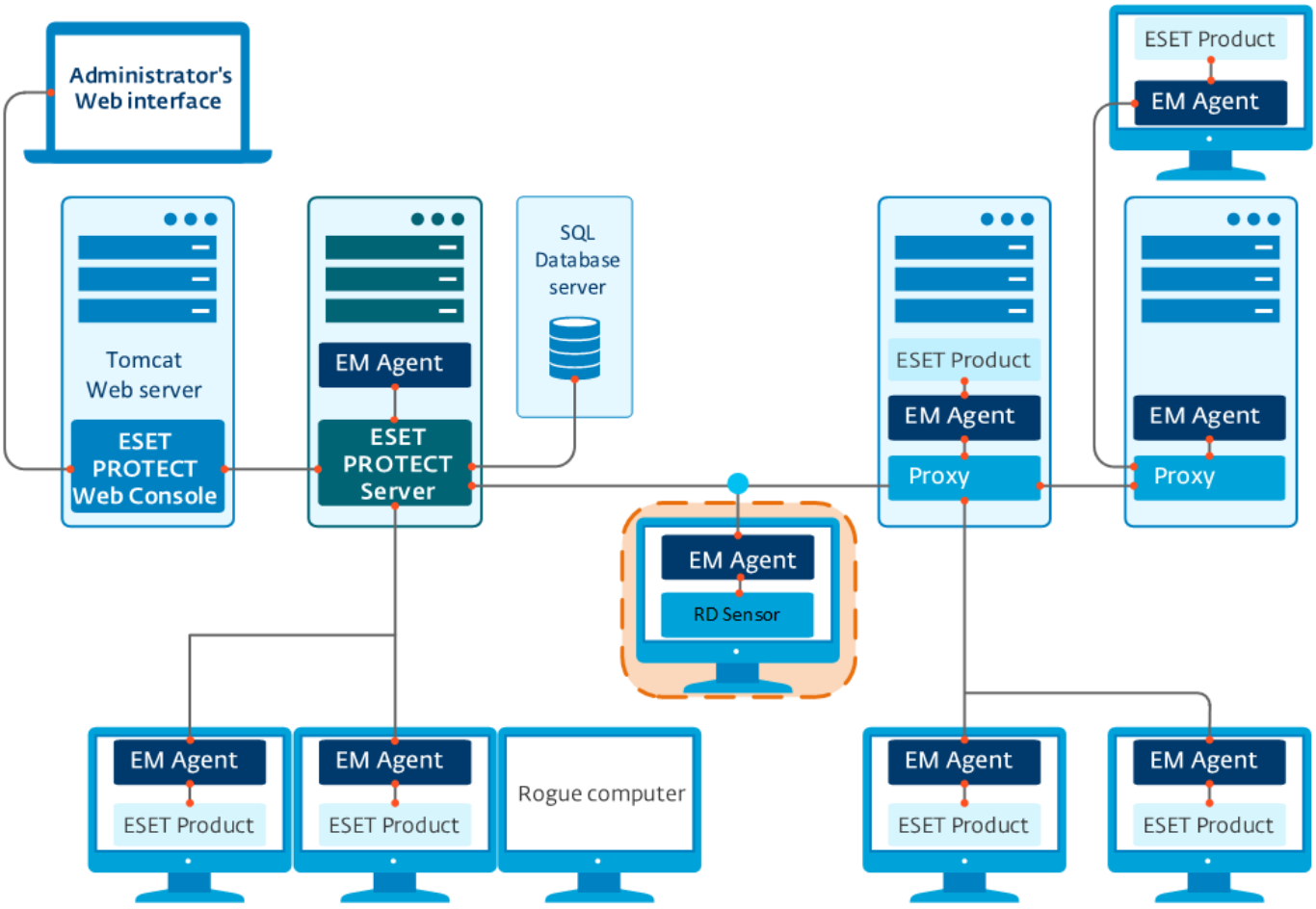
Rogue Detection Sensor (RD Sensor)はネットワークのコンピューターを検索するローグシステム検出ツールです。Sensorは、手動で検索および追加せずに、ESET PROTECT On-Premから新しいコンピューターを検索できるため便利です。検出されたコンピューターはただちに定義済みレポートで特定されて報告されます。これらのコンピューターを特定の状態グループに移動して、管理タスクを続行できます。

RD SensorはARPブロードキャストをアクティブに待機します。RD Sensorが新しいアクティブなネットワークコンポーネントを検出すると、RD SensorはARPユニキャストを送信し、(複数のポートを使用して)ホストフィンガープリントを実行し、検出されたコンピューターに関する情報をESET PROTECTサーバーに送信します。ESET PROTECTサーバーは、ネットワーク上で検出されたPCがESET PROTECTにとって不明か、既に管理されているかどうかを評価します。

ホストフィンガープリントはRD Sensorのメイン機能であるため、無効にできません。

> 複数のネットワークセグメントがある場合、Rogue Detection Sensorを各ネットワークセグメントに個別にインストールし、ネットワーク全体のすべてのデバイスの包括的なリストを生成する必要があります。

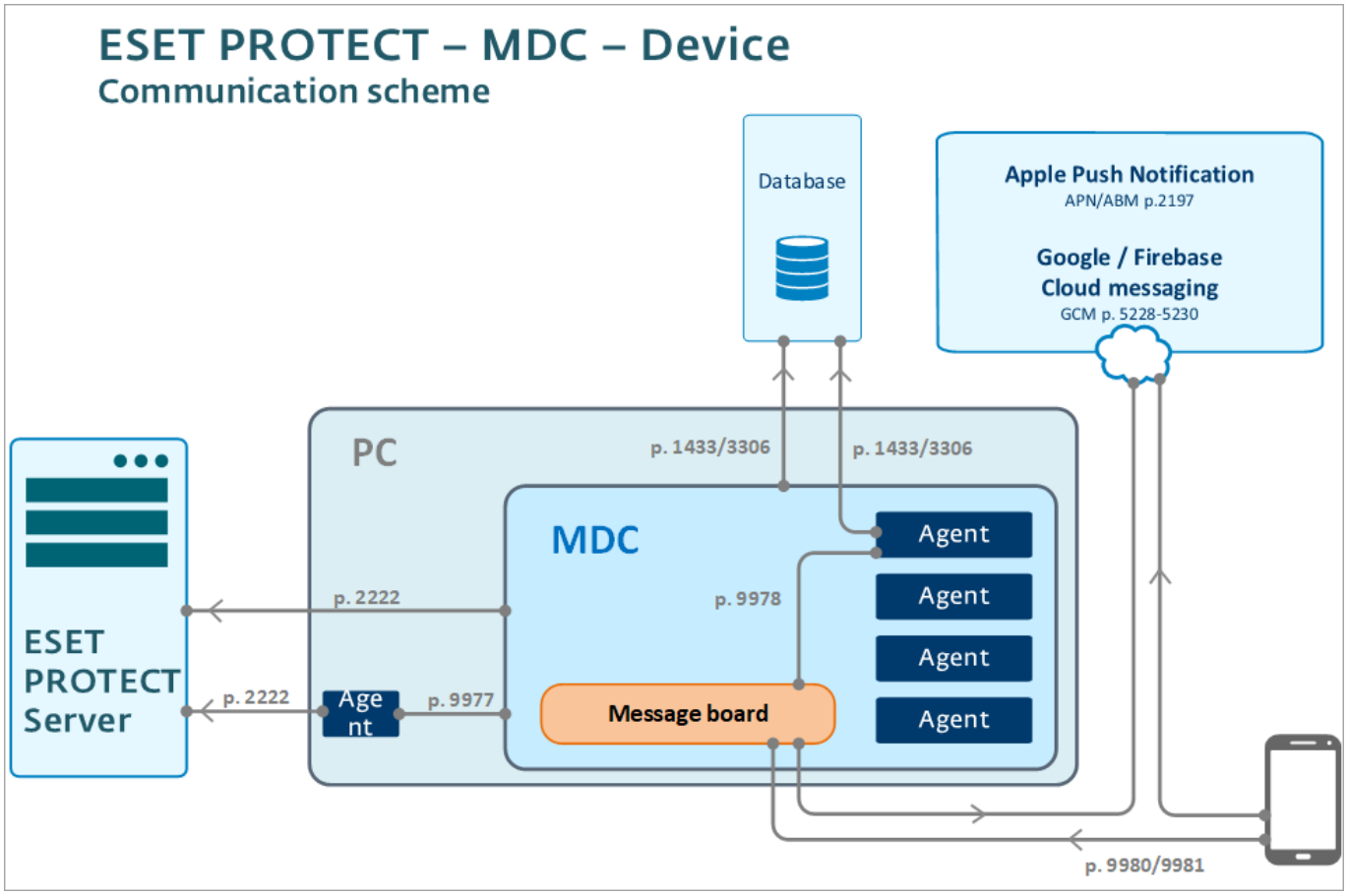
サーバー同期タスクによって、ネットワーク構造内(ドメイン、LDAP、Windowsネットワーク)内のすべてのコンピューターがESET PROTECTサーバーのコンピューターリストに自動的に追加されます。RD sensorの使用は、ドメインまたは他のネットワーク構造内にないコンピューターを検出し、ESET PROTECTサーバーに追加する場合に便利です。RD Sensorは既に検出されたコンピューターを記憶し、同じ情報を2回送信しません。



モバイルデバイスコネクター

ESET PROTECT Mobile Device Connectorは、ESET PROTECT On-Premでモバイルデバイス管理を可能にするコンポーネントであり、モバイルデバイス(AndroidおよびiOS)の管理と、ESET Endpoint Security for Androidの管理を可能にします。

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。



大きい画像を表示します

ESET PROTECTサーバーがホストされているデバイスとは別のホストデバイスにMDMコンポーネントを展開することをお勧めします。

約80台の管理対象モバイルデバイスの推奨ハードウェア前提条件は以下のとおりです。

ハードウェア	推奨構成
プロセッサ	4コア2.5 GHz
RAM	4 GB (推奨)
HDD	100 GB

81台以上の管理対象のモバイルデバイスの場合、ハードウェア要件はそれほど大きくなりませんESET PROTECT On-Premからのタスクの送信とモバイルデバイスでのタスクの実行までの遅延時間は、環境内のデバイス数に比例して長くなります。

Windows (オールインワンインストーラーまたはコンポーネントインストール) またはLinuxのMDMインストール手順に従います。

ESET Bridge HTTP Proxy、ミラーツール、および直接接続の違い

ESET製品の通信には、検出エンジンおよびプログラムモジュールのアップデートの他に、ESET LiveGrid®データ(以下の表を参照)とライセンス情報の交換があります。

ESET PROTECT On-Premはリポジトリから最新の製品をダウンロードし、クライアントコンピューターに配布します。配布されると、製品をターゲットコンピューターに展開できます。

ESETセキュリティ製品がインストールされたら、アクティベートする必要があります。アクティベーションの後、検出エンジンとプログラムモジュールが定期的にアップデートされます。

ESET LiveGrid®早期警告システムでは、お客様を迅速に保護するためにESETに即時に継続的に新しい侵入が通知されます。新しい検出をESET Research Labに送信し、分析および処理することができます。

ほとんどのネットワークトラフィックは製品モジュールアップデートによって生成されます。一般的に、ESETセキュリティ製品は、毎月約23.9MBの検出エンジンとプログラムモジュールアップデートをダウンロードします。

ESET LiveGrid®データ(約22.3MB)とアップデートバージョンファイル(最大11KB)はキャッシュに保存できない唯一の配布ファイルです。

レベルアップデートとナノアップデートの2種類のアップデートがあります。アップデートの種類の詳細については、ナレッジベース記事を参照してください

コンピューターのネットワークにアップデートを配布するときには、ESET Bridge HTTP Proxyまたはミラーツール(WindowsおよびLinux版で提供)というネットワーク負荷を削減するための2つの方法があります。

> このナレッジベース記事を読み、ミラーツールチェーンを設定(別のミラーツールからアップデートをダウンロードするようにミラーツールを設定)してください。

ESET通信タイプ

通信の種類	通信の頻度	ネットワークトラフィックの影響	プロキシ転送通信	プロキシキャッシュオプション1	ミラーリングオプション2	オフライン環境オプション
エージェント展開(プッシュ/リポジトリからのライブインストーラー)	1回限り	約 各クライアントにつき50 MB	はい	はい3	いいえ	はい(GPO / SCCM編集されたライブインストーラー)4
エンドポイントインストール(リポジトリからのソフトウェアインストール)	1回限り	約 各クライアントにつき100 MB	はい	はい3	いいえ	はい(GPO / SCCMパッケージURLによるインストール)4
検出エンジンモジュール/プログラムモジュールアップデート	1日に6回以上	毎月2.6 MB8	はい	はい	はい	はい(オフラインMirror Toolとカスタム HTTPサーバー)5
update.verのアップデートバージョンファイル	1日に最大8回	毎月2.6 MB8	はい	いいえ	-	-
アクティベーション/ライセンス確認	1日に4回	無視可能	はい	いいえ	いいえ	はい(ESET Business Accountで生成されたオフラインファイル)8
ESET LiveGrid®クラウドレピュテーション	都度	11 MB (毎月)	はい	いいえ	いいえ	いいえ

1.プロキシキャッシュの影響/利点については、ESET Bridge HTTP Proxyの使用を開始するときを参照してください。

2.ミラーの影響については、ミラーツールの使用を開始するときを参照してください。

3.インストール/アップグレードごとに、最初は1つのエージェント(特定のバージョンに1つ)/エ

ンドポイントを展開し、インストーラーがキャッシュに保存されるようにすることをお勧めします。

4.大規模ネットワークでのESET Managementエージェントの展開については、GPOとSCCMを使用したエージェント展開を参照してください。

5.初期検出エンジンアップデートは、インストールパッケージの期間によっては標準よりも大きくなる場合があります。これは、すべての新しい検出エンジンアップデートおよびモジュールアップデートがダウンロードされるためです。最初は1つのクライアントをインストールし、アップデートして、必要な検出エンジンおよびプログラムモジュールアップデートがキャッシュに保存されるようにすることをお勧めします。

6.インターネット接続がない場合Mirror Toolは検出エンジンアップデートをダウンロードできませんApache TomcatをHTTPサーバーとして使用し、ミラーツール(WindowsおよびLinux版で提供)で使用可能なディレクトリにアップデートをダウンロードできます。

7.検出エンジンアップデートを確認するときには、*update.ver*ファイルが常にダウンロードおよび解析されます。既定ではESETエンドポイント製品のスケジューラーは、新しいアップデートを1時間ごとに問い合わせます。クライアントワークステーションが1日8時間オンになっていることを前提としています。*update.ver*ファイルは約11 kbです。

8.はオフラインライセンスファイルをダウンロードしましたESET Business Account

ESET Bridge HTTP Proxyを使用してバージョン4および5製品のアップデートをキャッシュに保存できません。これらの製品のアップデートを配布するには、ミラーツールを使用します。

使用を開始するときESET Bridge (HTTP Proxy)

ベストプラクティスに基づき、37台以上のコンピューターがある場合は、ESET Bridge HTTP Proxyを展開することをお勧めします。

HTTPプロキシサーバーの日付と時刻が正しく設定されていることは、効果的なキャッシュ利用のために重要です。数分の違いにより、キャッシュメカニズムが効果的に機能せず、必要以上に多くのファイルがダウンロードされます。

複数のインストールとアンインストールが発生する1000コンピューターのテストネットワークにおけるアップデートでのみ使用されるネットワーク帯域幅の分析により、次のことが示されました。

- 直接インターネットに接続される場合(HTTP Proxyが使用されない場合)、1台のコンピューターは平均で毎月23.9 MBのアップデートをダウンロードします。
- HTTP Proxyを使用して、ネットワーク全体で合計毎月900 MBをダウンロードします。

コンピューターのネットワークで直接インターネット接続またはHTTP Proxyを使用して、毎月ダウンロードされるアップデートデータの簡易比較:

企業ネットワークのPC数	25	36	50	100	500	1.000
インターネットへの直接接続(MB/月)	375	900	1.250	2.500	12.500	25.000
ESET BridgeHTTP Proxy (MB/月)	30	50	60	150	600	900

使用を開始するときMirror Tool

オフライン環境の場合、つまり、ネットワークのコンピューターが長期間(数ヶ月、1年)インターネットに接続しない場合、ミラーツール(WindowsおよびLinux版で提供)によってのみ、製品モジュールアップデートを配布できます。これは、新しいアップデートが使用可能な場合に、新しいアップデートの要求ごとに、すべての使用可能なレベルアップデートおよびナノアップデートをダウンロードするためです。

このナレッジベース記事を読み、ミラーツールチェーンを設定(別のミラーツールからアップデートをダウンロードするようにミラーツールを設定)してください。

ESET Bridge HTTP Proxyとミラーツールの主な違いはESET Bridge HTTP Proxyは不足しているアップデート(たとえば、ナノアップデート3)のみをダウンロードしますがMirror Toolは特定の製品モジュールで不足しているアップデートに関係なく、すべての使用可能なレベルおよびナノアップデート(または指定されている場合はレベルアップデートのみ)をダウンロードすることです。

ストリームされたアップデートはミラーツールでは利用できません。可能な場合は、ミラーからアップデートするESET Bridge (HTTPプロキシ)経由のアップデートを優先することをお勧めします。コンピューターがオフラインで、インターネットに接続されている別のコンピューターにアクセスできESET Bridge HTTP Proxyを実行してアップデートファイルをキャッシュに保存できる場合でも、このオプションを選択します。

1. 000台のコンピューターの同じネットワークで、ESET Bridge HTTP Proxyの代わりにミラーツールをテストしました。分析は、毎月5,500MBのアップデートがダウンロードされたことを示しました。ダウンロードされたアップデートのサイズは、ネットワークにコンピューターを追加しても増加しませんでした。クライアントが直接インターネットに接続する構成と比較して負荷が大幅に減少しますがHTTP Proxyを使用したときほどのパフォーマンスの改善は見られません。

企業ネットワークのPC数	25	36	50	100	500	1.000
インターネットへの直接接続(MB/月)	375	900	1.250	2.500	12.500	25.000
ミラーツール(MB/月)	5.500	5.500	5.500	5.500	5.500	5.500

ネットワークに1. 000台以上のコンピューターがある場合でも、アップデートに関する帯域幅の使用は、ESET Bridge HTTP Proxyまたはミラーツールを使用して大幅に増加しません。

システム要件とサイジング

ESET PROTECT On-Premをインストールし、動作させるには、システムがハードウェアデータベースネットワーク、およびソフトウェアの前提条件のセットを満たす必要があります。

サポート対象のオペレーティングシステム

次のセクションでは、WindowsLinuxmacOSモバイルオペレーティングシステムバージョンのESET PROTECTコンポーネントサポートについて説明します。

Windows

次の表は、各ESET PROTECTコンポーネントでサポートされているWindowsオペレーティングシステムを示します。

ESET Managementエージェントのバージョン管理とサポート

ESET Managementエージェントは、ESET PROTECT On-Premのバージョン番号とサポート終了ポリシーに従います。

- サポートされているESET Managementエージェントのバージョンは9.x–11.xです。
- 各ESET Managementエージェントバージョンには、6か月の完全サポートと2年間の限定サポートがあります。その後、バージョンはサポート終了に移行します。

サポートされている最新のESET Managementエージェントのバージョンは11.xです。 最新バージョンのESETセキュリティ製品とその機能を完全に管理するには、最新バージョンのESET Managementエージェントを使用することをお勧めします。ESET PROTECTサーバーバージョンよりも以前のESET Managementエージェントを使用している場合、最新の管理機能の一部を使用できないことがあります。

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

OS	サーバー	エージェント	RD Sensor	MDM
Windows Server 2012 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 CORE x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 R2 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 R2 CORE x64	✔	9.x—10.x, 11.0	✔	✔
Windows Storage Server 2012 R2 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2016 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Storage Server 2016 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2019 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2022 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2022 CORE x64	✔	11.0		

OS	サーバー	エージェント	RD Sensor	MDM
Windows 10 x86		9.x—10.x, 11.0	✔	
Windows 10 x64（すべての正式リリース）	*	9.x—10.x, 11.0	✔	*
ARMのWindows 10		9.x—10.x, 11.0		
Windows 11 x64	*	9.x (21H2) 10.x, 11.0 (21H2と22H2) 10.1, 11.0 (23H2)	✔	*
ARMのWindows 11		10.x, 11.0		

* クライアントOSでのESET PROTECTコンポーネントのインストールは、Microsoftライセンスポリシーと一致しない場合があります。 詳細についてはMicrosoftライセンスポリシーを確認するか、ソフトウェ

アベンダーにご確認ください。SMB/小規模ネットワーク環境では、Linux ESET PROTECT On-Premインストールまたは仮想アプライアンス(該当する場合)を考慮することをお勧めします。

ESETは違法または海賊版のオペレーティングシステムをサポートしていません。

ESXiがなくても、サーバー以外のOSでESET PROTECT On-Premを実行できます。デスクトップオペレーティングシステムにVMware Playerをインストールし、ESET PROTECT仮想アプライアンスを展開します。

それよりも前のMicrosoft Windowsシステム:

- ESET Managementエージェント10.xは、Windows 7/8.xおよびWindowsServer 2008 R2/Microsoft SBS 2011をサポートする最後のバージョンです。
- 必ず最新のサービスパックをインストールしてください(特に、Server 2008、Windows 7などの古いシステムの場合)。
- ESET PROTECT On-Premは、実行中のコンピュータ、Windows 7 (SPがない)、Widows Vista、Windows XPの管理をサポートしません。

Linux

次の表は、各ESET PROTECTコンポーネントでサポートされているLinuxオペレーティングシステムを示します。

ESET Managementエージェントのバージョン管理とサポート

ESET Managementエージェントは、ESET PROTECT On-Premのバージョン番号とサポート終了ポリシーに従います。

- サポートされているESET Managementエージェントのバージョンは9.x–11.xです。
- 各ESET Managementエージェントバージョンには、6か月の完全サポートと2年間の限定サポートがあります。その後、バージョンはサポート終了に移行します。

サポートされている最新のESET Managementエージェントのバージョンは11.xです。 最新バージョンのESETセキュリティ製品とその機能を完全に管理するには、最新バージョンのESET Managementエージェントを使用することをお勧めします。ESET PROTECTサーバーバージョンよりも以前のESET Managementエージェントを使用している場合、最新の管理機能の一部を使用できないことがあります。

ESET PROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細、クラウドMDMに移行することをお勧めします。

ESET Managementエージェントは、リストされているLinuxディストリビューションの最新のマイナーバージョンでテストされ、実行されました。

OS	サーバー	エージェント	RD Sensor	MDM
Ubuntu 18.04.1 LTS x64 Desktop	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 18.04.1 LTS x64 Server	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 20.04 LTS x64	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 22.04 LTS x64		10.x, 11.0	✔	
Linux Mint 20		10.x, 11.0	✔	
Linux Mint 21		10.1, 11.0	✔	
RHEL Server 7 x64	✔	9.x—10.x, 11.0	✔	✔
RHEL Server 8 x64		9.x—10.x, 11.0		
RHEL Server 9 x64		9.x—10.x, 11.0	✔	

OS	サーバー	エージェント	RD Sensor	MDM
CentOS 7 x64	✔	9.x—10.x, 11.0	✔	✔
SLED 15 x64		9.x—10.x, 11.0	✔	
SLES 12 x64		9.x—10.x, 11.0	✔	
SLES 15 x64		9.x—10.x, 11.0	✔	
Debian 9 x64		9.x—10.x, 11.0	✔	
Debian 10 x64	✔	9.x—10.x, 11.0	✔	✔
Debian 11 x64		9.x—10.x, 11.0	✔	
Debian 12 x64		10.1, 11.0	✔	
Oracle Linux 8		9.x—10.x, 11.0	✔	
Amazon Linux 2		9.x—10.x, 11.0	✔	
Alma Linux 9		10.1, 11.0	✔	
Rocky Linux 8		10.1, 11.0		
Rocky Linux 9		10.1, 11.0		

macOS

ESET Managementエージェントのバージョン管理とサポート

ESET Managementエージェントは、ESET PROTECT On-Premのバージョン番号とサポート終了ポリシーに従います。

- サポートされているESET Managementエージェントのバージョンは9.x–11.xです。
- 各ESET Managementエージェントバージョンには、6か月の完全サポートと2年間の限定サポートがあります。その後、バージョンはサポート終了に移行します。

サポートされている最新のESET Managementエージェントのバージョンは11.xです。 最新バージョンのESETセキュリティ製品とその機能を完全に管理するには、最新バージョンのESET Managementエージェントを使用することをお勧めします。ESET PROTECTサーバーバージョンよりも以前のESET Managementエージェントを使用している場合、最新の管理機能の一部を使用できないことがあります。

OS	エージェント
macOS Catalina (10.15)	9.x—10.x, 11.0
macOS Big Sur (11.0)	9.x—10.x, 11.0
macOS Monterey (12.0)	9.x—10.x, 11.0
macOS Ventura (13.0)	9.x—10.x, 11.0
macOS Sonoma (14.0)	10.1, 11.0

MacOSはクライアント専用としてサポートされています。ESET Managementエージェントと ESET製品(macOS版) はmacOSにインストールできます。ただしESETPROTECTサーバーはmacOSにインストールできません。

モバイル

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

OS	EESA	EESAデバイス所有者	MDM iOS	MDM iOS ABM
Android 6	✔			
Android 7	✔	✔		
Android 8	✔	✔		
Android 9	✔	✔		
Android 10	✔	✔		
Android 11	✔	✔		
Android 12	✔	✔		
Android 13	✔	✔		
Android 14	✔	✔		
iOS 9			✔	?*
iOS 10			✔	?*
iOS 11			✔	?*
iOS 12			✔	?*
iOS 13			✔	✔
iOS 14			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iOS 17			✔	✔
iPadOS 13			✔	✔
iPadOS 14			✔	✔
iPadOS 15			✔	✔
iPadOS 16			✔	✔
iPadOS 17			✔	✔

* iOS ABMは一部の国でのみ提供されています。

モバイルデバイスのOSを最新バージョンにアップデートし、重要なセキュリティパッチを常に受信することをお勧めします。

iOS 10.3以降の要件:

iOS 10.3のリリース以降では、登録プロファイルの一部としてインストールされるCAは自動的に信頼されない場合があります。この問題を解決するには、次の手順に従ってください。
a)Appleによって信頼される証明書発行元が発行した証明書を使用します。
b)登録前に手動で証明書の信頼をインストールします。つまり、登録前に手動でモバイルデバイスにルートCAをインストールし、インストールされた証明書の完全な信頼を有効にする必要があります。

iOS 12の要件:

iOS 10.3以降の要件を確認してください。

- 接続は、**TLS 1.2以降**を使用する必要があります。
- 接続は**AES-128**または**AES-256シンメトリック暗号**を使用する必要があります。ネゴシエーションされたTLS接続暗号スイートは、**Elliptic Curved Diffie-Hellman Ephemeral (ECDHE)鍵交換**によって**perfect forward secrecy (PFS)**をサポートする必要があり、次のいずれかでなければなりません。

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- **2048ビット**の長さの**RSA鍵**で署名します。証明書のハッシュアルゴリズムは、少なくとも長さ256ビットの**ダイジェストのSHA-2**（「フィンガープリント」）でなければなりません(つまり、**SHA-256以上**)。高度なセキュリティをオンにしてESET PROTECT On-Premでこれらの要件の証明書を生成できます。
- 証明書には、**ルートCAを含む証明書チェーン全体**を含める必要があります。証明書に含まれるルートCAは、デバイスとの信頼を確立するために使用されMDM登録プロファイルの一部してインストールされます。

iOS 13の要件:

- iOS 13モバイルデバイスの管理は、新しいApple通信証明書(MDM HTTPS)要件を満たす必要があります。2019年7月1日より前に発行された証明書も、これらの基準を満たす必要があります。
- ESMC CAによって署名されたHTTPS証明書は、これらの要件を満たしていません。

> Apple通信証明書要件を満たす前には、モバイルデバイスをiOS 13にアップグレードしないことを強くお勧めします。先にアップグレードすると、デバイスがESET PROTECT MDMに接続しなくなります。

- 正しい証明書を使用せずに先にアップグレードして、デバイスがESET PROTECT MDMへの接続を停止した場合は、まずiOSデバイスとの通信で使用される現在のHTTPS証明書を、Apple通信証明書(MDM HTTPS)要件を満たす証明書に変更してからiOSデバイスを再登録する必要があります。
- iOS 13にアップグレードしていない場合は、iOSデバイスとの通信で使用される現在のMDM HTTPS証明書がApple通信証明書(MDM HTTPS)要件を満たすことを確認します。満たす場合は、続行してiOSデバイスをiOS 13にアップグレードできます。要件を満たさない場合は、現在のMDM HTTPS証明書を、Apple通信証明書(MDM HTTPS)要件を満たすHTTPS証明書に変更し、続行してiOSデバイスをiOS 13にアップグレードします。

サポートされているデスクトッププロビジョニング環境

デスクトッププロビジョニングによりデバイス管理がより容易になり、デスクトップコンピューターをより迅速にエンドユーザーにハンドオフできます。

プロビジョニングされたデスクトップは通常物理または仮想です。ストリームOS (Citrixプロビジョニングサービス)を使用する仮想環境の場合は、以下のサポートされているハイパーバイザーと拡張の一覧を参照してください。

ESET PROTECT On-Prem は以下をサポートします:

- 非永続ディスクが搭載されたシステム
- VDI環境
- 複製されたコンピュータの特定

サポートされているハイパーバイザーとハイパーバイザー拡張

ハイパーバイザ	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔（セキュアブートはサポートされていません）
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMware Fusion	✔ x64 X ARM	✔ (12.2.3)
Parallels	X	✔

ハイパーバイザー拡張	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

ツール

（仮想マシンおよび物理コンピューターの両方に適用）

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Windows Admin Center

ハードウェアおよびインフラストラクチャのサイジング

ESET PROTECTサーバーコンピューターは、次の表のハードウェア推奨事項を満たす必要があります。

クライアント数	ESET PROTECTサーバ+ SQLデータベースサーバー				
	CPUコア	CPUクロック速度(GHz)	RAM (GB)	ディスクドライブ1	ディスクIOPS2
最大1000	4	2.1	4	シングル	500
5.000	8	2.1	8		1.000

クライアント数	ESET PROTECTサーバ+ SQLデータベースサーバー				
	CPUコア	CPUクロック速度(GHz)	RAM (GB)	ディスクドライブ1	ディスクIOPS2
10,000 3	4	2.1	16	別	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

1単一/個別のディスクドライブ – 10, 000クライアントを超えるシステムでは、別のドライブにデータベースをインストールすることをお勧めします。

2 IOPS (1秒あたりの合計I/O処理数) – 必要最小限の値。

- 接続されたクライアントごとに約0.2 IOPSかつ500未満にすることをお勧めします。
- diskspdツールを使用してドライブのIOPSを確認できます。次のコマンドを使用します。

クライアント数	コマンド
最大5000クライアント	`diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat`
5, 001クライアント以上	`diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat`

3 10, 000クライアント環境のシナリオ例を参照してください。

ディスクドライブの推奨事項

ディスクドライブは、ESET PROTECT On-Premパフォーマンスに影響する重要な要因です。

- SQL serverインスタンスはリソースをESET PROTECTサーバーと共有し、使用率を最大化し、遅延を最小化できますESET PROTECTのパフォーマンスを高める場合は、1台のコンピューターでESET PROTECT On-Premサーバーとデータベースサーバーを実行します。
- データベースとトランザクションログファイルを別々のドライブ(推奨は別の物理SSDドライブ)に配置するとSQL Serverのパフォーマンスが高くなります。
- ディスクドライブが1つの場合は、SSDドライブを使用することをお勧めします。
- オールフラッシュアーキテクチャを使用することをお勧めします。ソリッドステートディスク(SSD)は標準のHDDよりも大幅に高速です。
- 高RAM構成の場合は、R5のSAS設定で十分です。テスト済みの構成:R5で10x 1.2TB SASディスク – 4+1に2つのパリティグループ、追加キャッシュなし。
- 高IOPSのエンタープライズグレードSSDを使用しても、パフォーマンスは改善されません。
- クライアント数に関係なく、容量は100 GBで十分です。データベースを頻繁にバックアップする場合は、容量が大きいディスクが必要になることがあります。
- ネットワークドライブは使用しないでくださいESET PROTECT On-Premのパフォーマンスが低下します。

• オンラインストレージ移行が可能なマルチティアストレージインフラストラクチャが動作している場合は、共有低速ティアで開始し、ESET PROTECT On-Premのパフォーマンスを監視することをお勧めします。読み取り/書き込み遅延が20ミリ秒を超える場合は、ストレージレイヤーを高速のティアに無停止で移行し、最も費用対効果が高いバックエンドを使用できます。ハイパーバイザーで同じ手順を実行できます(ESET PROTECT On-Premを仮想マシンとして使用する場合)。

異なるクライアント数のサイズに関する推奨事項

次に、1年間に設定された数のクライアントが実行されている仮想環境のパフォーマンスの結果を示します。

データベースとESET PROTECT On-Premが同じハードウェア構成の別の仮想マシンで実行されています。

CPUコア	CPUクロック速度(GHz)	RAM (GB)	パフォーマンス		
			10,000クライアント	20,000クライアント	40,000クライアント
8	2.1	64	高	高	通常
8	2.1	32	通常	通常	通常
4	2.1	32	通常	通常	低
2	2.1	16	低	低	不十分
2	2.1	8	非常に低い(非推奨)	非常に低い(非推奨)	不十分

展開に関する推奨事項

ESET PROTECT On-Premの展開のベストプラクティス

クライアント数	最大1000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000以上
同じコンピューターのESET PROTECTサーバーとデータベースサーバー	✔	✔	✔	X	X	X
Microsoft SQL Expressの使用	✔	*	X	X	X	X
Microsoft SQLの使用	✔	✔	✔	✔	✔	✔
MySQLの使用	✔	✔	✔	X	X	X
ESET PROTECT仮想アプライアンスの使用	✔	✔	非推奨	X	X	X
VMサーバーの使用	✔	✔	✔	任意	X	X
推奨される接続間隔(展開フェーズ中)	60秒	5分	10分	15分	20分	25分
推奨される接続間隔(展開後、標準使用中)	10分	10分	20分	30分	40分	60分

* ESET PROTECTデータベースが満杯になるのを回避するためにESET Inspect On-Premも使用する場合は、このシナリオは推奨されません。

接続間隔

ESET PROTECTサーバーは、永久的な接続を使用してESET Managementエージェントに接続します。永続的な接続にもかかわらず、データ転送は接続間隔の間に一度だけ行われます。たとえば、5,000クライ

アントのレプリケーション間隔が8分に設定されている場合、480秒で5,000回の送信が行われます。これは毎秒10.4回です。適切なクライアント接続間隔を設定したことを確認します。高パフォーマンスハードウェア構成には、エージェント/サーバー間の通信の合計数を必ず毎秒1,000未満に保ってください。

サーバが過負荷状態またはマルウェアの大発生があると（例えば、10分間に処理できるクライアントが10,000であるサーバに20,000のクライアントを接続した場合）、接続されている一部のクライアントが処理されなくなります。未接続のクライアントは後からESET PROTECTサーバー(またはERAプロキシ)に接続しようとします。

1台のサーバー(小規模事業)

小規模ネットワーク(クライアント数が1,000以下)を管理するにはESET PROTECTサーバーとすべてのESETPROTECTコンポーネントがインストールされた1台のサーバーを使用しますSMB/小規模ネットワーク環境ではLinux ESET PROTECT On-Premインストールまたは仮想アプライアンス(該当する場合)を考慮することをお勧めします。

プロキシを使用したリモートオフィス

クライアントコンピューターがESET PROTECTサーバーで直接認識されない場合は、プロキシを使用してESET製品の通信を転送しますHTTPプロキシは、通信を集約したり、レプリケーションのトラフィックを削減します。

高可用性(エンタープライズ)

エンタープライズ環境(クライアント数が10,000以上)の場合は、次の点を考慮してください。

- RD Sensorでは、ネットワークを検索し、新しいコンピュータを検出できます。
- フェールオーバークラスタにESET PROTECTサーバーをインストールできます。
- クライアント数が多い場合は、HTTPプロキシを設定するか、追加のプロキシを使用します。

エンタープライズソリューションまたは低パフォーマンスシステムのWebコンソール設定

既定ではWindows版のオールインワンインストーラーでインストールされたESET PROTECT Webコンソールは、Apache Tomcat用に1024 MBのメモリ上限を予約します。

インフラストラクチャに基づいて、既定のWebコンソール設定を変更できます。

- エンタープライズ環境では、既定のWebコンソール設定では、多数のオブジェクトを処理するときに、不安定になる可能性がありますTomcat設定を変更し、メモリ不足を防止します。これらの変更を行う前に、システムに十分なRAM (16 GB以上)があることを確認してください。
- ハードウェア リソースが限られたパフォーマンスの低いシステムの場合は、Tomcatメモリ使用量を減らすことができます。

以下に示すメモリ値は推奨値です。ハードウェアリソースに基づいてTomcatメモリ設定を調整できます。

Windows

1.*tomcat9w.exe* を開くか、`Configure Tomcat`アプリケーションを実行します。

2.**Java**タブに切り替えます。

3.メモリ使用量を変更します。

a.増やす(エンタープライズ):**Initial memory pool**の値を2048 MBに、**Maximum memory pool**を16384 MBに変更します。

b.減らす(低パフォーマンスシステム):**Initial memory pool**の値を256 MBに、**Maximum memory pool**を2048 MBに変更します。

4.Tomcatサービスを再起動します。

LINUXおよびESET PROTECT仮想アプライアンス

1.ターミナルをrootで開くか、`sudo`を使用します。

2.ファイルを開きます:

a.ESET PROTECT仮想アプライアンス / CentOS: `/etc/sysconfig/tomcat`

b.Debian: `/etc/default/tomcat9`

3.次の行をファイルに追加します。

a.メモリ使用量を増やす(エンタープライズ): `JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.メモリ使用量を減らす(低パフォーマンスシステム): `JAVA_OPTS="-Xms256m -Xmx2048m"`

4.ファイルを保存し、Tomcatサービスを再起動します。

```
service tomcat restart
```

10,000クライアントの展開

次に、10,000クライアントが1年間実行されている仮想環境のパフォーマンスの結果を示します。

ハイパーバイザーサーバーの設定

コンポーネント	値
VMware	ESXi 6.7 Update以降(VMバージョン15)
ハイパーバイザ	VMware ESXi, 6.7.0
論理プロセッサー	112
プロセッサタイプ	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

専用コンピューターで実行されたテスト
データベースとESET PROTECT On-Premが同じハードウェア構成の別の仮想マシンで実行されています。

仮想マシンで使用されるソフトウェア

ESET PROTECT On-Prem:

- OS: Microsoft Windows Server 2016 Standard (64-bit)

データベース:

- データベースサーバ:Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- OS: Microsoft Windows Server 2016 Standard (64-bit)

ESET PROTECT On-Prem環境の説明

- 10,000接続クライアント
- 約2,000の動的グループ、約2,000の動的グループのテンプレート
- 約255の静的グループ
- 20ユーザー
- ESET Managementエージェントの接続間隔が15分
- 環境が1年間実行された後、データベースサイズは15 GBになります。

CPU数	RAM (GB)	パフォーマンス
8	64	高
4	32	通常
2	16	低
2	8	非常に低い (非推奨)

データベース

ESET PROTECTサーバーをインストールするときに使用するデータベースサーバーとコネクターを指定します。現在の環境で稼動している既存のデータベースサーバーを使用できますが、次の要件を満たしている必要があります。

ESET PROTECT On-Prem 11.0オールインワンインストーラーでは、既定でMicrosoft SQL Server Express 2019がインストールされます。

- 古いWindowsエディション(サーバー2012またはSBS 2011)を使用している場合は、Microsoft SQL Server Express 2014が既定でインストールされます。
- インストーラーはデータベース認証(*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*に保存)のランダムなパスワードを自動的に生成します。

Microsoft SQL Server Expressには各関係データベース10 GBのサイズ制限があります。次の環境では Microsoft SQL Server Expressの使用は推奨されません。
- エンタープライズ環境または大規模ネットワーク。
- ESET PROTECT On-PremとESET Inspect On-Premを使用する場合。

サポートされているデータベースサーバーとデータベースコネクター

ESET PROTECT On-Premは、Microsoft SQL ServerとMySQLの2種類のデータベースサーバーをサポートします。

ESET PROTECT On-PremはMariaDBをサポートしません MariaDBは最新のLinux環境の既定のデータベースであり MySQLのインストールを選択するとインストールされます。

サポートされているデータベースサーバー	サポートされているデータベースバージョン	サポートされているデータベースコネクター
Microsoft SQL Server	• Expressおよび非Expressエディション • 2014, 2016, 2017, 2019, 2022	• SQLサーバー • SQL Serverネイティブクライアント10. 0 • ODBCドライバ SQL Server 11 13 17 18
MySQL	• 5.6* • 5.7 • 8.0 • 8.1	MySQL ODBCドライバーバージョン: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.x (8.0.x, 8.1.x)

* MySQL 5.6は2021年2月にサポート終了しました MySQLデータベースサーバーをバージョン5. 7以降にアップグレードすることをお勧めします。

次のMySQL ODBCドライバーバージョンはサポートされていません。
- 5. 3. 11および5.3.x以降

データベースサーバーハードウェア要件

ハードウェアおよびサイジング手順を参照してください。

パフォーマンスに関する推奨事項

最適なパフォーマンスのため ESET PROTECTデータベースとしてサポートされている最新のMicrosoft SQL Serverを使用することをお勧めします ESET PROTECT On-PremはMySQLに対応していますが、ダッシュボード、検出、クライアントを含む大量のデータを処理すると場合は、MySQLを使用すると、システムパフォーマンスに悪影響を及ぼすことがあります Microsoft SQL Serverがインストールされている同じハードウェアは、MySQLがインストールされているハードウェアよりも大幅に多い数のクライアントを処理できます。

次の場所にSQLデータベースサーバーをインストールするかどうかを決定できます。

- ESET PROTECTサーバーと同じコンピューター。
- 同じコンピューターの別のディスク。
- SQLデータベースサーバーをインストールするための専用サーバー。

10,000以上のクライアントを管理する場合は、リソースが予約された専用コンピューターを使用することをお勧めします。

データベース	SMB顧客	エンタープライズ顧客	クライアント上限	Windows	Linux
Microsoft SQL Express	✔	(任意)	5.000	✔	
Microsoft SQL Server	✔	✔	なし	✔	
MySQL	✔	✔	10.000	✔	✔

詳細情報

ESET PROTECTサーバーは統合バックアップを使用しません。データベースサーバーをバックアップし、データ損失を防止することを強くお勧めします。

- ドメインコントローラーにはSQL Serverをインストールしないでください(たとえばWindows SBS / Essentials)別のサーバーにESET PROTECT On-Premをインストールするか、インストール中にSQL Server Expressコンポーネントを選択しない(この場合、既存のSQL ServerまたはMySQLを使用してESET PROTECTデータベースを実行する必要があります)ことをお勧めします。

- ESET PROTECTデータベースにのみアクセスする専用データベースユーザーアカウントを使用する場合は、インストール前に特定の権限があるユーザーアカウントを作成する必要があります。詳細については、「専用データベースユーザーアカウント」を参照してください。またESET PROTECT On-Premで使用される空のデータベースを作成する必要があります。

- MySQL for WindowsおよびMySQL for Linuxをインストールし、ESET PROTECT On-Premと正常に動作するように設定する手順を参照してください。

- LinuxのMicrosoft SQL Serverはサポートされていません。ただし、LinuxのESET PROTECTサーバーをWindowsのMicrosoft SQL Serverに接続することができます。

- ESET PROTECTサーバーとMicrosoft SQL Serverを別のコンピューターにインストールする場合は、データベースへの暗号化接続を有効にすることができます。

- Windows環境でのデータベースのクラスタ設定は、Microsoft SQL ServerでのみサポートされていますMySQLではサポートされていません。

サポートされているApache TomcatとJavaのバージョン

Apache Tomcat

Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。

ESET PROTECT On-PremはApacheTomcat 9.x (64ビット)のみをサポートします。最新のApache Tomcat 9.xを使用することをお勧めします。

ESET PROTECT On-Premは、アルファ/ベータ/RCバージョンのApache Tomcatをサポートしません。

Java

Apache Tomcatには64ビット版のJava/OpenJDKが必要です。

システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

サポート対象のWebブラウザ、ESETセキュリティ製品および言語

ESET PROTECT On-Premでは、次のオペレーティングシステムがサポートされています。

- Windows、Linux、macOS

ESET PROTECT Webコンソールは次のWebブラウザーで実行できます。

Webブラウザー
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

ESET PROTECT Webコンソールの最適なエクスペリエンスを得るため、Webブラウザーを常に最新の状態にすることをお勧めします。

ESET PROTECT On-Prem11.0で管理可能な最新バージョンのESET製品

以下のESETセキュリティ製品バージョンは、ESET Managementエージェントバージョン11.0以降で管理できます。
最新バージョンのESETセキュリティ製品とその機能を完全に管理するには、最新バージョンのESET Managementエージェントを使用することをお勧めします。ESET PROTECTサーバーバージョンよりも以前のESET Managementエージェントを使用している場合、最新の管理機能の一部を使用できないことがあります。
以下の表よりも前のESETセキュリティ製品のバージョンは、ESET PROTECT On-Prem 11.0を使用して管理できません。
互換性の詳細については、ESETビジネス製品のサポート終了ポリシーを参照してください。

製品	製品のバージョン
ESET Endpoint Security for Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus for Windows	7.3, 8.x, 9.x, 10.x

製品	製品のバージョン
ESET Endpoint Security for macOS	6. 10以降
ESET Endpoint Antivirus for macOS	6. 10以降
ESET Endpoint Security for Android	3.3+
ESET Server Security for Microsoft Windows Server (旧ESET File Security for Microsoft Windows Server)	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security for Microsoft Exchange Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Security for Microsoft SharePoint Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security for IBM Domino	7.3, 8.x, 9.x, 10.x
ESET Server Security for Linux (旧ESET File Security for Linux)	7.2, 8.1, 9.x, 10.x
ESET Endpoint Antivirus for Linux	7.1, 8.1, 9.x, 10.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.8+
ESET Full Disk Encryption for Windows	
ESET Full Disk Encryption for macOS	

サブスクリプションライセンス経由でのアクティベーションをサポートする製品

ESET製品	利用可能なバージョン
ESET Endpoint Antivirus/Security for Windows	7.0
ESET Endpoint Antivirus/Security for macOS	6.8.x
ESET Endpoint Security for Android	2.0.158
ESET Mobile Device Management for Apple iOS	7.0
ESET File Security for Microsoft Windows Server	7.0
ESET Mail Security for Microsoft Exchange	7.0
ESET File Security for Windows Server	7.0
ESET Mail Security for IBM Domino	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security for Linux	7.0
ESET Endpoint Antivirus for Linux	7.0
ESET Server Security for Windows	8.0
ESET Server Security for Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect On-Prem (Windows ESET Endpoint 7. 3以降)	1.5

サポートされている言語

言語	コード
英語(米国)	en-US
アラビア語(エジプト)	ar-EG
簡体中国語	zh-CN

言語	コード
繁体中国語	zh-TW
クロアチア語(クロアチア)	hr-HR
チェコ語(チェコ共和国)	cs-CZ
フランス語(フランス)	fr-FR
フランス語(カナダ)	fr-CA
ドイツ語(ドイツ)	de-DE
ギリシャ語(ギリシャ)	el-GR
ハンガリー語(ハンガリー)*	hu-HU
インドネシア語(インドネシア)*	id-ID
イタリア語(イタリア)	it-IT
日本語(日本)	ja-JP
韓国語(韓国)	ko-KR
ポーランド語(ポーランド)	pl-PL
ポルトガル語(ブラジル)	pt-BR
ロシア語(ロシア)	ru-RU
スペイン語(チリ)	es-CL
スペイン語(スペイン)	es-ES
スロバキア語(スロバキア)	sk-SK
トルコ語(トルコ)	tr-TR
ウクライナ語(ウクライナ)	uk-UA

*製品のみがこの言語で提供されています。オンラインヘルプはありません。

ネットワーク

ESET PROTECTサーバーとESET PROTECT On-Premで管理されるクライアントコンピューターの両方がインターネットに接続し、ESETリポジトリとアクティベーションサーバーに接続できることが重要です。クライアントを直接インターネットに接続しない場合は、プロキシサーバー(ESET Bridge HTTPプロキシとは異なる)を使用して、ネットワークおよびインターネットと通信できます。

ESET PROTECTサーバーはクライアントコンピューターで表示できる必要があります。クライアントコンピューターはESET PROTECTサーバーと通信して、リモート展開とウェイクアップコール機能を使用できる必要があります。

Windows/Linux版ESET PROTECT On-Premは、IPv4およびIPv6インターネットプロトコルの両方に対応しますESET PROTECT仮想アプライアンスはIPv4とのみ互換性があります。

使用されるポート

ネットワークがファイアウォールを使用する場合ESET PROTECT On-Premとコンポーネントがインフラストラクチャにインストールされるときに使用されるネットワーク通信ポートの一覧を参照してください。

ESET PROTECTサーバーとESET Managementエージェント通信のネットワークトラフィックへの影響

クライアントのアプリケーションはESET PROTECTサーバーで直接通信せずESET Managementエージェントがこの通信を容易にしています。このソリューションは管理しやすく、ネットワーク上で転送されるデータの負荷を減らします。ネットワークトラフィックはクライアント接続間隔と、クライアントによって実行されるタスクのタイプによって異なります。タスクがクライアントで実行またはスケジュールされていない場合でも、各接続間隔でESET Managementエージェントが ESET PROTECTサーバーに1回通信します。各接続はトラフィックを生成します。トラフィックの例については、以下の表を参照してください。

アクションのタイプ	単一接続間隔のトラフィック
クライアントタスク:検査して駆除する	4 kB
クライアントタスク:モジュールアップデート	4 kB
クライアントタスク:SysInspectorログ要求	300 kB
ポリシーウイルス対策 – 最大のセキュリティ	26 kB

ESET Managementエージェントレプリケーション間隔	アイドル状態のESET Managementエージェントによって生成された毎日のトラフィック
1 分	16 MB
15分	1 MB
30分	0.5 MB
1時間	144 kB
1 日	12 kB

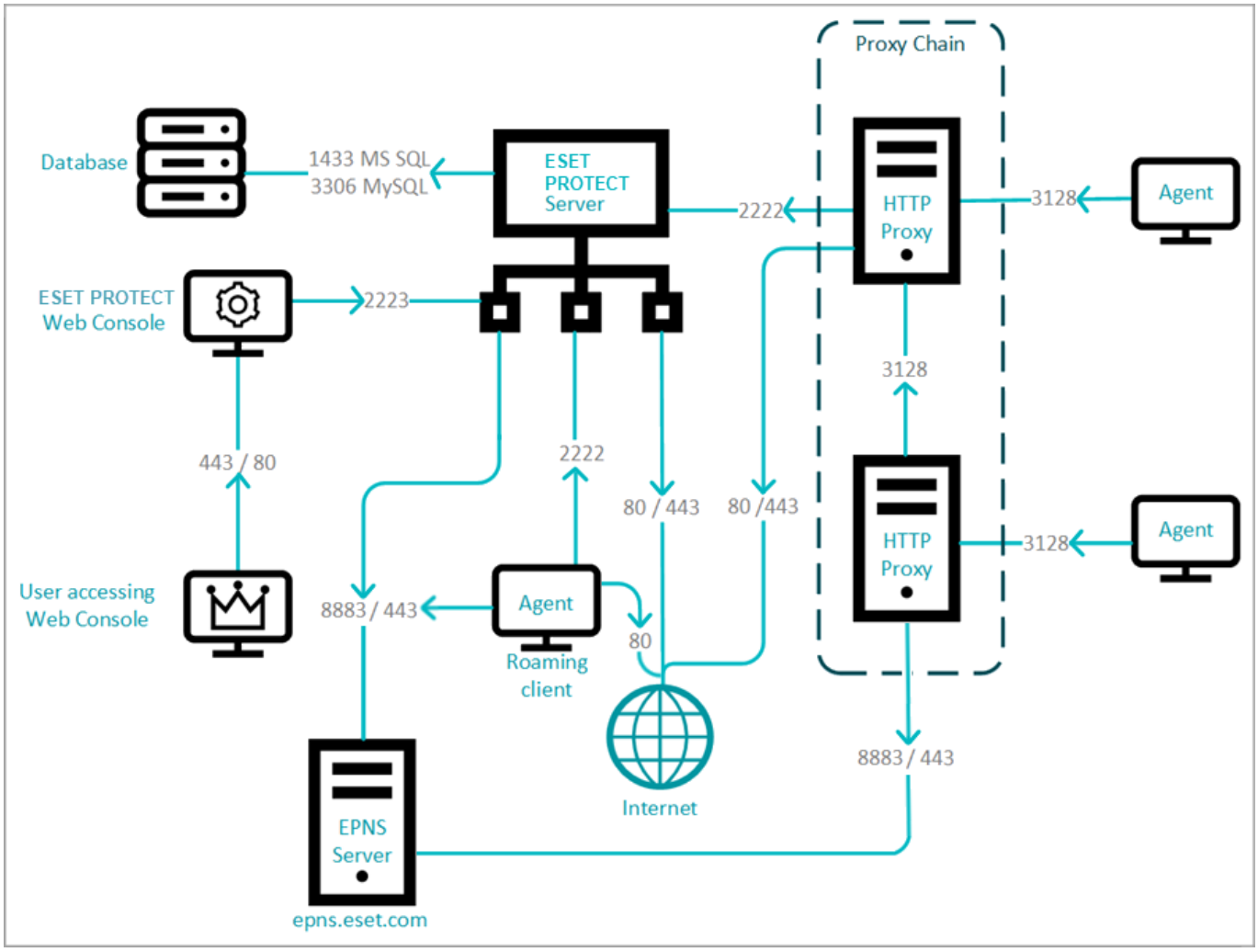
ESET Managementエージェントによって生成された全体的なトラフィックを推定するには、次の式を使用します。

クライアント数 *（アイドル状態のエージェントの1日のトラフィック +（特定のタスクのトラフィック * 1日のタスクの発生数））

ESET Inspect On-Premを使用する場合ESET Inspectコネクターは毎日2~5 MBのトラフィックを生成します(この値はイベント数によって異なります)。

使用されるポート

ESET PROTECTサーバーはデータベースESET PROTECT Webコンソール、および HTTPプロキシと同じコンピューターにインストールできます。以下の図は、コンポーネントごとに使用されるポートを示します(矢印はネットワークトラフィックを示します)。



次の表は、ESET PROTECT On-Premとそのコンポーネントをインフラストラクチャにインストールした場合に使用されるネットワーク通信ポートを一覧で示します。その他の通信は、ネイティブオペレーティングシステムプロセス経由で実行されます(NetBIOS over TCP/IPなど)。

ESET PROTECT On-Premが正常に機能するには、下記のどのポートも他のアプリケーションによって使用されていてはなりません。
ネットワーク内でファイアウォールを設定し、下記のポート経由の通信を許可することを確認してください。

クライアント(ESET Managementエージェント)またはESET Bridge HTTPプロキシコンピューター

プロトコル	ポート	説明
TCP	2222	ESET Managementエージェントと ESET PROTECT間の通信
TCP	80	ESETリポジトリへの接続
MQTT	8883, 443	ESETプッシュ通知サービス - ESET PROTECTサーバーとESET Managementエージェントの間のウェイクアップコール。443はフェールオーバーポートです。
TCP	3128	ESET Bridge (HTTPプロキシ)との通信
TCP	443	ESET LiveGuard Advancedとの通信(プロキシのみ)

ESET Managementエージェント- Windows OSのターゲットコンピューターへのリモート展開で使用されます。

プロトコル	ポート	説明
TCP	139	ADMIN$共有の使用
TCP	445	リモートインストール中にTCP/IPを使用して共有リソースに直接アクセス(TCP 139の代替)
UDP	137	リモートインストール中の名前解決
UDP	138	リモートインストール中の参照

ESET PROTECT Webコンソールコンピュータ(ESET PROTECTサーバーコンピューターと同じではない場合)

プロトコル	ポート	説明
TCP	2223	ESET PROTECT WebコンソールとESET PROTECTサーバー間の通信。支援型インストールで使用されます。
TCP	443/80	WebコンソールをブロードキャストするTomcat
TCP	443	サポートニュースRSSフィード: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

ESET PROTECTサーバーコンピューター

プロトコル	ポート	説明
TCP	2222	ESET ManagementエージェントとESET PROTECT間の通信
TCP	80	ESETリポジトリへの接続
MQTT	8883	ESETプッシュ通知サービス - ESET PROTECTサーバーとESET Managementエージェントの間のウェイクアップコール
TCP	2223	DNS解決とMQTTフォールバック
TCP	3128	ESET Bridge (HTTPプロキシ)との通信
TCP	1433 (Microsoft SQL) 3306 (MySQL)	外部データベースへの接続(データベースが別のコンピューターの場合)
TCP	389	LDAP同期ADコントローラーでもこのポートを開きます。
UDP	88	Kerberosチケット(ESET PROTECT仮想アプライアンスにのみ適用)

Rogue Detection (RD) Sensor

プロトコル	ポート	説明
TCP	22, 139	SMB (TCP 139)およびSSH (TCP 22)プロトコルでのオペレーティングシステムの検出。
UDP	137	NetBIOSでのコンピューターホスト名解決。

ESET PROTECT MDCコンピューター

プロトコル	ポート	説明
TCP	9977 9978	**モバイルデバイスコネクターと**ESET Managementエージェント間の内部通信
TCP	9980	モバイルデバイス登録
TCP	9981	モバイルデバイス通信
HTTPS	2197	Appleプッシュ通知とフィードバック(*api.push.apple.com*)
TCP	2222	ESET ManagementエージェントMDCESET PROTECTサーバー間の通信(レプリケーション)
TCP	1433 (Microsoft SQL) 3306 (MySQL)	外部データベースへの接続(データベースが別のコンピューターの場合)

MDM管理対象デバイス

プロトコル	ポート	説明
TCP	9980	モバイルデバイス登録
TCP	9981	モバイルデバイス通信
TCP	5223	Apple Push Notificationサービスとの外部通信(iOS)
TCP	443	• デバイスがポート5223でAPNに到達できない場合にWi-Fiのみでフォールバック(iOS) • GCMサーバーへのAndroidデバイス接続。 • ESETライセンスポータルへの接続。 • ESET LiveGrid® (Android) (受信: *https://l1.c.eset.com*、送信: *https://l3.c.eset.com*) • ESET Research Labへの匿名の統計情報(Android) (*https://ts.eset.com*) • デバイスにインストールされているアプリ分類。一部のアプリカテゴリのブロックが定義されているときにアプリケーションコントロールで使用されます(Android) (*https://play.eset.com*) • サポート要求機能を使用してサポート要求を送信(Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Google Cloud Messagingへの通知の送信(Android)* Firebase Cloud Messagingへの通知の送信(Android)*
TCP	80	• モジュールアップデート(Android) (*http://update.eset.com*) • Webバージョンでのみ使用されます。最新のアプリバージョンアップデートと新しいバージョンのダウンロードに関する情報(Android) (*http://go.eset.eu*)

* GCM (Google Cloud Messaging)サービスは廃止され、2019年4月11日付けで削除されましたFCM (Firebase Cloud Messaging)に代わりましたMDM v7は、この日になった時点で、GCMサービスをFCMサービスに置き換えました。そのときにはFCMサービスの通信を許可することのみが必要です。

必要に応じて、定義済みポート2222、2223を変更できます。

インストール処理

インストールガイドでは、主にエンタープライズのお客様向けにESET PROTECT On-Premをインストールするためのさまざまな方法が説明されています。Windowsプラットフォームで ESET PROTECT On-Premをインストールして、最大250のWindows ESETエンドポイント製品を管理する場合は、オールインワンインストールを参照してください。
既存のESET PROTECT On-Premインストールをアップグレードする手順については、「アップグレード手順」を参照してください。

ESET PROTECTインストーラーは、ESET Webサイトの ESET PROTECTダウンロードセクションで提供されています。さまざまなインストール方法をサポートするために、さまざまな形式があります。既定では、**オールインワンインストーラー**タブが選択されています。VAまたはスタンドアロンインストーラーをダウンロードする場合は、該当するタブをクリックします。使用可能なダウンロードは次のとおりです。

- Zip形式のESET PROTECT On-Premオールインワンインストーラーパッケージ(Windows版)
- すべてのESET PROTECTインストーラ(ESET PROTECT Virtual Applianceを除く)を含むISOイメージ
- 仮想アプライアンス(OVA ファイル)仮想環境でESET PROTECTを実行するユーザーまたは簡単なインストールが必要なユーザーの場合は、ESET PROTECT On-Prem Virtual Applianceの展開をお勧めします。段階的な手順については、『ESET PROTECT Virtual Appliance展開ガイド』を参照してください。
- WindowsおよびLinuxプラットフォームの各コンポーネントの個別のインストーラ

その他のインストール方法:

- 段階的なインストール手順(Linux版)

2022年11月以降、ESET PROTECT仮想アプライアンスはAzure Marketplaceで提供されていません。あるいは、ESET PROTECT (cloud)を使用し、ESETですべての必要なインフラストラクチャコンポーネントを管理できます。

インストール後にESET PROTECTサーバーコンピューターのコンピューター名を変更しないでください。詳細については、「ESET PROTECTサーバーのIPアドレスまたはホスト名の変更」を参照してください。

環境に適したESET PROTECT On-Premインストールの種類を決定するには、次の決定表を参照して、最適な選択を行ってください。例:

- クラウドではESET PROTECT On-Premで低速インターネット接続を使用しないでください。
- SMBユーザーはオールインワンインストーラーを選択してください。

ハードウェアおよびインフラストラクチャのサイジングも参照してください。物理マシンまたは仮想マシンにESET PROTECT On-Premをインストールできます。

インストール方法	顧客タイプ		移行		ESET PROTECT On-Premインストールの環境					インターネット接続		
	SMB	エンタープライズ	はい	いいえ	サーバーなし	専用サーバー	共有サーバー	仮想化プラットフォーム	クラウドサーバー	なし	高品質	低品質
オールインワン Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
オールインワン Windows Desktop	✓		✓		✓					✓	✓	✓
仮想アプライアンス	✓		✓					✓		✓	✓	✓
コンポーネントLinux		✓	✓			✓	✓		✓	✓	✓	✓
コンポーネントWindows		✓	✓			✓	✓		✓	✓	✓	✓

Windowsでのオールインワンインストール

いくつかの方法でESET PROTECT On-Premをインストールできます。ニーズと環境に最適なインストールタイプを選択してください。最も簡単な方法はESET PROTECT All-in-oneインストーラを使用することです。この方法ではESET PROTECT On-Premとコンポーネントを1台のコンピューターにインストールできます。

コンポーネントインストールでは、インストールをカスタマイズし、システム要件を満たす場合は、各ESET PROTECTコンポーネントを個別のコンピューターにインストールできます。

次の方法でESET PROTECT On-Premをインストールできます。

- ESET PROTECTサーバーESET Bridge HTTP Proxyモバイルデバイスコネクターのオールインワンパッケージインストール
- ESET PROTECTコンポーネントのスタンドアロンインストーラー(コンポーネントインストール)

カスタムインストールシナリオには次が含まれます。

- カスタム証明書を使用したインストール
- フェールオーバークラスターのインストール

ほとんどのインストールシナリオでは、コンピューターによって異なるESET PROTECTコンポーネントをインストールし、さまざまなネットワークアーキテクチャに対応し、パフォーマンス要件やその他の要求に対応する必要があります。次のインストールパッケージは、個別のESET PROTECTコンポーネントで使用できます。

コアコンポーネントインストール:

- ESET PROTECTサーバー
- ESET PROTECT Webコンソール - ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。
- ESET Managementエージェント(クライアントコンピュータにインストールする必要がありますESET PROTECTサーバーでは任意)

オプションコンポーネントインストール:

- RD Sensor
- モバイルデバイスコネクター
- ESET BridgeHTTPプロキシ
- ミラーツール

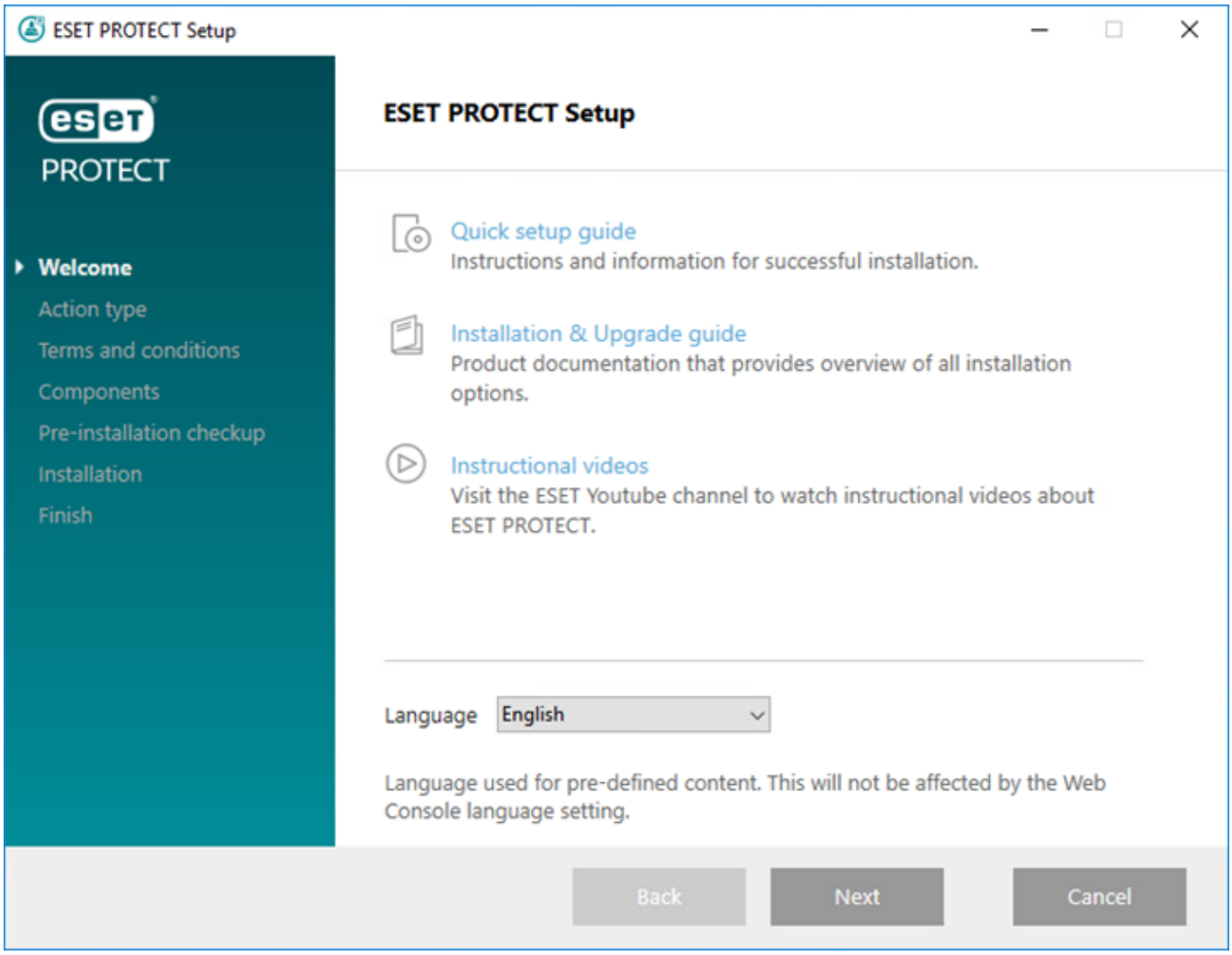
ESET PROTECTオールインワンインストールも参照してください。

以前のESET PROTECT On-Premを最新のESET PROTECT On-Prem 11.0にアップグレードする手順については、アップグレード手順を参照してください。

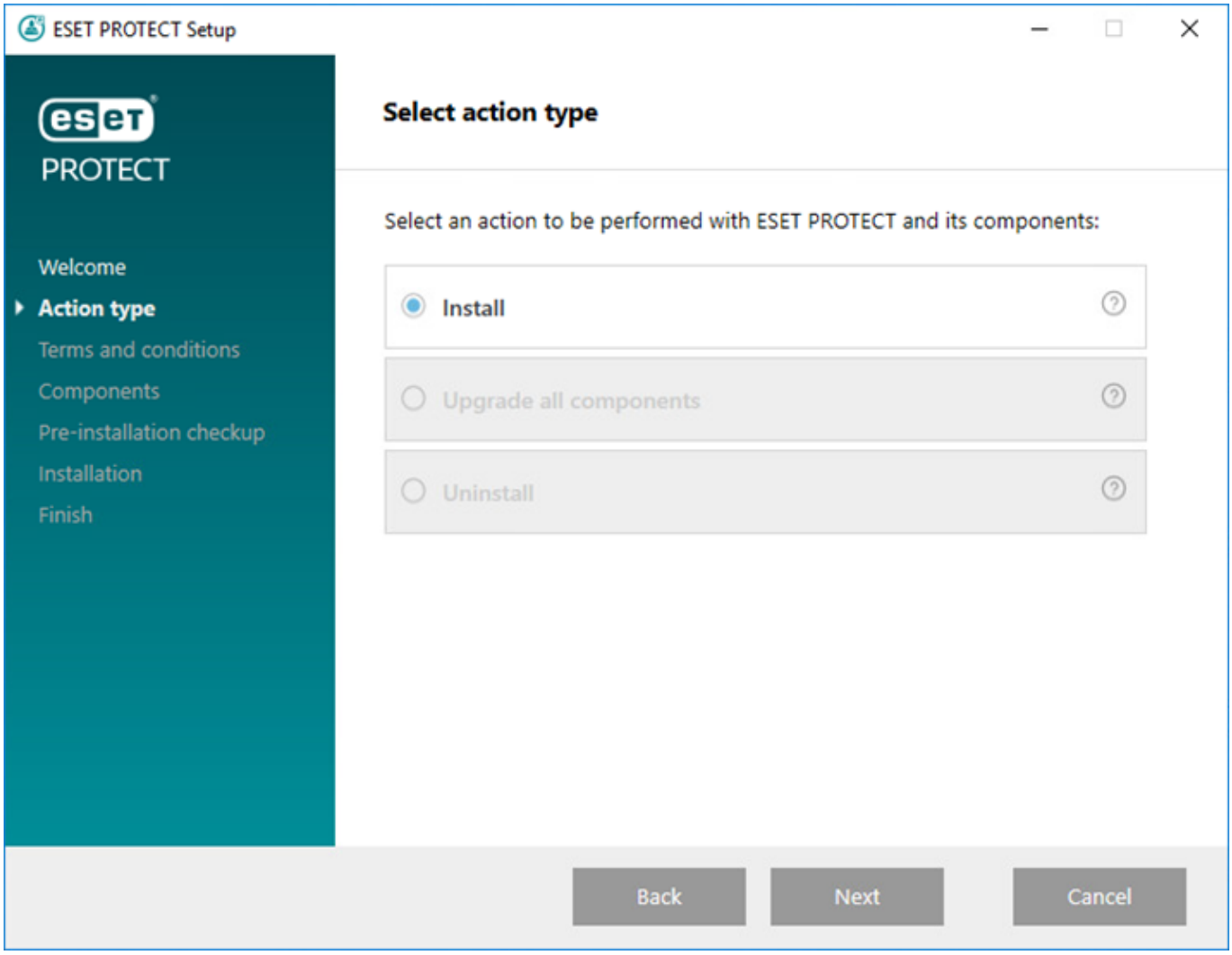
ESET PROTECTサーバーのインストール

ESET PROTECTオールインワンインストーラーはWindowsオペレーティングシステムでのみ使用できます。オールインワンインストーラーではESET PROTECTインストールウィザードを使用して、すべてのESET PROTECT On-Premコンポーネントをインストールできます。

1. インストールパッケージを開きます。ようこそ画面で、**言語**ドロップダウンメニューを使用して、言語設定を調整します。**次へ**をクリックして続行します。



2. **インストール**を選択して、**次へ**をクリックします。



3. **製品改善プログラムに参加する**の横のチェックボックスをオンにして、クラッシュレポートと匿名のテレメトリーデータ(OSのバージョンと種類、ESET製品バージョン、および他の製品固有の情報)をESETに送信します。EULAに同意した後、[**次へ**]をクリックします。

4. インストールするコンポーネントを選択し、**次へ**をクリックします。

Microsoft SQL Server Express

- ESET PROTECT On-Prem 11.0オールインワンインストーラーでは、既定でMicrosoft SQL Server Express 2019がインストールされます。
  - 古いWindowsエディション(サーバー2012またはSBS 2011)を使用している場合は、Microsoft SQL Server Express 2014が既定でインストールされます。
  - インストーラーはデータベース認証(*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*に保存)のランダムなパスワードを自動的に生成します。

> Microsoft SQL Server Expressには各関係データベース10 GBのサイズ制限があります。次の環境ではMicrosoft SQL Server Expressの使用は推奨されません。
> - エンタープライズ環境または大規模ネットワーク。
> - ESET PROTECT On-PremとESET Inspect On-Premを使用する場合。

- 既に他のサポートされているバージョンのMicrosoft SQL ServerまたはMySQLがインストールされている場合、または別のSQL Serverに接続する予定の場合、**Microsoft SQL Server Express**の横のチェックボックスを解除してください。
- ドメインコントローラーにはSQL Serverをインストールしないでください(たとえばWindows SBS / Essentials)。別のサーバーにESET PROTECT On-Premをインストールするか、インストール中にSQL Server Expressコンポーネントを選択しない(この場合、既存のSQL ServerまたはMySQLを使用してESET PROTECTデータベースを実行する必要があります)ことをお勧めします。

Webコンソールのカスタム HTTPS証明書を追加

- ESET PROTECT Webコンソールでカスタム HTTPS証明書を使用する場合は、このオプションを選択します。
- このオプションを選択しない場合は、インストーラーによってTomcatの新しい鍵ストア(自己署名HTTPS証明書)が自動的に生成されます。

ESET Bridgeプロキシ

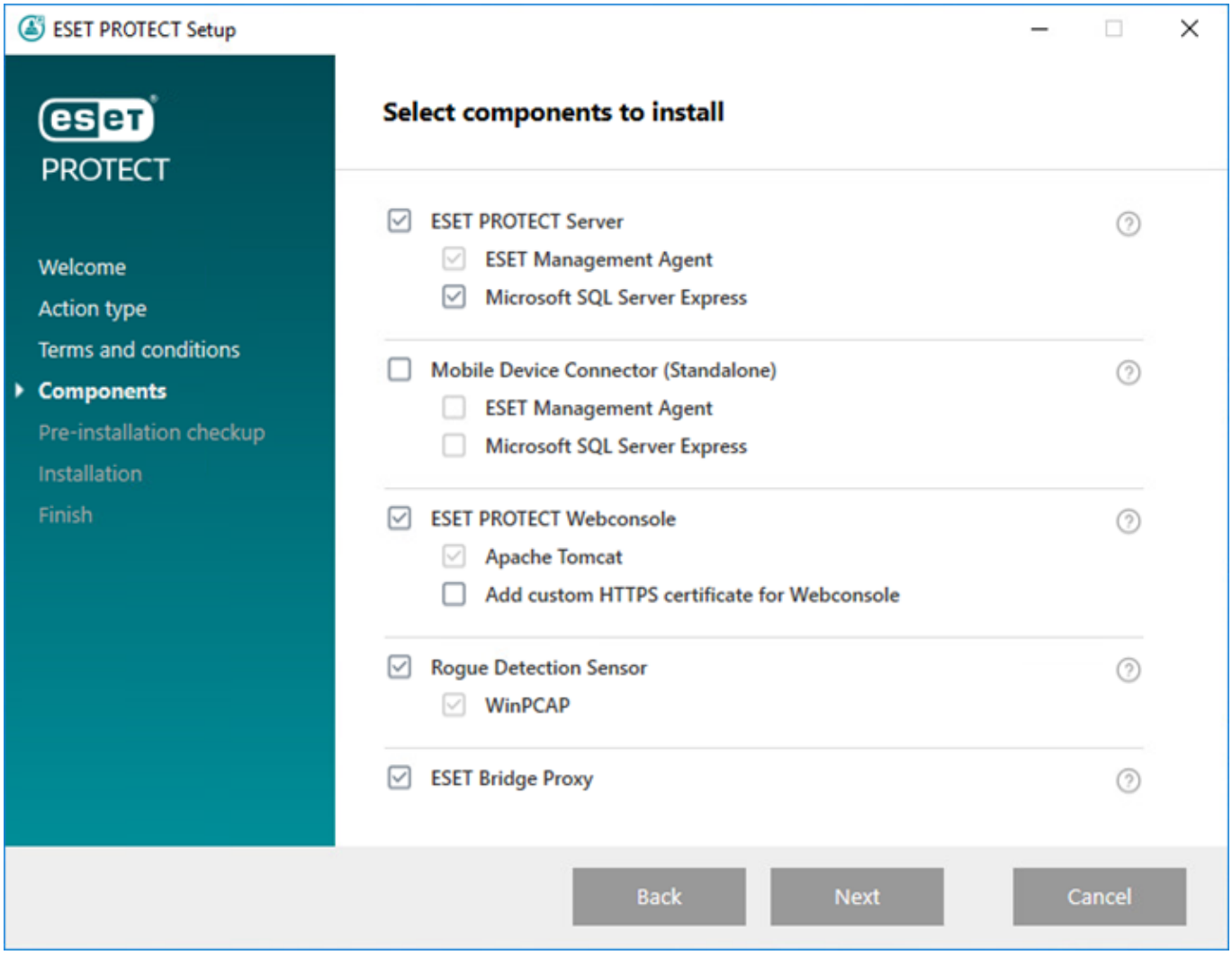
ESET Bridge Proxyオプションは、ローミングクライアントがない小規模または一元化されたネットワーク専用です。このオプションが選択されている場合、クライアントが既定でESET PROTECTサーバーと同じコンピューターにインストールされたプロキシ経由でESETとの通信をトンネルするようにインストーラーによって設定されます。クライアントとESET PROTECTサーバー間で直接ネットワーク可視がない場合は、この接続は動作しません。

- HTTPプロキシを使用すると、インターネットからダウンロードされるデータの大量の帯域幅を節約し、製品アップデートのダウンロード速度を改善できます。ESET PROTECT On-Premから37台以上のコンピューターを管理する場合は、**ESET Bridge Proxy**の横のチェックボックスをオンにすることをお勧めします。後からESET Bridgeをインストールすることもできます。
- 詳細については、ESET Bridge (HTTPプロキシ)とESET Bridge (HTTPプロキシ)、ミラーツール、および直接接続の違いを参照してください。

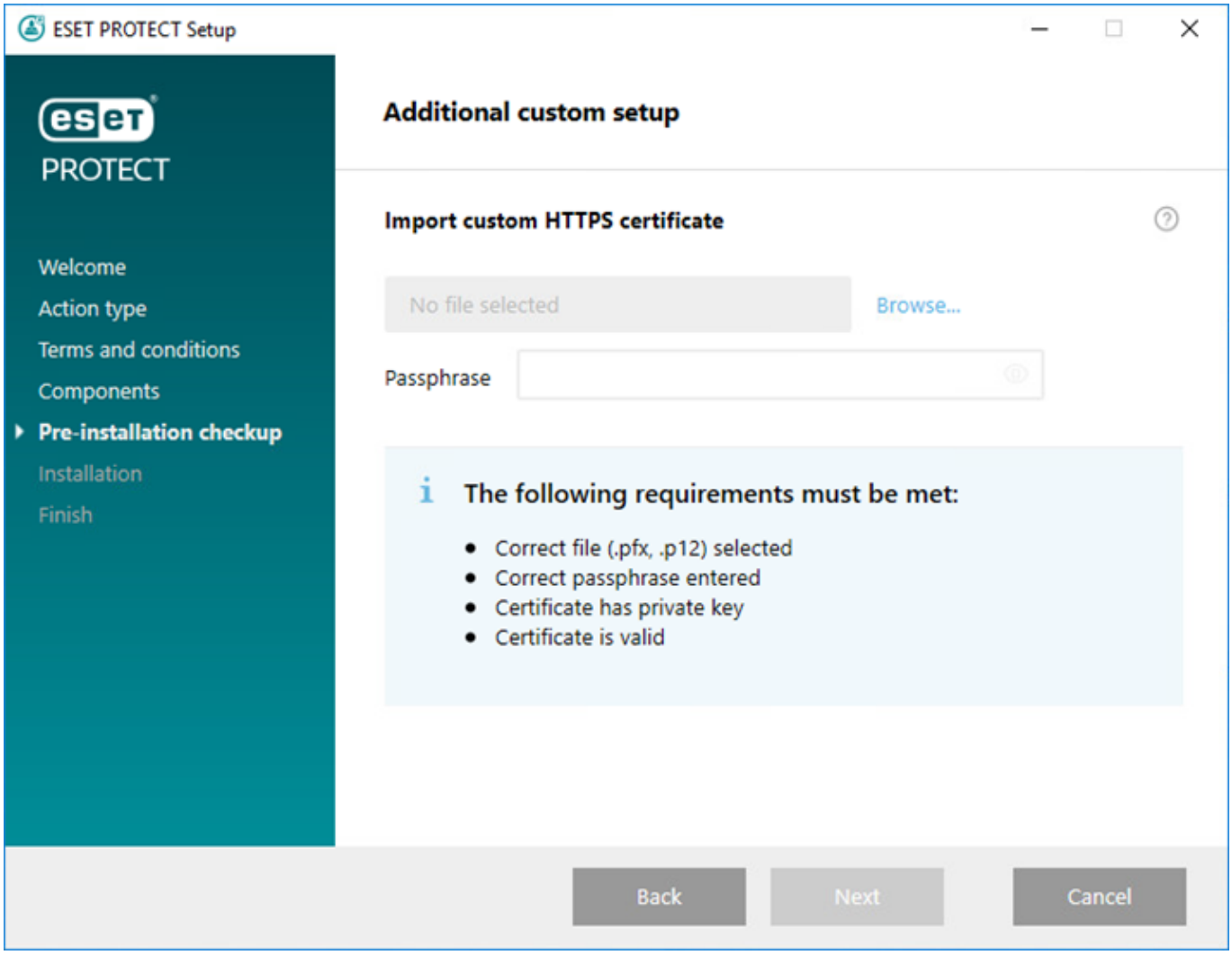
オールインワンインストーラーは、**すべて**の静的グループに適用されたESET Managementエージェントおよび ESSETセキュリティ製品の既定の**HTTPProxy使用**ポリシーを作成します。ポリシーは、管理されたコンピューターでESET Managementエージェントと ESETセキュリティ製品を自動的に設定し、アップデートパッケージをキャッシュに保存するために ESET Bridgeをプロキシとして使用します。HTTPSトラフィックキャッシュは規定で有効になっています。

- ESET Bridgeポリシーに HTTPS証明書が含まれており、**HTTPSトラフィックをキャッシュに保存する**トグルが有効になっています。
- ESET Endpoint for Windowsの**HTTP Proxy使用**ポリシーには HTTPSトラフィックキャッシュの認証局が含まれています。

HTTPプロキシホストは、ESET PROTECTサーバーのローカルIPアドレスとポート3128に設定されています。認証は無効になっています。他の製品を設定する必要がある場合は、これらの設定を他のポリシーにコピーできます。



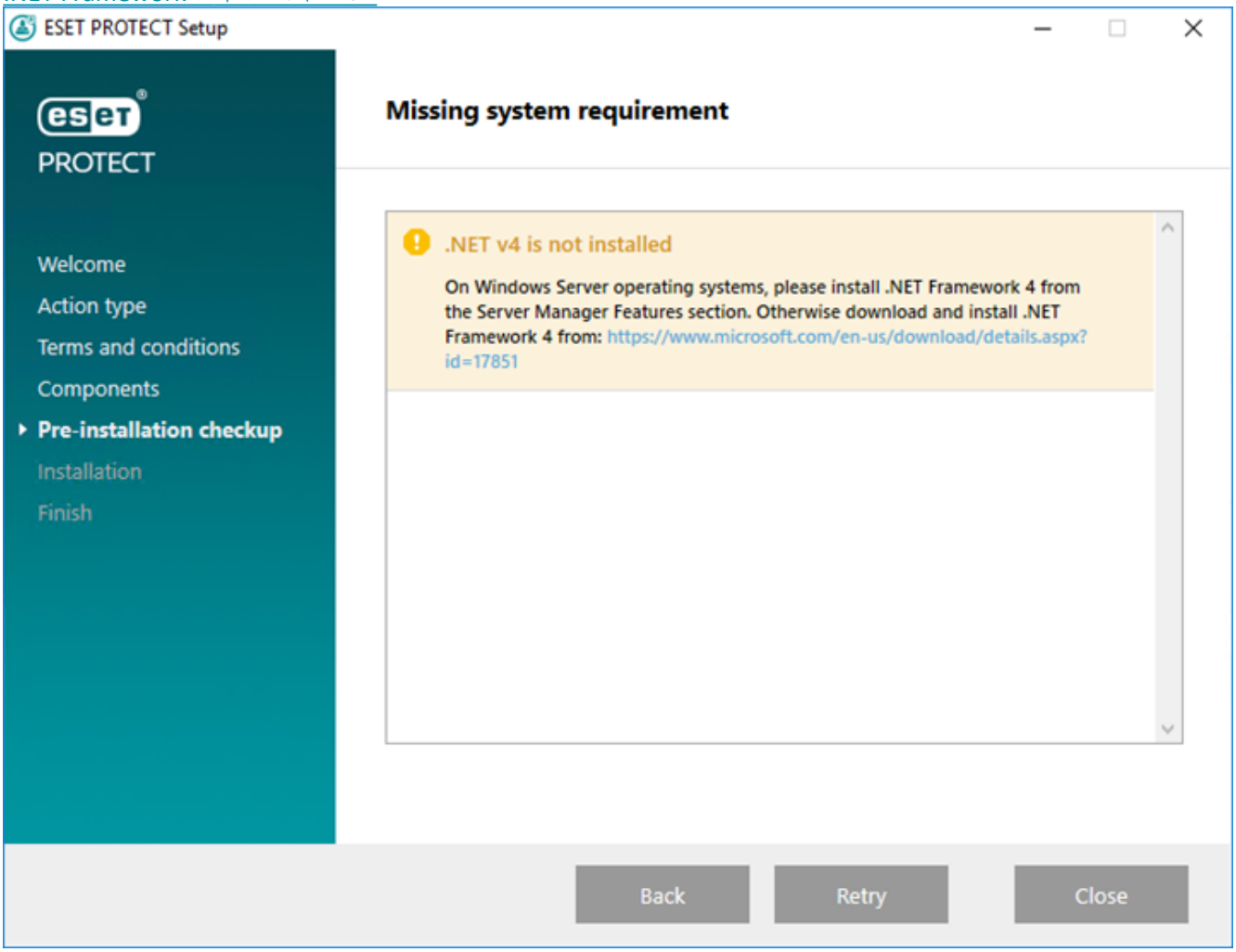
5. **Webコンソールのカスタム HTTPS証明書を追加**を選択した場合は、**参照**をクリックして、有効な証明書(*.pfx*またはp12ファイル)を選択し、**パスフレーズ**を入力(またはパスフレーズがない場合は空欄)します。インストーラーは、TomcatサーバーにWebコンソールアクセスの証明書をインストールします。**次へ**をクリックして続行します。



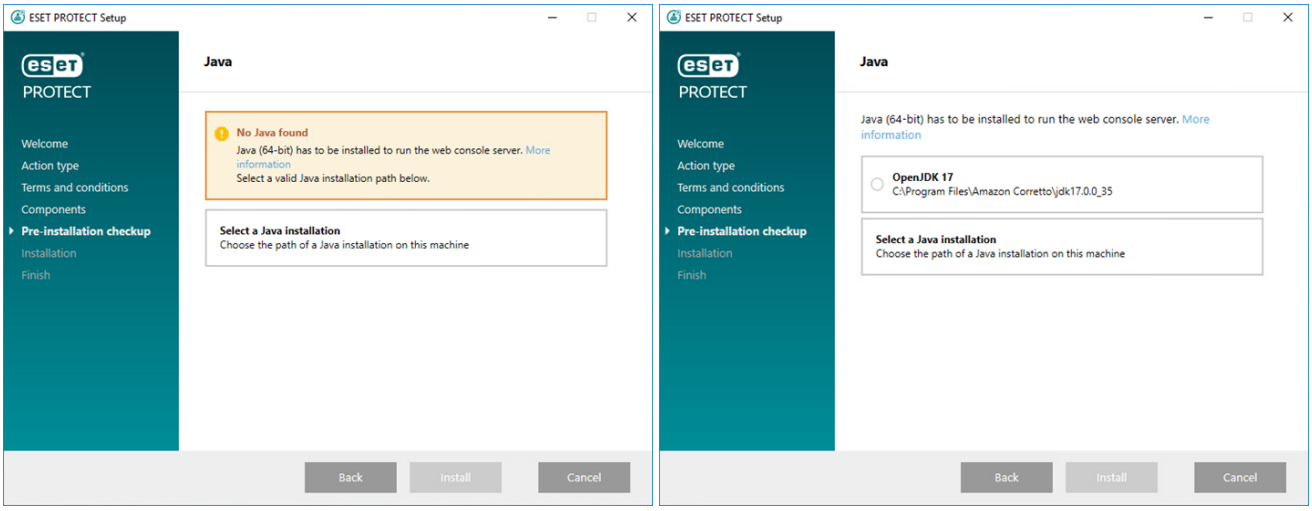
6. 前提条件チェック中にエラーが見つかった場合は、エラーを修正します。システムがすべての前提条件を満たしていることを確認します。

.NET v4がインストールされていません

.NET Frameworkのインストール



Javaが見つからない/Java (64ビット) が検出される



システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

a)既にインストールされているJavaを選択するには、**Javaインストールを選択**をクリックして、Javaがインストールされているフォルダー(および*C:\Program Files\Amazon Corretto\jdk1.8.0_212*などのサブフォルダー*bin*)を選択し、**OK**をクリックします。無効なパスを選択した場合は、インストーラーでメッセージが表示されます。

b)**インストール**をクリックして続行するか、**変更**をクリックしてJavaインストールパスを変更します。

設定が有効な状態ではありません/Microsoft SQL Server Express

インストーラーは、次のような複数の理由によりこの通知を表示する場合があります。

- インストーラーが破損している場合。たとえば、一部のインストーラーファイルが見つからないことがあります。オールインワンインストーラーを再度ダウンロードして実行します。
- オールインワンインストーラーへのパスには、発音区別符号付きの文字などの特殊文字が含まれています。特殊文字のないパスからESET PROTECTオールインワンインストーラーを実行します。

システムディスクには32 MBしか空き領域がありません

ESET PROTECT On-Premをインストールするための十分なディスク領域がない場合は、次の通知が表示される場合があります。

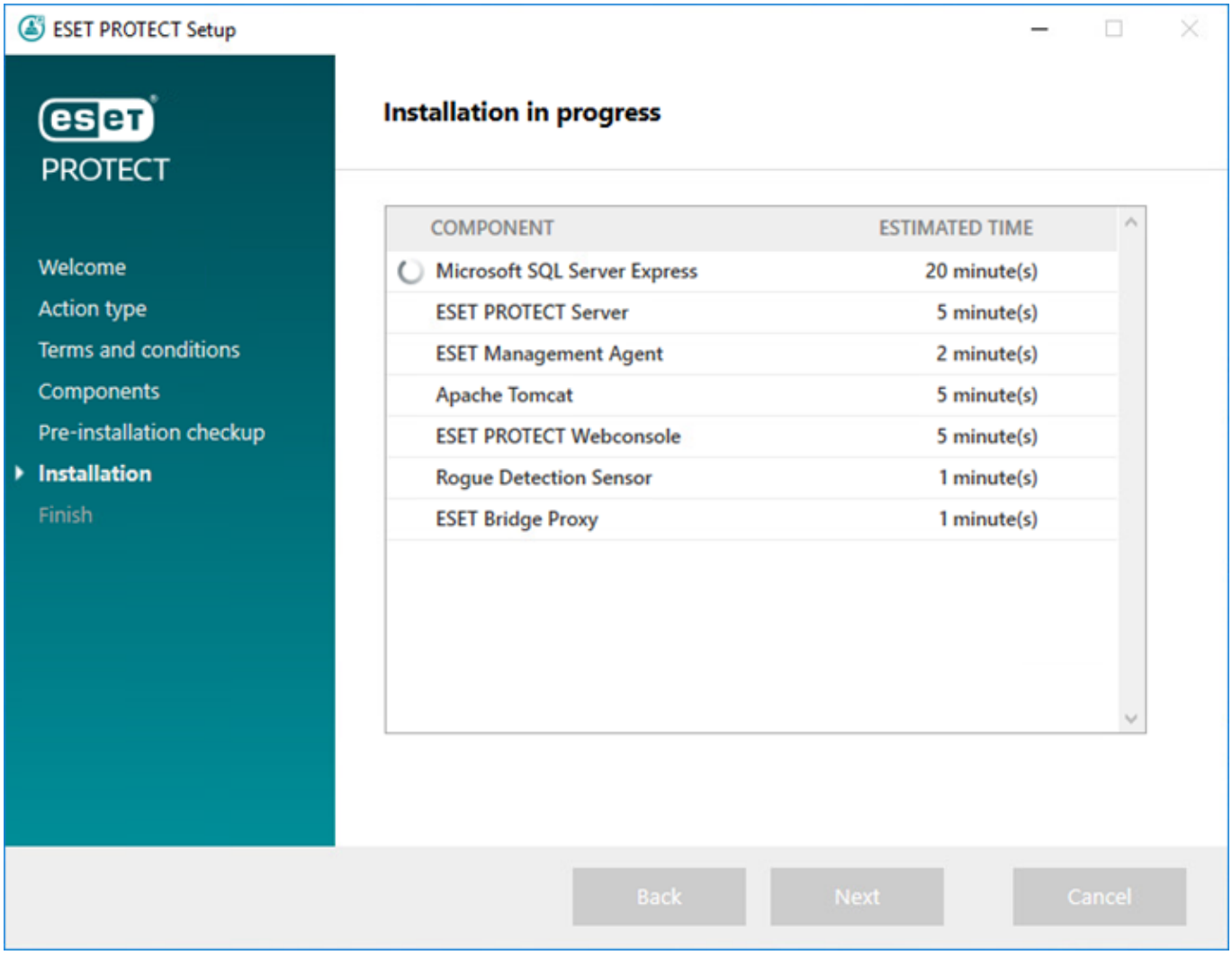
ESET PROTECT On-Premとすべてのコンポーネントをインストールするには、4,400 MB以上の空きディスク領域が必要です。

ESET Remote Administrator 5.x以前がコンピュータにインストールされているため、インストーラを続行できません。

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。ERA 5.x/6.xまたはESMC 7.0/7.1をお持ちの場合、ESET PROTECT On-Prem11.0への直接アップグレードはサポートされていません。ESET PROTECT On-Prem11.0のクリーンインストールを実行してください。

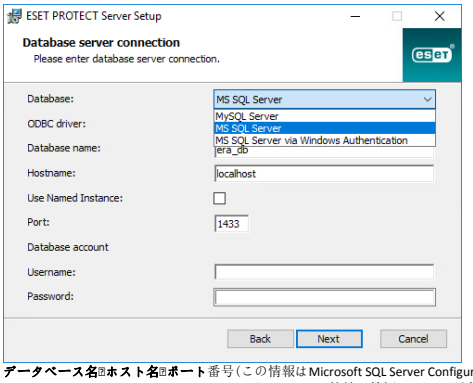
7. 前提条件チェックが完了し、環境がすべての要件を満たしたら、インストールが開始します。システムとネットワーク構成によっては、インストールに1時間以上かかる場合があります。

インストール中には、ESET PROTECT On-Premインストールウィザードが応答しません。



8. 手順4で**Microsoft SQL Server Express**をインストールすることを選択した場合は、データベース接続チェックが実行されます。既存のデータベースサーバーがある場合は、データベース接続詳細情報を入力する必要があります。

SQL/MySQL Serverへの接続を設定する

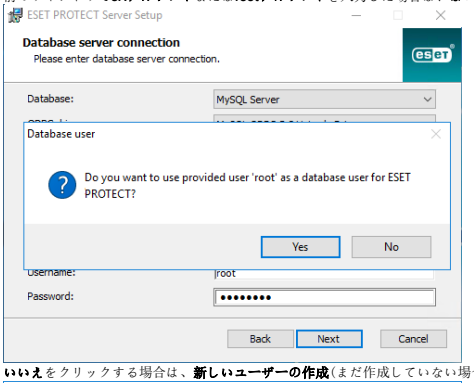


データベース名、**ホスト名**、**ポート**番号(この情報はMicrosoft SQL Server Configuration Managerで確認できます)と**データベース管理者アカウント**詳細情報(**ユーザー名**と**パスワード**)を該当するフィールドに入力し、**[次へ]**をクリックします。インストーラーは、データベース接続を検証します。既存のデータベース(前のESET PROTECT On-Premインストール)がデータベースサーバーにある場合は、これが検出されます。**既存のデータベースを使用してアップグレードを適用**するか、**既存のデータベースを削除して新しいバージョンをインストール**するかを選択できます。

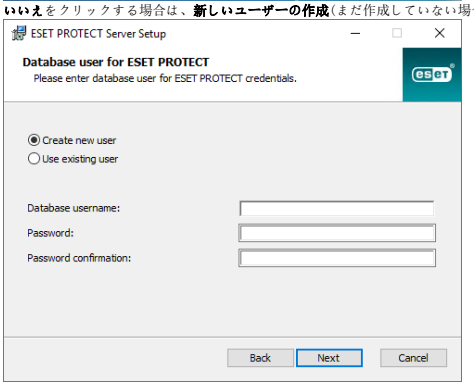
名前付きインスタンスを使用する - Microsoft SQLデータベースを使用している場合は、**名前付きインスタンスを使用する**チェックボックスを選択し、カスタムデータベースインスタンスを使用できます。*HOSTNAME\DB_INSTANCE*の形式で**ホスト名**フィールドで設定できます。(例: *192.168.0.10\ESMC7SQL*)。クラスタデータベースの場合、クラスタ名のみを使用します。このオプションを選択する場合、データベース接続ポートを変更できません。Microsoftの既定のポートが使用されます。フェールオーバークラスターにインストールされたMicrosoft SQLデータベースにサーバーを接続するには、**ホスト名**フィールドにESET PROTECTクラスタ名一を入力します。

データベースアカウント情報を入力するときには2つのオプションがあります。ESET PROTECTデータベースにのみアクセスできる**専用データベースユーザーアカウント**、**SAアカウント** (Microsoft SQL)または**rootアカウント** (MySQL)を使用できます。専用ユーザーアカウントを使用する場合は、このアカウントを特定の権限で作成する必要があります。詳細については、「専用データベースユーザーアカウント」を参照してください。専用ユーザーアカウントを使用しない場合は、管理者アカウント(SAまたはroot)を入力します。

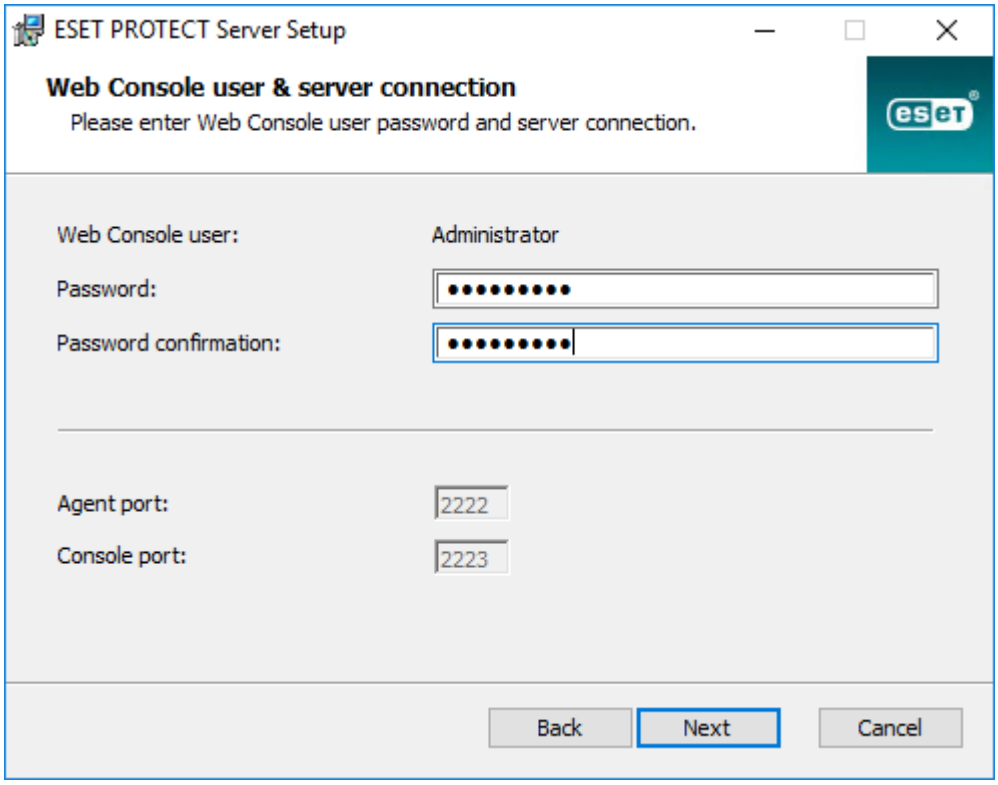
前のウィンドウで**SAアカウント**または**rootアカウント**を入力した場合は、**はい**をクリックし、SA/rootアカウントをESET PROTECTのデータベースユーザーとして使用し続けます。



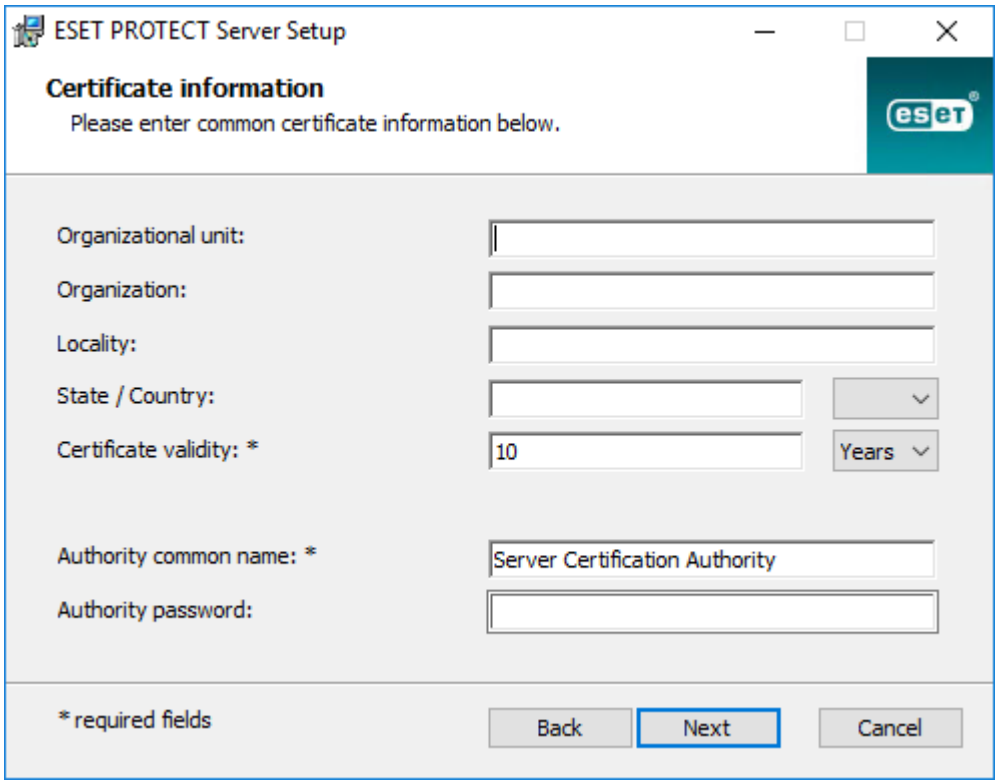
いいえをクリックする場合は、**新しいユーザーの作成**(まだ作成していない場合)または**既存のユーザーを使用する** (専用データベースユーザーアカウントがある場合)を選択する必要があります。



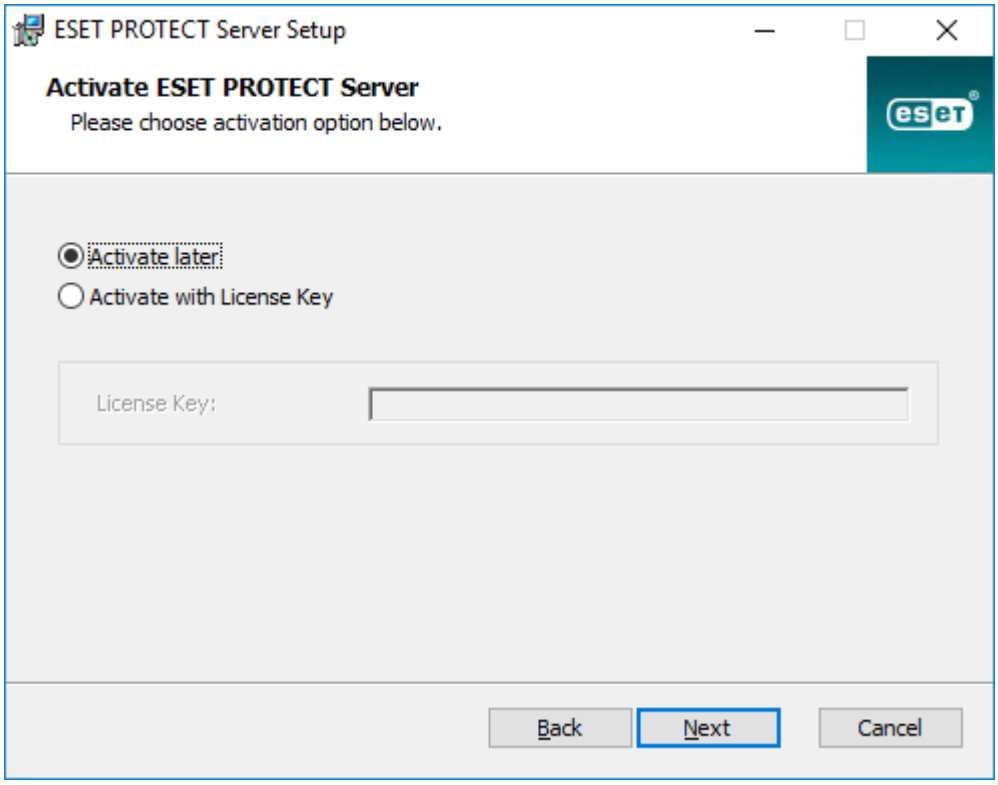
9. Webコンソール管理者アカウントのパスワードを入力するように指示されます。このパスワードはESET PROTECT Webコンソールにログインするときに使用するため重要です。**次へ**をクリックします。



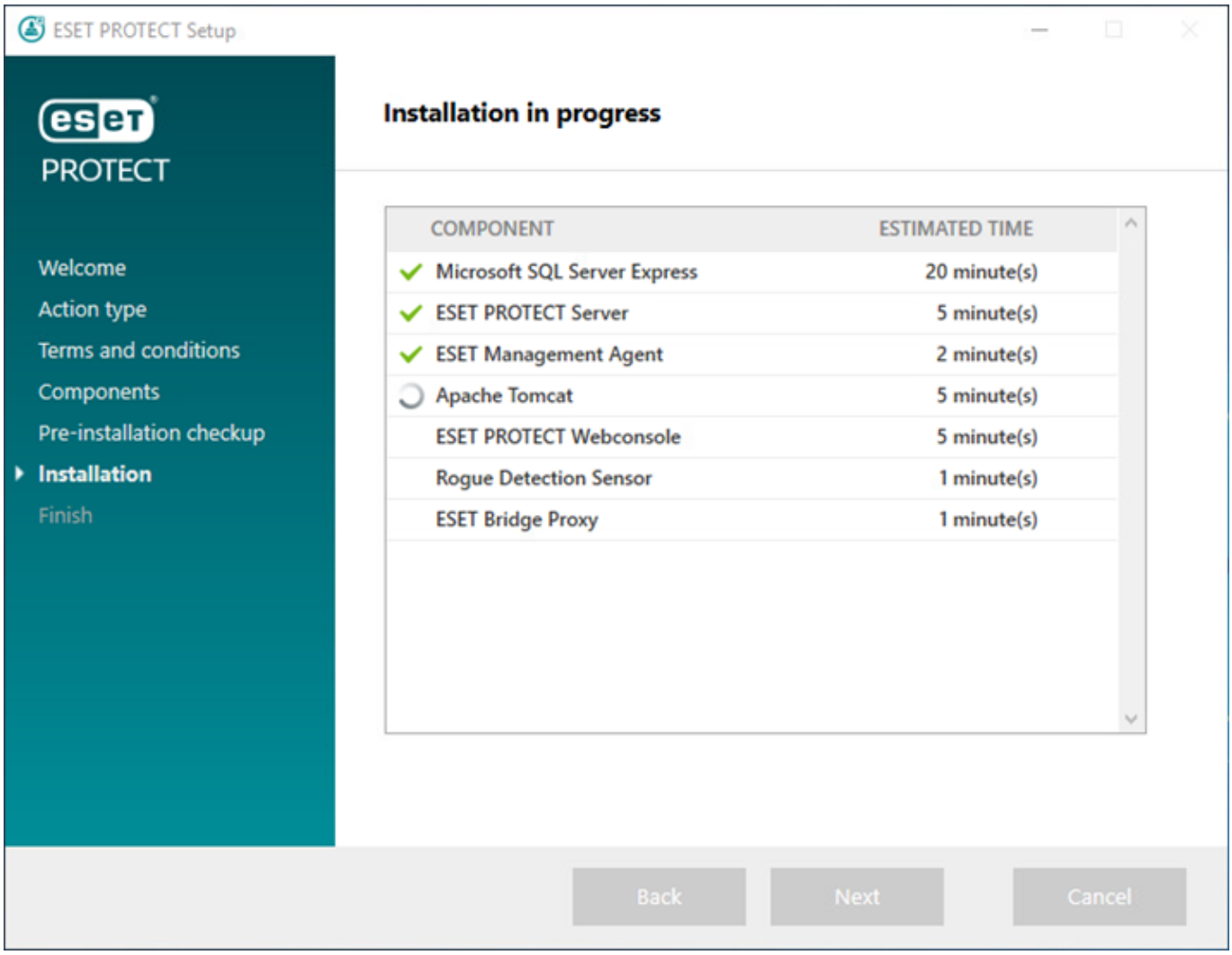
10. フィールドをそのままにするか、ESET Managementエージェントと ESET PROTECTサーバー証明書の詳細に表示する企業情報を入力できます。**認証パスワード**フィールドにパスワードを入力する場合は、必ず覚えておいてください。**次へ**をクリックします。



11. 有効な**ライセンスキー**(ESETから受信した新しい購入メールに記載)を入力し、**次へ**をクリックします。あるいは、**後でアクティベート**を選択できます(詳細な手順については、「アクティベーション」の章を参照してください)。



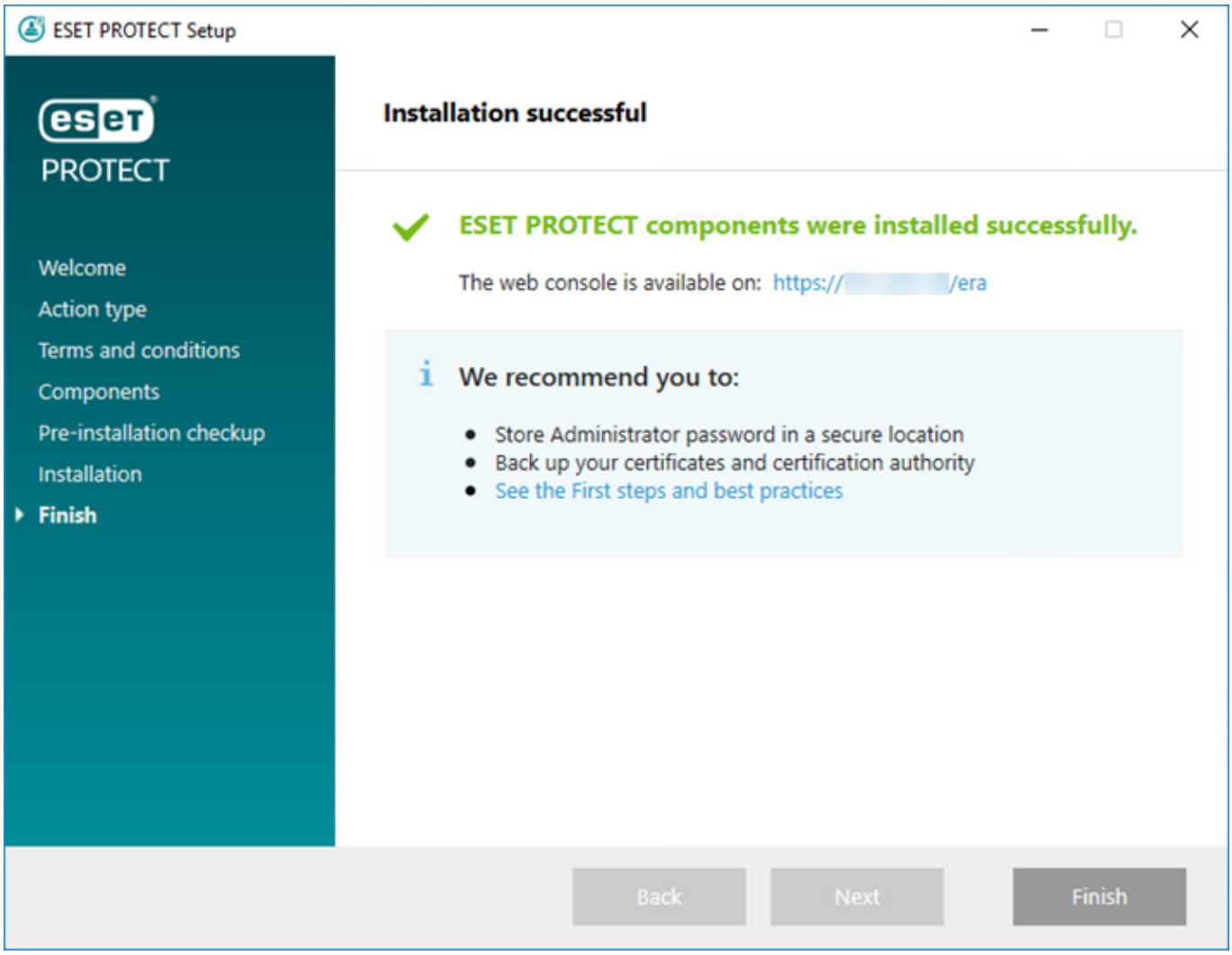
12. インストールの進行状況が表示されます。



13. **Rogue Detection Sensor**のインストールを選択した場合は、WinPcapドライバにインストールウィ

ンドウが表示されます。**起動時にWinPcapドライバを自動的に起動する**チェックボックスを必ず選択してください。

14. インストールが完了すると「ESET PROTECTコンポーネントのインストールが成功しました」とESET PROTECT WebコンソールURLアドレスが表示されますURLをクリックしてWeb コンソールを開くか、[完了]をクリックします。



インストールが失敗する場合:

- オールインワンインストールパッケージのインストールログファイルを確認します。ログディレクトリはオールインワンインストーラーのディレクトリと同じです。たとえば次のとおりです。
  `C:\Users\Administrator\Downloads\x64\logs\`

- 問題を解決するための追加手順については、トラブルシューティングを参照してください。

ESET PROTECT モバイルデバイスコネクター(スタンドアロン)のインストール

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

スタンドアロンツールとしてモバイルデバイスコネクターをインストールするにはESETPROTECTサーバー

が実行されているサーバーとは別のコンピューターで次の手順を実行します。

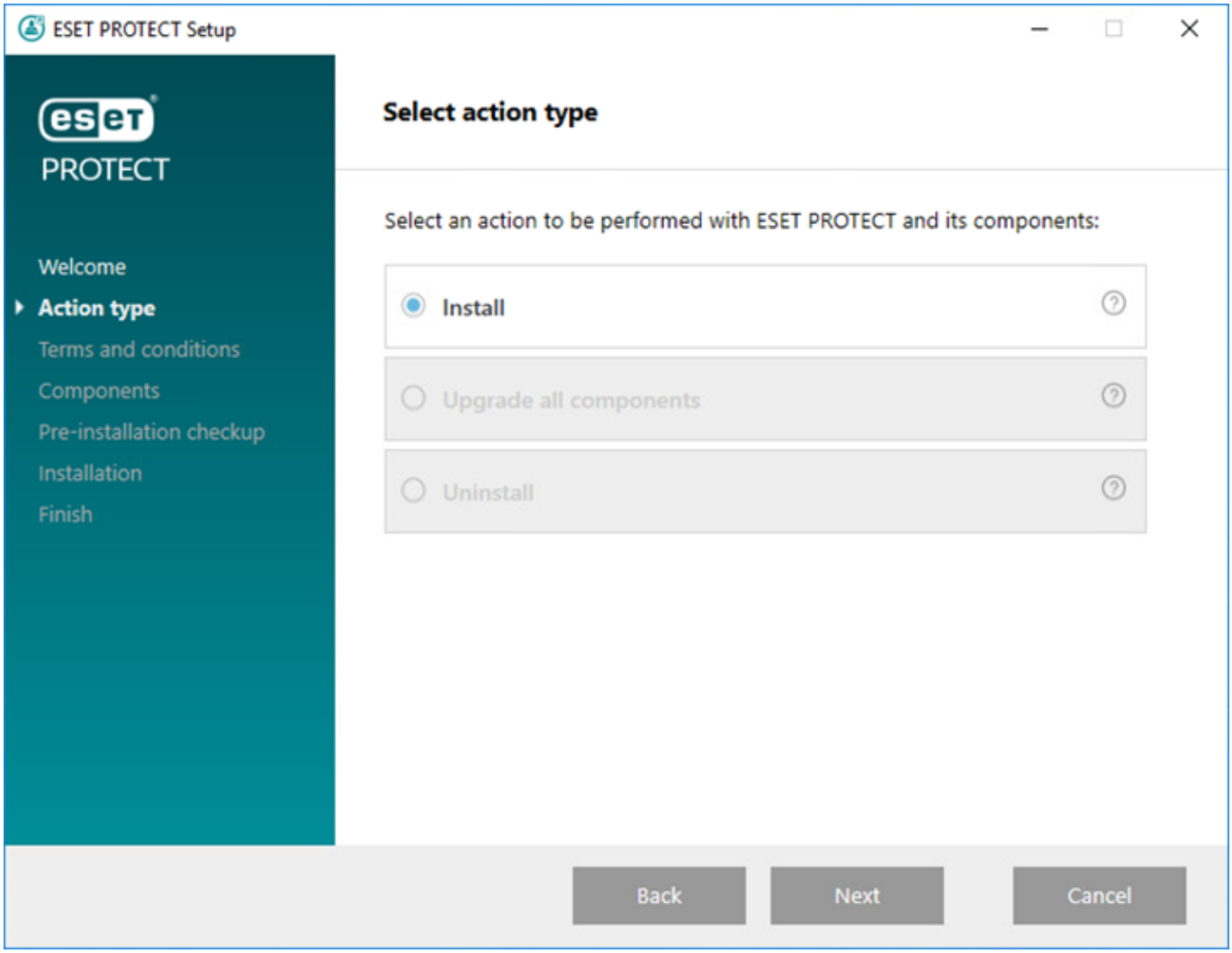
場所に関係なく、常にモバイルデバイスを管理できるように、モバイルデバイスコネクターはインターネットからアクセスできる必要があります。

モバイルデバイスはモバイルデバイスコネクターと通信するため、モバイルデータの使用に必然的に影響することを考慮してください。これは特にローミングに当てはまります。

次の手順に従い、Windowsにモバイルデバイスコネクターをインストールします。

1. まず前提条件を読み、すべてが満たされていることを確認します。

2. インストールパッケージをダブルクリックし、**インストール**を選択して、**次へ**をクリックします。

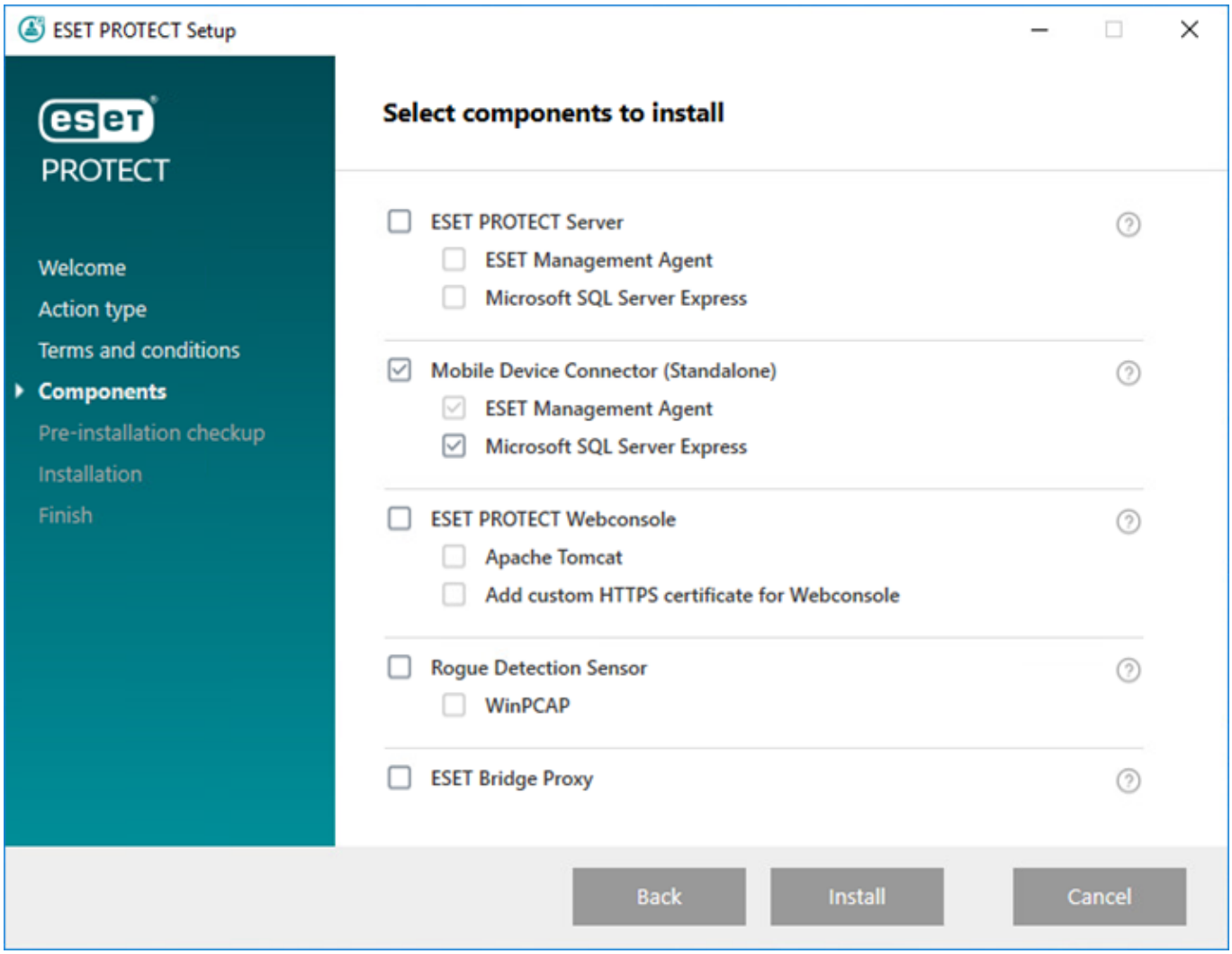


3. **製品改善プログラムに参加する**の横のチェックボックスをオンにして、クラッシュレポートと匿名のテレメトリーデータ(OSのバージョンと種類、ESET製品バージョン、および他の製品固有の情報)をESETに送信します。

4. EULAに同意した後、[**次へ**]をクリックします。

5. **Mobile Device Connector (スタンドアロン)**の横のチェックボックスのみを選択します。ESET PROTECT On-Prem モバイルデバイスコネクターには、処理のための**データベース**が必要です。データベースをインストールする場合は、**Microsoft SQL Server Express**を選択します。あるいは、チェックボックスを空欄にします。既存のデータベースに接続する場合は、インストール中に接続できます。**インストー**

ルをクリックすると、インストールを続行します。



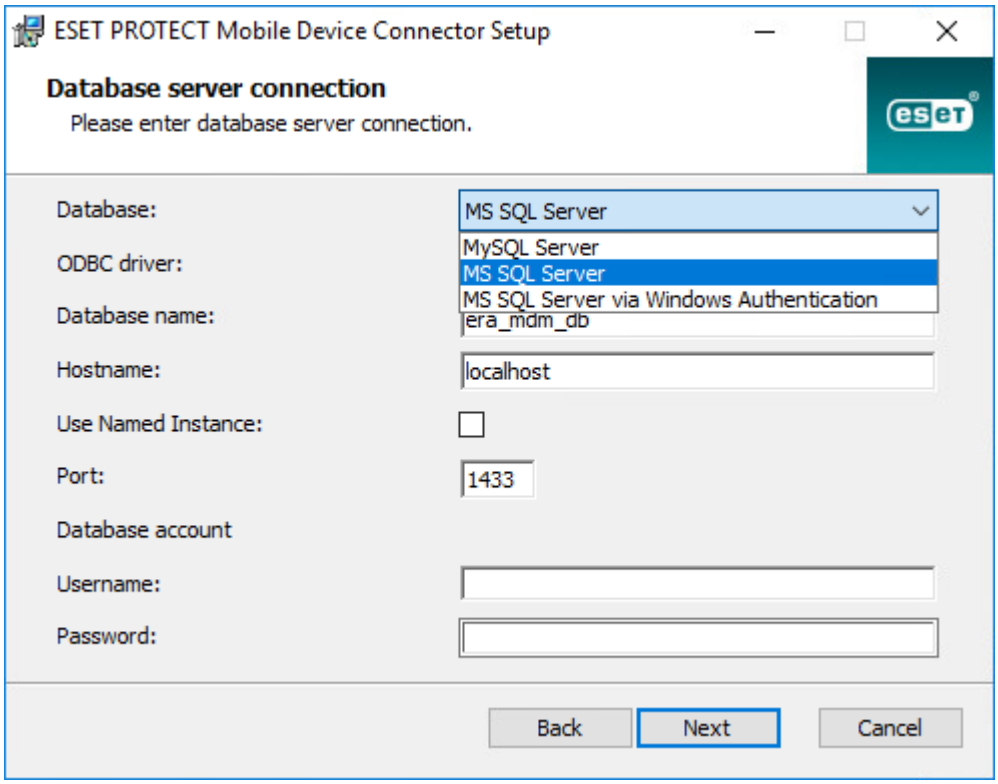
6. ステップ5でこのインストールの一部としてデータベースをインストールした場合は、データベースが自動的にインストールされ、ステップ8にスキップできます。ステップ5でデータベースをインストールしなかった場合は、MDMコンポーネントを既存のデータベースに接続するように指示されます。

ESET PROTECTデータベースと同じデータベースサーバーを使用できますが、80台以上のモバイルデバイスを登録する計画の場合には、別のDBサーバーを使用することをお勧めします。

7. インストーラーはモバイルデバイスコネクターで使用される既存のデータベースに接続する必要があります。次の接続詳細を指定します。

- **データベース**:Windows認証によるMySQL Server/MS SQL Server/MS SQL Server
- **ODBCドライバ**:MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **データベース名**:定義済みの名前を使用するか、必要に応じて変更することをお勧めします。
- **ホスト名**:ホスト名またはデータベースサーバーのIPアドレス

- **ポート**: データベースとの接続で使用されます。
- データベース管理者アカウントの**ユーザー名/パスワード**
- **名前付きインスタンスを使用する** - Microsoft SQLデータベースを使用している場合は、**名前付きインスタンスを使用する**チェックボックスを選択し、カスタムデータベースインスタンスを使用できます。*HOSTNAME\DB_INSTANCE*の形式で**ホスト名**フィールドで設定できます。(例: *192.168.0.10\ESMC7SQL*)。クラスタデータベースの場合、クラスタ名のみを使用します。このオプションを選択する場合、データベース接続ポートを変更できません。Microsoftの既定のポートが使用されます。フェールオーバークラスターにインストールされたMicrosoft SQLデータベースにサーバーを接続するには、**ホスト名**フィールドにESET PROTECTクラスタ名ーを入力します。

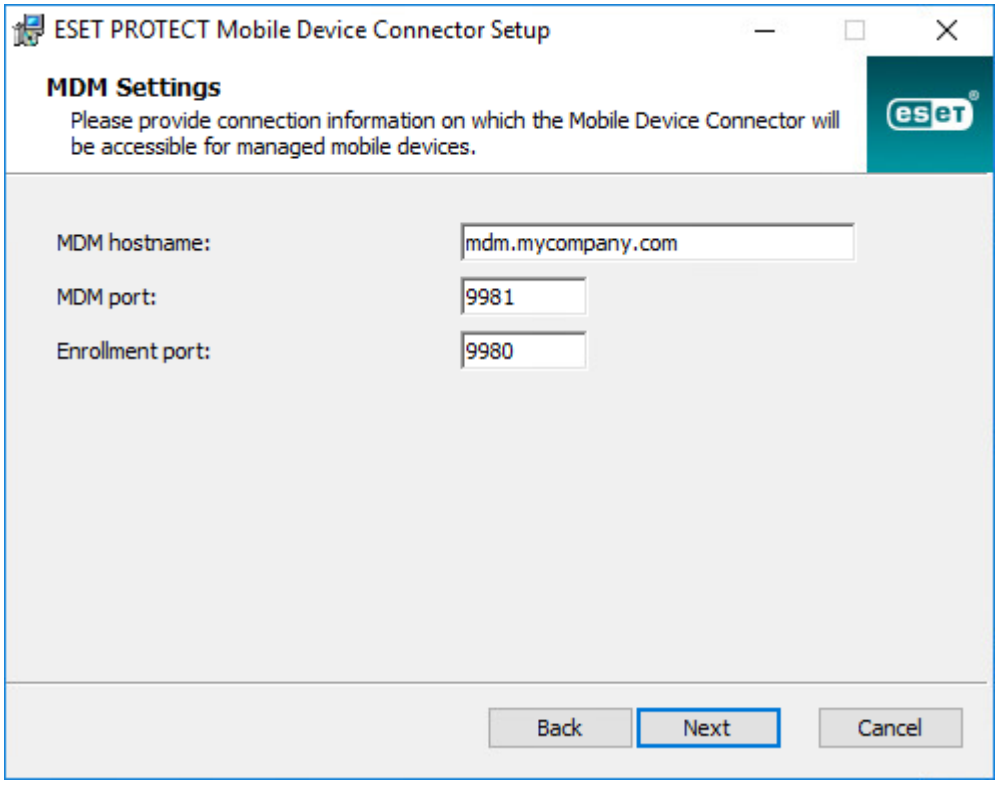


8. 接続が成功した場合は、ESET PROTECT MDMのデータベースユーザーとして指定されたユーザーを使用することを確認するように指示されます。

9. 新しいデータベースが正常にインストールされたか、インストーラが正常に既存のデータベースに接続した後に、MDMインストールを続行できます。**MDMホスト名**:を指定しますこれはMDMサーバーの公開ドメインまたは公開IPアドレスであり、インターネットからモバイルデバイスがアクセスできます。

MDMホスト名を**HTTPSサーバー証明書**で指定されたフォームに入力する必要があります。そうでない場合、iOSモバイルデバイスはMDMプロファイルのインストールを拒否します。たとえば、HTTPS証明書でIPアドレスが指定されている場合、このIPアドレスを**MDMホスト名またはIPアドレス**フィールドに入力します。FQDN (たとえば`mdm.mycompany.com`)がHTTPS証明書で指定されている場合、このFQDNを**MDMホスト名**フィールドに入力します。ワイルドカード`*`(たとえば`*.mycompany.com`)がHTTPS証明書で使用される場合、`mdm.mycompany.com`を**MDMホスト名**フィールドで使用できます。

> ⚠ インストールのこのステップで**MDMホスト名**フィールドに入力する内容には十分に注意してください。情報が正しくないか、形式が正しくない場合、MDMコネクターは正常に動作しません。修正する唯一の方法は、コンポーネントの再インストールです。



10. 次のステップで、**次へ**をクリックして、データベースへの接続を確認します。

11. MDMコネクターをESET PROTECTサーバーに接続するためのポートESET PROTECTサーバーへの接続に必要な**サーバーホスト**と**サーバーポート**を入力し、**サーバー支援インストール**または**オフラインインストール**を選択して続行します。

- **サーバー支援インストール** - ESET PROTECT Webコンソール管理者資格情報を提供します。インストーラーが必要な証明書を自動的にダウンロードします。また、サーバー支援インストールに必要な権限も確認します。

  1.**サーバーホスト** (ESET PROTECTサーバーの名前またはIPアドレス)と**Webコンソールポート**(カスタムポートを使用しない場合は既定のポート2223を使用)を入力します。またWebコンソール管理者認証情報(**ユーザー名/パスワード**)を指定します。

  2.証明書を許可するように指示されたら、**[はい]**をクリックします。手順10に進みます。

- **オフラインインストール** – プロキシ証明書と認証局を指定する必要があります。これはESET PROTECT On-Premからエクスポートできます。あるいは、カスタム証明書と適切な認証局を使用できます。

  1.ピア証明書の横の**[参照]**をクリックし、**ピア証明書**の場所に移動します(これはESET PROTECT On-Premからエクスポートしたプロキシ証明書です)。**[証明書パスワード]**テキストフィールドは空欄にします。この証明書にはパスワードが必要ないためです。

  2.認証局の手順を繰り返し、手順11に進みます。

> ESET PROTECT On-Premで(ESET PROTECT On-Premインストール中に自動的に生成された既定の証明書の代わりに)カスタム証明書を使用する場合、プロキシ証明書を指定するように指示されるときにこれらを使用する必要があります。

12. モバイルデバイスコネクターのインストール先フォルダ(既定の場所を推奨)を指定し、**[次へ]**をクリックしてから、**[インストール]**をクリックします。

MDMインストールが完了した後、エージェントインストールが確認されます。**次へ**をクリックすると、インストールを開始し、同意する場合はEULAを承諾して、以下の手順を実行します。

1. **サーバーホスト**(ESET PROTECTサーバーのホスト名またはIPアドレス)と**サーバーポート**(既定のポートは2222です。別のポートを使用する場合は、既定のポートをカスタムポート番号で置き換えます)。

サーバーホストが[**サーバー証明書**]の[**ホスト**]で定義された1つ以上の値(FQDNを推奨)と一致していることを確認します。そうでない場合、「受信したサーバー証明書が無効です」というエラーが表示されます。ただし、[サーバー証明書ホスト]フィールドにワイルドカード(*)がある場合を除きます。この場合、すべての[**サーバーホスト**]で動作します。

2. プロキシを使用している場合は、**プロキシを使用する**チェックボックスをオンにします。選択すると、インストーラーは**オフラインインストール**を続行します。

このプロキシ設定は、ESET Managementエージェントと ESET PROTECTサーバーの間のレプリケーションでのみ使用され、アップデートのキャッシュには使用されません。
- **プロキシホスト名**: HTTPプロキシコンピュータのホスト名またはIPアドレス。
- **プロキシポート**: 既定値は3128です。
- **ユーザー名**と**パスワード**: 認証を使用する場合は、プロキシによって使用される認証資格情報を入力します。

ポリシーで後からプロキシ設定を変更できます。プロキシ経由のエージェントとサーバー間の接続を設定する前に、プロキシをインストールする必要があります。

3. 次のインストールオプションのいずれかを選択し、該当する次のセクションの手順に従います。

サーバー支援インストール - ESET PROTECT Webコンソール管理者の認証情報を指定する必要があります(必要な証明書はインストーラによって自動的にダウンロードされます)。

オフラインインストール – エージェント証明書および認証局を指定する必要があります。これはESET PROTECT On-Premからエクスポートできます。あるいは、カスタム証明書を使用できます。

- **サーバー支援エージェントインストール**を続行するには、以下の手順に従います。

1. [**サーバーホスト**]フィールドにESET PROTECT Webコンソール(ESET PROTECTサーバーと同じ)のホスト名またはIPアドレスを入力します。カスタムポートを使用しない場合は、[**Webコンソールポート**]を既定の2223のままにします。また、[**ユーザー名**]と[**パスワード**]フィールドにWebコンソールアカウントの資格情報を入力します。ドメインユーザーとしてログインするには、**ドメインにログイン**の横のチェックボックスをオンにします。

- **サーバーホスト**が[**サーバー証明書**]の[**ホスト**]で定義された1つ以上の値(FQDNを推奨)と一致していることを確認します。そうでない場合、「受信したサーバー証明書が無効です」というエラーが表示されます。ただし、[サーバー証明書ホスト]フィールドにワイルドカード(*)がある場合を除きます。この場合、すべての[**サーバーホスト**]で動作します。
- サーバー支援インストールでは、二要素認証のユーザーを使用できません。

2. 証明書を許可するかどうかを確認するメッセージが表示されたら、[**はい**]をクリックします。

3. **コンピューターを作成しない(コンピューターは初回接続中に自動的に作成されます)**または**カスタム静的グループを選択**を選択します。[**カスタム静的グループを選択**]をクリックするとESET PROTECTOn-Premの既存の静的グループのリストから選択できます。コンピューターは選択したグループに追加されます。

4. ESET Managementエージェントのインストール先フォルダ(既定の場所を推奨)を指定し、**[次へ]**をクリックしてから、**[インストール]**をクリックします。

- **オフラインエージェントインストール**を続行するには、以下の手順に従います。

1. 前のステップで**プロキシを使用**を選択した場合は、**プロキシホスト名**⍰**プロキシポート**(既定のポートは3128)、**ユーザー名**、および**パスワード**を入力し、**次へ**をクリックします。

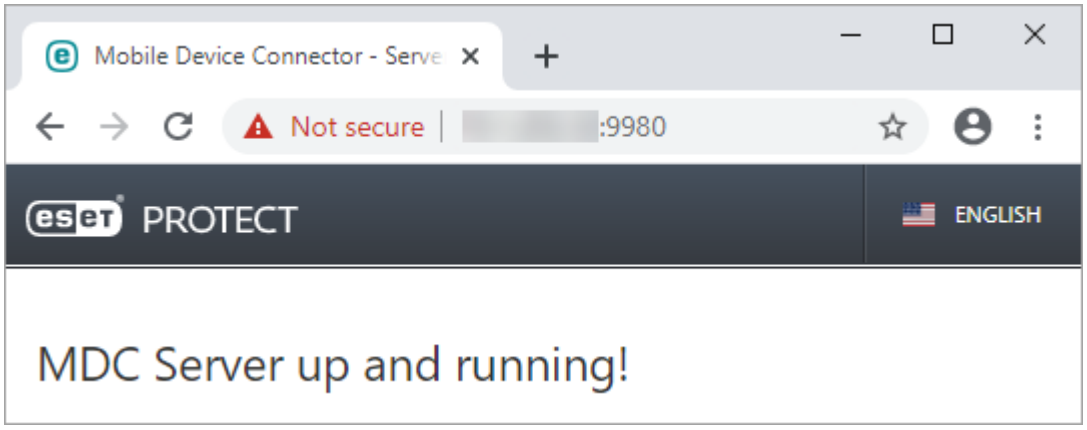
2. **[参照]**をクリックし、ピア証明書の場所に移動します(これはESET PROTECT On-Premからエクスポートしたエージェント証明書です)。**[証明書パスワード]**テキストフィールドは空欄にします。この証明書にはパスワードが必要ないためです。**認証局**を参照する必要はありません。このフィールドは空欄にします。

ESET PROTECT On-Premでカスタム証明書を使用する場合(ESET PROTECT On-Premインストール中に自動生成された既定の証明書を使用しない場合)は、適宜カスタム証明書を使用してください。

証明書パスフレーズには、次の文字を含めることはできません:" \ これらの文字は、エージェントの初期化中に重大なエラーが発生する原因となります。

3. **[次へ]**をクリックして、既定のフォルダにインストールするか、**[変更]**をクリックして別のフォルダを選択します(既定の場所を推奨)。

インストールが完了したら⍰https://*https://your-mdm-hostname:enrollment-port* (*https://mdm.company.com:9980*など)をブラウザで開き、モバイルデバイスコネクターが実行中であるかどうかを確認してください。インストールが成功したら、次のメッセージが表示されます。



ESET PROTECT On-PremからMDMをアクティブ化できます。

Windowsでのコンポーネントインストール

ほとんどのインストールシナリオでは、コンピューターによって異なるESET PROTECTコンポーネントをインストールし、さまざまなネットワークアーキテクチャに対応し、パフォーマンス要件やその他の要求に対応する必要があります。次のインストールパッケージは、個別のESET PROTECTコンポーネントで

使用できます。

コアコンポーネントインストール:

- ESET PROTECTサーバー
- ESET PROTECT Webコンソール - ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。
- ESET Managementエージェント(クライアントコンピュータにインストールする必要があります。ESET PROTECTサーバーでは任意)

オプションコンポーネントインストール:

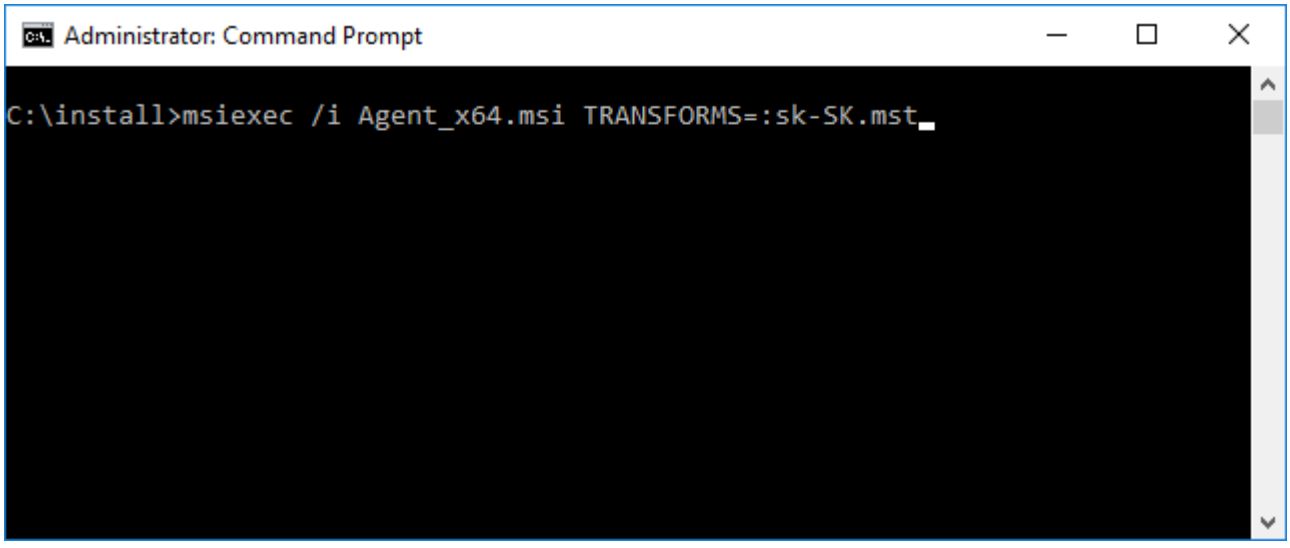
- RD Sensor
- モバイルデバイスコネクター
- ESET BridgeHTTPプロキシ
- ミラーツール

ESET PROTECTオールインワンインストールも参照してください。

以前のESET PROTECT On-Premを最新のESET PROTECT On-Prem 11.0にアップグレードする手順については、アップグレード手順を参照してください。

ローカル言語でインストールを実行する場合は、コマンドライン経由で特定のESET PROTECTコンポーネントのMSIインストーラーを起動する必要があります。

次に、スロバキア語でインストールを実行する例を示します。



インストールを実行する言語を選択するには、この表に従って対応するTRANSFORMSパラメータを指定します。

言語	コード
英語(米国)	en-US
アラビア語(エジプト)	ar-EG

言語	コード
簡体中国語	zh-CN
繁体中国語	zh-TW
クロアチア語(クロアチア)	hr-HR
チェコ語(チェコ共和国)	cs-CZ
フランス語(フランス)	fr-FR
フランス語(カナダ)	fr-CA
ドイツ語(ドイツ)	de-DE
ギリシャ語(ギリシャ)	el-GR
ハンガリー語(ハンガリー)*	hu-HU
インドネシア語(インドネシア)*	id-ID
イタリア語(イタリア)	it-IT
日本語(日本)	ja-JP
韓国語(韓国)	ko-KR
ポーランド語(ポーランド)	pl-PL
ポルトガル語(ブラジル)	pt-BR
ロシア語(ロシア)	ru-RU
スペイン語(チリ)	es-CL
スペイン語(スペイン)	es-ES
スロバキア語(スロバキア)	sk-SK
トルコ語(トルコ)	tr-TR
ウクライナ語(ウクライナ)	uk-UA

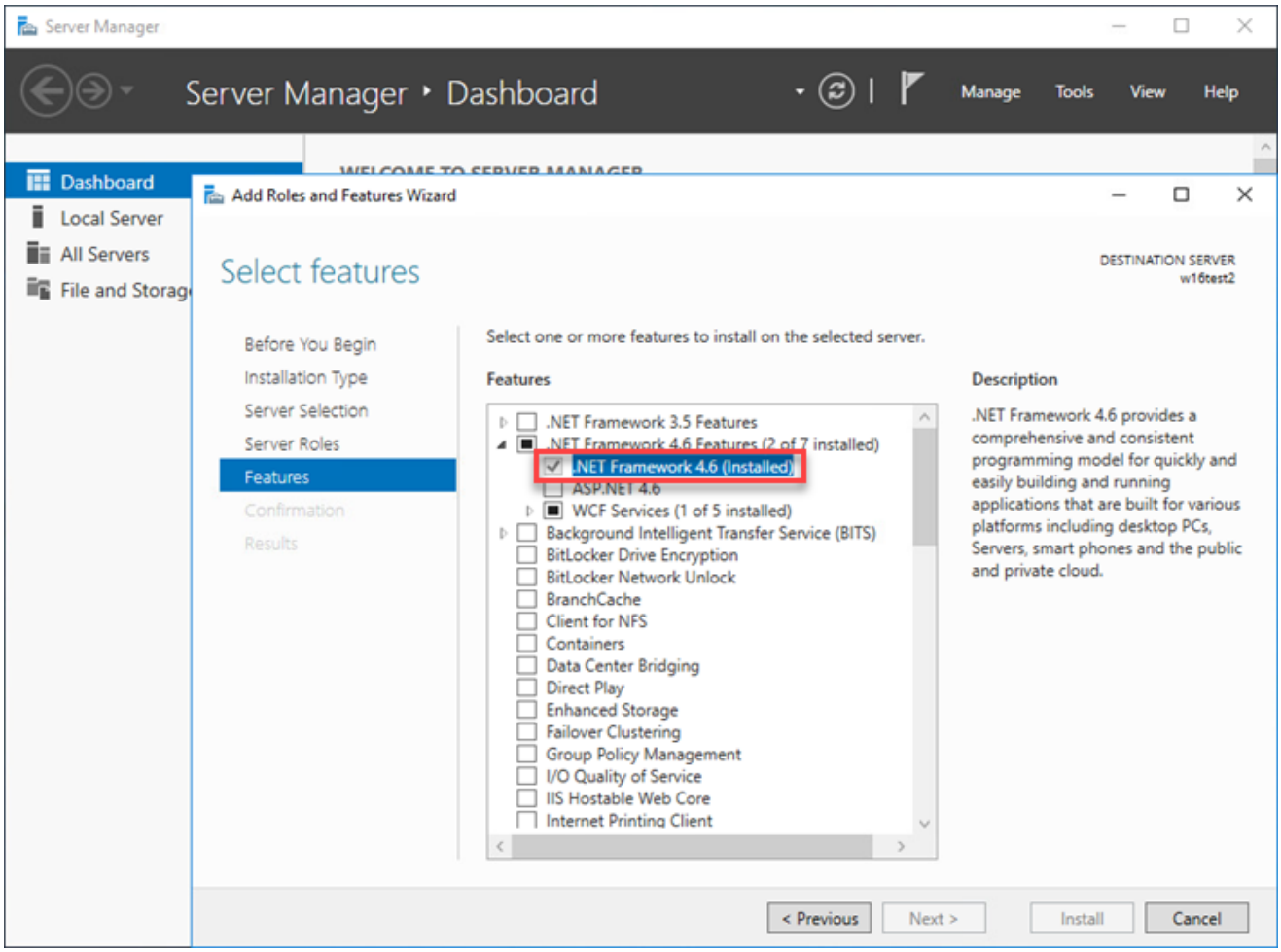
*製品のみがこの言語で提供されています。オンラインヘルプはありません。

サーバーインストール - Windows

前提条件

- 有効な製品認証キーが必要です。
- サポートされているWindowsオペレーティングシステムが必要です。
- 必要なポートが開いていて使用可能である必要があります。ポートの一覧については、ここを参照してください。
- サポートされているデータベースサーバーとコネクター(Microsoft SQL ServerまたはMySQL)がインストールされ、実行中でなければなりません。ESET PROTECT On-Premで使用するためにデータベースをただしく設定するには、データベースサーバー設定詳細(Microsoft SQL ServerまたはMySQL)を確認することをお勧めします。Microsoft SQLまたはMySQLのデータベースとユーザーアカウントを設定するには、ナレッジベース記事をお読みください。
- ESET PROTECTサーバーを管理するには、ESET PROTECTWebコンソールがインストールされている必要があります。

- Microsoft SQL Server Expressインストールには□Microsoft .NET Framework 4が必要です。**ロールと機能の追加ウィザード**を使用してインストールできます。



インストール

次の手順に従って□WindowsでESET PROTECTサーバーをインストールします。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。（*server_x64.msi*）.

2. ESET PROTECTサーバーインストーラを実行し、同意する場合はEULAに同意します。

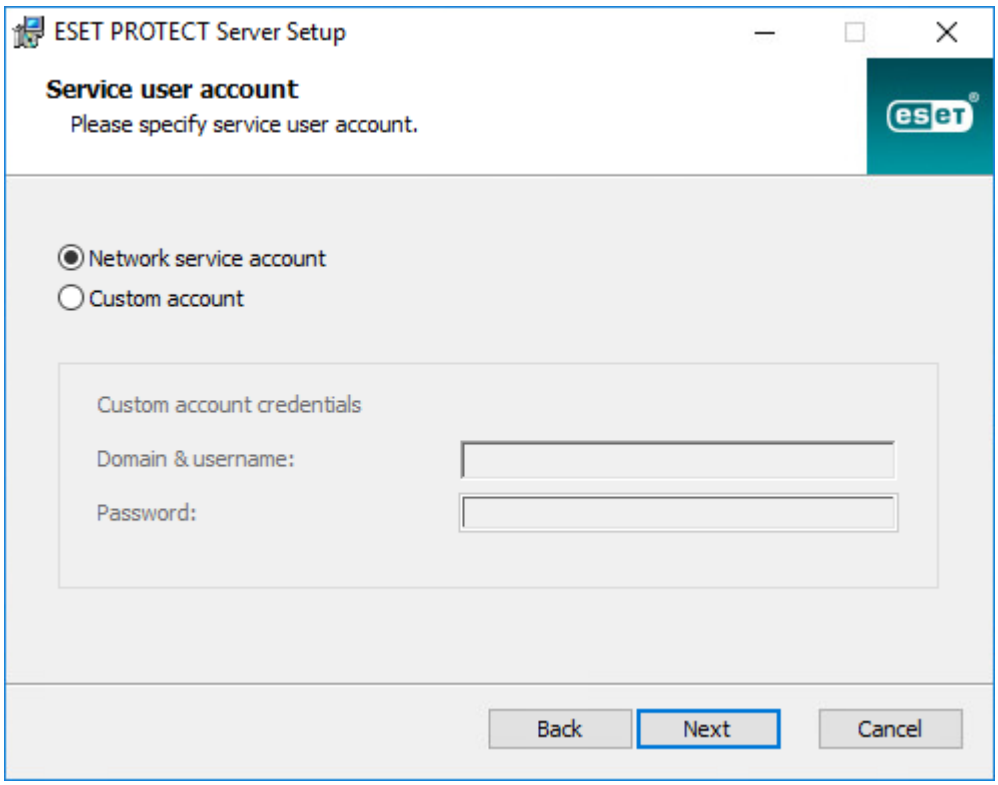
3. **製品改善プログラムに参加する**の横のチェックボックスをオンにして、クラッシュレポートと匿名のテレメトリーデータ(OSのバージョンと種類□ESET製品バージョン、および他の製品固有の情報)をESETに送信します。

4.[**これはクラスターインストールです**]の横のチェックボックスは空欄のままにして、[**次へ**]をクリックします。これはクラスターインストールですか。

フェールオーバークラスタでESET PROTECTサーバーをインストールする場合は、[**これはクラスターインストールです**]の横のチェックボックスをオンにします。**カスタムアプリケーションデータパス**を指定し、クラスターの共有ストレージを参照します。データは、クラスタ内のすべてのノードがアクセスできる1つの場所に格納されている必要があります。

5. [**サービスユーザーアカウント**]を選択します。このアカウントを使用してESET PROTECT Serverサービスを実行します。使用可能なオプションは次のとおりです。

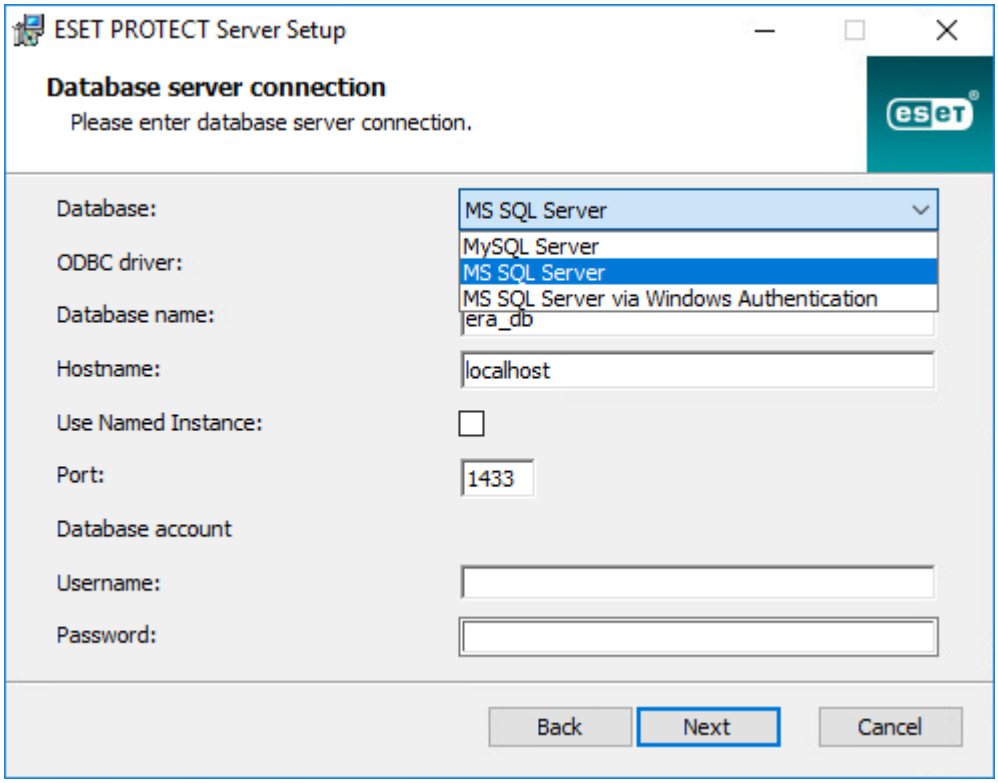
- **ネットワークサービスアカウント** – ドメインを使用しない場合は、このオプションを選択します。
- **カスタムアカウント**: 次のドメインユーザー資格情報を入力します。ドメイン\ユーザー名およびパスワード。



6. データベースに接続します。すべてのデータ(ESET PROTECT Webコンソールのパスワードからクライアントコンピューターのログなど)がここに格納されます。

- **データベース**:Windows認証によるMySQL Server/MS SQL Server/MS SQL Server
- **ODBCドライバ**:MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **データベース名**:定義済みの名前を使用するか、必要に応じて変更することをお勧めします。
- **ホスト名**:ホスト名またはデータベースサーバーのIPアドレス
- **ポート**: データベースとの接続で使用されます。
- データベース管理者アカウントの**ユーザー名/パスワード**
- **名前付きインスタンスを使用する** - Microsoft SQLデータベースを使用している場合は、**名前付きインスタンスを使用する**チェックボックスを選択し、カスタムデータベースインスタンスを使用できます。*HOSTNAME\DB_INSTANCE*の形式で**ホスト名**フィールドで設定できます。(例: *192.168.0.10\ESMC7SQL*)。クラスタデータベースの場合、クラスタ名のみを使用します。このオプションを選択する場合、データベース接続ポートを変更できませんMicrosoftの既定のポートが使

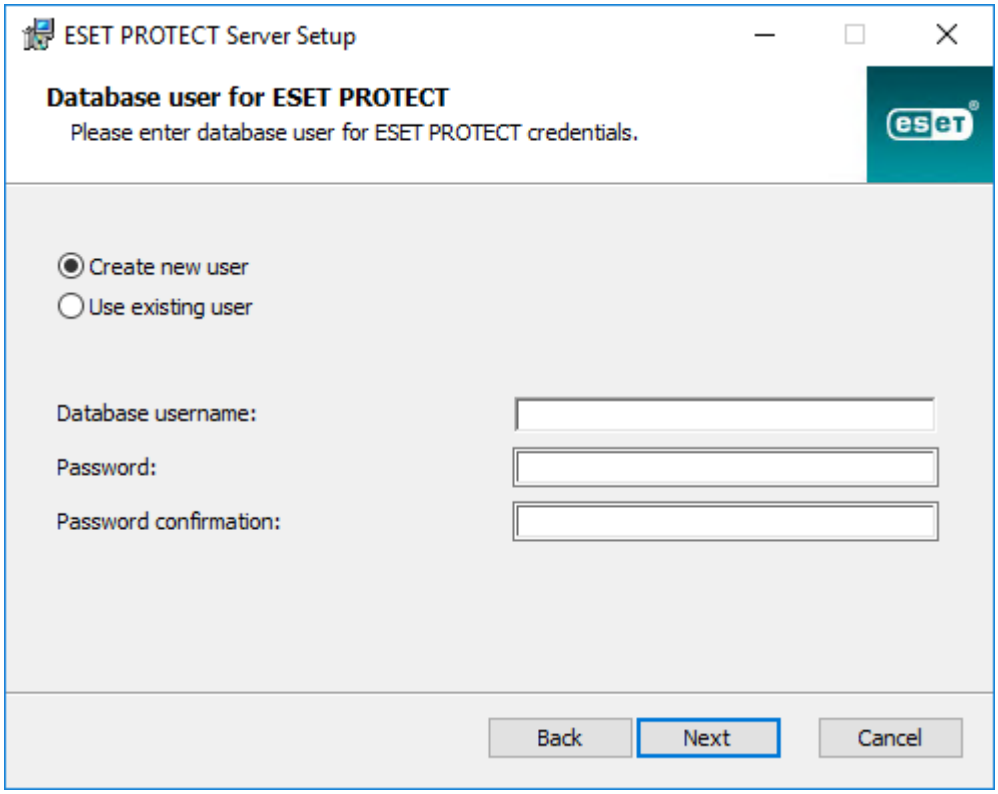
用されます。フェールオーバークラスターにインストールされたMicrosoft SQLデータベースにサーバーを接続するには、**ホスト名**フィールドにESET PROTECTクラスタ名ーを入力します。



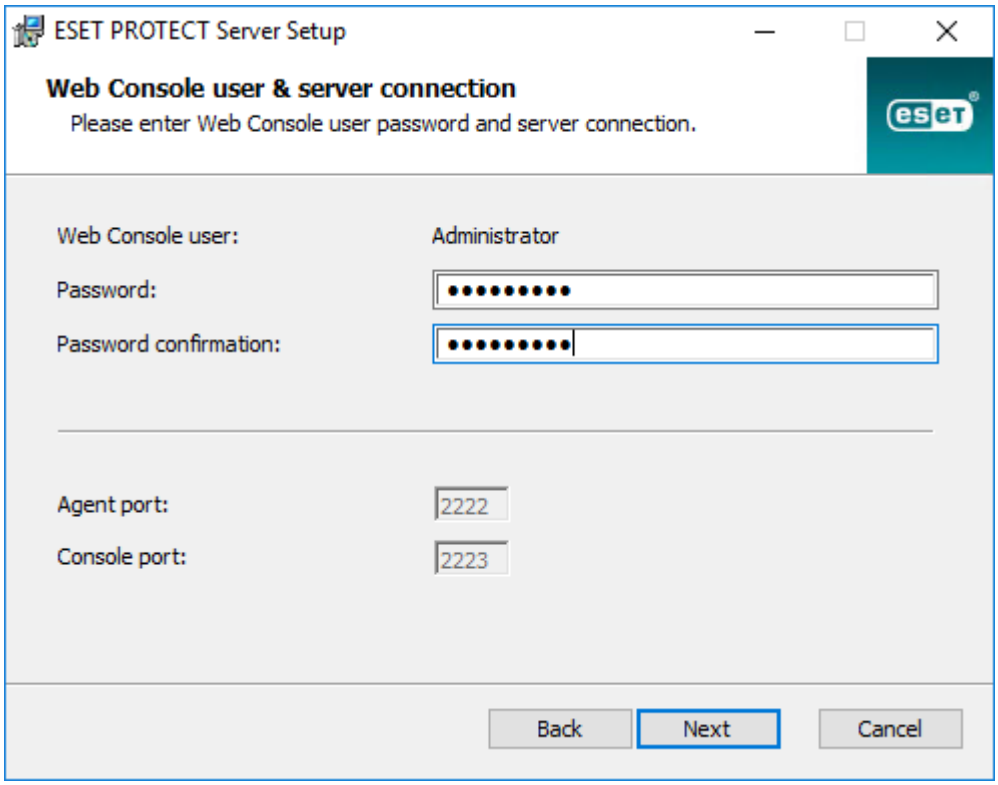
ESET PROTECTサーバーは、大きいデータをBLOBデータベースに格納します。このためESET PROTECT On-Premを適切に実行するために、大きなパケットを受け入れられるようにMySQLを設定する必要があります。

この手順では、データベースへの接続を検証します。接続が正常の場合、次の手順に進みます。

7. データベースへのアクセス権があるESET PROTECT On-Premのユーザーを選択します。既存ユーザーを使用するか、または設定で作成することができます。



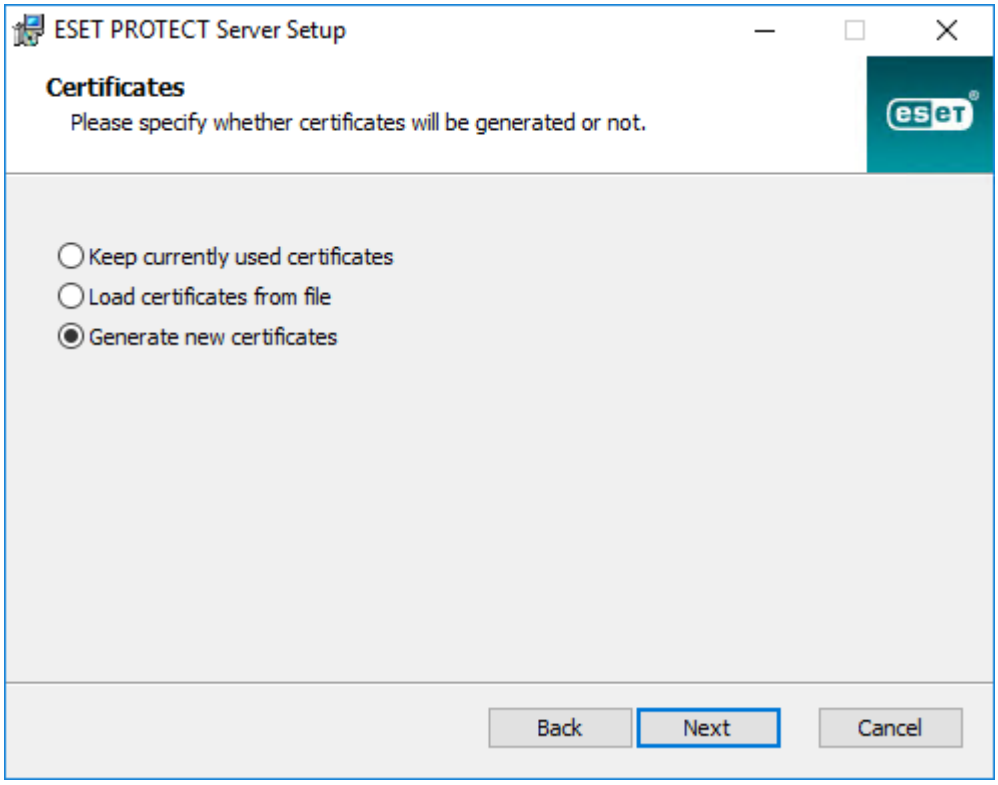
8. **Webコンソール**へアクセスするパスワードを入力します。



9. ESET PROTECT On-Premでは、クライアントサーバー通信の証明書を使用します。次のオプションのいずれかを選択します。

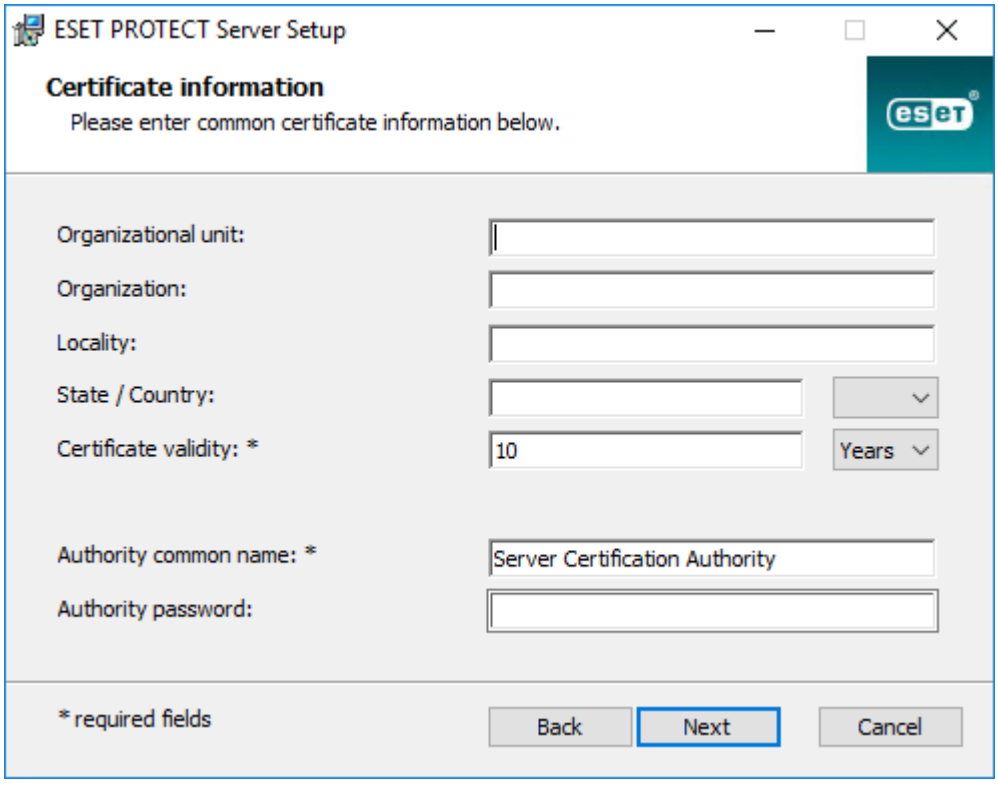
- **現在使用さ れている証明書を保持する** – このオプションは、データベースが既に別のESET PROTECTサーバーで使用されている場合にのみ使用できます。
- **証明書をファイルからロード** – 既存のサーバー証明書と認証局を選択します。

• **新しい証明書を生成** – インストーラーは新しい証明書を生成します。



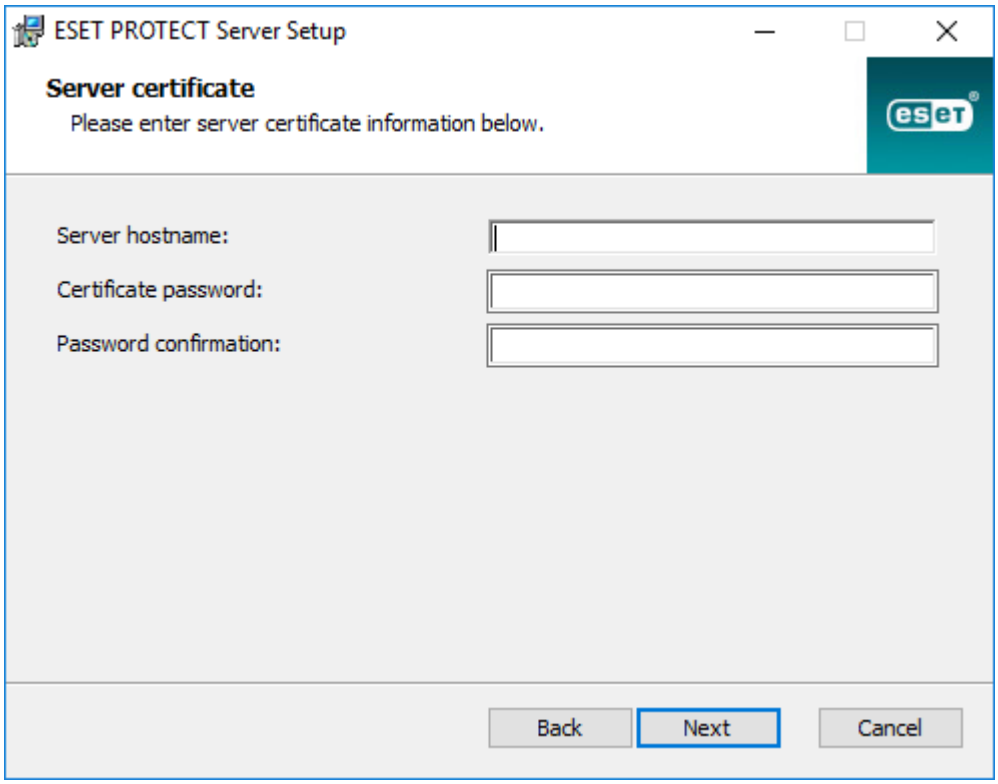
10. 前の手順で**新しい証明書を生成**オプションを選択した場合は、この手順を実行します。

a)証明書に関する追加情報を指定します(任意)。**権限パスワード**を入力する場合は、必ず覚えておいてください。

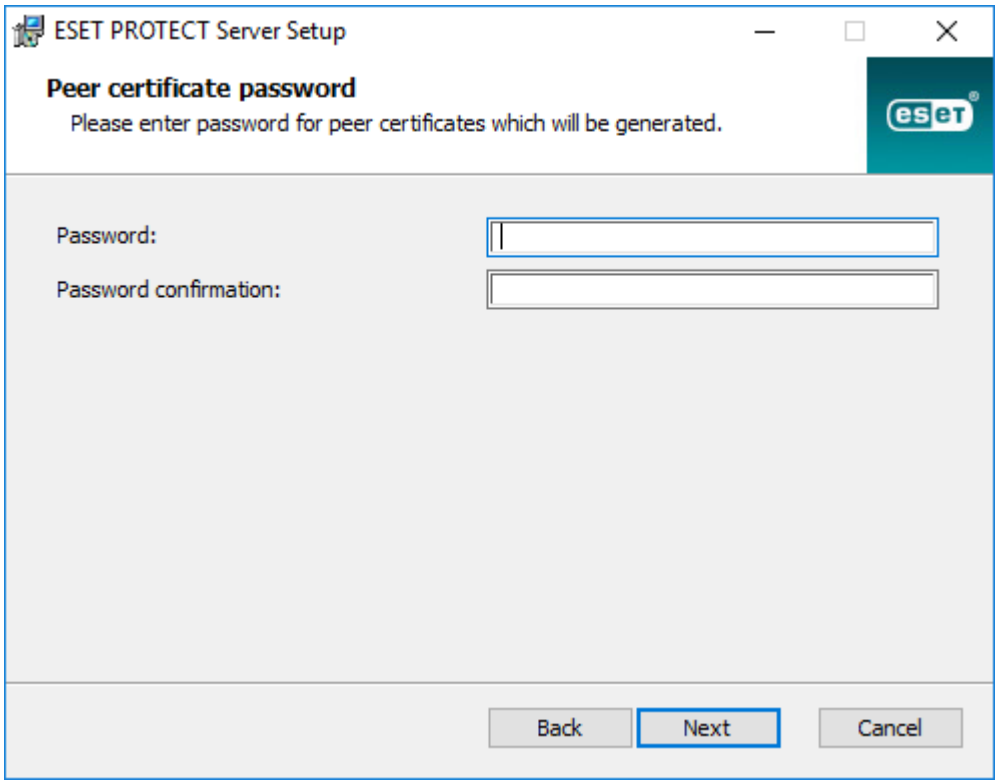


b)**サーバー証明書**フィールドに**サーバーホスト名**と**証明書パスワード**を入力します(任意)。

サーバー証明書の**サーバーホスト名**には次のキーワードを使用できません。server proxy agent

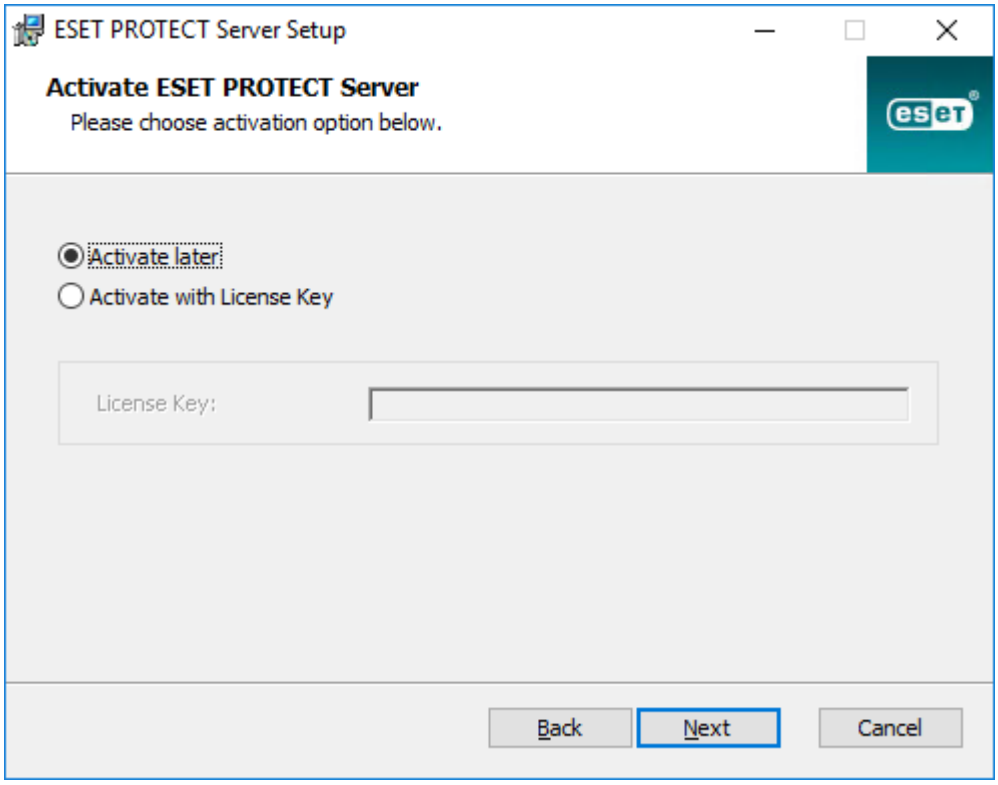


c) **ピア証明書パスワード**フィールドにエージェントおよびプロキシピア証明書のパスワードを入力します。



11. 設定では、はじめに静的グループの同期タスクを実行します。方法(**同期しない Windowsネットワークと同期 Active Directoryと同期**)を選択して、**次へ**をクリックします。

12. 有効な製品認証キーを入力するか、**後でアクティベーション**を選択します。



13. サーバーのインストールフォルダを確認または変更して、**次へ**をクリックします。

14. **インストール**をクリックしてESET PROTECTサーバーをインストールします。

ESET PROTECTサーバーインストールが完了したら、クライアントコンピューターを管理する場合と同じ方法で、同じコンピューターにESETManagementエージェントをインストール(任意)し、サーバーの管理を有効にできます。

Microsoft SQL Serverの要件

Microsoft SQL Serverに関する次の要件を満たす必要があります。

- サポートされているバージョンのMicrosoft SQL Serverをインストールします。インストール中に**混合モード**認証を選択します。
- Microsoft SQL Serverが既にインストールされている場合は、認証を**混合モード(SQL Server認証とWindows認証**に設定します。このためには、このナレッジベース記事の手順に従います。**Windows認証**を使用してMicrosoft SQL Serverにログインする場合は、このナレッジベース記事の手順に従います。
- SQL ServerへのTCP/IP接続を許可します。このためには、このナレッジベース記事の「**II.SQLデータベースへのTCP/IP接続を許可する**」の手順に従います。

- Microsoft SQL Server (データベースおよびユーザー) を設定、管理、監視するには、SQL Server Management Studio (SSMS)をダウンロードします。
- ドメインコントローラーにはSQL Serverをインストールしないでください(たとえばWindows SBS / Essentials)別のサーバーにESET PROTECT On-Premをインストールするか、インストール中にSQL Server Expressコンポーネントを選択しない(この場合、既存のSQL ServerまたはMySQLを使用してESET PROTECTデータベースを実行する必要があります)ことをお勧めします。

MySQL Serverインストールおよび構成

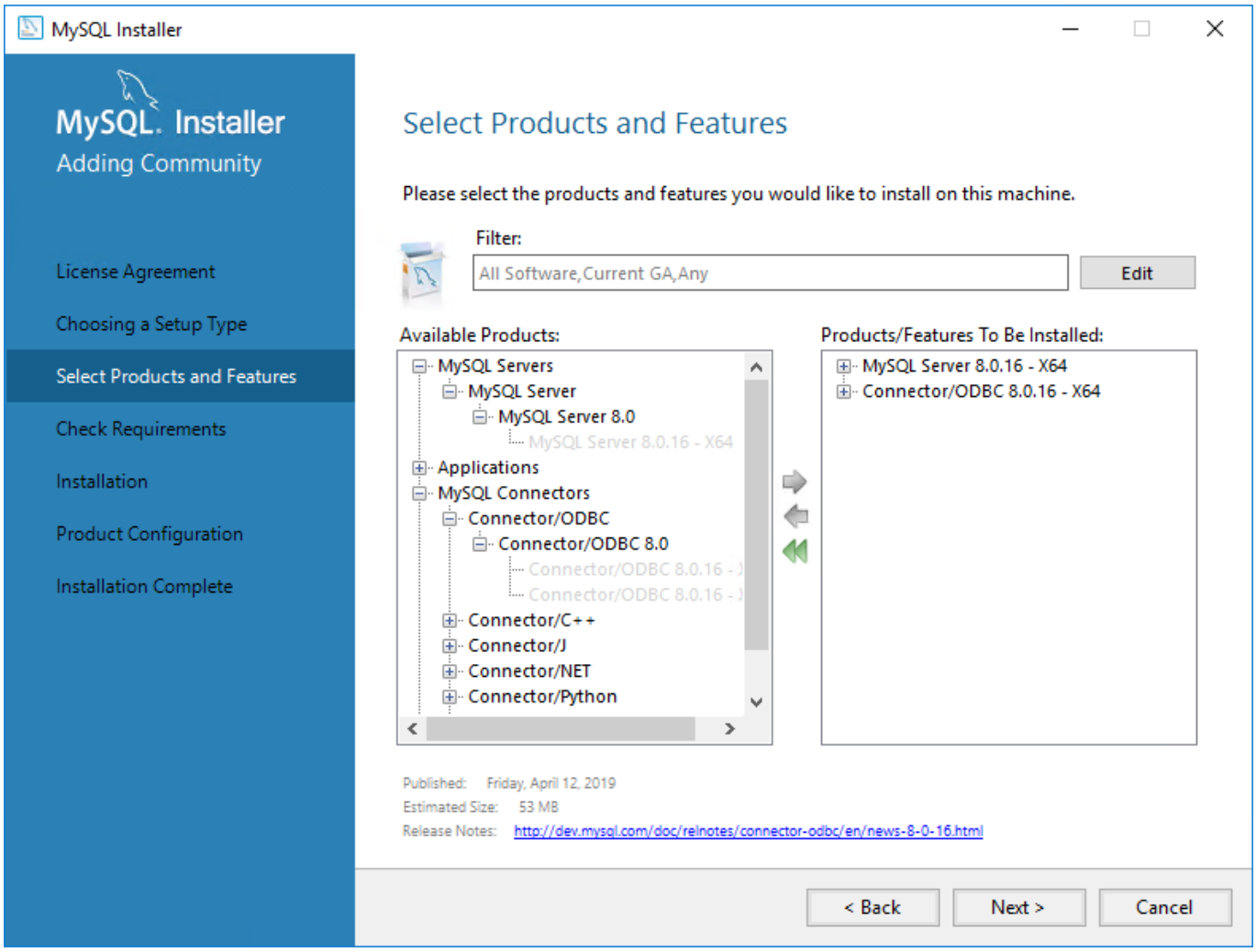
インストール

必ずサポートされているバージョンのMySQL ServerとODBCコネクターをインストールしてください。

1. MySQL 8 Windowsインストーラーをhttps://dev.mysql.com/downloads/installer/からダウンロードし、実行します。

2. **ライセンス条項に同意**チェックボックスを選択し、**次へ**をクリックします。

3. インストールセットアップ中に**カスタム**を選択し、インストールする**MySQL Server**と**ODBCコネクター**を選択しますODBCコネクターがインストールされているMySQL Serverのビット数(x86またはx64)と一致することを確認してください。



4. **次へ**実行をクリックし、MySQL ServerとODBCコネクターをインストールします。

5. **Next**(次へ)をクリックします。**高可用性**で、**スタンドアロンMySQL Server/クラシックMySQLレプリケーション**を選択し、**次へ**をクリックします。

6. **タイプとネットワークで設定**タイプドロップダウンメニューから**サーバーコンピューター**を選択し、**次へ**をクリックします。

7. **認証方法**で、**認証で強力なパスワード暗号化を使用する**推奨オプションを選択し、**次へ**をクリック

します。

8. **アカウントとロール**で、**MySQL Root**パスワードを2回入力します。専用データベースユーザーアカウントを作成することもお勧めします。

9. **Windowsサービスで**、あらかじめ選択された値を保持し、**次へ**をクリックします。

10. **実行**をクリックし、MySQLサーバーのインストールが完了するまで待機します。**完了**をクリックし、**次へ**>**完了**をクリックしてインストールウィンドウを閉じます。

設定

1. テキストエディターで次のファイルを開きます。

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. *[mysqld]*ファイルの`my.ini`セクションで次の構成を見つけて編集するか、追加します。

- ファイルに存在しない場合は、`[mysqld]`セクションを作成します。
- パラメーターがファイルにない場合は、`[mysqld]` セクションに追加します。
- MySQLバージョンを決定するには、次のコマンドを実行します。`mysql --version`

パラメータ	コメントと推奨値	MySQLバージョン
`max_allowed_packet=33M`		すべてのサポートされているバージョン
`log_bin_trust_function_creators=1`	あるいは、バイナリロギングを無効にすることができます。`log_bin=0`	8.x
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	これらの2つのパラメーターの値の乗数は、**200**以上でなければなりません。`innodb_log_files_in_group`の最小値は**2**で、最大値は**100**です。値は整数である必要があります)。	8.x 5.7 5.6.22(以降5.6.x)
`innodb_log_file_size=200M`	**200M**以上、**3000M**以下に値を設定します。	5.6.20と5.6.21

3. *my.ini*ファイルを保存して閉じます。

4. コマンドプロンプトを開き、次のコマンドを入力してMySQLサーバーを再起動し、設定を適用します(プロセス名はMySQLのバージョンによって異なります。例: バージョン8.0 = mysql80)

```
net stop mysql80
net start mysql80
```

5. コマンドプロンプトで次のコマンドを入力し、MySQLサーバーが実行中かどうかを確認します。

```
sc query mysql80
```

専用データベースユーザーアカウント

SAアカウント(Microsoft SQL)または**ルートアカウント**(MySQL)を使用しない場合は、**専用データベースユーザーアカウント**を作成できます。この専用ユーザーアカウントは、ESET PROTECTデータベースにアクセスするためにのみ使用されますESET PROTECT On-Premインストールを開始する前に、データベースサー

バー内で専用データベースユーザーアカウントを作成することをお勧めします。また、この専用ユーザーアカウントを使用して□ESET PROTECT On-Premがアクセスする空のデータベースを作成する必要があります。

最低セットの権限を専用データベースユーザーアカウントに割り当てる必要があります。

- MySQLユーザー権限: ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER.- MySQL権限の詳細については、http://dev.mysql.com/doc/refman/8.0/en/grant.htmlを参照してください。

- Microsoft SQL Serverデータベースロール:ESET PROTECTデータベースユーザーはdb_ownerデータベースロールのメンバーでなければなりません□Microsoft SQL Serverデータベースレベルのロールの詳細については、https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspxを参照してください。

Microsoft SQLとMySQLのデータベースとユーザーアカウントを設定する方法の詳細ガイドについては、ナレッジベース記事を参照してください。

エージェントインストール - Windows

使用可能な方法

WindowsワークステーションでのESET Managementエージェントのインストールでは、さまざまなインストールおよび展開方法があります。

方法	ドキュメント	説明
*.msi*インストーラーからGUIベースのインストール	• この章 • KB	• **標準**インストール方法。 • この方法は、サーバー支援またはオフラインインストールとして実行できます。 • ESET PROTECTサーバーコンピューターにエージェントをインストールするときには、この方法を使用します。
ESET Remote Deployment Tool	• オンラインヘルプ	• ローカルネットワークでの一括展開で推奨されます。 • オールインワンインストーラー(エージェントとESETセキュリティ製品)を展開するために使用できます
オールインワンエージェントインストーラー	• オールインワンエージェントインストーラーの作成 • KB	• インストーラーには、セキュリティ製品と埋め込まれたポリシーを含めることもできます。 • インストーラーのサイズは、数百MBになります。
エージェントスクリプトインストーラー	• エージェントスクリプトインストーラーの作成 • KB	• インストーラーは実行可能なスクリプトです。サイズは小さいですが、*.msi*インストーラーの場所にアクセスできる必要があります。 • スクリプトは、ローカルインストーラーとHTTPプロキシを使用するように編集できます。
SCCMおよびGPO展開	• SCCM • GPO • KB	• リモート一括展開の高度な方法。 • 小さい*.ini*ファイルを使用します。
サーバータスク – エージェント展開	• オンラインヘルプ • KB	• SCCMおよびGPOの代替策。 • HTTPプロキシ経由では実行できません。 • ESET PROTECTサーバーによって□ESET PROTECT Webコンソールから実行されます。 • この方法を使用して、Active Directory から同期されたコンピューターにESET Managementエージェントを展開します。

エージェントとESET PROTECTサーバー間の通信プロトコルは、認証をサポートしません□ESET PROTECTサーバーへのエージェント通信の転送で使用されるプロキシソリューションと必要な認証は動作しません。
Webコンソールまたはエージェントで既定以外のポートを使用する場合は、ファイアウォールの調整が必要になることがあります。そうでない場合、インストールが失敗する可能性があります。

GUIベースのインストール

次の手順に従い、WindowsでESET Managementエージェントコンポーネントをローカルでインストールします。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。(*agent_x86.msi*□*agent_x64.msi*、また

は *agent_arm64.msi*)。

2. ESET Managementエージェントインストーラを実行し、同意する場合はEULAに同意します。

3. **製品改善プログラムに参加する**の横のチェックボックスをオンにして、クラッシュレポートと匿名のテレメトリーデータ(OSのバージョンと種類、ESET製品バージョン、および他の製品固有の情報)をESETに送信します。

4. **サーバーホスト**(ESET PROTECTサーバーのホスト名またはIPアドレス)と**サーバーポート**(既定のポートは2222です。別のポートを使用する場合は、既定のポートをカスタムポート番号で置き換えます)。

サーバーホストが[**サーバー証明書**]の[**ホスト**]で定義された1つ以上の値(FQDNを推奨)と一致していることを確認します。そうでない場合、「受信したサーバー証明書が無効です」というエラーが表示されます。[サーバー証明書ホスト]フィールドでワイルドカード(*)を使用すると、証明書はすべての[**サーバーホスト**]で動作します。

5. エージェントとサーバーの接続でプロキシを使用する場合は、**プロキシを使用する**チェックボックスをクリックします。選択すると、インストーラーはオフラインインストールを続行します。

このプロキシ設定は、ESET Managementエージェントと ESET PROTECTサーバーの間のレプリケーションでのみ使用され、アップデートのキャッシュには使用されません。
- **プロキシホスト名**: HTTPプロキシコンピュータのホスト名またはIPアドレス。
- **プロキシポート**: 既定値は3128です。
- **ユーザー名**、**パスワード**: 認証を使用する場合は、プロキシによって使用される認証資格情報を入力します。

ポリシーで後からプロキシ設定を変更できます。プロキシ経由のエージェントとサーバー間の接続を設定する前に、プロキシをインストールする必要があります。

6. 次のインストールオプションのいずれかを選択し、該当する次のセクションの手順に従います。

- サーバー支援インストール - ESET PROTECT Webコンソール管理者の認証情報を指定する必要があります。インストーラは必要な証明書を自動的にダウンロードします。

サーバー支援インストールでは、二要素認証のユーザーを使用できません。

- オフラインインストール – エージェント証明書および認証局を指定する必要があります。いずれもESET PROTECT On-Premからエクスポートできます。あるいは、カスタム証明書を使用できます。

コマンドラインインストール

*MSI*インストーラーはローカルまたはリモートで実行できます。ESETのWebサイトからESET Managementエージェントをダウンロードします。

パラメータ	説明と許可された値
P_HOSTNAME=	ESET PROTECTサーバーのホスト名またはIPアドレス。
P_PORT=	エージェント接続のサーバーポート(任意: 指定されていない場合は、既定のポート2222が使用されます)。
P_CERT_PATH=	*.txt*ファイルのBase64形式のエージェント証明書へのパス(ESET PROTECT Webコンソールからエクスポート)。
P_CERT_AUTH_PATH=	*.txt*ファイル(ESET PROTECT Webコンソールからエクスポート)のBase64形式による認証局へのパス。
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**。*.txt*ファイルに保存されているエージェント証明書および認証局を参照するときに、このパラメーターを使用します。
P_CERT_PASSWORD=	このパラメーターを使用して、エージェント証明書のパスワードを指定します。
P_CERT_CONTENT=	Base64形式のエージェント証明書文字列(ESET PROTECT Webコンソールからエクスポート)。
P_CERT_AUTH_CONTENT=	Base64形式の認証局文字列(ESET PROTECT Webコンソールからエクスポート)。
PASSWORD=	パスワードで保護されたエージェントをアンインストールするためのパスワード。
P_ENABLE_TELEMETRY=	**0** – 無効(既定のオプション)。**1** – 有効。クラッシュレポートとテレメトリーデータをESETに送信する(任意のパラメーター)。
P_INSTALL_MODE_EULA_ONLY=	**1**。セミサイレントESET Managementエージェントインストールではこのパラメーターを使用します。エージェントインストールウィンドウが表示され、エンドユーザーライセンス契約に同意して、テレメトリを有効/無効にするように指示されます(P_ENABLE_TELEMETRYが指定されると無視されます)。他のエージェントインストール設定はコマンドラインパラメーターから取得されます。エージェントインストール処理の完了が表示されます。
P_USE_PROXY=	**1**。このパラメーターを使用して、ESET Managementエージェントと ESET PROTECTサーバー(アップデートのキャッシュ用ではない)の間のレプリケーションのために、既にネットワークにインストールされているHTTPプロキシの使用を有効にします。
P_PROXY_HTTP_HOSTNAME=	HTTPプロキシのホスト名またはIPアドレス。

パラメータ	説明と許可された値
P_PROXY_HTTP_PORT=	エージェント接続のHTTPプロキシポート。

コマンドラインインストールの例

必要に応じて、次のオレンジのコードを置換します。

- 既定のポート接続を使用したサイレントインストール(/qパラメーター)、ファイルに保存されたテレメトリ、エージェント証明書、認証局が有効です。

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- エージェント証明書、認証局、エージェント証明書のパスワード、およびHTTPプロキシパラメータ用に提供された文字列を使用したサイレントインストール。

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvkpqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- セミサイレントインストール:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

サーバー支援エージェントインストール

サーバー支援エージェントインストールを続行するには、以下の手順に従います。

1. **[サーバーホスト]**フィールドにESET PROTECT Webコンソール(ESET PROTECTサーバーと同じ)のホスト名またはIPアドレスを入力します。カスタムポートを使用しない場合は、**[Webコンソールポート]**を既定の2223のままにします。また、**[ユーザー名]**と**[パスワード]フィールド**にWebコンソールアカウントの資格情報を入力します。ドメインユーザーとしてログインするには、**ドメインにログイン**の横のチェックボックスをオンにします。

> - **サーバーホスト**が**[サーバー証明書]**の**[ホスト]**で定義された1つ以上の値(FQDNを推奨)と一致していることを確認します。そうでない場合、「受信したサーバー証明書が無効です」というエラーが表示されます。ただし、[サーバー証明書ホスト]フィールドにワイルドカード(*)がある場合を除きます。この場合、すべての**[サーバーホスト]**で動作します。
> - サーバー支援インストールでは、二要素認証のユーザーを使用できません。

2. 証明書を許可するかどうかを確認するメッセージが表示されたら、**[はい]**をクリックします。

3. **コンピューターを作成しない(コンピューターは初回接続中に自動的に作成されます)**または**カスタム静的グループを選択**を選択します。**[カスタム静的グループを選択]**をクリックするとESET PROTECTOn-Premの既存の静的グループのリストから選択できます。コンピューターは選択したグルー

プに追加されます。

4. ESET Managementエージェントのインストール先フォルダ(既定の場所を推奨)を指定し、**[次へ]**をクリックしてから、**[インストール]**をクリックします。

オフラインエージェントインストール

オフラインエージェントインストールを続行するには、以下の手順に従います。

1. 前のステップで**プロキシを使用**を選択した場合は、**プロキシホスト名**⍰**プロキシポート**(既定のポートは3128)、**ユーザー名**、および**パスワード**を入力し、**次へ**をクリックします。

2. **[参照]**をクリックし、ピア証明書の場所に移動します(これはESET PROTECT On-Premからエクスポートしたエージェント証明書です)。**[証明書パスワード]**テキストフィールドは空欄にします。この証明書にはパスワードが必要ないためです。**認証局**を参照する必要はありません。このフィールドは空欄にします。

ESET PROTECT On-Premでカスタム証明書を使用する場合(ESET PROTECT On-Premインストール中に自動生成された既定の証明書を使用しない場合)は、適宜カスタム証明書を使用してください。

証明書パスフレーズには、次の文字を含めることはできません:" \ これらの文字は、エージェントの初期化中に重大なエラーが発生する原因となります。

3. **[次へ]**をクリックして、既定のフォルダにインストールするか、**[変更]**をクリックして別のフォルダを選択します(既定の場所を推奨)。

ESET Remote Deployment Tool

ESET Remote Deployment Toolは、ESET PROTECT On-Premによって作成されたインストーラーパッケージを配布して⍰ESET Managementエージェントと ESETセキュリティ製品をネットワーク経由でコンピューターにリモート展開するための便利な方法です。

ESET Remote Deployment Toolは、スタンドアロンESET PROTECT On-Premコンポーネントとして ESETのWebサイトから無償で提供されています。展開ツールは小規模から中規模のネットワークで主に配布するためのもので、管理者権限で実行されます。

ESET Remote Deployment Toolは、サポートされているMicrosoft Windowsオペレーティングシステムのクライアントコンピューターに ESETManagementエージェントを展開するための専用ツールです。

ツールの前提条件と使用方法の詳細については、「ESET Remote Deployment Tool」の章を参照してください。

Webコンソールインストール - Windows

WindowsでESET PROTECT Web コンソールをインストールするには、次の2つの方法があります。

- オールインワンインストーラーを使用する ことをお勧めします。
- 上級ユーザーは手動インストールを実行できます。

ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。

オールインワンインストーラーを使用したWebコンソールのインストール

前提条件

- ESET PROTECTサーバーがインストールされている。

ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。 この手順には、追加のステップが必要です。

- Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。
- Apache Tomcatには64ビット版のJava/OpenJDKが必要です。 システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

インストール

オールインワンインストーラーを使用して、WindowsでESET PROTECT Webコンソールコンポーネントをインストールするには、次の手順に従います。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESET Webサイトから ESET PROTECTオールインワンインストーラーをダウンロードして、ダウンロードしたファイルを解凍します。

2. 最新バージョンのApache Tomcatをインストールする予定で、オールインワンインストーラーに古いバージョンのApache Tomcatが含まれている場合(この手順は任意です。最新バージョンのApache Tomcatが必要でない場合は手順4に進んでください):

   a. *x64*フォルダーを開き、*installers*フォルダーに移動します。

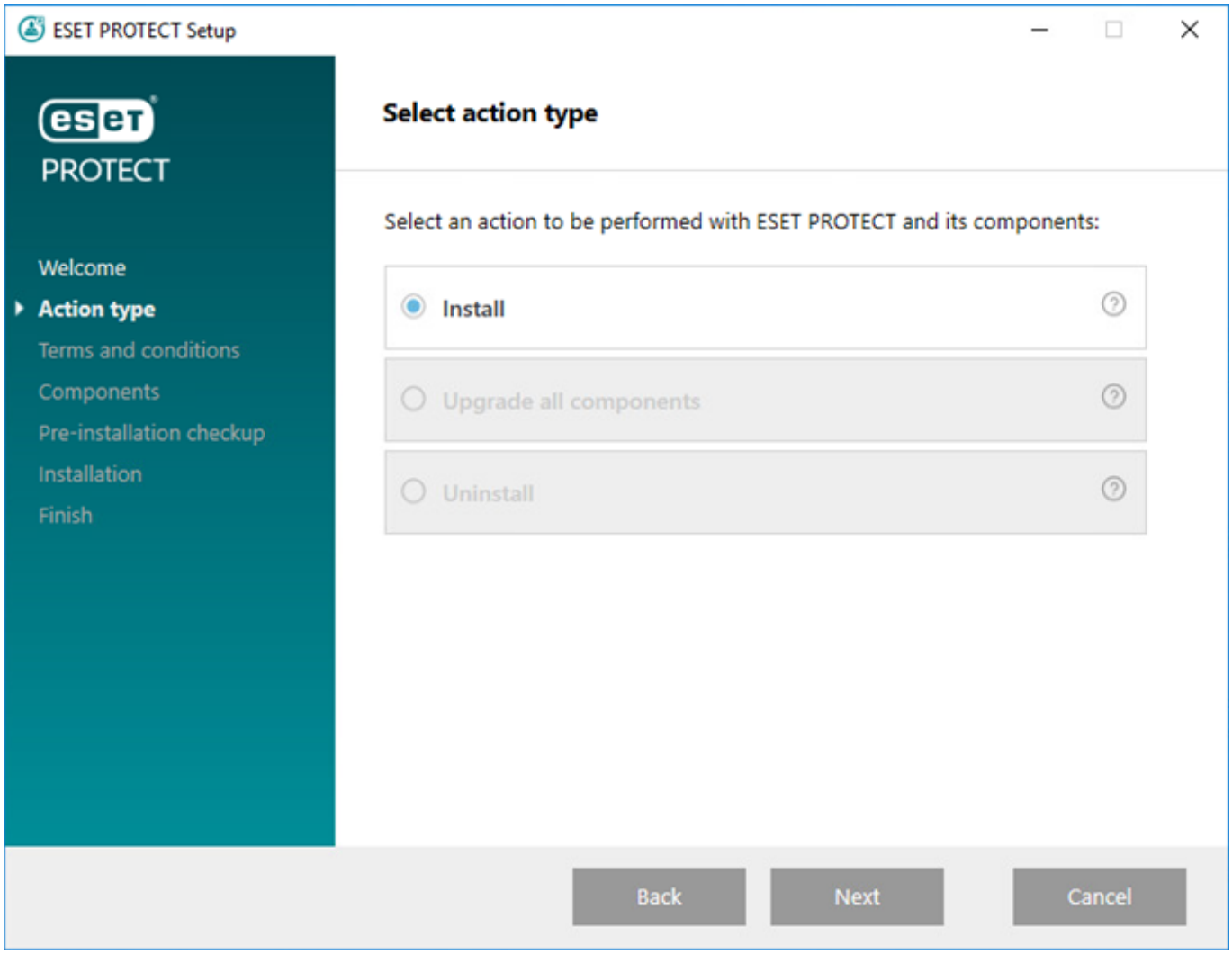
b.*installers*フォルダーにある*apache-tomcat-9.0.x-windows-x64.zip*ファイルを削除します。

c.Apache Tomcat 9 64ビットWindows zipパッケージをダウンロードします。

d.ダウンロードしたzipパッケージを*installers*フォルダーに移動します。

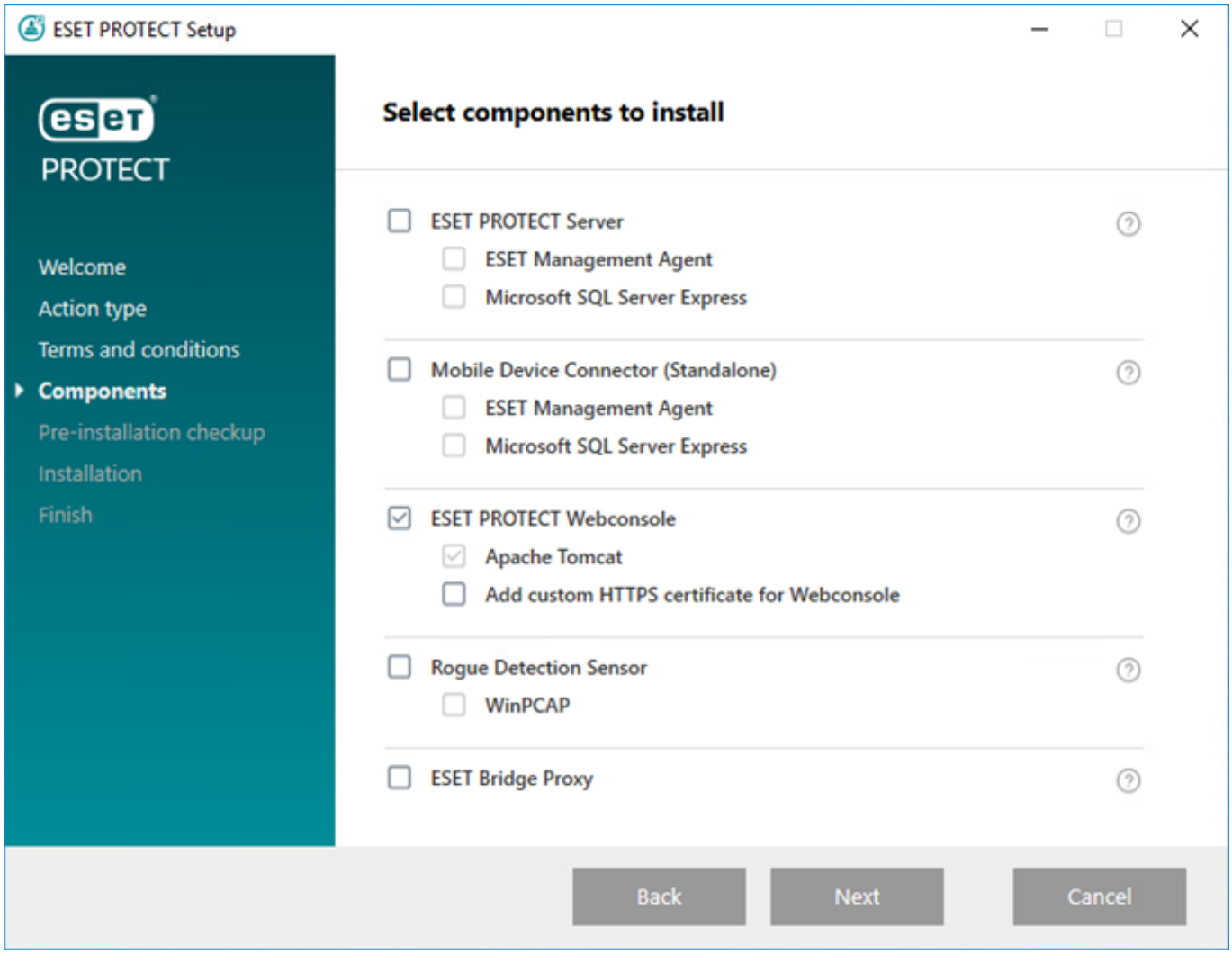
3. オールインワンインストーラーを起動するには、*Setup.exe*ファイルをダブルクリックし、**ようこそ**画面で**次へ**をクリックします。

4. **インストール**を選択して、**次へ**をクリックします。



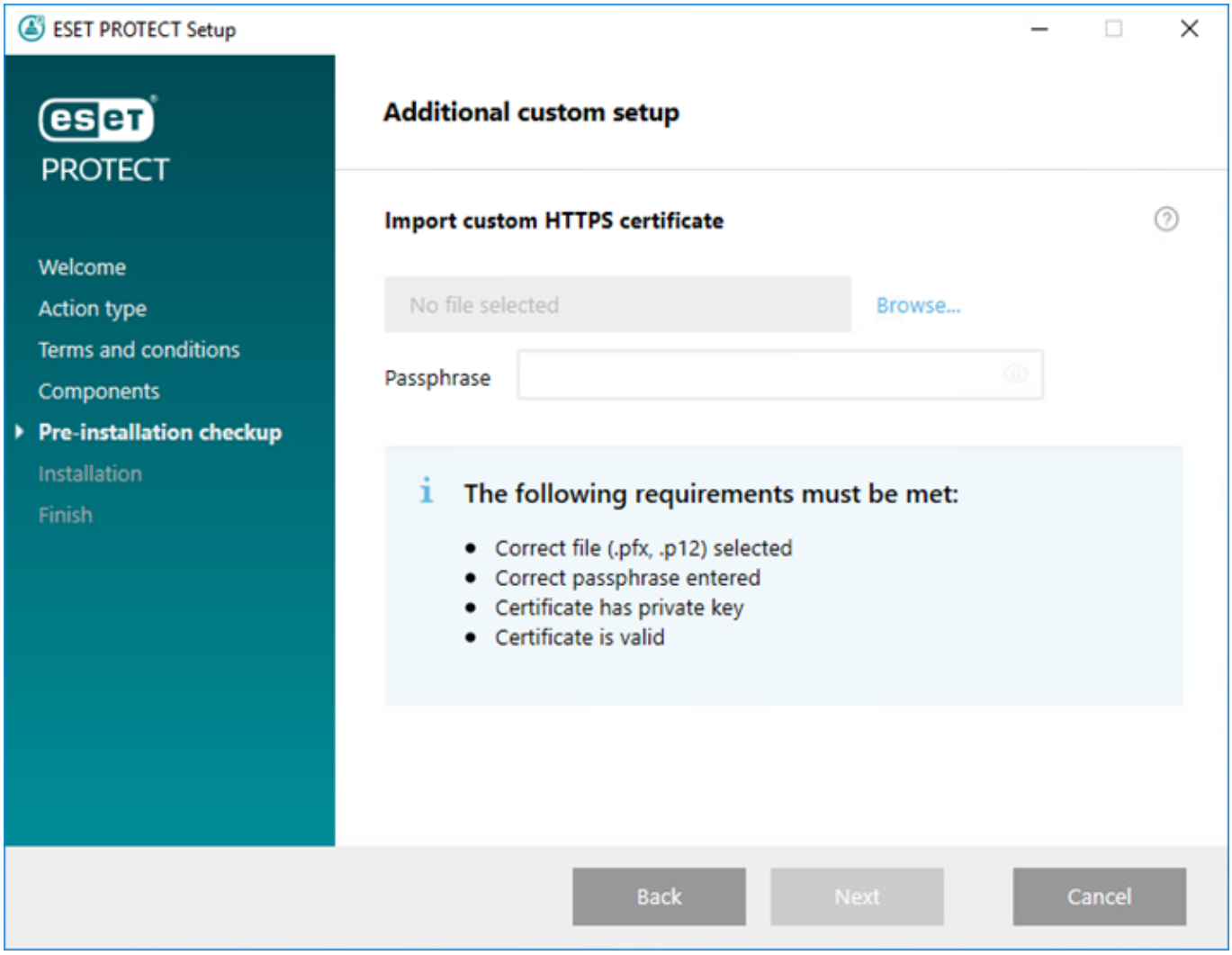
5. EULAに同意した後、[**次へ**]をクリックします。

6. **インストールするコンポーネントを選択**で、 **ESET PROTECT Webコンソール**チェックボックスのみをオンにして、**次へ**をクリックします。



必要に応じて、**Webコンソールのカスタム HTTPS証明書を追加**チェックボックスをオンにします。

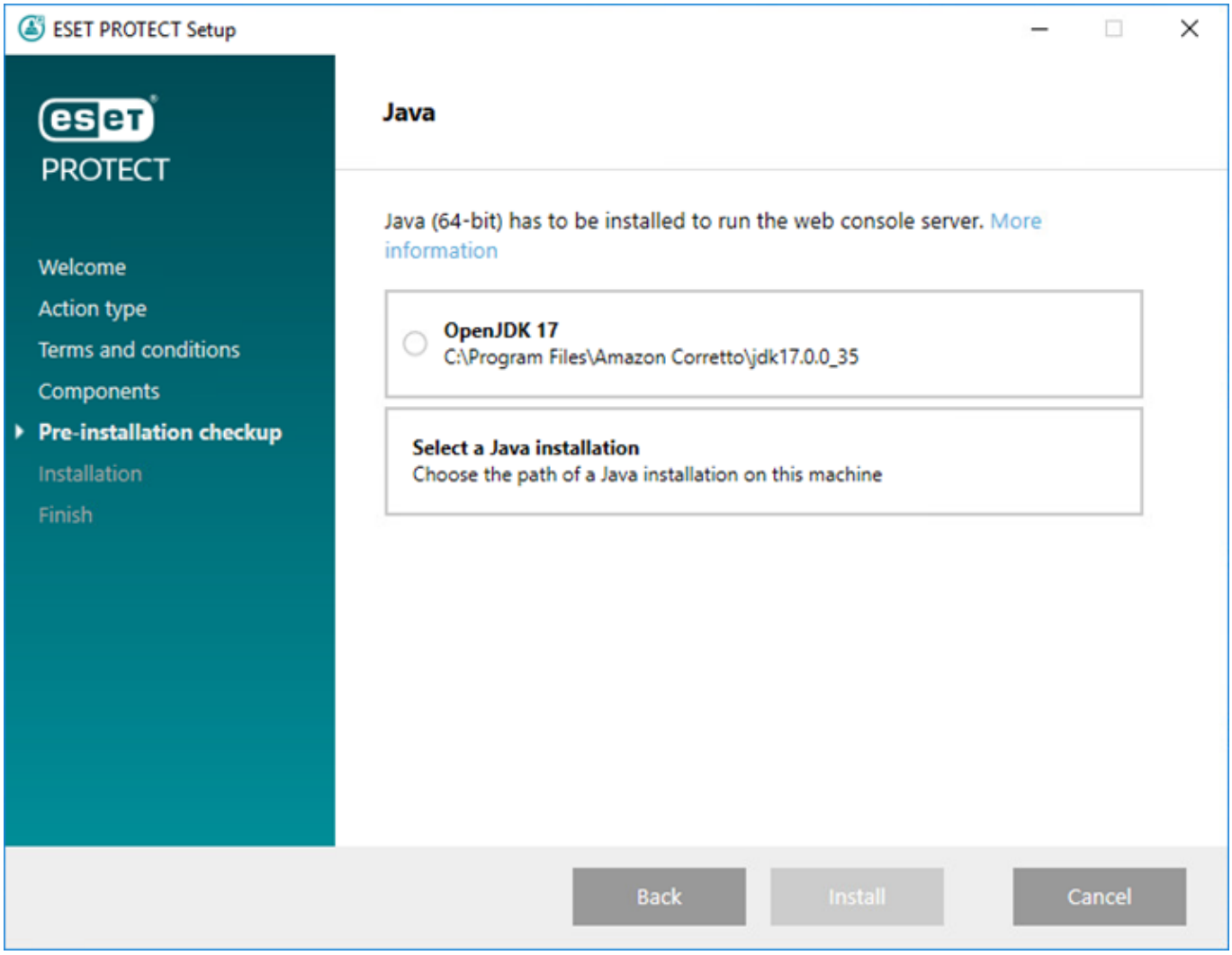
- ESET PROTECT Webコンソールでカスタム HTTPS証明書を使用する場合は、このオプションを選択します。
- このオプションを選択しない場合は、インストーラーによってTomcatの新しい鍵ストア(自己署名HTTPS証明書)が自動的に生成されます。
- **Webコンソールのカスタム HTTPS証明書を追加**を選択した場合は、**参照**をクリックして、有効な証明書(*.pfx*またはp12ファイル)を選択し、**パスフレーズ**を入力(またはパスフレーズがない場合は空欄)します。インストーラーは、TomcatサーバーにWebコンソールアクセスの証明書をインストールします。**次へ**をクリックして続行します。



7. コンピューターでJavaインストールを選択します。最新バージョンのJava/OpenJDKを使用していることを確認します。

a)既にインストールされているJavaを選択するには、**Javaインストールを選択**をクリックして、Javaがインストールされているフォルダー(および*C:\Program Files\Amazon Corretto\jdk1.8.0_212*などのサブフォルダー*bin*)を選択し、**OK**をクリックします。無効なパスを選択した場合は、インストーラーでメッセージが表示されます。

b)**インストール**をクリックして続行するか、**変更**をクリックしてJavaインストールパスを変更します。



8. インストールが完了したら、**完了**をクリックします。

ESET PROTECTサーバー以外のコンピューターでESET PROTECT Webコンソールをインストールした場合、これらの追加手順を実行し、ESET PROTECT Webコンソールと ESET PROTECTサーバー間の通信を有効にします。
a)Apache Tomcat サービスを停止します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**停止**を選択します。
b)管理者としてメモ帳を実行し、を編集します *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)`server_address=localhost`を見つけます。
d)`localhost`をESET PROTECTサーバーのIPアドレスにし、ファイルを保存します。
e) Apache Tomcatサービスを起動します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**開始**を選択します。

9. サポートされているWebブラウザーでESET PROTECT Webコンソールを開きます。ログイン画面が表示されます。

- ESET PROTECT Webコンソールをホストするコンピューターから次のコマンドを実行します。*https://localhost/era*

- ESET PROTECT Webコンソールにインターネットに接続している任意のコンピューターから次のコマンドを実行します(*IP_ADDRESS_OR_HOSTNAME*をESET PROTECT WebコンソールのIPアドレスまたはホスト名に置き換える)。*https://IP_ADDRESS_OR_HOSTNAME/era*

エンタープライズソリューションまたは低パフォーマンス ステムの追加のWebコンソール設定も参照してください。

Webコンソールを手動でインストールする

ESET PROTECT Webコンソールの手動インストールは高度な手順です。オールインワンインストーラーを使用してESET PROTECT Web コンソールをインストールすることをお勧めします。

前提条件

- ESET PROTECTサーバーがインストールされている。

ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。 この手順には、追加のステップが必要です。

- Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。Apache Tomcatのインストール:

  a)最新のサポートされているバージョンのApache Tomcatインストーラーファイル(32-bit/64-bit Windows Service Installer) *apache-tomcat-[バージョン].exe*をhttp://tomcat.apache.orgからダウンロードします。

  b)インストーラーを実行します。

  c)インストール中に、Javaへのパス(Java *bin*および*lib*フォルダーの親フォルダー)を選択し、**Run Apache Tomcat**チェックボックスをオンにします。

  d)インストール後、Apache Tomcatサービスが実行中であり、スタートアップの種類が**自動**に設定されていることを確認します(**services.msc**)。

- Apache Tomcatには64ビット版のJava/OpenJDKが必要です。 システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

インストール

Windows上にESET PROTECT Webコンソールコンポーネントをインストールするには、次の手順になります。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。(Webコンソールへの接続*era.war*)。

2. *era.war*をApache Tomcat Webアプリケーションフォルダーにコピーします。

C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps

3. Apache Tomcatは自動的に*era.war*ファイルを*era*フォルダーに展開し、ESET PROTECT Webコンソール

をインストールします。展開が完了するまで数分待機します。展開が実行されない場合は、トラブルシューティングの手順に従います。

4. ESET PROTECT WebコンソールをESET PROTECTサーバーと同じコンピューターにインストールする場合、Apache Tomcatサービスを再起動します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**停止**を選択します。30秒待機し、**開始**をクリックします。

ESET PROTECTサーバー以外のコンピューターでESET PROTECT Webコンソールをインストールした場合、これらの追加手順を実行し、ESET PROTECT WebコンソールとESET PROTECTサーバー間の通信を有効にします。
a)Apache Tomcatサービスを停止します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**停止**を選択します。
b)管理者としてメモ帳を実行し、を編集します *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)`server_address=localhost`を見つけます。
d)`localhost`をESET PROTECTサーバーのIPアドレスにし、ファイルを保存します。
e) Apache Tomcatサービスを起動します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**開始**を選択します。

5. サポートされているWebブラウザーでESET PROTECT Webコンソールを開きます。ログイン画面が表示されます。

- ESET PROTECT Webコンソールをホストするコンピューターから次のコマンドを実行します。*http://localhost:8080/era*

- ESET PROTECT Webコンソールにインターネットに接続している任意のコンピューターから次のコマンドを実行します(*IP_ADDRESS_OR_HOSTNAME*をESET PROTECT WebコンソールのIPアドレスまたはホスト名に置き換える)。*http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. インストール後にWebコンソールを設定します。

- Apache Tomcatの手動インストール中に、既定のHTTPポートは8080に設定されます。 Apache TomcatのHTTPS接続を設定することをお勧めします。

- エンタープライズソリューションまたは低パフォーマンス システムの追加のWebコンソール設定も参照してください。

RD Sensorインストール - Windows

前提条件

- WinPcap – 最新のWinPcapバージョン(4.1.0以降)を使用します

- ネットワークを正しく設定されている(適切なポートが開き、受信通信がファイアウォールでブロックされていないなど)

- ESET PROTECTサーバーと通信可能である

- すべてのプログラム機能を完全にサポートするにはESET Managementエージェントをローカルコンピュータにインストールする必要があります

複数のネットワークセグメントがある場合、Rogue Detection Sensorを各ネットワークセグメントに個別にインストールし、ネットワーク全体のすべてのデバイスの包括的なリストを生成する必要があります。

インストール

次の手順に従ってWindowsでRD Sensorをインストールします。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。（*rdsensor_x86.msi*または*rdsensor_x64.msi*）

2. RD Sensorインストーラファイルをダブルクリックしてインストールを開始します。

3. EULAに同意し、[**次へ**]をクリックします。

4. **製品改善プログラムに参加する**の横のチェックボックスをオンにして、クラッシュレポートと匿名のテレメトリーデータ(OSのバージョンと種類、ESET製品バージョン、および他の製品固有の情報)をESETに送信します。

5. RD Sensorのインストール場所を選択し、**次へ > インストール**をクリックします。

6. ESET Rogue Detection Sensorは、インストールが完了した後に起動します。

ログファイルにはRogue Detection Sensorログファイルがあります：*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

ミラーツール - Windows

Linuxユーザーの場合

ミラーツールは、オフライン検出エンジンアップデートで必要です。クライアントコンピューターがインターネットに接続せず、検出エンジンアップデートが必要な場合、ミラーツールを使用してESETアップデートサーバーからアップデートファイルをダウンロードし、ローカルに保存できます。

ミラーツールには次の機能があります。
- モジュールアップデート— 検出エンジンアップデートおよび他のプログラムモジュールをダウンロードしますが、自動アップデート(uPCU)はダウンロードしません。
- リポジトリ作成 — 自動アップデート(uPCU)を含む完全オフラインリポジトリを作成できます。

ミラーツールはESET LiveGrid®データをダウンロードしません。

前提条件

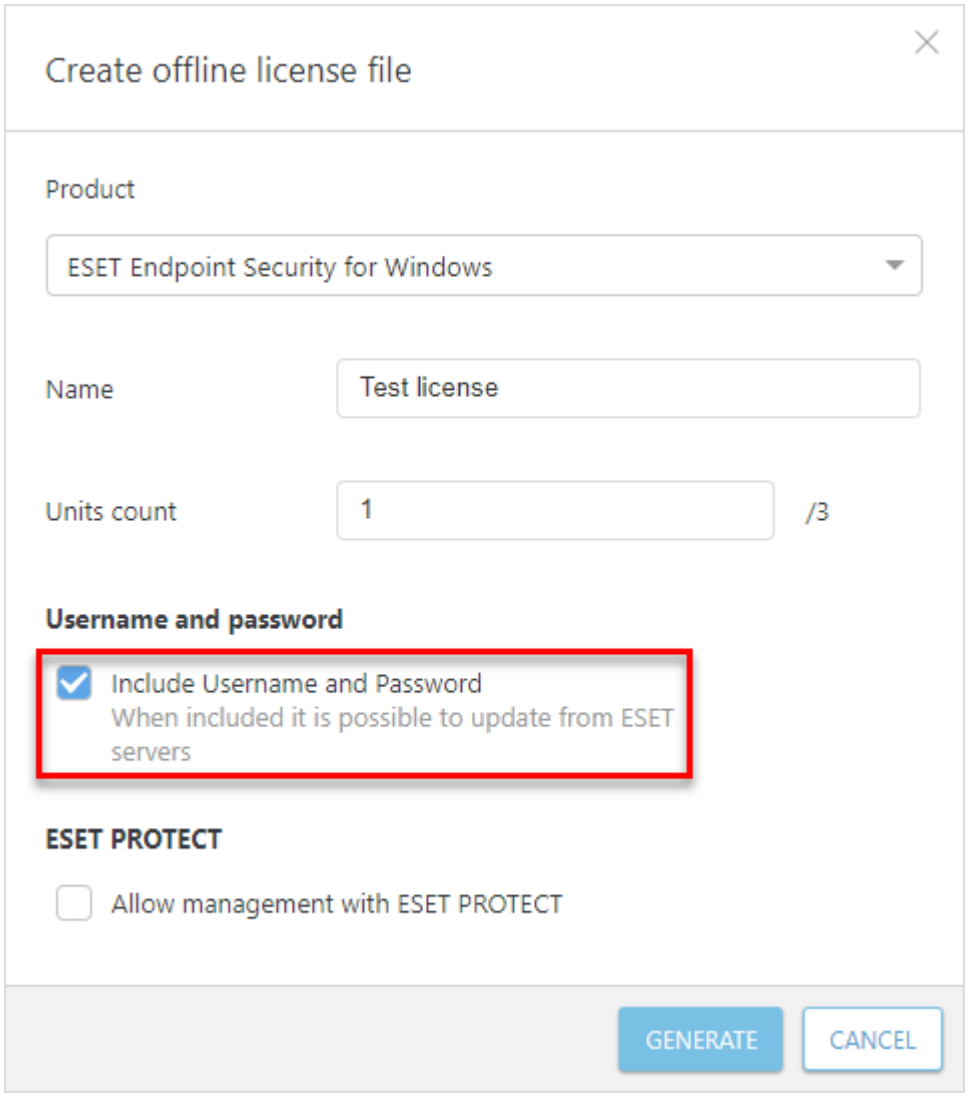
ミラーツールは、Windows XPおよびWindows Server 2003をサポートしません。

- アップデートをアクセス可能にする方法に応じて、ターゲットフォルダは共有、Samba/Windows、またはHTTP/FTPサービスに対応している必要があります。

  - ESETセキュリティ製品(Windows版) - HTTPまたは共有フォルダーを使用して、リモートでアップデートできます。

  - ESETセキュリティ製品(Linux/macOS版) - HTTPのみを使用してリモートでアップデートできます。共有フォルダーを使用する場合は、ESETセキュリティ製品と同じコンピューターにインストールする必要があります。

- ユーザー名とパスワードを含む有効なオフラインライセンスファイルが必要です。ライセンスファイルを生成するときには、**[ユーザー名とパスワードを含む]**の横のチェックボックスをオンにします。また、ライセンス**名**を入力する必要があります。ミラーツールのアクティベーションとアップデートミラーの生成には、オフラインライセンスファイルが必要です。



- ミラーツールを実行する前に、次のパッケージをインストールする必要があります。
- Visual C++ Redistributable for Visual Studio 2010
- Visual C++ 2015 Redistributable x86

ミラーツールの使用方法

1.ESETダウンロードページ(**スタンドアロンインストーラー**)からミラーツールをダウンロードします。

2.ダウンロードしたフォルダーを解凍します。

3.コマンドプロンプトを開き、*MirrorTool.exe*ファイルが格納されたフォルダーに移動します。

4.次のコマンドを実行すると、ミラーツールで使用可能なすべてのパラメーターとそのバージョンが表示されます。

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

すべてのフィルターは大文字と小文字を区別します。

パラメーターを使用して、リポジトリミラーまたはモジュールミラーを作成できます。

リポジトリとモジュールミラーの両方のパラメーター

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

リポジトリ固有のパラメーター

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

モジュール固有のパラメーター

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

パラメータ	説明
--updateServer	Mirror Toolは、エンドポイントミラーが作成するフォルダー構造とは異なるフォルダー構造を作成します。各フォルダーには、製品のグループのアップデートファイルが格納されます。 ミラーを使用する製品のアップデート設定で、アップデートサーバーの完全リンク(正しいフォルダーへの完全パス)を指定する必要があります。

パラメータ	説明
`--offlineLicenseFilename`	オフラインライセンスファイルへのパス(前述のとおり)を指定する必要があります。
`--mirrorOnlyLevelUpdates`	引数は不要です。設定すると、レベルアップデートのみがダウンロードされます(ナノアップデートはダウンロードされません)。アップデートの種類の詳細については、ナレッジベース記事をお読みください。
`--mirrorFileFormat`	⚠ `--mirrorFileFormat`パラメーターを使用する前に、環境に古い(6.5以降)バージョンと新しいバージョン(6.6. 以降)の両方のESETセキュリティ製品が含まれていないことを確認してください。このパラメーターの使用が正しくないとESETセキュリティ製品が誤って更新される可能性があります。 ダウンロードするアップデートファイルの種類を指定できます。指定可能な値(大文字と小文字を区別): • `dat` - ESETセキュリティ製品バージョン6.5以前のみの環境では、この値を使用します。 • `dll` - ESETセキュリティ製品バージョン6.6以降のみの環境では、この値を使用します。 レガシー製品(`ep4`–`ep5`)のミラーを作成する場合、このパラメーターは無視されます。
`--compatibilityVersion`	この任意のパラメーターは、ESET PROTECT On-Prem8.1以降で配布されるミラーツールに適用されます。 ミラーツールは、`x.x`または`x.x.x.x`の形式でパラメーター引数で指定したESET PROTECT On-Premリポジトリバージョンと互換性のあるアップデートファイルをダウンロードします(例: `--compatibilityVersion 11.0`または`--compatibilityVersion 8.1.13.0`)。 `--compatibilityVersion`パラメーターは自動アップデート(uPCU)をミラーから除外します。環境内で自動アップデート(uPCU)が必要で、ミラーサイズを小さくする場合は、`--filterFilePath`パラメーターを使用します。

ℹ ESETリポジトリからダウンロードされるデータの量を減らすにはESET PROTECT On-Prem 9で配布されるミラーツールの新しいパラメーターである`--filterFilePath`と`--dryRun`を使用することをお勧めします。

1. *JSON*形式でフィルターを作成します(以下の`--filterFilePath`を参照)。
2. `--dryRun`パラメーター(以下を参照)でミラーツールのテストを実行し、必要に応じてフィルターを調整します。
3. `--filterFilePath`パラメーター、定義されたダウンロードフィルター、`--intermediateRepositoryDirectory`パラメーター、`--outputRepositoryDirectory`パラメーターを使用して、ミラーツールを実行します。
4. ミラーツールを定期的に実行し、最新のインストーラーを常に使用してください。

パラメータ	説明

--filterFilePath	この任意のパラメーターを使用して、ミラーツールと同じフォルダーに配置された*JSON*形式のテキストファイルに基づいてESETセキュリティ製品をフィルタリングします(例: --filterFilePath filter.txt)
	フィルター設定の説明:
	製品フィルタリングの設定ファイル形式は次の構造の*JSON*です。
	• ルート*JSON*オブジェクト:
	ouse_legacy (ブール値、任意) - trueの場合は、レガシー製品が含まれます。
	odefaults (*JSON*オブジェクト、任意) – すべての製品に適用されるフィルタープロパティを定義します。
	■languages (リスト) – フランス語タイプの"fr_FR"など、含める言語のISO言語コードを指定します。他の言語コードは以下の表を参照してください。その他の言語を追加するには、カンマとスペースで区切ります。例: (["en_US", "zh_TW", "de_DE"])
	■platforms (リスト) – 含めるプラットフォーム(["x64", "x86", "arm64"])
	⚠ platformsフィルターは注意して使用してください。たとえば、ミラーツールが64ビットのインストーラーのみをダウンロードし、インフラストラクチャに32ビットコンピューターがある場合、64ビットのESETセキュリティ製品は32ビットコンピューターにインストールされません。
	■os_types (リスト) – 含めるOSタイプ(["windows"]["linux"]["mac"])
	oproducts (JSONオブジェクトのリスト、任意) – 特定の製品に適用するフィルター – 指定された製品defaultsを上書き。オブジェクトには次のプロパティがあります。
	■app_id (文字列) – nameが指定されていない場合は必須。
	■name (文字列) – app_idが指定されていない場合は必須。
	■version (文字列) – 含めるバージョンまたはバージョンの範囲を指定します。
	■languages (リスト) – 含める言語のISO言語コード(以下の表を参照)
	■platforms (リスト) – 含めるプラットフォーム(["x64", "x86", "arm64"])
	■os_types (リスト) – 含めるOSタイプ(["windows"]["linux"]["mac"])
	ℹ フィールドの適切な値を決定するには、管理者実行モードでミラーツールを実行し、作成されたCSVファイルで該当する製品を検索します。
	バージョン文字列形式の説明
	すべてのバージョン番号はドットで区切られた4つの数字で構成されています(例: 7.1.0.0)。バージョンフィルター(例: 7.1)を書き込むときにはそれよりも小さい数値を指定できます。残りの数字は 0 (7.1は7.1.0.0と同じ)になります。
	バージョン文字列には次の2つの形式のいずれかを使用できます。
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	o指定したバージョン以下/以下のバージョンを選択します。
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	o下限以上および上限以下のバージョンを選択します。
	比較は、バージョン番号の各部分で、左から右に数字で実行されます。
	JSONの例
	✓
	{
	"use_legacy": true,
	"defaults": {
	"languages": ["en_US"],
	"platforms": ["x64", "x86"]
	},
	"products": [
	{
	"app_id": "com.eset.apps.business.ees.windows",
	"version": "7.1.0.0–8.0.0.0"
	},
	{
	"app_id": "com.eset.apps.business.eea.windows",
	"version": ">7.1.0.0"
	}
	]
	}
	--filterFilePathパラメーターは、古いミラーツールバージョン(ESET PROTECT On-Prem 8.xでリリース済みの製品)で使用されているツールを使用するときには、ミラーツールでファイルがダウンロードされませんが、ダウンロードされるすべてのリポジトリを置換えまたは出力した*.csv*ファイルが生成されます。

--dryRun	必須パラメーターの--intermediateRepositoryDirectoryと--outputRepositoryDirectoryを使用せずにこのパラメーターを使用できます(例:)。 • Windows: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv • Linux: sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv ℹ 一部のESETインストーラーは言語に汎用的です(multilang言語コードを使用)。ミラーツールは、--filterFilePathで言語を指定する場合でも*.csv*ファイルに一覧表示されます。 --dryRunパラメーターのほかに、--intermediateRepositoryDirectoryおよび--outputRepositoryDirectoryパラメーターも使用する場合、ミラーツールは*outputRepositoryDirectory*を消去しません。
--listUpdatableProducts	(--excludedProductsが使用されていない場合は)Mirror ToolがモジュールのアップデートをダウンロードできるESET製品がすべて一覧表示されます。 パラメーターは次のバージョンのMirror Toolから使用できます。1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Mirror Toolのフォルダー構造

既定では、`--updateServer`パラメーターを指定しない場合、MirrorToolはHTTPサーバーでこのフォルダー構造を作成します。

HTTP専用ミラーサーバーを使用しない

ローカルミラーサーバーがHTTPおよびHTTPSプロトコル、またはHTTPSのみを使用していることを確認します。ミラーサーバーがHTTPのみを使用する場合は、ESETセキュリティ製品のエンドユーザーライセンス契約をHTTPサーバーから取得できないため、ソフトウェアインストールクライアントタスクを使用できません。

Mirror Toolの既定のフォルダー	ESETセキュリティ製品	アップデートサーバー(HTTPサーバールートの場所による)
mirror/eset_upd/era6	ESET PROTECT On-Prem (すべてのバージョン)	ミラーからESET PROTECT On-Prem11.0をアップデートするには、アップデートサーバーを*http://your_server_address/mirror/eset_upd/era6*に設定します。
mirror/eset_upd/ep[バージョン]	ESET Endpoint Antivirus/Securityバージョン6.x（以降)(Windows)各メジャーバージョンには、フォルダーがあります。例：バージョン10.xの*ep10*	*http://your_server_address/mirror/eset_upd/ep10*（バージョン10.xの例）
mirror/eset_upd/v5	ESET Endpoint Antivirus/Securityバージョン5.x (Windows)	*http://your_server_address/mirror/eset_upd/v5*

ESETセキュリティ製品ポリシーLinux/macOS

`--updateServer`パラメーターを指定し、追加のフォルダーを作成してHTTPミラーからLinux/macOS版のESETセキュリティ製品をアップデートする必要があります(以下を参照)。

--updateServer	追加のMirror Toolフォルダー	ESETセキュリティ製品	アップデートサーバー(HTTPサーバールートの場所による)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus for Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security for Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Securityバージョン7.x+(macOS)	*http://your_server_address/mirror/eset_upd/BusinessMac*
http://update.eset.com/eset_mobile/eesa	*mirror/eset_upd/*EndpointAndroid	ESET Endpoint Security for Android	*http://your_server_address/mirror/eset_upd/EndpointAndroid*

言語コード表

ミラーを作成するには、少なくとも必須パラメーターを指定してミラーツールを実行します。次に例を示します。

```
MirrorTool.exe --mirrorType regular ^

--intermediateUpdateDirectory c:\temp\mirrorTemp ^

--offlineLicenseFilename c:\temp\offline.lf ^

--outputDirectory c:\temp\mirror
```

次に、製品、言語が選択され、*filter.txt*ファイルで定義されたレガシーファイルのダウンロードが有効になっている、オフラインのリポジトリの高度な設定の例です(上記の`--filterFilePath`の詳細のファイル内容の例を参照)。

```
MirrorTool.exe --repositoryServer AUTOSELECT ^

--intermediateRepositoryDirectory c:\temp\repoTemp ^

--outputRepositoryDirectory c:\temp\repository ^

--filterFilePath filter.txt
```

ミラーツールとアップデート設定

- モジュールアップデートのダウンロードを自動化するには、ミラーツールを実行するスケジュールを作成できます。このためにはWebコンソールを開き、**[クライアントタスク] > [オペレーティングシステム] > [コマンドの実行]に移動します。 実行するコマンドライン** (*MirrorTool.exe*へのパスを含む)と合理的なトリガー(毎時0 0 * * * ?*のCRONなど)を選択します。*). あるいはWindowsタスクスケジューラまたはLinuxの`Cron`を使用できます。

- クライアントコンピューターでアップデートを構成するには、新しいポリシーを作成し、**アップデートサーバー**を構成してミラーアドレスまたは共有フォルダを参照します。

> HTTPSミラーサーバーを使用している場合は、その証明書をクライアントコンピューターの信頼できるルートストアにインポートする必要がありますWindowsでの信頼できるルート証明書のインストールを参照してください。

> このナレッジベース記事を読み、ミラーツールチェーンを設定(別のミラーツールからアップデートをダウンロードするようにミラーツールを設定)してください。

モバイルデバイスコネクターインストール - Windows

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

場所に関係なく、常にモバイルデバイスを管理できるように、モバイルデバイスコネクターはインターネットからアクセスできる必要があります。

ESET PROTECTサーバーがホストされているデバイスとは別のホストデバイスにMDMコンポーネントを展開することをお勧めします。

次の手順に従い、WindowsでESET PROTECTサーバーのMobile Device Connectorをインストールします。

すべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。（*mdmcore_x64.msi*).

2. モバイルデバイスコネクター インストーラを実行し、同意する場合はEULAを承諾します。

3. [**参照**]をクリックしてHTTPS経由の通信で使用するSSL証明書の場所に移動し、この証明書のパスワードを入力します。

4. **MDMホスト名またはIPアドレス**:MDMホスト名またはIPアドレスを指定します。インターネットからモバイルデバイスがアクセスする場合は公開ドメインまたは公開IPアドレスを指定します。

MDMホスト名を**HTTPSサーバー証明書**で指定されたフォームに入力する必要があります。そうでない場合iOSモバイルデバイスはMDMプロファイルのインストールを拒否します。たとえばHTTPS証明書でIPアドレスが指定されている場合、このIPアドレスを**MDMホスト名またはIPアドレス**フィールドに入力しますFQDN (たとえば`mdm.mycompany.com`)がHTTPS証明書で指定されている場合、このFQDNを**MDMホスト名**フィールドに入力します。ワイルドカード*（たとえば`*.mycompany.com`)がHTTPS証明書で使用される場合、`mdm.mycompany.com`を**MDMホスト名**フィールドで使用できます。

5. インストーラーはモバイルデバイスコネクターで使用される既存のデータベースに接続する必要があります。次の接続詳細を指定します。

- **データベース**:Windows認証によるMySQL Server/MS SQL Server/MS SQL Server

- **ODBCドライバ**:MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

- **データベース名**:定義済みの名前を使用するか、必要に応じて変更することをお勧めします。

- **ホスト名**:ホスト名またはデータベースサーバーのIPアドレス

- **ポート**: データベースとの接続で使用されます。

- データベース管理者アカウントの**ユーザー名/パスワード**

- **名前付きインスタンスを使用する** - Microsoft SQLデータベースを使用している場合は、**名前付きインスタンスを使用する**チェックボックスを選択し、カスタムデータベースインスタンスを使用できます。*HOSTNAME\DB_INSTANCE*の形式で**ホスト名**フィールドで設定できます。(例:

192.168.0.10\ESMC7SQL）。クラスタデータベースの場合、クラスタ名のみを使用します。このオプションを選択する場合、データベース接続ポートを変更できません。Microsoftの既定のポートが使用されます。フェールオーバークラスターにインストールされたMicrosoft SQLデータベースにサーバーを接続するには、**ホスト名**フィールドにESET PROTECTクラスタ名ーを入力します。

ESET PROTECTデータベースと同じデータベースサーバーを使用できますが、80台を超えるモバイルデバイスを登録する計画の場合には、別のDBサーバーを使用することをお勧めします。

6. 新しく作成されたモバイルデバイスコネクターデータベースのユーザーを指定します。**新しいユーザーを作成する**か、**既存のデータベースユーザーを使用**できます。データベースユーザーのパスワードを入力します。

7. **サーバーホスト**(ESET PROTECTサーバーの名前またはIPアドレス)と**サーバーポート**(既定のポートは2222です。別のポートを使用する場合は、既定のポートをカスタムポート番号で置換します)

8. MDMコネクターをESET PROTECTサーバーに接続するためのポートESET PROTECTサーバーへの接続に必要な**サーバーホスト**と**サーバーポート**を入力し、**サーバー支援インストール**または**オフラインインストール**を選択して続行します。

- **サーバー支援インストール** - ESET PROTECT Webコンソール管理者資格情報を提供します。インストーラーが必要な証明書を自動的にダウンロードします。また、サーバー支援インストールに必要な権限も確認します。

    1.**サーバーホスト** (ESET PROTECTサーバーの名前またはIPアドレス)と**Webコンソールポート**(カスタムポートを使用しない場合は既定のポート2223を使用)を入力します。またWebコンソール管理者認証情報(**ユーザー名/パスワード**)を指定します。

    2.証明書を許可するように指示されたら、[**はい**]をクリックします。手順10に進みます。

- **オフラインインストール** - **プロキシ証明書**と**認証局**を指定する必要があります。これはESET PROTECT On-Premからエクスポートできます。あるいは、カスタム証明書と適切な認証局を使用できます。

    1.ピア証明書の横の[**参照**]をクリックし、**ピア証明書**の場所に移動します(これはESET PROTECT On-Premからエクスポートしたプロキシ証明書です)。[**証明書パスワード**]テキストフィールドは空欄にします。この証明書にはパスワードが必要ないためです。

    2.認証局の手順を繰り返し、手順10に進みます。

ESET PROTECT On-Premで(ESET PROTECT On-Premインストール中に自動的に生成された既定の証明書の代わりに)カスタム証明書を使用する場合、プロキシ証明書を指定するように指示されるときにこれらを使用する必要があります。

9. モバイルデバイスコネクターのインストール先フォルダ(既定の場所を推奨)を指定し、[**次へ**]をクリックしてから、[**インストール**]をクリックします。

10. インストールが完了した後、Webブラウザーまたはモバイルデバイスから*https://your-mdm-hostname:enrollment-port*（たとえば*https://mdm.company.com:9980*）を開き、Mobile Device Connectorが正常に実行されているかどうかを確認します。インストールが成功したら、次のメッセージが表示されますMDMサーバーが起動して実行中です。

11. ESET PROTECT On-PremからMDMをアクティブ化できます。

モバイルデバイスコネクター前提条件

MDMサーバーのポートまたはホスト名が変更された場合は、すべてのモバイルデバイスを再登録する必要があります。
このためMDMサーバーに専用のホスト名を設定し、MDMサーバーのホストデバイスを変更する必要がある場合には、新しいホストデバイスのIPアドレスをDNS設定のMDMホスト名に再割り当てすることで実行できるようにすることをお勧めします。

Windowsにモバイルデバイスコネクターをインストールするには、次の要件を満たす必要があります。

- インターネットからアクセス可能な公開IPアドレス/ホスト名または公開ドメイン。

MDMサーバーのホスト名を変更する必要がある場合は、MDMコンポーネントを再インストールする必要がありますMDMサーバーのホスト名を変更する場合MDMが正常に動作し続けるには、この新しいホスト名を含む新しい**HTTPSサーバー証明書**をインポートしなければならない場合があります。

- ポートが開いていて使用可能である – ポートの一覧については、ここを参照してください。既定のポート9981および9980を使用することをお勧めしますが、これらも必要に応じてMDMサーバーの設定ファイルで変更できます。モバイルデバイスが指定されたポート経由で接続できることを確認します。必要に応じてファイアウォールまたはネットワーク設定を変更し、通信を可能にします。MDMアーキテクチャの詳細をお読みください。

- ファイアウォール設定 - Windows 7などのサーバー以外のOSにモバイルデバイスコネクターをインストールしている場合(評価目的のみ)は、次のファイアウォールルールを作成して通信ポートを必ず許可してください。

*C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe*TCPポート9980

*C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe*TCPポート9981

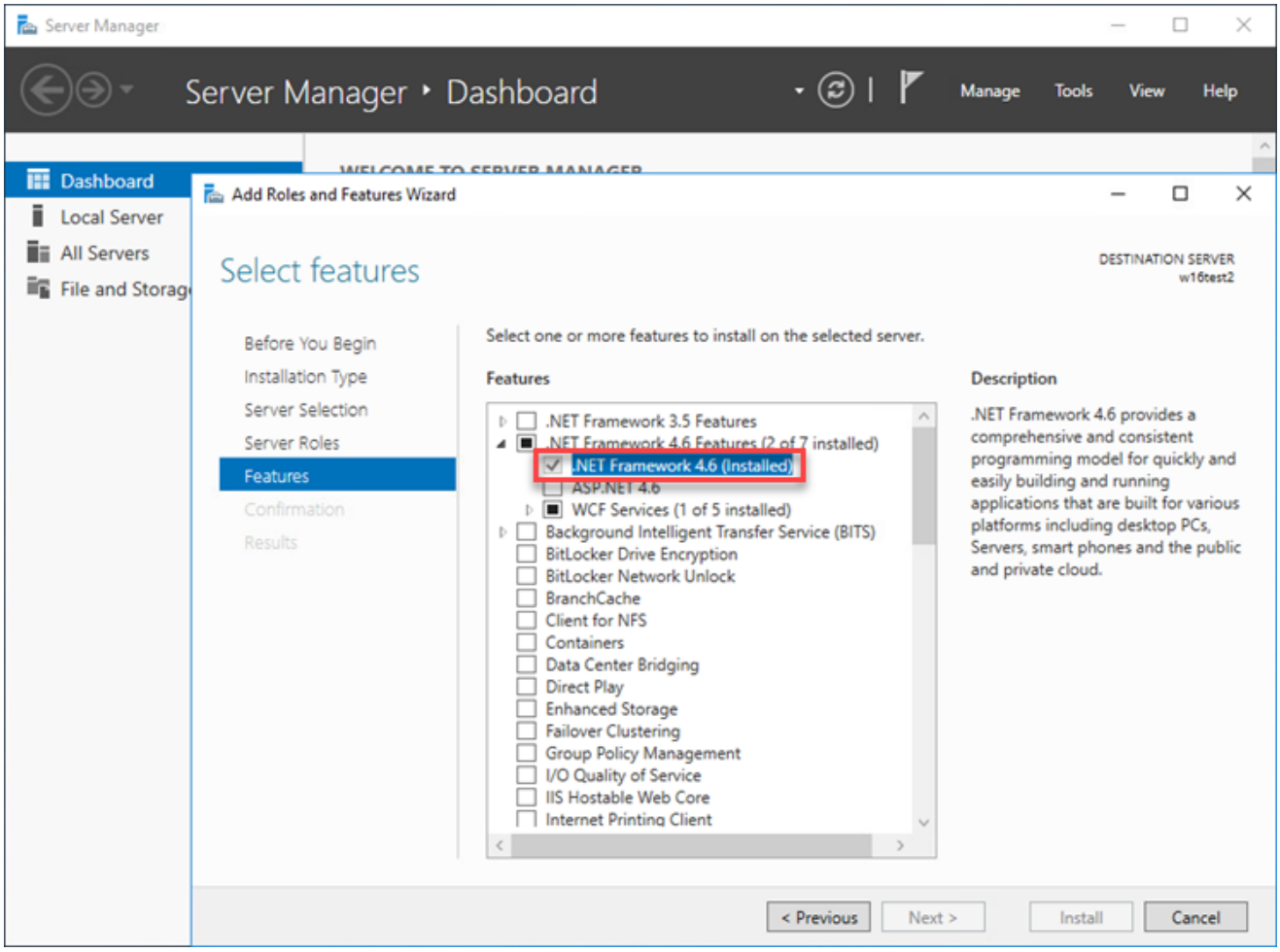
*C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe*TCPポート2222

*.exe*ファイルへの実際のパスは、クライアントOSシステムに各ESET PROTECTコンポーネントがインストールされている場所によって異なる場合があります。

- データベースサーバーがインストールおよび構成済みである。Microsoft SQLまたはMySQLを満たしていることを確認します。

- MDMコネクターのRAM使用率は最適化されているため、最大48の「ESET PROTECT MDMCore Moduleプロセスを同時に実行できます。ユーザーがこれより多いデバイスに接続する場合は、現在リソースを使用する必要がある各デバイスに対してプロセスが定期的に変化します。

- Microsoft SQL Server Expressインストールには.NET Framework 4が必要です。**ロールと機能の追加ウィザード**を使用してインストールできます。



証明書要件

• HTTPS上の安全な通信のため、*.pfx*形式の**SSL証明書**が必要です。第三者の認証局(CA)が提供した証明書を使用することをお勧めします。一部のモバイルデバイスでは、ユーザーが自己署名証明書を許可しないため、自己署名証明書(ESET PROTECT On-Prem CAが署名した証明書を含む)は推奨されません。

• CAが署名した証明書、対応する秘密鍵が必要です。また、標準手順を利用して、これら(従来はOpenSSLを使用)を1つの *.pfx*ファイルに統合する必要があります。

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```

これはSSL証明書を使用するほとんどのサーバーの標準の手順です。

• オフラインインストールの場合ESET PROTECT On-Premからエクスポートされたピア証明書(**エージェント証明書**)も必要です。あるいはESET PROTECT On-Premではカスタム証明書を使用できます。

モバイルデバイスコネクターのアクティベーション

モバイルデバイスコネクターをインストールした後に、ESETエンドポイント、ビジネス、オフィスライセンスでアクティベートする必要があります。

1.ESETエンドポイント、ビジネス、またはオフィスライセンスをESET PROTECT On-Prem のライセンス管理に追加します。

2.製品アクティベーションクライアントタスクを使用してMobile Device Connectorをアクティベーションします。この手順は、クライアントコンピューターでESET製品をアクティベーションするときの手順と同じです。この場合は、モバイルデバイスコンピューターがクライアントコンピューターです。

MDM iOSライセンス機能

ESETはApple App Storeでアプリケーションを提供しないためESETモバイルデバイスコネクターはiOSデバイスのすべてのライセンス詳細を保存します。

ライセンスはデバイス単位であり、製品アクティベーションタスクを使用してアクティベーションできます(Androidと同じ)。

iOSライセンスは次の方法で無効にできます。

- 管理の停止タスクでデバイスを管理から削除する
- MDCのアンインストールは、**[データベースを削除する]**オプションでアンインストールされます
- 他の方法でのアクティベーション解除(ESET PROTECT On-PremまたはEBAアクティベーション解除)

MDCはiOSデバイスに代わってESETライセンスサーバーと通信するためEBAポータルはMDCの状態を反映しますが、個別のデバイスの状態は反映しません。現在のデバイス情報は常にESET PROTECT Webコンソールで確認できます。

アクティベーションされていないデバイスまたはライセンスが期限切れのデバイスには保護の状態が赤色で表示され、「製品がアクティベーションされていません」というメッセージが表示されます。これらのデバイスはタスクの処理、ポリシーの設定、重要ではないログの配信ができません。

MDMのアンインストール中に、**データベースを削除しない**が選択されている場合、取得されたライセンスが無効化されませんMDMが再インストールされる場合またはEBAアクティベーション解除した場合ESET PROTECT On-Premによって、これらのライセンスを再利用できます。別のMDMサーバーに移動するときには、製品アクティベーションタスクを再実行する必要があります。

HTTPS認証要件

ESETモバイルデバイスコネクターでモバイルデバイスを登録するにはHTTPSサーバーが完全な認証チェーンを返すことを確認します。

証明書が正しく動作するには、次の要件を満たす必要があります。

- HTTPS証明書(pkcs#12/pfxコンテナー)には、ルートCAを含む完全な証明書チェーンを含める必要があります。
- 証明書は必要な期間の間有効である必要があります(有効開始日/有効終了日)
- **CommonName**または**subjectAltNames**はMDMホスト名と一致する必要があります

MDMホスト名がhostname.mdm.domain.comなどの場合には、証明書に次のような名前を含めることができます。
- hostname.mdm.domain.com
- *.mdm.domain.com

ただし、次のような名前は使用できません。
- *
- *.com
- *.domain.com

基本的に、「*」は「ドット」を置換するために使用できません。この動作は、iOSがMDMの証明書を許可する方法で確認されます。

一部のデバイスは、証明書の有効期限を確認するときに現在のタイムゾーンを考慮しますが、そうでないデバイスもあります。証明書の有効期限を現在の日付の1、2日前に設定し、潜在的な問題を回避します。

オフラインリポジトリ - Windows

ミラーツールを使用して、オフラインリポジトリを作成できます(Windows)。一般的に、遮断されたコンピューターネットワークまたは制限されたインターネットアクセスのネットワークに必要です。ミラーツールを使用して、ローカルフォルダーでESETリポジトリの複製を作成できます。この複製されたリポジトリは後から遮断されたネットワークのローカルに移動できます(外部ディスクなど)。リポジトリをローカルネットワークの安全な場所にコピーし、HTTPサーバー経由で使用可能にすることができます(ESET Bridgeなど)。

オフラインリポジトリをアップデートするには、オフラインリポジトリの作成時と同じパラメーターを使用して、同じコマンドを実行します。中間フォルダーの既存のデータは再利用されます。古いファイルのみがダウンロードされます。

リポジトリのサイズが拡大し、中間ディレクトリが同じサイズになります。この手順を開始する前には、必ず**1.2 TB**以上の空き領域を確保してください。

ベストプラクティス

オフライン環境でのESET PROTECT On-Prem使用に関するベストプラクティスについてはESETナレッジベース記事も参照してください。

Windowsのシナリオの例

I. リポジトリ複製の作成

1. ミラーツールをダウンロードします。
2. ダウンロードされた*.zip*ファイルからミラーツールを展開します。
3. 次のフォルダーを準備(作成)します。
   - 中間ファイル
   - 最終リポジトリ
4. コマンドプロンプトを開き、ミラーツールが展開されたフォルダー(`cd`コマンド)にディレクトリ

を変更します。

5. 次のコマンドを実行します(中間および出力リポジトリディレクトリを手順3のフォルダーに変更します)。

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory C:\Intermediary ^
--outputRepositoryDirectory C:\Repository
```

6. リポジトリが`outputRepositoryDirectory`フォルダーにコピーされた後、フォルダーと内容を遮断されたネットワークがアクセスできる別のコンピューターに移動します。

II.HTTPサーバーのセットアップ

1. 遮断されたネットワークのコンピューターで実行中のHTTPサーバーが必要です。次を使用できます。

- ESETダウンロードサイトからのESET Bridgeプロキシ(このシナリオ)
- 別のHTTPサーバー

2. ESET Bridgeプロキシをインストールします。

III.オフラインリポジトリの実行

1. *C:\Program Files\ESET\Bridge*ファイルに移動し、単純なテキストエディタを使用して*pkgid*ファイルを開きます。`http_proxy_settings_static_content_enabled`設定を`true`に変更して、オフラインリポジトリサーバーをアクティベーションします。変更を保存し、*pkgid*ファイルを閉じます。

2. 手順6(上記のセクションI)でダウンロードしたリポジトリをオフラインリポジトリサーバーディレクトリにコピーします。

- 規定のオフラインリポジトリサーバーディレクトリは、適切なアクセス権を持つ*C:\ProgramData\ESET\Bridge\OfflineRepository*です。

- カスタムディレクトリを使用するには、オフラインリポジトリ用の新しいフォルダーを作成します(*C:\Repository*など)。*pkgid*ファイルで、行`"http_proxy_settings_offline_repository_dirPath": "%DATADIR%\\OfflineRepository"`を`"http_proxy_settings_offline_repository_dirPath": "C:\\Repository"`に置き換えます。NETWORK SERVICEユーザーは、ディレクトリへのフルアクセス権が必要です。

3. コマンドラインコマンド(`net stop "EsetBridge"`と`net start "EsetBridge"`)を使用してESET Bridgeサービスを再起動します。*pkgid*ファイルを変更した後にサービスを再起動してください。リポジトリデータが変更、削除、または追加された場合は、サービスの再起動は不要です。

4. オフラインリポジトリは、アドレス*http://YourIPaddress:4449*(*http://10.1.1.10:4449*など)で実行されます。

5. ESET PROTECT Webコンソールを使用して、新しいリポジトリアドレスを設定します。

a.ESET PROTECTサーバー - **詳細** > **設定** > **詳細設定** > **リポジトリ**をクリックし、オフラインリポジ

トリアドレスを**サーバー**フィールドに入力します。

b.ESET Managementエージェント - **ポリシー**をクリックします。エージェントポリシー > **編集 > 設定 > 詳細設定 > リポジトリ**をクリックし、オフラインリポジトリアドレスを**サーバー**フィールドに入力します。

c.ESETエンドポイント製品(Windows) - **ポリシー**をクリックします。**ESET Endpoint for Windows**ポリシー > **編集 > 設定 > アップデート > プロファイル > アップデート > 製品のアップデート**をクリックし、オフラインリポジトリアドレスを**カスタムサーバー**フィールドに入力します。

フェールオーバークラスタ - WIndows

フェールオーバー環境にESET PROTECT On-Premをインストールするための概要手順は次のとおりです。

ESET PROTECTサーバーのクラスタインストールに関するナレッジベース記事を参照してください。

1. 共有ディスクがあるフェールオーバークラスターの作成

- Windows Server 2016および2019でフェールオーバークラスタを作成する手順
- Windows Server 2012および2012 R2でフェールオーバークラスタを作成する手順

2. **クラスターの作成ウィザード**で、任意のホスト名(1つ)とIPアドレスを入力します。

3. ノード1でオンラインのクラスターの共有ディスクを取得し、スタンドアロンインストーラーを使用してESET PROTECTサーバーをインストールします。インストール中に**これはクラスターインストールです**が選択されていることを確認し、共有ディスクをアプリケーションデータストレージとして選択します。ホスト名を作成し、入力されたホスト名の横にESET PROTECT Serverのサーバー証明書用に入力します。このホスト名を記録し、手順6でCluster ManagerでESET PROTECTサーバーロールを作成するときに使用します。

4. ノード1のESET PROTECT Serverを停止し、ノード2でオンラインのクラスターの共有ディスクを取得します。スタンドアロンインストーラーを使用してESET PROTECTをインストールします。**これはクラスターインストール**がインストール中に選択されていることを確認します。共有ディスクをアプリケーションデータストレージに選択します。データベース接続と証明書情報はそのままにします。これはノード1でESET PROTECT Serverのインストール中に構成されます。

5. ESET PROTECT Serverによって使用されるすべてのポートで、受信接続を許可するようにファイアウォールを構成します。

6. クラスター構成マネージャーで、ESET PROTECT Serverサービスのロール(**ロールの構成 > ロールの選択 > 汎用サービス**)を作成および開始します。使用可能なサービスのリストから**ESET PROTECT Server**サービスを選択します。サーバー証明書に関連する手順3で使用されたホスト名をロールのホスト名として使用することが非常に重要です。

7. スタンドアロンインストーラーを使用してすべてのクラスターノードにESET Managementエージェントをインストールします。**エージェント構成**と**ESET PROTECT Serverへの接続**画面で、手順6で使用したホスト名を使用します。ローカルノード(クラスタディスクではない)でエージェントデータを保存します。

8. Webサーバ(Apache Tomcat)はクラスターでサポートされていないため、非クラスターディスクまたは別のコンピューターにインストールする必要があります。

a.Webコンソールを別のコンピューターにインストールし、ESET PROTECTサーバークラスタロールに接続するように正しく設定します。

b.Webコンソールがインストールされた後、次の場所の構成ファイルを見つけます。 *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

c.メモ帳または他の簡易テキストエディターでファイルを開きます。`server_address=localhost`行で、localhostをESET PROTECTサーバークラスタロールのIPアドレスまたはホスト名で置換します。

Linuxでのコンポーネントインストール

ほとんどのインストールシナリオでは、コンピューターによって異なるESET PROTECTコンポーネントをインストールし、さまざまなネットワークアーキテクチャに対応し、パフォーマンス要件やその他の要求に対応する必要があります。

段階的なESET PROTECT On-Premインストールの手順に従います。

コアコンポーネントインストール:

- ESET PROTECTサーバー
- ESET PROTECT Webコンソール - ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。
- ESET Managementエージェント
- データベースサーバー

オプションコンポーネントインストール:

- RD Sensor
- モバイルデバイスコネクター
- ESET BridgeHTTPプロキシ
- ミラーツール

Linux版のESET PROTECT On-Premを最新バージョンにアップグレードするには、コンポーネントアップグレードタスクの章またはナレッジベース記事を参照してください。

Linuxでの段階的なESETPROTECTOn-Premのインストール

このインストールシナリオではESET PROTECTサーバーとESET PROTECT Webコンソールの段階的なインストールをシミュレートします。ここではMySQLを使用してインストールをシミュレートします。

選択したLinuxディストリビューションのインストール手順
ナレッジベース記事とディストリビューション固有の手順に従ってください。
- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

インストール前の手順

1.ネットワークでのデータベースサーバーの存在を確認し、ローカルまたはリモートサーバーからデータベースサーバーにアクセスできることを確認します。データベースサーバーがインストールされていない場合、新しいサーバーをインストールして設定します。

2. ESET PROTECT Linuxスタンドアロンコンポーネント(エージェント、サーバ、Webコンソール)をダウンロードします。これらのインストールファイルは、ESET Webサイトで提供されているESET PROTECTスタンドアロンインストーラーカテゴリにあります。

インストール処理

インストールを完了するには、`sudo`コマンドを使用するか、`root`権限の下でインストールできる必要があります。

1. ESET PROTECTサーバーの必須パッケージをインストールします。

2. MySQL構成トピックに従い、MySQLサーバーへの接続を構成します。

3. MySQL ODBCの設定を確認する。詳細については、ODBCインストールおよび構成を参照してください)。

4. インストールパラメータをカスタマイズし、ESET PROTECTサーバーインストールを実行します。詳細は、サーバーインストール - Linuxを参照してください。

5. 必須のJavaおよびTomcatパッケージをインストールして、ESET PROTECT WebコンソールをインストールしますESET PROTECT WebコンソールへのHTTPS接続の問題が発生する場合は、HTTPS/SSL接続設定を参照してください。

6. サーバーコンピューターでESET Managementエージェントをインストールします。

ESETは、コマンドライン履歴から機密データ(パスワードなど)を含むコマンドを削除することをお勧めします。
1.`history`を実行すると、履歴のすべてのコマンドの一覧を表示します。
2.`history -d line_number`を実行(コマンドの行番号を指定)します。あるいは、`history -c`を実行し、コマンドライン履歴全体を削除します。

MySQLインストールおよび構成

インストール

必ずサポートされているバージョンのMySQL ServerとODBCコネクターをインストールしてください。

MySQLを既にインストールして構成した場合は、構成に進みます。

1. MySQLリポジトリを追加します。

Debian, Ubuntu	ターミナルで次のコマンドを実行します。
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	パッケージインストール中にインストールするコンポーネントのバージョンを選択できます。既定のオプションを選択することをお勧めします。MySQL APTリポジトリの追加を参照してください。

CentOS, Red Hat	MySQL Yumリポジトリの追加
SUSE Linux Enterprise Server	MySQL SLESリポジトリの追加

2. ローカルリポジトリキャッシュを更新します。

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
SUSE Linux Enterprise Server	`sudo zypper update`

3. MySQLのインストールは、使用されるLinux配布とバージョンによって異なります。

Linuxディストリビューション:	MySQLサーバーインストールコマンド:	MySQLサーバー詳細インストール:
Debian, Ubuntu	`sudo apt-get install mysql-server`	Installing MySQL from Source with the MySQL APT Repository
CentOS, Red Hat	`sudo yum install mysql-community-server`	Installing MySQL on Linux Using the MySQL Yum Repository
SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Steps for a Fresh Installation of MySQL

手動インストール用にMySQL Community Serverをダウンロードします。

設定

1. テキストエディターで*my.cnf*構成ファイルを開きます。

```
sudo nano /etc/my.cnf
```

ファイルが存在しない場合は、`/etc/mysql/my.cnf`、`/etc/my.cnf.d/community-mysql-server.cnf`、または`/etc/mysql/mysql.conf.d/mysqld.cnf`を試してください。

2. `my.cnf`構成ファイルの*[mysqld]*セクションで次の設定を見つけ、値を修正します。

> - ファイルに存在しない場合は、`[mysqld]`セクションを作成します。
> - パラメーターがファイルにない場合は、`[mysqld]` セクションに追加します。
> - MySQLバージョンを決定するには、次のコマンドを実行します。`mysql --version`

パラメータ	コメントと推奨値	MySQLバージョン
max_allowed_packet=33M		すべてのサポートされているバージョン
log_bin_trust_function_creators=1	あるいは、バイナリロギングを無効にすることができます。log_bin=0	8.x
innodb_log_file_size=100M innodb_log_files_in_group=2	これらの2つのパラメーターの値の乗数は、**200**以上でなければなりません。innodb_log_files_in_groupの最小値は**2**で、最大値は**100**です。値は整数である必要があります)。	8.x 5.7 5.6.22(以降5.6.x)
innodb_log_file_size=200M	**200M**以上、**3000M**以下に値を設定します。	5.6.20と5.6.21

3. **CTRL + X**を押して、**Y**と入力すると、変更を保存し、ファイルを閉じます。

4. MySQLサーバーを再起動し、構成を適用します(場合によっては、サービス名はmysqldです)。

```
sudo systemctl restart mysql
```

5. MySQL権限とパスワードを設定します(これは任意であるため、一部のLinuxディストリビューションでは動作しない場合があります)。

a)一時MySQLパスワードを表示します。`sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)パスワードをコピーして保存します。

c)次のオプションのいずれかを使用して、新しいパスワードを設定します。

- /usr/bin/mysql_secure_installationを実行し、一時パスワードを入力します。次に、新しいパスワードを作成する必要があります。
- mysql -u root -pを実行し、一時パスワードを入力します。ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';を実行し、ルートパスワードを変更(strong_new_passwordを自分のパスワードで置換)して、Quitと入力します。

MySQLリファレンスマニュアルのMySQLインストールセキュリティの改善も参照してください。

6. MySQL Serverサービスが実行中であることを確認します。

```
sudo systemctl status mysql
```

ODBCインストールおよび構成

必ずサポートされているバージョンのMySQL ServerとODBCコネクターをインストールしてください。

Microsoft ODBCドライバー(バージョン13以降)をインストールしてLinuxのESET PROTECTサーバーをWindowsのMicrosoft SQL Serverに接続できます。詳細については、このナレッジベース記事をご覧ください。

ターミナルを使用してMySQL ODBCドライバーをインストールしますLinuxディストリビューションの手順に従います。

- Debian、Ubuntu
- CentOS 7
- その他のサポートされているLinuxディストリビューション

Debian, Ubuntu

1. unixODBCドライバーをインストールします。

```
sudo apt-get install unixodbc
```

2. ODBCコネクターをダウンロードします。

Ubuntu 16	wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz
Ubuntu 18	wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz
Ubuntu 20	wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
Debian 10	wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz

⚠
- 必ず、ご使用のLinuxディストリビューションおよびバージョンと互換性があるバージョンを選択してダウンロードしてください。
- 公式MySQLサイトからMySQLのODBCコネクターをダウンロードします。

3. ODBCドライバーアーカイブを解凍します(使用されるリンクによってパッケージ名が異なります)。

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. ODBCドライバーを展開します(使用されるリンクによってパッケージ名が異なります)。

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. ODBCドライバーフォルダーに移動します(使用されるリンクによってパッケージ名が異なります)。

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. ODBCドライバーファイルをコピーします。

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. ODBCのドライバーを登録します。

- Ubuntu 20.xなどの新しいLinuxバージョンではUnicodeドライバーを使用することをお勧めします。

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- その他のシステムの場合、またはUnicodeドライバーが動作しない場合は、次のコマンドを使用してください。

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. インストールされているドライバーのリストを出力します。

```
sudo myodbc-installer -d -l
```

詳細については、https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.htmlを参照してください。

CentOS 7

1. unixODBCドライバーをインストールします。

```
sudo yum install unixODBC -y
```

2. ODBCコネクターをダウンロードします。

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.el7.x86_64.rpm
```

> ⚠ • YUMを使用してODBCコネクターをインストールしないでください。互換性のあるバージョンではなく、最新バージョンがインストールされます。
> • 必ず、ご使用のLinuxディストリビューションおよびバージョンと互換性があるバージョンを選択してダウンロードしてください。
> • 公式MySQLサイトから MySQLのODBCコネクターをダウンロードします。

3. ODBCドライバーをインストールします。

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. ODBCドライバーを設定します。

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. インストールされているドライバーのリストを出力します。

```
sudo myodbc-installer -d -l
```

その他のサポートされているLinuxディストリビューション

> ⚠ • 必ず、ご使用のLinuxディストリビューションおよびバージョンと互換性があるバージョンを選択してダウンロードしてください。
> • 公式MySQLサイトから MySQLのODBCコネクターをダウンロードします。

1. ODBCドライバーをインストールするには、次の手順に従います。

   • **SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`.https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.htmlを参照してください。

   • バイナリTarballディストリビューションからのコネクタ/ODBCのインストール

2. 次のコマンドを実行し、テキストエディタで*odbcinst.ini*ファイルを開きます。

```
sudo nano /etc/odbcinst.ini
```

または`sudo nano/etc/unixODBC/odbcinst.ini`

3. 次の構成を*odbcinst.ini*ファイルにコピー(**Driver**と**Setup**へのパスが正しいことを確認)し、ファイルを保存して閉じます。

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

ディストリビューションによってはDriverの場所が異なる場合があります。次のコマンドを使用してファイルを検索できます。

```
sudo find /usr -iname "*libmyodbc*"
```

4. 次のコマンドを実行し、現在のホスト上のデータベースサーバーへのODBCアクセスを制御する構成ファイルを更新します。

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

または`sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

サーバーインストール - Linux

> **選択したLinuxディストリビューションのインストール手順**
> ナレッジベース記事とディストリビューション固有の手順に従ってください。
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

インストール

ターミナルコマンドを使用してLinuxにESET PROTECTサーバーコンポーネントをインストールするには、次の手順に従います。

> すべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTサーバーコンポーネントをダウンロードします。

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. ダウンロードされたファイルを実行可能にします。

```
chmod +x server-linux-x86_64.sh
```

3. インストールスクリプトを準備し、`sudo`を使用して実行します。

次の例に従い、インストールスクリプトを実行します(コマンド全体を端末にコピーするために、「\」

で区切って改行してあります)。

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

次の属性を変更できます。

属性	説明	必要
`--uninstall`	製品のアンインストール	-
`--keep-database`	データベースはアンインストール中に削除されません。	-
`--locale`	インストールされているサーバーのロケール識別子(LCID)(既定では`en_US`です)。使用可能なオプションについては、サポートされている言語を参照してください。 `--locale`を指定しない場合は、ESETPROTECTサーバーが英語でインストールされます。ESET PROTECT On-Premのインストール後には、各ESET PROTECT Webコンソールセッションの言語を設定できます。Webコンソールの一部の要素は言語を変更しても変更されません。一部の要素(既定のダッシュボード、ポリシー、タスクなど)はESET PROTECT On-Premのインストール中に作成され、言語は変更できません。	はい
`--skip-license`	インストールでは、ライセンス契約の確認をユーザーに要求しません	-
`--skip-cert`	証明書の生成をスキップします(`--server-cert-path`パラメータと一緒に使用してください)。	-
`--license-key`	ESETのライセンスキー。後から製品認証キーを入力できます。	-
`--server-port`	ESET PROTECTサーバーポート(既定値は`2222`)	-
`--console-port`	ESET PROTECT Webコンソールポート(既定値は`2223`)	-
`--server-root-password`	Webコンソールの「管理者」ユーザーのログインパスワードは、少なくても8文字の長さにする必要があります。	はい
`--db-type`	使用するデータベースの種類(使用可能な値: `"MySQL Server"`, `"MS SQL Server"`) Linux の Microsoft SQL Server はサポートされていません。ただし、Linux の ESET PROTECT サーバーを Windows の Microsoft SQL Server に接続することができます。	-

属性	説明	必要
--db-driver	*odbcinst.ini*ファイルで指定されたデータベースに接続するために使用されるODBCドライバー(コマンドodbcinst -q -dは、使用可能なドライバーの一覧を出力し、これらのドライバーのいずれかを使用します。例: --db-driver="MySQL ODBC 8.0 Driver"--db-driver="MySQL ODBC 8.0 Unicode Driver"、または--db-driver="MySQL ODBC 8.0.17")	はい
--db-hostname	コンピューター名またはデータベースサーバーのIPアドレス。名前付きデータベースインスタンスはサポートされません。	はい
--db-port	データベースサーバーのポート(既定値は3306)	はい
--db-name	ESET PROTECTサーバーデータベースサーバーの名前(既定値はera_db)	-
--db-admin-username	データベース管理者のユーザー名(インストールで使用し、データベースの作成および変更を行います)。以前に作成されたデータベースユーザーが--db-user-usernameおよび--db-user-passwordによって定義されている場合は、このパラメーターを省略できます。	はい
--db-admin-password	データベース管理者のパスワード以前に作成されたデータベースユーザーが--db-user-usernameおよび--db-user-passwordによって定義されている場合は、このパラメーターを省略できます。	はい
--db-user-username	ESET PROTECT サーバーデータベースのユーザー名(ESET PROTECTサーバーで使用し、データベースへ接続します)は、16文字以内にする必要があります。	はい
--db-user-password	データベースESET PROTECTサーバーユーザーパスワード	はい
--cert-hostname	ESET PROTECTサーバーコンピューターのすべての名前やIPアドレスが含まれています。値は、サーバーに接続しようとするエージェントの証明書に指定されたサーバー名と一致する必要があります。	はい
--server-cert-path	サーバーピア証明書へのパス(--skip-certも指定した場合、このオプションを使用します)	-
--server-cert-password	サーバーピア証明書のパスワード	-
--agent-cert-password	エージェントピア証明書のパスワード	-
--cert-auth-password	認証機関のパスワード	-
--cert-auth-path	サーバーの認証機関ファイルへのパス	-
--cert-auth-common-name	認証機関の共通名(""を使用します)	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	証明書の有効期間の日数または年数(引数--cert-validity-unitで指定)	-

属性	説明	必要
--cert-validity-unit	証明書有効期間の単位。使用可能な値は「年」または「日」になります。(既定値ではYearsです)	-
--ad-server	Active Directoryサーバー	-
--ad-user-name	ADネットワークの検索ができる権限を保有するユーザー名	-
--ad-user-password	Active Directoryのユーザーパスワード	-
--ad-cdn-include	同期されるActive Directoryツリーのパス。ツリー全体を同期するには、空の括弧""を使用します。	-
--enable-imp-program	製品改善プログラムをオンにします。	-
--disable-imp-program	製品改善プログラムをオフにします。	-

ESETは、コマンドライン履歴から機密データ(パスワードなど)を含むコマンドを削除することをお勧めします。
1.historyを実行すると、履歴のすべてのコマンドの一覧を表示します。
2.history -d line_numberを実行(コマンドの行番号を指定)します。あるいは、history -cを実行し、コマンドライン履歴全体を削除します。

4.インストール手順では、製品改善プログラムに参加するかどうかが確認されます。クラッシュレポートやテレメトリデータをESETに送信することに同意する場合は**Y**を押します。データを送信しない場合は、**N**を押します。

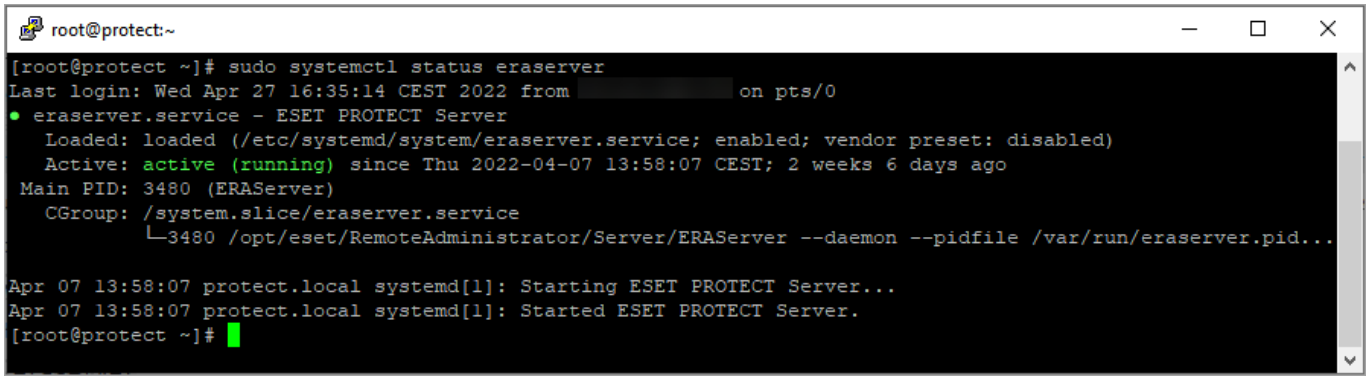
5. ESET PROTECTサーバーおよび eraserverサービスは、次の場所にインストールされます。

/opt/eset/RemoteAdministrator/Server

インストールは、**SELinux policy... failure**で終了する場合があります。SELinuxを使用しない場合は無視できます。

6. インストール後に、以下のコマンドを使用して、ESET PROTECT Serverサービスが実行中であることを確認します。

```
sudo systemctl status eraserver
```



インストーラのログ

インストーラーのログファイルは、トラブルシューティングに役に立つ場合があり、こちらで確認することができます。

サーバー前提条件 - Linux

LinuxでESETPROTECTサーバーをインストールするには、次の前提条件を満たしていることを確認します。

- 有効なライセンスが必要です。
- サポートされているLinuxオペレーティングシステムが必要です。
- 必要なポートが開いていて使用可能である必要があります。ポートの一覧については、ここを参照してください。
- データベースサーバーがインストールされ、ルートアカウントで構成されている必要があります。ユーザーアカウントはインストール前に作成する必要はありません。インストーラーがアカウントを作成できます。 LinuxのMicrosoft SQL Serverはサポートされていません。ただし、LinuxのESET PROTECTサーバーをWindowsのMicrosoft SQL Serverに接続することができます。

ESET PROTECTサーバーは、大きいデータをBLOBデータベースに格納します。ESET PROTECT On-Premが正常に実行されるには、大きいパケットサイズを許可するようにMySQLを設定します。

- **ODBCドライバー** - ODBCドライバーはデータベースサーバー (My SQL)との接続を確立するために使用されます。
- ターミナルコマンドを使用して、サーバーインストールファイルを実行ファイルとして設定します。

```
chmod +x server-linux-x86_64.sh
```

- **最新バージョンのOpenSSL1.1.1**を使用することをお勧めします。ESET Managementエージェントは OpenSSL 3.xもサポートします。OpenSSL for Linuxのサポートされている最低バージョンは、openssl-1.0.1e-30です。1つのシステムに同時に複数のバージョンのOpenSSLをインストールすることができます。1つ以上のサポートされているバージョンがシステムに存在している必要があります。
  - o`openssl version`コマンドを使用して、現在の既定のバージョンを表示できます。
  - oシステムに存在するすべてのバージョンのOpenSSLを一覧表示できます。`sudo find / -iname *libcrypto.so*`コマンドを使用して、ファイル名の末尾の一覧を確認してください
  - o次のコマンドを使用して、Linuxクライアントが対応しているかどうかを確認できます。`openssl s_client -connect google.com:443 -tls1_2`

OpenSSL 3.xサポート
- ESET Managementエージェントは OpenSSL 3.xをサポートします。
- ESET PROTECTサーバ/MDMは OpenSSL 3.xをネイティブにサポートしていませんが、ESET PROTECT On-PremのOpenSSL 3.xサポートを有効にすることができます。

- **Xvfb** – グラフィカルインターフェイスを使用しないLinuxサーバーシステムでの適切なレポート印刷に必要です(レポートの生成)。
- **Xauth** – パッケージは**xvfb**と一緒にインストールされます。**xvfb**をインストールしない場合は、**xauth**をインストールする必要があります。
- **cifs-utils** - Windows OSへのエージェント展開で必要です。

- **Qt4 WebKitライブラリ** - PDFとPS形式でレポートを出力するために使用されます(バージョン5ではなく、4.8でなければなりません)。その他のすべてのQt4依存関係は自動的にインストールされます。パッケージがオペレーティングシステムリポジトリにない場合は、ターゲットコンピューターで自分でコンパイルするか、サードパーティのリポジトリ(EPELリポジトリなど)からインストールできます。CentOS 7手順Ubuntu 20.04手順

- **kinit + klist** - Kerberosは、ログイン時のドメインユーザー認証とActive Directory同期タスクで使用されますKerberosの設定(*/etc/krb5.conf*)が正しいことを確認しますESET PROTECT On-Prem は複数のドメインとの同期をサポートします。

- **ldapsearch** - AD同期タスクと認証で使用されます。

- **snmptrap** – 任意SNMPトラップを送信するために使用されますSNMPも構成が必要です。

- **SELinux develパッケージ** – 製品インストール中にSELinuxポリシーモジュールを構築するために使用されます。このパッケージは、SELinuxが有効なシステムでのみ必要です(CentOSRHEL)SELinuxは他のアプリケーションでの問題の原因になることがありますESET PROTECTサーバーでは必要ありません。

- **lshw** - ESET Managementエージェントがハードウェアインベントリを正しく報告できるように、クライアント/サーバーのLinuxコンピューターに`lshw`パッケージをインストールします。

次の表は、さまざまなLinuxディストリビューションについて、上記で説明した各パッケージの該当するターミナルコマンドを示します(`sudo`または`root`としてコマンドを実行します)。

パッケージ	Debian Ubuntuディストリビューション	CentOSおよびRed Hatディストリビューション
ODBCドライバー	ODBCインストールおよび構成を参照してください。	ODBCインストールおよび構成を参照してください。
OpenSSL	`apt-get install openssl`	`yum install openssl -y`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`

Qt4 WebKitライブラリ	`apt-get install libqtwebkit4`
	Ubuntu 20.04の手順を参照してください。
		Qt4 WebKitは、標準リポジトリCentOSではありません。次のパッケージをインストールします。
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		あるいは、Fedoraリポジトリからパッケージをインストールできます。

kinit + klist - 任意(Active Directoryサービスで必要)	`apt-get install krb5-user`	`yum install krb5-workstation`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`
SELinux devel パッケージ(任意ESET PROTECTサーバーでは不要SELinuxは他のアプリケーションでの問題の原因になることがあります。)	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`
samba (任意。リモート展開でのみ必要)	`apt-get install samba`	`yum install samba samba-winbind-clients`
lshw	`apt-get install -y lshw`	`yum install -y lshw`

エージェントインストール - Linux

前提条件

- **最新バージョンのOpenSSL1.1.1**を使用することをお勧めしますESET Managementエージェントは OpenSSL 3.xもサポートしますOpenSSL for Linuxのサポートされている最低バージョンは、openssl-1.0.1e-30です。1つのシステムに同時に複数のバージョンのOpenSSLをインストールすることができます。1つ以上のサポートされているバージョンがシステムに存在している必要があ

ります。

- `openssl version`コマンドを使用して、現在の既定のバージョンを表示できます。
- システムに存在するすべてのバージョンのOpenSSLを一覧表示できます。`sudo find / -iname *libcrypto.so*`コマンドを使用して、ファイル名の末尾の一覧を確認してください
- 次のコマンドを使用してLinuxクライアントが対応しているかどうかを確認できます。`openssl s_client -connect google.com:443 -tls1_2`

OpenSSL 3.xサポート

- ESET Managementエージェントは OpenSSL 3.xをサポートします。
- ESET PROTECTサーバ/MDMは OpenSSL 3.xをネイティブにサポートしていませんが、ESET PROTECT On-PremのOpenSSL 3.xサポートを有効にすることができます。

- ESET Managementエージェントがハードウェアインベントリを正しく報告できるように、クライアント/サーバーのLinuxコンピューターに`lshw`パッケージをインストールします。

Linuxディストリビューション	ターミナルコマンド
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- Linux CentOSの場合、`policycoreutils-devel`パッケージをインストールすることをお勧めします。パッケージをインストールするコマンドを実行します。

```
yum install policycoreutils-devel
```

- サーバー支援エージェントインストール:
  - サーバーコンピューターはネットワークから接続可能で、ESET PROTECTサーバーとESET PROTECT Webコンソールがインストールされている必要があります。
- オフラインエージェントインストール:
  - サーバーコンピューターはネットワークから接続可能で、ESET PROTECTサーバーがインストールされている必要があります。
  - エージェントの証明書が存在する必要があります。
  - サーバー認証機関公開鍵が存在する必要があります。

インストール

ターミナルコマンドを使用してLinuxにESET Managementエージェントコンポーネントをインストールするには、次の手順に従います。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. エージェントインストールスクリプトをダウンロードします。

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. ファイルを実行可能にします。

```
chmod +x agent-linux-x86_64.sh
```

3. 次の例に従い、インストールスクリプトを実行します(コマンド全体を端末にコピーするために、「\」で区切って改行してあります)。

詳細については、次のパラメーターを参照してください。

サーバー支援インストール:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

オフラインインストール:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

ESETは、コマンドライン履歴から機密データ(パスワードなど)を含むコマンドを削除することをお勧めします。
1.`history`を実行すると、履歴のすべてのコマンドの一覧を表示します。
2.`history -d line_number`を実行(コマンドの行番号を指定)します。あるいは、`history -c`を実行し、コマンドライン履歴全体を削除します。

4. メッセージが表示されたら、**y**を押して、証明書を承諾します。インストーラーによって返されたSELinuxのエラーは無視できます。

5. インストール後、ESET Managementエージェントサービスが実行中であることを確認します。

```
sudo systemctl status eraagent
```

6. 起動時に開始する**eraagent**サービスを設定します。`sudo systemctl enable eraagent`

インストーラのログ
インストーラーのログファイルは、トラブルシューティングに役に立つ場合があります。インストーラーのログは、ログファイルにあります。

パラメータ

ESET PROTECTサーバーへの接続は、パラメータ--hostnameと--portを使用して解決されます(SRVレコードが指定されるときにはポートは使用されません)。使用可能な接続形式:.

- **ホスト名とポート**
- **IPv4アドレスとポート**
- **IPv6アドレスとポート**
- サービスレコード(SRVレコード)-LinuxでDNSリソースレコードを構成するには、コンピューターが、稼動中のDNSサーバーがあるドメインになければなりません。DNSリソースレコードを参照してください。SRVレコードの先頭は、プレフィックス_NAME._tcpでなければなりません。NAMEはカスタム名(eraなど)を表します。

属性	説明	必要
--hostname	接続するESET PROTECTサーバーのホスト名またはIPアドレス	はい
--port	ESET PROTECT ()サーバーポート(既定値は2222)	はい
--cert-path	エージェント証明書ファイルへのローカルパス(証明書)	はい(オフライン)
--cert-auth-path	サーバーの認証機関ファイルへのパス(認証)	はい(オフライン)
--cert-password	エージェント証明書パスワード。	はい(オフライン)
--cert-auth-password	認証機関のパスワード。	はい(使用されている場合)
--skip-license	インストールでは、ライセンス契約の確認をユーザーに要求しません	いいえ
--cert-content	サーバーとエージェントとの安全な通信チャネルを設定するために使用されるPKCS12暗号化公開鍵証明書と秘密鍵のBase64暗号化内容。--cert-path または--cert-contentオプションのいずれかだけを使用します。	いいえ
--cert-auth-content	リモートピア(プロキシまたはサーバー)を検証するために使用されるDER暗号化認証機関秘密鍵のBase64暗号化内容。--cert-auth-path または--cert-auth-contentオプションのいずれかだけを使用します。	いいえ
--webconsole-hostname	サーバーに接続するためにWebコンソールによって使用されるホスト名またはIPアドレス(空の場合は、値が「hostname」からコピーされます)	いいえ
--webconsole-port	サーバーに接続するWebコンソールが使用するポート(既定値は2223)	いいえ
--webconsole-user	サーバーに接続するWebコンソールが使用するユーザー名(既定値はAdministrator) サーバー支援インストールでは、二要素認証のユーザーを使用できません。	いいえ
--webconsole-password	サーバーに接続するためにWebコンソールによって使用されるパスワード	はい(サーバー支援)
--proxy-hostname	HTTPプロキシホスト名。このパラメーターを使用してESET Managementエージェントと ESET PROTECTサーバー(アップデートのキャッシュ用ではない)の間のレプリケーションのために、既にネットワークにインストールされているHTTPプロキシの使用を有効にします。	プロキシが使用される場合
--proxy-port	サーバーに接続するためのHTTPプロキシポート。	プロキシが使用される場合
--enable-imp-program	製品改善プログラムをオンにします。	いいえ
--disable-imp-program	製品改善プログラムをオフにします。	いいえ

接続と証明書

- **ESET PROTECTサーバーへの接続**を指定する必要があります。--hostname, --port (サーバーレコードが提供される場合は、ポートは不要です。既定のポート値は2222)

- サーバー支援インストールのために**次の接続情報を提供します。** --webconsole-port, --webconsole-user, --webconsole-password

- オフラインインストールのための**証明書情報を指定します。** --cert-path, --cert-passwordインストールパラメーター--cert-pathおよび --cert-auth-pathにはESET PROTECT Webコンソールからエクスポートできる証明書ファイル(*.pfx*および*.der*)が必要です。(.pfxファイルと.derファイルをエクスポートする方法をお読みください)

パスワードタイプパラメータ

パスワードタイプパラメータは`stdin`から読み取られる環境変数のファイルとして指定できます。あるいは、プレーンテキストとして指定できます。つまり次のとおりです。

`--password=env:SECRET_PASSWORD` `SECRET_PASSWORD`はパスワードの環境変数です。

`--password=file:/opt/secret` 標準ファイル`/opt/secret`の最初の行にパスワードが含まれます。

`--password=stdin` 標準入力からパスワードを読み取るようにインストーラに指示します。

`--password="pass:PASSWORD"` は`--password="PASSWORD"`と同じです。実際のパスワードが`"stdin"`(標準入力)または`"env:"` `"file:"` `"pass:"`で始まる文字列の場合に必須です。

証明書パスフレーズには、次の文字を含めることはできません:" \ これらの文字は、エージェントの初期化中に重大なエラーが発生する原因となります。

HTTPプロキシ構成

(アップデートのキャッシュではなく)ESET Managementエージェントと ESET PROTECTサーバーとの間のレプリケーションでHTTPプロキシを使用する場合は、`--proxy-hostname`と`--proxy-port`で接続パラメーターを指定できます。

例 - HTTPプロキシ接続があるオフラインエージェントインストール

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

エージェントと ESET PROTECTサーバー間の通信プロトコルは、認証をサポートしません ESET PROTECTサーバーへのエージェント通信の転送で使用されるプロキシソリューションと必要な認証は動作しません。
Webコンソールまたはエージェントで既定以外のポートを使用する場合は、ファイアウォールの調整が必要になることがあります。そうでない場合、インストールが失敗する可能性があります。

Linuxでのエージェントのインストールのアップグレードと修復

エージェントが既にインストールされているシステムで手動でエージェントインストールを実行する場合は、次のシナリオが発生する可能性があります。

- **アップグレード** – 新しいバージョンのインストーラーを実行します。

  oサーバー支援インストール – アプリケーションはアップグレードされますが、前の証明書を使用し続けます。

  oオフラインインストール – アプリケーションはアップグレードされますが、新しい証明書が使用されます。

- **修復** – 同じバージョンのインストーラーを実行します。このオプションを使用して、エージェントを別のESET PROTECTサーバーに移行できます。

  oサーバー支援インストール – アプリケーションが再インストールされESET PROTECTサーバーから現在の証明書を取得します(`hostname` パラメーターで定義)。

  oオフラインインストール – アプリケーションが再インストールされ、新しい証明書が使用されます。

古いサーバーから別の新しいESET PROTECTサーバーに手動でエージェントを移行し、サーバー支援インストールを使用している場合は、インストールコマンドを2回実行します。最初にエージェントがアップグレードされ、2回目に新しい証明書が取得されるため、エージェントはESET PROTECTサーバーに接続できます。

Webコンソールインストール - Linux

次の手順に従いESET PROTECT Webコンソールをインストールします。

ESET PROTECTサーバーがインストールされているコンピューター以外のコンピューターでESET PROTECT Webコンソールをインストールすることを選択できます。 この手順には、追加のステップが必要です。

1. Apache TomcatおよびJavaパッケージをインストールします。

次のサンプルパッケージ名は、ご使用のLinuxディストリビューションリポジトリパッケージとは異なる場合がありますLinuxディストリビューションの既定のリポジトリには、サポートされている最新バーンのApache TomcatとJavaが含まれていない場合があります。

Linuxディストリビューション	ターミナルコマンド
DebianとUbuntuディストリビューション	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOSとRed Hatディストリビューション	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. Webコンソールファイル(*era.war*)をダウンロードします。

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. *era.war*ファイルをTomcatフォルダーにコピーします。

Debian, Ubuntu	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, Red Hat	`sudo cp era.war /var/lib/tomcat/webapps/`
SUSE Linux Enterprise Server	`sudo cp era.war /usr/share/tomcat/webapps/`

4. Tomcatサービスを再起動し、*era.war*ファイルを展開します。

Debian, Ubuntu	`sudo systemctl restart tomcat9`
CentOS, Red Hat	`sudo systemctl restart tomcat`
SUSE Linux Enterprise Server	`sudo systemctl restart tomcat`

5. *era*フォルダーがTomcatフォルダーにあることを確認します。

Debian, Ubuntu	`ls /var/lib/tomcat9/webapps`
CentOS, Red Hat	`ls /var/lib/tomcat/webapps`
SUSE Linux Enterprise Server	`ls /usr/share/tomcat/webapps`

出力は次のように表示されます。`era era.war`

6. 起動時に開始するTomcatサービスを設定します。`sudo systemctl enable tomcat`（サービス名によっては、`tomcat9`)

7. ESET PROTECTサーバー以外のコンピューターでESET PROTECT Webコンソールをインストールした場合、これらの追加手順を実行し、ESET PROTECT Webコンソールと ESET PROTECTサーバー間の通信を有効にします。

a)Tomcatサービスを停止します。`sudo systemctl stop tomcat`

b)*EraWebServerConfig.properties* ファイルを編集します:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

EraWebServerConfig.properties ファイルが上記のパスにない場合は、次のコマンドを使用して、祠宇ステム宇のファイルを検索します。

```
find / -iname "EraWebServerConfig.properties"
```

c)`server_address=localhost`を見つけます

d)`localhost`をESET PROTECTサーバーのIPアドレスにし、ファイルを保存します。

e)Tomcatサービスを再起動します。`sudo systemctl restart tomcat`（サービス名によっては`tomcat9`)

f)起動時に開始するTomcatサービスを設定します。`sudo systemctl enable tomcat`（サービス

名によっては、tomcat9)

8. サポートされているWebブラウザーでESET PROTECT Webコンソールを開きます。ログイン画面が表示されます。

- ESET PROTECT Webコンソールをホストするコンピューターから次のコマンドを実行します。*http://localhost:8080/era*

- ESET PROTECT Webコンソールにインターネットに接続している任意のコンピューターから次のコマンドを実行します(*IP_ADDRESS_OR_HOSTNAME*をESET PROTECT WebコンソールのIPアドレスまたはホスト名に置き換える)。*http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. インストール後にWebコンソールを設定します。

- Apache Tomcatの手動インストール中に、既定のHTTPポートは8080に設定されます。 Apache TomcatのHTTPS接続を設定することをお勧めします。

- エンタープライズソリューションまたは低パフォーマンス システムの追加のWebコンソール設定も参照してください。

rogue detection sensorインストール - Linux

前提条件

- ネットワークが検索可能である(ポートが開き、ファイアウォールが受信通信をブロックしていないなど)。

- ESET PROTECTサーバーコンピューターに接続可能です。

- すべてのプログラム機能を完全にサポートするには、ESET Managementエージェントをローカルコンピュータにインストールする必要があります。

複数のネットワークセグメントがある場合Rogue Detection Sensorを各ネットワークセグメントに個別にインストールし、ネットワーク全体のすべてのデバイスの包括的なリストを生成する必要があります。

インストール

ターミナルコマンドを使用してLinuxにRD Sensorコンポーネントをインストールするには、次の手順に従います。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESET PROTECTダウンロードセクションにアクセスし、このESET PROTECTコンポーネントのスタンドアロンインストーラーをダウンロードします。(*rdsensor-linux-i386.sh*または*rdsensor-linux-x86_64.sh*)

2. RD Sensorインストールファイルを実行ファイルとして設定します。`chmod +x rdsensor-linux-x86_64.sh`

3. 次のコマンドを使用してsudoとしてインストールファイルを実行します。

```
sudo ./rdsensor-linux-x86_64.sh
```

4. エンドユーザーライセンス契約を読みます。**スペースバー**を使用してEULAの次のページに進みます。
契約に同意するかどうかを指定するように指示されます。同意する場合はキーボードの**Y**を押し。そうでない場合は、**N**を押します。

5. 製品改善プログラムに参加する場合は**Y**を押します。そうでない場合は、**N**を押します。

6. ESET Rogue Detection Sensorは、インストールが完了した後に起動します。

7. インストールが成功したかどうかを確認するには、サーバーが次のコマンドを実行して実行中であることを確認します。

```
sudo systemctl status rdsensor
```

ログファイルにはRogue Detection Sensorログファイルがあります:
/var/log/eset/RogueDetectionSensor/trace.log

モバイルデバイスコネクターインストール - Linux

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

モバイルデバイスコネクターはESET PROTECTサーバーが実行されているサーバーとは別のサーバーにインストールできます。たとえば、このインストールシナリオを使用し、インターネットからMobile Device Connectorにアクセスできるようにして、常にユーザーのモバイルデバイスを管理することができます。

ターミナルコマンドを使用してLinuxにMobile Device Connectorコンポーネントをインストールするには、次の手順に従います。

すべてのインストール前提条件を満たしていることを確認します。

1. Mobile Device Connectorインストールスクリプトをダウンロードします。

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. 次の例に従い、インストールスクリプトを実行します(コマンド全体を端末にコピーするために、「\」で区切って改行してあります)。

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
```

```
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

使用可能なパラメータヘルプメッセージの出力)の一覧については、次のものを使用してください。

```
--help
```

ESETは、コマンドライン履歴から機密データ(パスワードなど)を含むコマンドを削除することをお勧めします。
1.`history`を実行すると、履歴のすべてのコマンドの一覧を表示します。
2.`history -d line_number`を実行(コマンドの行番号を指定)します。あるいは、`history -c`を実行し、コマンドライン履歴全体を削除します。

必要なインストールコマンドパラメーター

さまざまな任意のインストールパラメータがありますが、一部は必須です。

- ピア証明書 - ESET PROTECT On-Premピア証明書を取得するには、2つの方法があります。

  • **サーバー支援インストール** - ESET PROTECT Webコンソール管理者の認証情報を指定する必要があります(必要な証明書はインストーラーによって自動的にダウンロードされます)。

  • **オフラインインストール** – ピア証明書(ESET PROTECT On-Premからエクスポートされたプロキシ証明書)を指定する必要があります。あるいは、カスタム証明書を使用できます。

  o**サーバー支援インストール**の場合、少なくとも次のパラメータを指定する必要があります。

  ```
  --webconsole-password=
  ```

  o**オフラインインストール**の場合、次のパラメータを指定する必要があります。

  ```
  --cert-path=
  --cert-password=
  ```

(ESET PROTECTはサーバーインストール中に作成された既定のエージェント証明書にはパスワードが必要ありません。)

- HTTPS (プロキシ)証明書:

  oHTTPS証明書がある場合

  ```
  --https-cert-path=
  --https-cert-password=
  ```

  o新しいHTTPS証明書を生成するには

```
--https-cert-generate
--mdm-hostname=
```

- ESET PROTECTサーバーへの接続(名前またはIPアドレス):

```
--hostname=
```

- データベース接続:

  oMySQLデータベースの場合、次のパラメータを指定する必要があります。

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

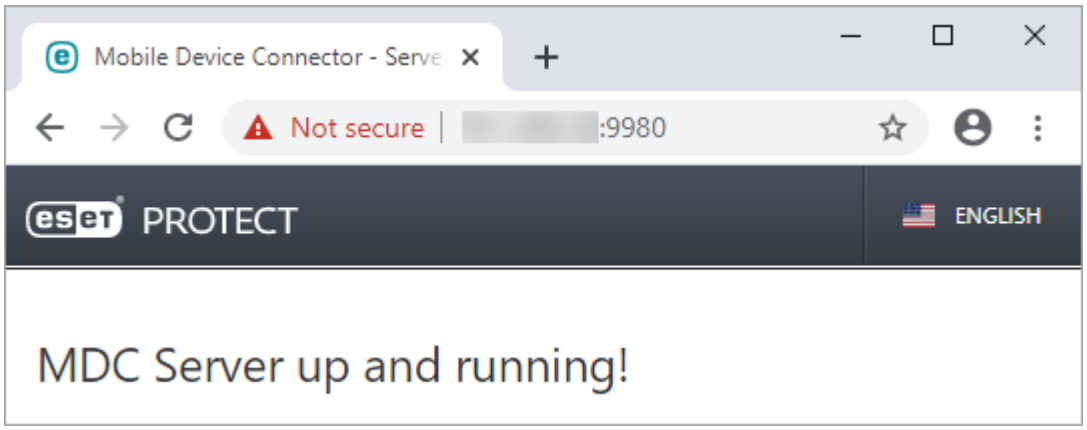
  oMicrosoft SQLデータベースの場合、次の情報を指定する必要があります。

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

インストーラのログ

インストーラーのログファイルは、トラブルシューティングに役に立つ場合があり、こちらで確認することができます。

インストールが完了したら、*https://your-mdm-hostname:enrollment-port* (*https://eramdm:9980*など)をブラウザで開き、モバイルデバイスコネクターが実行中であるかどうかを確認してください。インストールが成功したら、次のメッセージが表示されます。



また、モバイルデバイスからこのURLにアクセスすると、インターネットからモバイルデバイスコネクターサーバーの可用性を確認できます(このように構成されている場合)。ページを表示できない場合は、ファイアウォールとネットワークインフラストラクチャの構成を確認してください。

モバイルデバイスコネクター前提条件 - Linux

Linuxにモバイルデバイスコネクターをインストールするには、次の要件を満たす必要があります。

- ルートアカウントを使用してデータベースサーバーがインストールおよび構成済みである(インストーラで作成できるため、インストール前にユーザーアカウントを作成する必要はありません)。
- コンピュータにインストールされているデータベースサーバー(MySQL / Microsoft SQL)への接続のためのODBCドライバ。ODBCインストールおよび設定の章を参照してください。

MDCが問題なくMySQLに接続できるように、`unixODBC_23`パッケージ(既定の`unixODBC`ではない)を使用してください。これは特にSUSE Linuxの場合に当てはまります。

ESET PROTECTサーバーがホストされているデバイスとは別のホストデバイスにMDMコンポーネントを展開することをお勧めします。

- MDMCoreインストールファイルが実行ファイルとして設定されている。

```
chmod +x mdmcore-linux-x86_64.sh
```

- インストール後、MDMCoreサービスが実行されていることを確認します。

```
sudo systemctl status eramdmcore
```

- **最新バージョンのOpenSSL1.1.1**を使用することをお勧めします。ESET Managementエージェントは OpenSSL 3.xもサポートします。OpenSSL for Linuxのサポートされている最低バージョンは、openssl-1.0.1e-30です。1つのシステムに同時に複数のバージョンのOpenSSLをインストールすることができます。1つ以上のサポートされているバージョンがシステムに存在している必要があります。

  o`openssl version`コマンドを使用して、現在の既定のバージョンを表示できます。

  oシステムに存在するすべてのバージョンのOpenSSLを一覧表示できます。`sudo find / -iname *libcrypto.so*`コマンドを使用して、ファイル名の末尾の一覧を確認してください

  o次のコマンドを使用してLinuxクライアントが対応しているかどうかを確認できます。`openssl s_client -connect google.com:443 -tls1_2`

OpenSSL 3.xサポート

- ESET Managementエージェントは OpenSSL 3.xをサポートします。
- ESET PROTECTサーバ/MDMは OpenSSL 3.xをネイティブにサポートしていませんが、ESET PROTECT On-PremのOpenSSL 3.xサポートを有効にすることができます。

MySQLのMDMデータベースが大きすぎる場合(数千台のデバイス)、既定の`innodb_buffer_pool_size`値が小さすぎます。詳細なデータベースの最適化については、次を参照してください。https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

証明書要件

• HTTPS上の安全な通信のため、*.pfx*形式の**SSL証明書**が必要です。第三者の認証局(CA)が提供した証明書を使用することをお勧めします。一部のモバイルデバイスでは、ユーザーが自己署名証明書を許可しないため、自己署名証明書(ESET PROTECT On-Prem CAが署名した証明書を含む)は推奨されません。

• CAが署名した証明書、対応する秘密鍵が必要です。また、標準手順を利用して、これら(従来はOpenSSLを使用)を1つの *.pfx*ファイルに統合する必要があります。
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
これはSSL証明書を使用するほとんどのサーバーの標準の手順です。

• オフラインインストールの場合ESET PROTECT On-Premからエクスポートされたピア証明書(**エージェント証明書**)も必要です。あるいはESET PROTECT On-Premではカスタム証明書を使用できます。

ミラーツール - Linux

Windowsユーザーの場合

ミラーツールは、オフライン検出エンジンアップデートで必要です。クライアントコンピューターがインターネットに接続せず、検出エンジンアップデートが必要な場合、ミラーツールを使用してESETアップデートサーバーからアップデートファイルをダウンロードし、ローカルに保存できます。

ミラーツールには次の機能があります。
• モジュールアップデート— 検出エンジンアップデートおよび他のプログラムモジュールをダウンロードしますが、自動アップデート(uPCU)はダウンロードしません。
• リポジトリ作成 — 自動アップデート(uPCU)を含む完全オフラインリポジトリを作成できます。
ミラーツールはESET LiveGrid®データをダウンロードしません。

前提条件

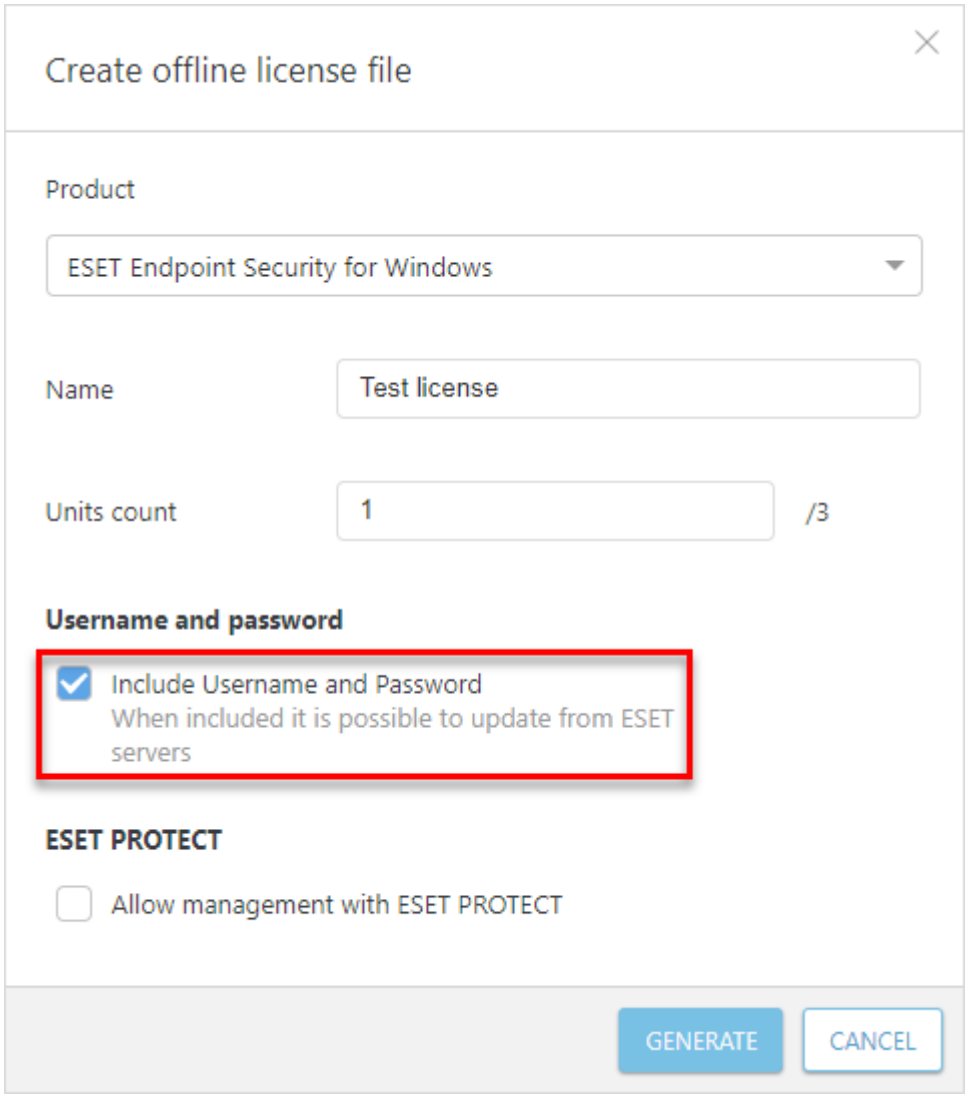
• ミラーが作成されるリポジトリには、すべてのユーザーの読み取りおよび実行権限が必要です。権限を付与するには、特権ユーザーで`chmod 755 mirror/folder/path`コマンドを実行します(`mirror/folder/path`はミラーフォルダーパスで置換)。

• アップデートをアクセス可能にする方法に応じて、ターゲットフォルダは共有、Samba/Windows、またはHTTP/FTPサービスに対応している必要があります。

OESETセキュリティ製品(Windows版) - HTTPまたは共有フォルダーを使用して、リモートでアップデートできます。

OESETセキュリティ製品(Linux/macOS版) - HTTPのみを使用してリモートでアップデートできます。共有フォルダーを使用する場合は、ESETセキュリティ製品と同じコンピューターにインストールする必要があります。

• ユーザー名とパスワードを含む有効なオフラインライセンスファイルが必要です。ライセンスファイルを生成するときには、[**ユーザー名とパスワードを含む**]の横のチェックボックスをオンにします。また、ライセンス**名**を入力する必要があります。ミラーツールのアクティベーションとアップデートミラーの生成には、オフラインライセンスファイルが必要です。



ミラーツールの使用方法

1.ESETダウンロードページ(**スタンドアロンインストーラー**)からミラーツールをダウンロードします。

2.ダウンロードしたフォルダーを解凍します。

3.*MirrorTool*ファイルが格納されたフォルダーでターミナルを開き、ファイルを実行可能にします。

```
chmod +x MirrorTool
```

4.次のコマンドを実行すると、ミラーツールで使用可能なすべてのパラメーターとそのバージョンが表示されます。

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

すべてのフィルターは大文字と小文字を区別します。

パラメーターを使用して、リポジトリミラーまたはモジュールミラーを作成できます。

リポジトリとモジュールミラーの両方のパラメーター

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

リポジトリ固有のパラメーター

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

モジュール固有のパラメーター

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

パラメータ	説明
--updateServer	Mirror Toolは、エンドポイントミラーが作成するフォルダー構造とは異なるフォルダー構造を作成します。各フォルダーには、製品のグループのアップデートファイルが格納されます。 ⚠ ミラーを使用する製品のアップデート設定で、アップデートサーバーの完全リンク(正しいフォルダーへの完全パス)を指定する必要があります。
--offlineLicenseFilename	オフラインライセンスファイルへのパス(前述のとおり)を指定する必要があります。

パラメータ	説明
--mirrorOnlyLevelUpdates	引数は不要です。設定すると、レベルアップデートのみがダウンロードされます(ナノアップデートはダウンロードされません)。アップデートの種類の詳細については、ナレッジベース記事をお読みください。
--mirrorFileFormat	⚠ --mirrorFileFormatパラメーターを使用する前に、環境に古い(6.5以降)バージョンと新しいバージョン(6.6. 以降)の両方のESETセキュリティ製品が含まれていないことを確認してください。このパラメーターの使用が正しくないとESETセキュリティ製品が誤って更新される可能性があります。 ダウンロードするアップデートファイルの種類を指定できます。指定可能な値(大文字と小文字を区別): • dat - ESETセキュリティ製品バージョン6.5以前のみの環境では、この値を使用します。 • dll - ESETセキュリティ製品バージョン6.6以降のみの環境では、この値を使用します。 レガシー製品(ep4ep5)のミラーを作成する場合、このパラメーターは無視されます。
--compatibilityVersion	この任意のパラメーターは、ESET PROTECT On-Prem8.1以降で配布されるミラーツールに適用されます。 ミラーツールは、x.xまたはx.x.x.xの形式でパラメーター引数で指定したESET PROTECT On-Premリポジトリバージョンと互換性のあるアップデートファイルをダウンロードします(例: --compatibilityVersion 11.0または--compatibilityVersion 8.1.13.0)。 --compatibilityVersionパラメーターは自動アップデート(uPCU)をミラーから除外します。環境内で自動アップデート(uPCU)が必要で、ミラーサイズを小さくする場合は、--filterFilePathパラメーターを使用します。

ℹ ESETリポジトリからダウンロードされるデータの量を減らすにはESET PROTECT On-Prem 9で配布されるミラーツールの新しいパラメーターである--filterFilePathと--dryRunを使用することをお勧めします。
1.*JSON*形式でフィルターを作成します(以下の--filterFilePathを参照)。
2.--dryRunパラメーター(以下を参照)でミラーツールのテストを実行し、必要に応じてフィルターを調整します。
3.--filterFilePathパラメーター、定義されたダウンロードフィルター、--intermediateRepositoryDirectoryパラメーター、--outputRepositoryDirectoryパラメーターを使用して、ミラーツールを実行します。
4.ミラーツールを定期的に実行し、最新のインストーラーを常に使用してください。

パラメータ	説明

--filterFilePath	この任意のパラメーターを使用して、ミラーツールと同じフォルダーに配置された*JSON*形式のテキストファイルに基づいてESETセキュリティ製品をフィルタリングします(例: --filterFilePath filter.txt)
	フィルター設定の説明:
	製品フィルタリングの設定ファイル形式は次の構造の*JSON*です。
	• ルート*JSON*オブジェクト:
	ouse_legacy (ブール値、任意) - trueの場合は、レガシー製品が含まれます。
	odefaults (*JSON*オブジェクト、任意) – すべての製品に適用されるフィルタープロパティを定義します。
	■languages (リスト) – フランス語タイプの"fr_FR"など、含める言語のISO言語コードを指定します。他の言語コードは以下の表を参照してください。その他の言語を追加するには、カンマとスペースで区切ります。例: (["en_US", "zh_TW", "de_DE"])
	■platforms (リスト) – 含めるプラットフォーム(["x64", "x86", "arm64"])
	⚠ platformsフィルターは注意して使用してください。たとえば、ミラーツールが64ビットのインストーラーのみをダウンロードし、インフラストラクチャに32ビットコンピューターがある場合、64ビットのESETセキュリティ製品は32ビットコンピューターにインストールされません。
	■os_types (リスト) – 含めるOSタイプ(["windows"]["linux"]["mac"])
	oproducts (JSONオブジェクトのリスト、任意) – 特定の製品に適用するフィルター – 指定された製品defaultsを上書き。オブジェクトには次のプロパティがあります。
	■app_id (文字列) – nameが指定されていない場合は必須。
	■name (文字列) – app_idが指定されていない場合は必須。
	■version (文字列) – 含めるバージョンまたはバージョンの範囲を指定します。
	■languages (リスト) – 含める言語のISO言語コード(以下の表を参照)
	■platforms (リスト) – 含めるプラットフォーム(["x64", "x86", "arm64"])
	■os_types (リスト) – 含めるOSタイプ(["windows"]["linux"]["mac"])
	ℹ フィールドの適切な値を決定するには、管理者実行モードでミラーツールを実行し、作成されたCSVファイルで該当する製品を検索します。
	バージョン文字列形式の説明
	すべてのバージョン番号はドットで区切られた4つの数字で構成されています(例: 7.1.0.0)。バージョンフィルター(例: 7.1)を書き込むときにはそれよりも小さい数値を指定できます。残りの数字は 0 (7.1は7.1.0.0と同じ)になります。
	バージョン文字列には次の2つの形式のいずれかを使用できます。
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	o指定したバージョン以下/以下のバージョンを選択します。
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	o下限以上および上限以下のバージョンを選択します。
	比較は、バージョン番号の各部分で、左から右に数字で実行されます。
	JSONの例
	✓
	{
	"use_legacy": true,
	"defaults": {
	"languages": ["en_US"],
	"platforms": ["x64", "x86"]
	},
	"products": [
	{
	"app_id": "com.eset.apps.business.ees.windows",
	"version": "7.1.0.0–8.0.0.0"
	},
	{
	"app_id": "com.eset.apps.business.eea.windows",
	"version": ">7.1.0.0"
	}
	]
	}
	--filterFilePathパラメーターは、古いミラーツールバージョン(ESET PROTECT On-Prem 8.xでリリース済みの製品)で使用されているツールを使用するときには、languageFilterおよびproductFilterパラメーターがサポートされません。

--dryRun	ダウンロードされるすべてのリポジトリを置換えはせず出力した*.csv*ファイルが生成されます。 必須パラメーターの--intermediateRepositoryDirectoryと--outputRepositoryDirectoryを使用せずにこのパラメーターを使用できます(例:)。 • Windows: MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv • Linux: sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv ℹ 一部のESETインストーラーは言語に汎用的です(multilang言語コードを使用)。ミラーツールは、--filterFilePathで言語を指定する場合でも*.csv*ファイルに一覧表示されます。 --dryRunパラメーターのほかに、--intermediateRepositoryDirectoryおよび--outputRepositoryDirectoryパラメーターも使用する場合、ミラーツールは*outputRepositoryDirectory*を消去しません。
--listUpdatableProducts	(--excludedProductsが使用されていない場合は)Mirror ToolがモジュールのアップデートをダウンロードできるESET製品がすべて一覧表示されます。 パラメーターは次のバージョンのMirror Toolから使用できます。1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Mirror Toolのフォルダー構造

既定では、`--updateServer`パラメーターを指定しない場合、MirrorToolはHTTPサーバーでこのフォルダー構造を作成します。

HTTP専用ミラーサーバーを使用しない

ローカルミラーサーバーがHTTPおよびHTTPSプロトコル、またはHTTPSのみを使用していることを確認します。ミラーサーバーがHTTPのみを使用する場合は、ESETセキュリティ製品のエンドユーザーライセンス契約をHTTPサーバーから取得できないため、ソフトウェアインストールクライアントタスクを使用できません。

Mirror Toolの既定のフォルダー	ESETセキュリティ製品	アップデートサーバー(HTTPサーバールートの場所による)
mirror/eset_upd/era6	ESET PROTECT On-Prem (すべてのバージョン)	ミラーからESET PROTECT On-Prem11.0をアップデートするには、アップデートサーバーを*http://your_server_address/mirror/eset_upd/era6*に設定します。
mirror/eset_upd/ep[バージョン]	ESET Endpoint Antivirus/Securityバージョン6.x（以降)(Windows)各メジャーバージョンには、フォルダーがあります。例：バージョン10.xの*ep10*	*http://your_server_address/mirror/eset_upd/ep10*（バージョン10.xの例）
mirror/eset_upd/v5	ESET Endpoint Antivirus/Securityバージョン5.x (Windows)	*http://your_server_address/mirror/eset_upd/v5*

ESETセキュリティ製品ポリシーLinux/macOS

`--updateServer`パラメーターを指定し、追加のフォルダーを作成してHTTPミラーからLinux/macOS版のESETセキュリティ製品をアップデートする必要があります(以下を参照)。

--updateServer	追加のMirror Toolフォルダー	ESETセキュリティ製品	アップデートサーバー(HTTPサーバールートの場所による)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus for Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security for Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Securityバージョン7.x+(macOS)	*http://your_server_address/mirror/eset_upd/BusinessMac*
http://update.eset.com/eset_mobile/eesa	*mirror/eset_upd/*EndpointAndroid	ESET Endpoint Security for Android	*http://your_server_address/mirror/eset_upd/EndpointAndroid*

言語コード表

ミラーを作成するには、少なくとも必須パラメーターを指定してミラーツールを実行します。次に例を示します。

```
sudo ./MirrorTool --mirrorType regular \

--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \

--offlineLicenseFilename /tmp/mirrorTool/offline.lf \

--outputDirectory /tmp/mirrorTool/mirror
```

次に、製品、言語が選択され、*filter.txt*ファイルで定義されたレガシーファイルのダウンロードが有効になっている、オフラインのリポジトリの高度な設定の例です(上記の`--filterFilePath`の詳細のファイル内容の例を参照)。

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \

--intermediateRepositoryDirectory /tmp/repoTemp \

--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \

--filterFilePath filter.txt
```

ESETは、コマンドライン履歴から機密データ(パスワードなど)を含むコマンドを削除することをお勧めします。
1.`history`を実行すると、履歴のすべてのコマンドの一覧を表示します。
2.`history -d line_number`を実行(コマンドの行番号を指定)します。あるいは、`history -c`を実行し、コマンドライン履歴全体を削除します。

ミラーツールとアップデート設定

- モジュールアップデートのダウンロードを自動化するには、ミラーツールを実行するスケジュールを作成できます。このためにはWebコンソールを開き、**[クライアントタスク] > [オペレーティングシステム] > [コマンドの実行]に移動します。 実行するコマンドライン** (*MirrorTool.exe*へのパスを含む)と合理的なトリガー(毎時0 0 * * * ?*のCRONなど)を選択します。*). あるいはWindowsタスクスケジューラまたはLinuxの`Cron`を使用できます。

- クライアントコンピューターでアップデートを構成するには、新しいポリシーを作成し、**アップデートサーバー**を構成してミラーアドレスまたは共有フォルダを参照します。

macOSでのコンポーネントインストール

ほとんどのインストールシナリオでは、コンピューターによって異なるESET PROTECTコンポーネントをインストールし、さまざまなネットワークアーキテクチャに対応し、パフォーマンス要件やその他の要求に対応する必要があります。

MacOSはクライアント専用としてサポートされています。ESET Managementエージェントと ESET製品(macOS版) はmacOSにインストールできます。ただしESETPROTECTサーバーはmacOSにインストールできません。

エージェントインストール- macOS

次の2つの方法で、macOSでESET Managementエージェントをインストールできます。

- リモート – サーバータスク**エージェント展開**を使用しますESET Managementエージェントのリモート展開で問題が発生する(サーバータスク**エージェント展開**が失敗ステータスで終了する)場合は、エージェント展開のトラブルシューティングを参照してください。
- ローカル – 以下の手順を参照してください。

前提条件

- ESET PROTECTサーバーおよびESET PROTECT Webコンソールがサーバーコンピュータ上にインストールされている。
- エージェントの証明書の作成およびローカルドライブ上に準備されていること。
- 認証局 がローカルドライブに準備されていること(未署名でのみ必要)。

インストール

次の手順に従い、macOSでESET Managementエージェントコンポーネントをローカルでインストールします。

上記のすべてのインストール前提条件を満たしていることを確認します。

1. ESETダウンロードサイトまたはシステム管理者からインストールファイル(*.dmg*)を取得します。
2. *Agent-MacOSX-x86_64.dmg*ファイルをダブルクリックしてから、*.pkg*ファイルをダブルクリックしてインストールを開始します。
3. インストールを続行します。確認メッセージが表示された場合、**サーバー接続**データを入力します。
   - **サーバーホスト名**: ESET PROTECTサーバーのホスト名またはIPアドレス
   - **サーバーポート**: エージェントのポート – サーバー通信。既定値は2222です。
   - **プロキシを使用する**: エージェント用HTTPプロキシ – サーバー接続を使用する場合はクリックします。

このプロキシ設定は、ESET Managementエージェントと ESET PROTECTサーバーの間のレプリケーションでのみ使用され、アップデートのキャッシュには使用されません。
• **プロキシホスト名**: HTTPプロキシコンピュータのホスト名またはIPアドレス。
• **プロキシポート**: 既定値は3128です。
• **ユーザー名パスワード**: 認証を使用する場合は、プロキシによって使用される認証資格情報を入力します。
ポリシーで後からプロキシ設定を変更できます。プロキシ経由のエージェントとサーバー間の接続を設定する前に、プロキシをインストールする必要があります。

4. ピア証明書とそのパスワードを選択します。必要に応じて、認証機関を追加できます。

証明書パスフレーズには、次の文字を含めることはできません: " \ これらの文字は、エージェントの初期化中に重大なエラーが発生する原因となります。

5. インストール先を確認し、[**インストール**]をクリックします。エージェントがお使いのコンピューターにインストールされます。

6. ESET Managementエージェントのフルディスクアクセスを有効にする:

ローカル:

a)**システム設定** > **セキュリティとプライバシー** > **プライバシー**を開きます。

b)左下の設定をロック解除します。

c)**フルディスクアクセス**をクリックします。

d)**+** > **アプリケーション** > **ESET** > **開く**をクリックし、ESET Managementエージェントを**フルディスクアクセス**フォルダーのアプリケーションリストに追加します。

e)左下の設定をロックします。

リモート:

a).plist設定ファイルをダウンロードします。

b)任意のUUID生成ツールを使用して、2つのUUIDを生成します。テキストエディターを使用して、文字列をテキストで置換します。ダウンロードした設定プロファイルにUUID 1およびUUID 2を挿入します。

c)MDMサーバーを使用して.plist設定プロファイルファイルを展開します。設定プロファイルをコンピューターに展開するには、コンピューターがMDMサーバーに登録されている必要があります。

7. エージェントがインストールされているコンピューターがESET PROTECT Webコンソールに表示されESET PROTECT On-Premを使用して管理できます。

エージェントインストールのトラブルシューティング

エージェントが実行中であることを確認します。**実行** > **ユーティリティ**クリックし、**アクティビティモニター**をダブルクリックします。**エネルギー**タブまたは**CPU**タブをクリックして、**ERAAgent**プロセスを見つけます。

ESET Managementエージェントログファイルは次の場所にあります。

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

エージェントとESET PROTECTサーバー間の通信プロトコルは、認証をサポートしません。ESET PROTECTサーバーへのエージェント通信の転送で使用されるプロキシソリューションと必要な認証は動作しません。
Webコンソールまたはエージェントで既定以外のポートを使用する場合は、ファイアウォールの調整が必要になることがあります。そうでない場合、インストールが失敗する可能性があります。

ISOイメージ

ISOイメージファイルは、ESET PROTECTインストーラをダウンロード(オールインワンインストーラカテゴリ)できる形式の1つです。ISOイメージには次のものが含まれています。

- ESET PROTECTインストーラーパッケージ
- 各コンポーネントの個別のインストーラ

すべてのESET PROTECTインストーラを1つの場所に保持する場合は、ISOイメージが便利です。また、インストールを実行するたびにESET Webサイトからインストーラをダウンロードする必要がありません。仮想マシンにESET PROTECT On-Premをインストールするときにはは、ISOイメージが便利です。

DNSサービスレコード

DNSリソースレコードを設定する手順

1.DNSサーバー(ドメインコントローラのDNSサーバー)で、**[コントロールパネル]** > **[管理ツール]**に移動します。

2.DNS値を選択します。

3.DNSマネージャで、ツリーから_tcpを選択し、新しい**サービスロケーション(SRV)**レコードを作成します。

4.DNS標準ルールに従い、**[サービス]**フィールドにサービス名を入力します。サービス名の前にはアンダースコア(_)を入力します(**_era**などの独自のサービス名を使用)。

5.**[プロコトル]**フィールドには次の形式で_tcpプロコトルを入力します。

6.**[ポート番号]**フィールドにはポート2222を入力します。

7.**[このサービスを提供するホスト]** フィールドにはESET PROTECTサーバーの完全修飾ドメイン名(FQDN)を入力します。

8.**OK** > **完了**をクリックして、レコードを保存します。レコードがリストに表示されます。

DNSレコードを検証する手順

1.ドメインの任意のコンピューターにログインし、コマンドプロンプト(cmd.exe)を開きます。

2. コマンドプロンプトに`nslookup`と入力し、**Enter**を押します。

3. `set querytype=srv`と入力し、**Enter**を押します。

4. `_era._tcp.domain.name`と入力し、**Enter**を押します。サービスロケーションが正しく表示されます。

異なるコンピュータでESET PROTECTサーバーをインストールするときには、必ず[このサービスを提供するホスト]を新しいサーバーのFQDNの値に変更してください。

ESET PROTECT On-Premのオフラインインストールシナリオ

インターネットに接続されていない環境でESET PROTECT On-Premとそのコンポーネントをインストールするには(ESET PROTECT On-PremがWindowsでインストールされている)ハイレベルのインストール手順に従います。

インターネットに接続しているコンピューターで

1. 共有ネットワークフォルダーを作成します。

2. 次のインストーラーを共有フォルダーにダウンロードします。

- ESET PROTECT オールインワンインストーラー
- サポートされているJDKパッケージ (Webコンソールに必要)。
- ESET Managementエージェントインストーラー
- ESETセキュリティ製品インストーラー(例: ESET Endpoint Security)

同じローカルネットワークのオフラインWindowsコンピューター

1. ネットワーク共有フォルダーからESET PROTECT On-Premをインストールするオフライン Windowsコンピューターにインストーラーをコピーします。

2. JDKパッケージをインストールします。

3. オールインワンインストーラーを使用してWindowsでESET PROTECT On-Premをインストールします。インストール中に**後でアクティベーション**を選択します。

4. オフラインライセンスでESET PROTECT On-Premをアクティベーションします。

5. エージェントインストーラースクリプトを使用してオフライン環境のコンピューターにESET Managementエージェントを展開します。共有ネットワークフォルダーからエージェントインストールパッケージにアクセスするには、インストールスクリプトを修正して、新しいURLを使用します。

6. ソフトウェアインストールタスクを使用してESETセキュリティ製品製品をワークステーションに展開します。**<Choose package>**を選択し、ローカルリポジトリからインストールパッケージのカスタムURLを入力します。

7. オフラインライセンスを使用して、管理されたエンドポイントをアクティベーションします。

8. ESET LiveGrid®を無効にします。

ローカルアップデートリポジトリを使用して、オフラインESETインフラストラクチャを最新の状態に保つことを強くお勧めします。ESETセキュリティ製品モジュールは定期的にアップデートしてください。モジュールがアップデートされない場合、コンピューターは**未アップデート**としてESET PROTECT Webコンソールでフラグが付きます。このWebコンソール警告をミュートするには、リストのコンピューターをクリックし、コンテキストメニューから**ミュート**を選択します。

ESET PROTECT On-Premのアップグレード手順については、オフライン環境でのESET PROTECTコンポーネントのアップグレードを参照してください。

アップグレード手順

以下ではESET PROTECTサーバーと他のESET PROTECTコンポーネントのアップグレードのためのさまざまな手順について説明します。移行および再インストール手順も参照してください。

ESET PROTECT On-Prem 11.0にアップグレードする前に、サポートされているオペレーティングシステムが実行されていることを確認してください。
アップグレードする前にESET PROTECTデータベースをバックアップすることをお勧めします。
古いサポートされていないデータベース(MySQL 5.5またはMicrosoft SQL 2008/2012)がインストールされている場合ESET PROTECTサーバーをアップグレードする前に、データベースを互換性があるデータベースバージョンにアップグレードしてください。

アップグレードERA 5.x/6.5 または ESMC 7.x

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。

ERA 5.x/6.xまたはESMC 7.0/7.1をお持ちの場合ESET PROTECT On-Prem11.0への直接アップグレードはサポートされていませんESET PROTECT On-Prem11.0のクリーンインストールを実行してください。

前のバージョンのESET PROTECT On-PremからESET PROTECT On-Prem 11.0へアップグレード

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。

アップグレード手順のいずれかを選択します。

アップグレード手順	OS	コメント
Web コンソールのコンポーネントアップグレードタスク	Windows/Linux	
ESET PROTECT On-Prem 11.0オールインワンインストーラー	Windows	既存のインストールがオールインワンインストーラーで実行された(Microsoft SQLデータベースApache Tomcatの既定のインストールがある)場合は、オールインワンインストーラーによるアップグレードが推奨されるオプションです。
手動コンポーネントベースアップグレード	Linux	上級ユーザー向けLinux手順。
ESET PROTECT仮想アプライアンスのアップグレード	Linux(仮想アプライアンス)	

実行中の各ESET PROTECTコンポーネントのバージョンを検索するにはESET PROTECTサーバーバージョンを確認しますESET PROTECT Webコンソールのバージョン情報ページに移動し、すべてのESET PROTECTコンポーネントバージョンの一覧を確認します。

ESET PROTECTコンポーネントアップグレードタスク

アップグレード前の推奨事項

ESET PROTECT Webコンソールで使用可能なESET PROTECTコンポーネントアップグレードタスクを使用してESET PROTECTインフラストラクチャをアップグレードすることをお勧めします。アップグレードする前に、ここで手順をよく確認してください。

コンポーネントアップグレードがESET PROTECTサーバーまたはWebコンソールを実行するコンピューターで失敗した場合は、リモートでWebコンソールにログインできない場合があります。このアップグレードを実行する前に、サーバーコンピューターへの物理アクセスを構成することをお勧めします。コンピューターへの物理アクセスを設定できない場合は、リモートデスクトップを使用して、管理者権限でログインできることを確認します。この操作を実行する前に、ESET PROTECTサーバーとMobile Device Connectorデータベースをバックアップすることをお勧めします。仮想アプライアンスをバックアップするには、スナップショットを作成するか、仮想マシンのクローンを作成します。

以前のESET PROTECT仮想アプライアンスからアップグレードしますか?

ESET PROTECTサーバーインスタンスがフェールオーバークラスタにインストールされている

ESET PROTECTサーバーインスタンスがフェールオーバークラスタにインストールされている場合は、各クラスタノードで手動でESET PROTECTサーバーコンポーネントをアップグレードする必要があります。ESET PROTECTサーバーをアップグレードした後は、コンポーネントアップグレードタスクを実行して、残りのインフラストラクチャ(クライアントコンピューターのESET Managementエージェントなど)をアップグレードできます。

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。

ESET PROTECT On-Premは、新しいバージョンのESET PROTECTサーバーが利用可能になると自動的に通知します。

アップグレードを実行する前に、次のデータをバックアップします。

- すべての証明書(認証局、サーバー証明書、プロキシおよびエージェント証明書)
- 既存のESET PROTECTサーバーの認証局証明書を*.der*ファイルにエクスポートし、外部ストレージに保存します。
- 古いESET Managementサーバーのピア証明書(ESET PROTECTエージェントの場合はESET PROTECTサーバー)と秘密鍵*.pfx*ファイルをエクスポートし、外部ストレージに保存します。
- ESET PROTECTデータベース。 古いサポートされていないデータベース(MySQL 5.5またはMicrosoft SQL 2008/2012)がインストールされている場合、ESET PROTECTサーバーをアップグレードする前に、データベースを互換性があるデータベースバージョンにアップグレードしてください。

ESET PROTECT On-Prem 11.0にアップグレードする前に、サポートされているオペレーティングシステムが実行されていることを確認してください。

ESETセキュリティ製品をアップグレードするには、最新のインストーラーパッケージを使用してソフトウェアインストールタスクを実行し、既存の製品の上にインストールします。

推奨されるアップグレード手順

1. ESET PROTECTサーバー – **ESET PROTECTコンポーネントアップグレード**タスクの対象としてESET PROTECTサーバーがインストールされているコンピューターのみを選択します。

2. テストサンプルとして(各オペレーティングシステム/ビットカテゴリから1つ以上)、一部のクライアントコンピューターを選択し、**ESET PROTECTコンポーネントアップグレード**タスクを実行します。

ネットワーク負荷を制限するには、ESET Bridge HTTPプロキシ（またはキャッシュが有効な別の透過Webプロキシ)を使用することをお勧めします。テストクライアントコンピューターはインストーラーのダウンロード/キャッシュをトリガーします。タスクをもう一度実行するときには、インストーラーがキャッシュから直接クライアントコンピューターに配布されます。

3. ESET Managementエージェントがアップグレードされたコンピューターが正常にESET PROTECTサーバーに接続した後、残りのクライアントのアップグレードに進みます。

ネットワークのすべての管理されたコンピューターでESETManagementエージェントをアップグレードするには、**ESET PROTECTコンポーネントアップグレード**タスクの対象として、静的グループ**すべて**を選択します。このタスクは、既に最新のESET Managementエージェントを実行しているコンピューターをスキップします。
ESET PROTECT On-Premは、管理されたコンピューターのESET Managementエージェントの自動アップグレードをサポートします。

自動的にアップグレードされたコンポーネント:

- ESET PROTECTサーバー
- ESET Managementエージェント
- ESET PROTECT Webコンソール - Apache TomcatがWindowsおよびLinuxディストリビューションの既定のインストールフォルダーにインストールされているときにのみ該当します(ESET PROTECT仮想アプライアンス(例: */var/lib/tomcat8/webapps/*、*/var/lib/tomcat7/webapps/*、*/var/lib/tomcat/webapps/*)を含む)。

Webコンソールアップグレードの制限事項

- Apache Tomcatは、ESET PROTECT Webコンソールアップグレード中に、コンポーネントアップグレードタスクによってアップグレードされません。
- ESET PROTECT Webコンソールアップグレードは、Apache Tomcatがカスタマイズされた場所にインストールされている場合には動作しません。
- Apache Tomcatのカスタムバージョンがインストールされている場合(Tomcatサービスの手動インストール)、後からオールインワンインストーラーまたはコンポーネントのアップグレードタスクを使用してESET PROTECT Webコンソールをアップグレードすることはできません。

- ESET PROTECT Mobile Device Connector

手動アップグレードが必要なコンポーネント:

ESETコンポーネント

- ESET Rogue Detection Sensor – アップグレードでソフトウェアインストールタスクを使用します。あるいは、最新のバージョンを前のバージョンの上にインストールしてアップグレードします(WindowsまたはLinuxのインストール手順に従ってください)。前のバージョンのESET PROTECT On-PremでRDSensorをインストールした場合は、新しいRDSensorリリースがないため、アップグレードする必要はありません。

サードパーティーコンポーネント

ESET PROTECT On-PremではESETコンポーネントの他に、手動アップデートが必要なサードパーティコンポーネントを使用しています。

ESET PROTECT Webコンソールで、**クイックリンク > サーバーコンポーネント**をクリックすると、新しいバージョンが利用可能なサードパーティコンポーネントが表示されます。

- すみやかに、最新バージョンのサードパーティコンポーネントをインストールすることをお勧めします。最新の使用可能なバージョンは、ESET PROTECTサーバーを実行するために使用されるオペレーティングシステムによって異なる場合があります。
- ESET PROTECT仮想アプライアンスは、サードパーティコンポーネントで使用可能なアップグレードを報告しません。

ESET PROTECT Webコンソールは、以下の一覧よりも前のバージョンをアップグレードすることを推奨します。

サードパーティーコンポーネント	バージョン:	注意:	アップグレード手順
Microsoft SQL Server	2019（ビルド 15.0.4335.1)	SQL Serverデータベースエンジンのバージョンとエディションを決定し、最新の累積的なアップデートをインストールします。	データベースサーバー
MySQL	8.0.0.0	ESET PROTECT Webコンソールで**ヘルプ > 情報**をクリックすると、インストールされているデータベースバージョンが表示されます。	データベースサーバー
OS	Windows Server 2016	ESET PROTECT On-PremはLinuxで使用可能なアップデートを報告しません。	OS
Apache Tomcat	9.0.82	インストールされているApache Tomcatバージョンを判別します。 • Windows - *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\RELEASE-NOTES*ファイルをテキストエディターで開き、バージョン番号を確認します。 • Linux - `tomcat version`ターミナルコマンドを実行します。	Apache Tomcat
Java	17.0	インストールされているJavaバージョンを判別します。 • Windows - コマンドプロンプトを開き、`java -version`コマンドを実行します。 • Linux - `java -version`ターミナルコマンドを実行します。	Java Runtime Environment
Apache HTTP Proxy	-	**Apache HTTP Proxyユーザー** ESET PROTECT On-Prem 10.0以降ではESET BridgeがApache HTTP Proxyに代わります。Apache HTTP Proxyは限定サポートに達しました。Apache HTTP Proxyを使用している場合は、ESET Bridgeへの移行をお勧めします。	ESET Bridgeへの移行

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

トラブルシューティング

- アップグレードされたコンピューターからESET PROTECT On-Premリポジトリにアクセスできるかどうかを確認します。

• 1つ以上のコンポーネントが既に新しいバージョンにアップグレードされている場合は、ESET PROTECTコンポーネントアップグレードタスクを再実行できません。

• ESET PROTECT Webコンソールが読み込めない場合、またはログイン中にエラーが表示される場合は、Webコンソールのトラブルシューティングを参照してください。

• アップグレードエラーの明確な理由がない場合は、コンポーネントを手動でアップグレードできます。WindowsまたはLinuxの手順を参照してください。

• アップグレードの問題を解決するためのその他の推奨事項については、一般的なトラブルシューティング情報を参照してください。

ESET PROTECT On-Prem11.0オールインインインストーラーを使用してアップグレード

ESET PROTECT On-Prem11.0オールインインインストーラーを使用して、前のバージョンのESET PROTECT On-Premを最新のESET PROTECT On-Prem11.0にアップグレードします。

既存のインストールがオールインワンインストーラーで実行された(Microsoft SQLデータベースApache Tomcatの既定のインストールがある)場合は、オールインワンインストーラーによるアップグレードが推奨されるオプションです。

ESET PROTECT On-Prem 11.0オールインワンインストーラーでは、既定でMicrosoft SQL Server Express 2019がインストールされます。

o古いWindowsエディション(サーバー2012またはSBS 2011)を使用している場合は、Microsoft SQL Server Express 2014が既定でインストールされます。

oインストーラーはデータベース認証(*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*に保存)のランダムなパスワードを自動的に生成します。

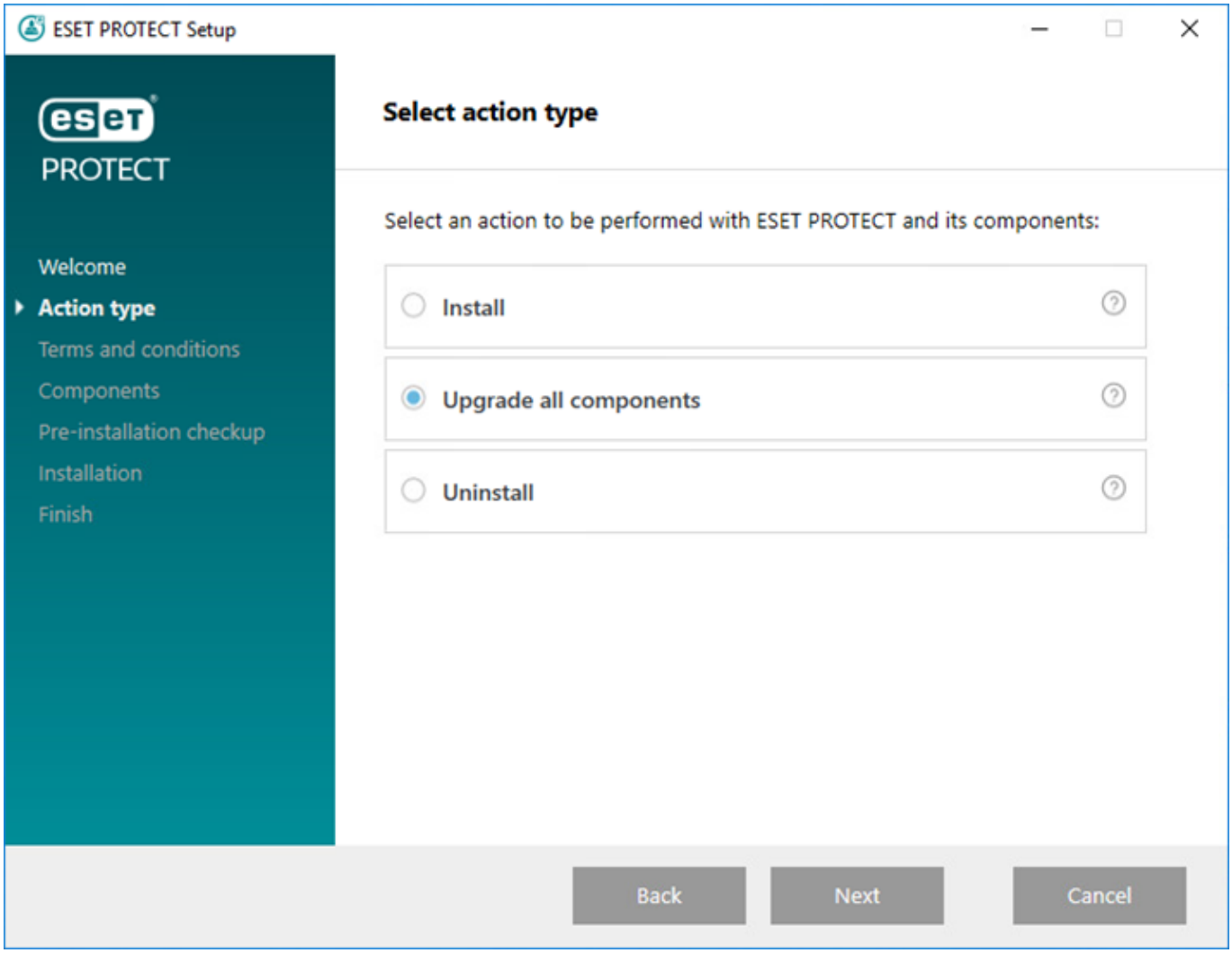
Microsoft SQL Server Expressには各関係データベース10 GBのサイズ制限があります。次の環境ではMicrosoft SQL Server Expressの使用は推奨されません。
- エンタープライズ環境または大規模ネットワーク。
- ESET PROTECT On-PremとESET Inspect On-Premを使用する場合。

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。
アップグレードを実行する前に、次のデータをバックアップします。
• すべての証明書(認証局、サーバー証明書、プロキシおよびエージェント証明書)
• 既存のESET PROTECTサーバーの認証局証明書を*.der*ファイルにエクスポートし、外部ストレージに保存します。
• 古いESET Managementサーバーのピア証明書(ESET PROTECTエージェントの場合はESET PROTECTサーバー)と秘密鍵*.pfx*ファイルをエクスポートし、外部ストレージに保存します。
• ESET PROTECTデータベース。 古いサポートされていないデータベース(MySQL 5.5またはMicrosoft SQL 2008/2012)がインストールされている場合ESET PROTECTサーバーをアップグレードする前に、データベースを互換性があるデータベースバージョンにアップグレードしてください。
ESET PROTECT On-Prem 11.0にアップグレードする前に、サポートされているオペレーティングシステムが実行されていることを確認してください。

1.*Setup.exe*を実行します。

2.言語を選択し、**次へ**をクリックします。

3.**すべてのコンポーネントをアップグレード**を選択し、**次へ**をクリックします。



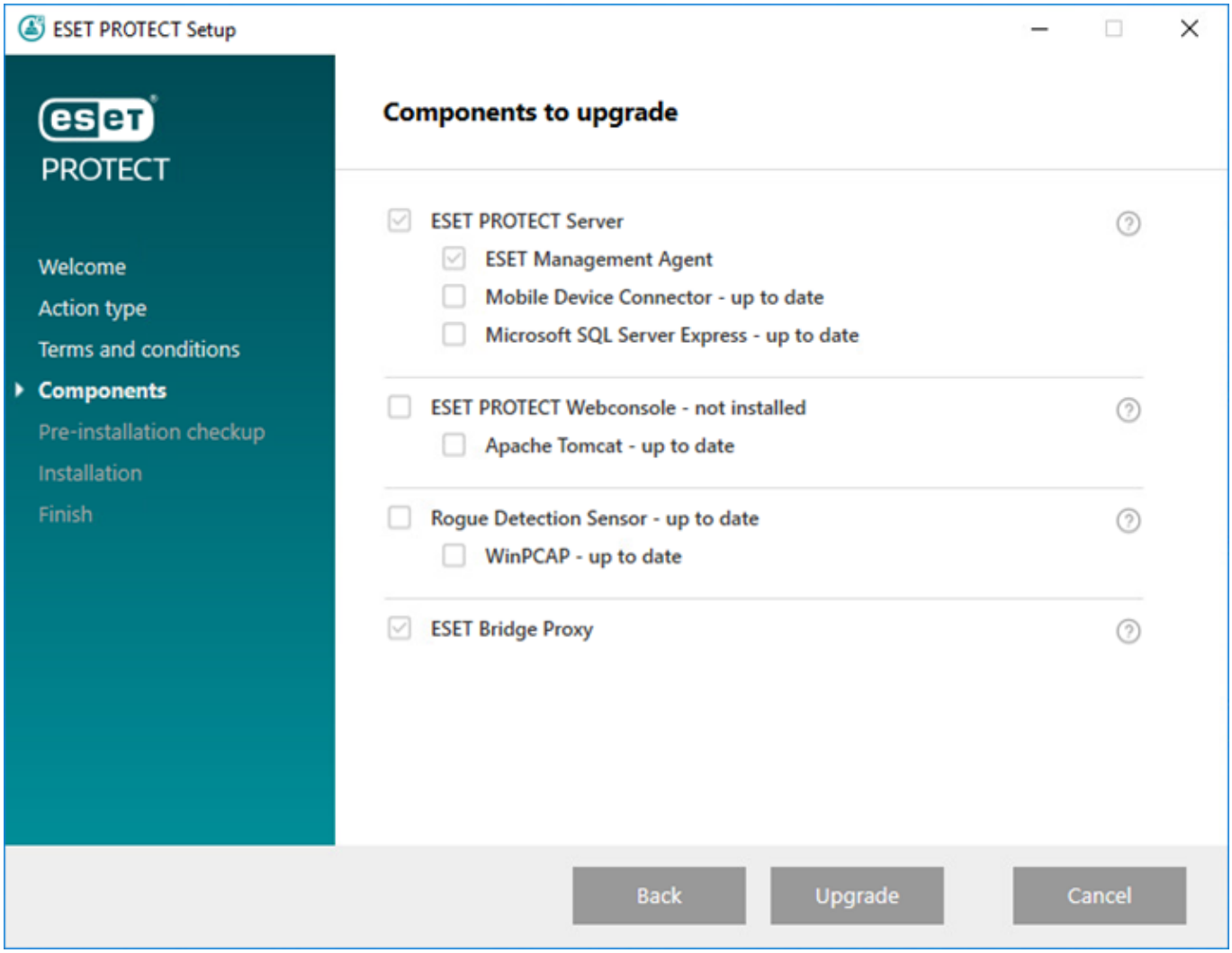
4.**エンドユーザーライセンス契約**を読んで、同意して、**次へ**をクリックします。

5.**コンポーネント**で、アップグレード可能なESETPROTECTコンポーネントを確認して、**次へ**をクリックします。

Apache TomcatおよびWebコンソールのアップグレードの制限事項

- Apache Tomcatのカスタムバージョンがインストールされている場合(Tomcatサービスの手動インストール)、後からオールインワンインストーラーまたはコンポーネントのアップグレードタスクを使用してESET PROTECT Webコンソールをアップグレードすることはできません。
- Apache Tomcatアップグレードは、次の場所にある*era*フォルダーを削除します。 *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\.era*フォルダーを使用して、追加のデータを保存する場合は、アップグレードする前に、必ずデータをバックアップしてください。
- *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps*に、*era*および*ROOT*フォルダー以外の追加データがある場合は、Apache Tomcatアップグレードが実行されずWebコンソールのみがアップグレードされます。
- Web コンソールとApache Tomcatアップグレードによって、オフラインヘルプファイルがクリアされます。古いバージョンのESET PROTECT On-Premのオフラインヘルプを使用していた場合は、アップグレード後にESET PROTECT On-Prem 11.0用に再作成して、最新のオフラインヘルプがESET PROTECT On-Premバージョンと一致するようにします。

Apache HTTP Proxyがインストールされ たWindowsコンピューターでオールインインワンインストーラーを実行する場合は、インストーラーで自動的にApache HTTP Proxyがアンインストールされ、代わりにESET Bridgeがインストールされます。



6.**インストール前チェック**に従い、システムがすべての前提条件を満たしていることを確認します。

7.**アップグレード**をクリックしてESET PROTECT On-Premアップグレードを開始します。システムとネットワーク構成によっては、アップグレードに時間がかかる場合があります。

8.アップグレードが完了したら、**完了**をクリックします。

ESET PROTECT Webコンソールが読み込めない場合、またはログイン中にエラーが表示される場合は、Webコンソールのトラブルシューティングを参照してください。

ESET PROTECT On-Premのアップグレード後、コンポーネントアップグレードタスクを使用して、管理されたコンピューターでESET Managementエージェントをアップグレードします。ESET PROTECT On-Premは、管理されたコンピューターのESET Managementエージェントの自動アップグレードをサポートします。

データベースサーバーバックアップ/アップグレード

ESET PROTECT On-Premはデータベースを使用して、クライアントデータを格納します。次のセクションではESET PROTECTサーバーデータベースまたはMDMデータベースのバックアップおよびアップグレードについて詳述します。

- ESET PROTECTサーバーで使用するためにデータベースを設定していない場合は、**Microsoft SQL Server Express**がインストーラーに含まれます。 ESET PROTECT On-Prem 11.0オールインワンインストーラーでは、既定でMicrosoft SQL Server Express 2019がインストールされます。

  o古いWindowsエディション(サーバー2012またはSBS 2011)を使用している場合は、Microsoft SQL Server Express 2014が既定でインストールされます。

  oインストーラーはデータベース認証(*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*に保存)のランダムなパスワードを自動的に生成します。

> Microsoft SQL Server Expressには各関係データベース10 GBのサイズ制限があります。次の環境ではMicrosoft SQL Server Expressの使用は推奨されません。
> - エンタープライズ環境または大規模ネットワーク。
> - ESET PROTECT On-PremとESET Inspect On-Premを使用する場合。

- 古いサポートされていないデータベース(MySQL 5.5またはMicrosoft SQL 2008/2012)がインストールされている場合ESET PROTECTサーバーをアップグレードする前に、データベースを互換性があるデータベースバージョンにアップグレードしてください。

ESET PROTECTデータベース移行も参照してください。

Microsoft SQL Serverに関する次の要件を満たす必要があります。

- サポートされているバージョンのMicrosoft SQL Serverをインストールします。インストール中に**混合モード**認証を選択します。

- Microsoft SQL Serverが既にインストールされている場合は、認証を**混合モード(SQL Server認証とWindows認証**に設定します。このためには、このナレッジベース記事の手順に従います。**Windows認証**を使用してMicrosoft SQL Serverにログインする場合は、このナレッジベース記事の手順に従います。

- SQL ServerへのTCP/IP接続を許可します。このためには、このナレッジベース記事の「**II.SQLデー**

タベースへのTCP/IP接続を許可する」の手順に従います。

- Microsoft SQL Server (データベースおよびユーザー) を設定、管理、監視するには、SQL Server Management Studio (SSMS)をダウンロードします。
- ドメインコントローラーにはSQL Serverをインストールしないでください (たとえばWindows SBS / Essentials)別のサーバーにESET PROTECT On-Premをインストールするか、インストール中にSQL Server Expressコンポーネントを選択しない (この場合、既存のSQL ServerまたはMySQLを使用してESET PROTECTデータベースを実行する必要があります) ことをお勧めします。

データベースサーバーバックアップと復元

すべてのESET PROTECT On-Prem情報と設定はデータベースに保存されます。データベースを定期的にバックアップし、データ損失を防止することをお勧めします。後からESET PROTECT On-Premを新しいサーバーに移行するときには、バックアップを使用できます。データベースについては、次の該当するセクションを参照してください。

- データベースとログファイルの名前は、製品名がESET Security Management CenterからESET PROTECT On-Premに変更された後でも同じままです。
- ESET PROTECT仮想アプライアンスを使用する場合は、VAデータベースバックアップ手順に従います。

Microsoft SQLバックアップの例

Microsoft SQLデータベースをファイルにバックアップするには、以下の例に従います。

これらの例は、既定の設定で使用することを意図しています (たとえば、既定のデータベース名とデータベース接続文字列)。既定の設定に行われた変更に対応するには、バックアップスクリプトをカスタマイズする必要があります。
次のコマンドを実行するための十分な権限が必要です。ローカル管理者ユーザーアカウントを使用していない場合は、バックアップパスを *'C:\USERS\PUBLIC\BACKUPFILE'* などに変更する必要があります。

1回限りのデータベースバックアップ

Windowsコマンドプロンプトでこのコマンドを実行し、ファイル**BACKUPFILE**にバックアップを作成します。

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

この例では、**HOST**はIPアドレスまたはホスト名を示し、**ERASQL**はMicrosoft SQLサーバーインスタンスの名前です。カスタム名のSQLインスタンスにESET PROTECTサーバーをインストールできます(Microsoft SQLデータベースを使用するとき)。このシナリオでバックアップスクリプトを修正します。

SQLスクリプトを使用した標準データベースバックアップ

次のSQLスクリプトのいずれかを選択します。

a)標準バックアップを作成し、作成日に基づいて保存します。

```
@ECHO OFF


SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"


REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)バックアップを1つのファイルに追加します。

```
@ECHO OFF


SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Microsoft SQL復元

Microsoft SQLデータベースをファイルから復元するには、以下の例に従います。

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

MySQLバックアップ

MySQLデータベースをファイルにバックアップするには、以下の例に従います。

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

この例では、**HOST**はMySQL ServerのIPアドレスまたはホスト名を示し、**ROOTLOGIN**はMySQL Serverのrootアカウント、**DBNAME**はESET PROTECTデータベース名を表します。

MySQL復元

MySQLデータベースをファイルから復元するには、以下の例に従います。

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

Microsoft SQL Serverバックアップの詳細については、Microsoft technet Webサイトをご覧ください。MySQL Serverバックアップの詳細については、MySQLドキュメントWebサイトをご覧ください。

データベースサーバーアップグレード

ESET PROTECTサーバーデータベースで使用するには、次の手順に従い、既存のデータベースサーバーインスタンスを新しいバージョンにアップグレードします。

1. アップグレードするデーターベースサーバーに接続しているすべての実行中のESET PROTECT Serverサービスを停止します。また、データベースサーバーインスタンスに接続している可能性があるその他のすべてのアプリケーションを停止します。

2. 続行する前のすべての該当するデータベースをバックアップします。

3. データベースサーバーのアップグレードを実行します。

SQL Server (Windows):

- Microsoft SQL Express データベースを最新バージョンにアップグレードするためのナレッジベース記事に従います。
- あるいは、データベースベンダーの手順に従います。https://msdn.microsoft.com/en-us/library/bb677622.aspx
- LinuxのMicrosoft SQL Serverはサポートされていません。ただし、LinuxのESET PROTECTサーバーをWindowsのMicrosoft SQL Serverに接続することができます。

MySQL Server (WindowsおよびLinux):

- MySQL 5.6からバージョン5.7へのアップグレード
- MySQL 5.7からバージョン8へのアップグレード

4. ESET PROTECT Serverサービスを開始し、トレースログを確認して、データベース接続が正常に動作していることを検証します。

Windowsでフェールオーバークラスタにインストールされた ESET PROTECT On-Premのアップグレード

Windowsのフェールオーバークラスタ環境にESET PROTECTをインストールし、最新のESET PROTECT On-Premにアップグレードする場合は、次の手順を実行します。

サポートされているオペレーティングシステムを確認してください。

1. Cluster ManagerでESET PROTECTサーバークラスターロールを停止します。サービス(**ESET Security Management Center Server**または**ESET PROTECT Server**)がすべてのクラスターノードで停止していることを確認します。

2. ノード1でオンラインのクラスター共有ディスクを取得し、最新の*.msi*インストーラーを実行して手動でサーバーコンポーネントをアップグレードします(コンポーネントインストールの場合)。

3. インストール(アップグレード)が完了した後に、**ESET PROTECT Server**サービスが停止していること

を確認します。

4. ノード2でオンラインのクラスター共有ディスクを取得し、手順2の方法でサーバーコンポーネントをアップグレードします。

5. ESET PROTECTサーバーがすべてのクラスターノードでアップグレードされたらCluster Managerで**ESET PROTECTサーバーロールを起動します**。

6. すべてのクラスターノードで最新の*.msi*インストーラーを実行し、ESET Managementエージェントを手動でアップグレードします。

7. ESET PROTECT Webコンソールで、すべてのノードのエージェントとサーバーバージョンがアップグレード先の最新バージョンを報告するかどうかを確認します。

Apache Tomcatのアップグレード

Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。

最新バージョンのESET PROTECT On-Premにアップグレードする場合、またはApache Tomcatを長期間アップグレードしていない場合は、Apache Tomcatを最新バージョンにアップグレードすることを検討してください。Apache Tomcatやその依存関係などの公開サービスを最新の状態に保つことで、環境へのセキュリティリスクを抑えることができます。

Apache Tomcatをアップグレードするには、次の手順に従います。

- Windows手順(最新のESET PROTECTのオールインインインストーラー) – 既存のApache Tomcatインストールがオールインワンインストーラーで実行された場合は、このアップグレードオプションが推奨されます。
- Windows手順(手動インストール) – 既存のApache Tomcatインストールを手動で実行したか、最新のESET PROTECTオールインワンインストーラーがない場合は、Apache Tomcatを手動でアップグレードします。
- Linux手順

オールインワンインストーラーを使用したApache Tomcatのアップグレード(Windows)

Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。 最新のESET PROTECT On-Prem11.0オールインワンインストーラーを使用してApache Tomcatをアップグレードするには、この方法を使用します。 既存のApache Tomcatインストールがオールインワンインストーラーで実行された場合は、このアップグレードオプションが推奨されます。 あるいは、手動でApache Tomcatをアップグレードできます。

アップグレード前の注意

次のファイルをバックアップします。

C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\conf\server.xml

C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

*Tomcat*フォルダーでカスタムSSL証明書ストアを使用している場合は、その証明書もバックアップします。

Apache TomcatおよびWebコンソールのアップグレードの制限事項

- Apache Tomcatのカスタムバージョンがインストールされている場合(Tomcatサービスの手動インストール)、後からオールインワンインストーラーまたはコンポーネントのアップグレードタスクを使用してESET PROTECT Webコンソールをアップグレードすることはできません。
- Apache Tomcatアップグレードは、次の場所にある*era*フォルダーを削除します。 *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\.era*フォルダーを使用して、追加のデータを保存する場合は、アップグレードする前に、必ずデータをバックアップしてください。
- *C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps*に、*era*および*ROOT*フォルダー以外の追加データがある場合は、Apache Tomcatアップグレードが実行されずWebコンソールのみがアップグレードされます。
- Web コンソールとApache Tomcatアップグレードによって、オフラインヘルプファイルがクリアされます。古いバージョンのESET PROTECT On-Premのオフラインヘルプを使用していた場合は、アップグレード後にESET PROTECT On-Prem 11.0用に再作成して、最新のオフラインヘルプがESET PROTECT On-Premバージョンと一致するようにします。

アップグレード手順

1. ESET WebサイトからESET PROTECTオールインワンインストーラーをダウンロードして、ダウンロードしたファイルを解凍します。

2. 最新バージョンのApache Tomcatをインストールする予定で、オールインワンインストーラーに古いバージョンのApache Tomcatが含まれている場合(この手順は任意です。最新バージョンのApache Tomcatが必要でない場合は手順4に進んでください):

   a.*x64*フォルダーを開き、*installers*フォルダーに移動します。

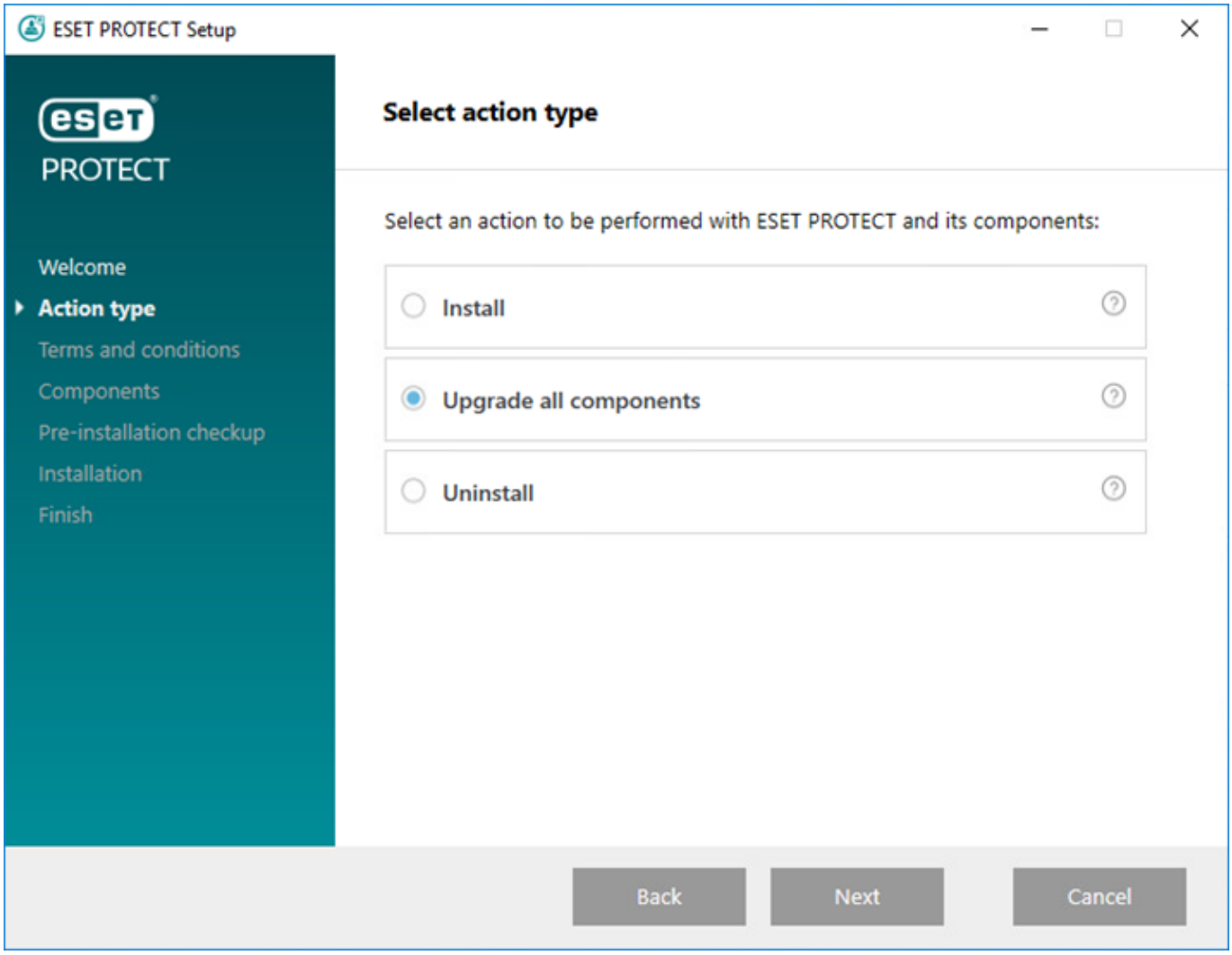
   b.*installers*フォルダーにある*apache-tomcat-9.0.x-windows-x64.zip*ファイルを削除します。

   c.Apache Tomcat 9 64ビットWindows zipパッケージをダウンロードします。

   d.ダウンロードしたzipパッケージを*installers*フォルダーに移動します。

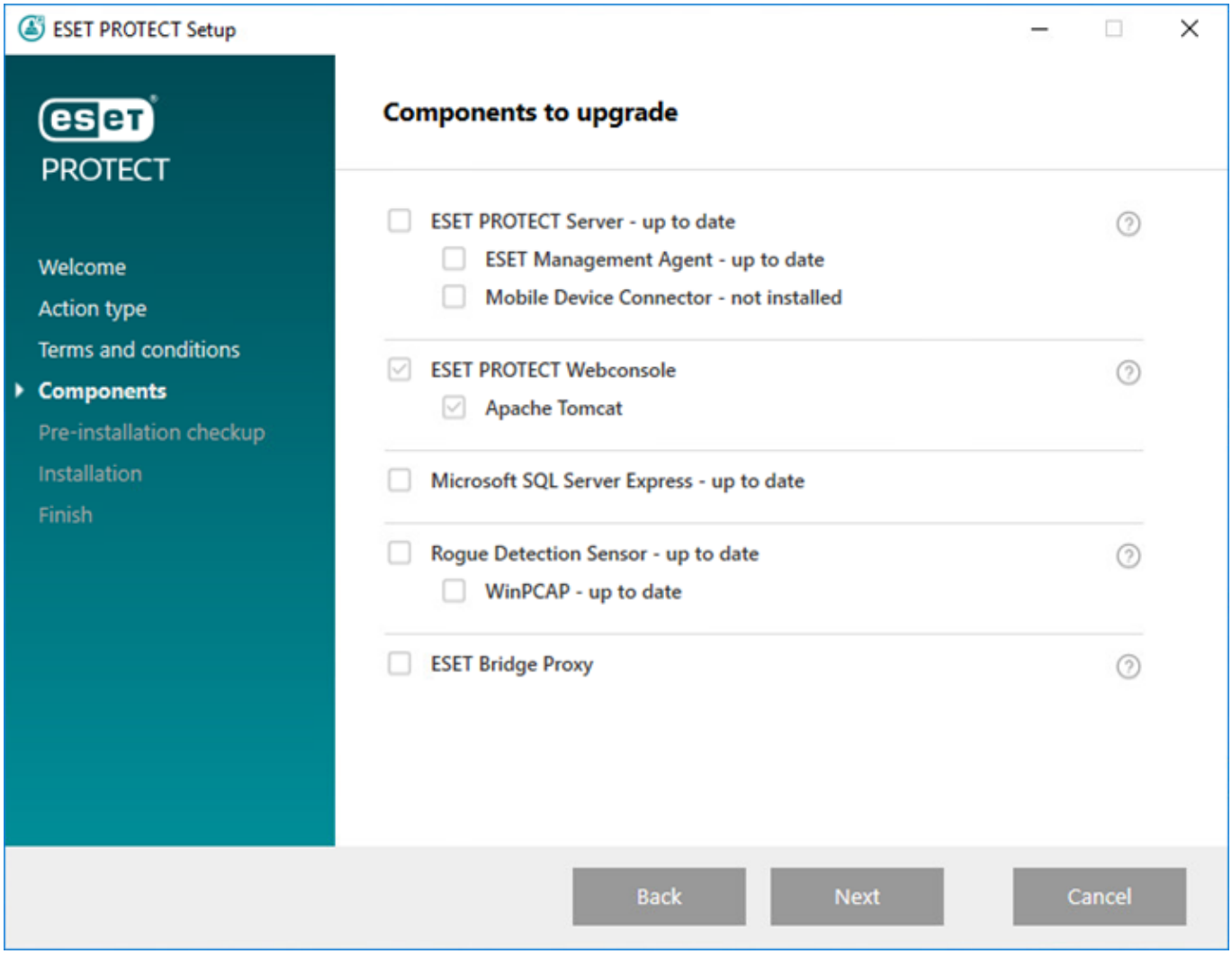
3. オールインワンインストーラーを起動するには、*Setup.exe*ファイルをダブルクリックし、**ようこそ**画面で**次へ**をクリックします。

4. **すべてのコンポーネントをアップグレード**を選択し、**次へ**をクリックします。



5. EULAに同意した後、[次へ]をクリックします。

6.オールインワンインストーラーは、アップグレードが利用可能かどうかを自動的に検出します。アップグレード可能なESET PROTECTコンポーネントの横にはチェックボックスがあります。**次へ**をクリックします。



7. コンピューターでJavaインストールを選択します。Apache Tomcatには64ビット版のJava/OpenJDKが必要です。 システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

8. **アップグレード**をクリックして、アップグレードを完了してから、**完了**をクリックします。

9. ESET PROTECTサーバー以外のコンピューターにWebコンソールをインストールした場合:

   a. Apache Tomcat サービスを停止します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**停止**を選択します。

   b.*EraWebServerConfig.properties*ファイル(手順1)を元の場所に復元します。

   c. Apache Tomcatサービスを起動します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**開始**を選択します。

10. ESET PROTECT Webコンソールに接続し、Webコンソールが正常に読み込まれることを確認します。

エンタープライズソリューションまたは低パフォーマンス ステムの追加のWebコンソール設定も参照してください。

トラブルシューティング

Apache Tomcatのアップグレードが失敗した場合は、Apache Tomcatをアンインストールしてから、もう一度インストールし、手順1から設定を適用します。

Apache Tomcatの手動アップグレード(Windows)

Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。 既存のApacheTomcatインストールを手動で実行したか、最新のESETPROTECTオールインワンインストーラーがない場合は、Apache Tomcatを手動でアップグレードします。

Apache Tomcatのカスタムバージョンがインストールされている場合(Tomcatサービスの手動インストール)、後からオールインワンインストーラーまたはコンポーネントのアップグレードタスクを使用して ESET PROTECT Webコンソールをアップグレードすることはできません。

アップグレード前の注意

- Apache Tomcatには64ビット版のJava/OpenJDKが必要です。 システムに複数のJavaバージョンがインストールされている場合は、前のJavaバージョンをアンインストールし、最新のサポートされているバージョンのJavaのみを保持することをお勧めします。

2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

- 現在使用中のApache Tomcatのバージョンを確認します。

  a.Apache Tomcatインストールフォルダーに移動します。
  C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]

  b.テキストエディターでRELEASE-NOTESファイルを開き、バージョン番号(9.0.34など)を確認します。

  c.新しいサポートされているバージョンがある場合は、アップグレードを実行します。

アップグレード手順

1. Apache Tomcat サービスを停止します。**スタート > サービス**に移動し、Apache Tomcatサービスを右クリックして、**停止**を選択します。

Windows通知領域で実行されている場合は、*Tomcat7w.exe*を閉じます。

2. 次のファイルをバックアップします。

   C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\.keystore
   C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\conf\server.xml
   C:\Program Files\Apache Software Foundation\[Tomcat フォルダ]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

*Tomcat*フォルダーでカスタムSSL証明書ストアを使用している場合は、その証明書もバックアップします。

3. 現在のバージョンのApache Tomcatをアンインストールします。

4. システムに存在している場合は、次のフォルダーを削除します。

C:\Program Files\Apache Software Foundation\[Tomcat フォルダー]

5. 最新のサポートされているバージョンのApache Tomcatインストーラーファイル(32-bit/64-bit Windows Service Installer) `apache-tomcat-[バージョン].exe`をhttp://tomcat.apache.orgからダウンロードします。

6. ダウンロードした新しいバージョンのApache Tomcatをインストールします:

- その他のJavaバージョンがインストールされている場合は、インストール中に最新のJavaへのパスを選択します。
- インストールが完了したら、**Apache Tomcatの実行**の横のチェックボックスをオフにします。

7. *.keystore*、*server.xml*、およびカスタム証明書を元の場所に復元します。

8. *server.xml*ファイルを開き、*keystoreFile*パスが正しくなっていることを確認します(上位のメジャーバージョンのApache Tomcatにアップグレードした場合は、パスを更新します)。

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat フォルダー]\.keystore"

9. ESET PROTECT Webコンソール用の[Apache TomcatのHTTPS接続](#)が正しく設定されていることを確認します。

10. ESET PROTECT Webコンソール(Webコンソールインストール - Windows)を展開します。

11. *EraWebServerConfig.properties* を元の場所に復元します。

12. Apache Tomcatを実行し、正しいJava VMを設定します。

a.フォルダーに移動 *C:\Program Files\Apache Software Foundation\[Tomcat フォルダー]\bin*フォルダーに移動し、*Tomcat9w.exe*を実行します。

b.**一般**タブで、**スタートアップの種類**を**自動**に設定し、**開始**をクリックします。

c.**Java**タブをクリックして、**既定を使用**をオフにします。**Java仮想マシン**に*jvm.dll*ファイルへのパスが含まれている(図解のナレッジベース手順を参照)ことを確認してから、**OK**をクリックします。

13. ESET PROTECT Webコンソールに接続し、Webコンソールが正常に読み込まれることを確認します。

> エンタープライズソリューションまたは低パフォーマンス ステムの追加のWebコンソール設定も参照してください。

トラブルシューティング

- Apache TomcatのHTTPS接続の設定が失敗した場合は、この手順をスキップし、一時的にHTTP接続を

使用できます。

- Apache Tomcatをアップグレードできない場合は、元のバージョンをインストールし、手順2から構成を適用します。

- Web コンソールとApache Tomcatアップグレードによって、オフラインヘルプファイルがクリアされます。古いバージョンのESET PROTECT On-Premのオフラインヘルプを使用していた場合は、アップグレード後にESET PROTECT On-Prem 11.0用に再作成して、最新のオフラインヘルプがESET PROTECT On-Premバージョンと一致するようにします。

ApacheTomcatとJava(Linux)をアップグレードします。

Apache Tomcatは、ESET PROTECT Webコンソールを実行するために必要な必須コンポーネントです。

アップグレード前の注意

1. 次のコマンドを実行し、インストールされているApache Tomcatのバージョンを確認します。（場合によってはフォルダー名が`tomcat7`または`tomcat8`です）

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. 新しいバージョンが利用可能な場合:

   a.新しいバージョンがサポートされていることを確認してください。

   b.Tomcat設定ファイル*/etc/tomcat7/server.xml*をバックアップします。

アップグレード手順

1. 次のコマンドを実行して Apache Tomcatサービスを停止します(場合によっては、サービス名は次のとおりです`tomcat7`)

```
sudo systemctl stop tomcat
```

2. Apache TomcatとJavaをアップグレードします。

> 次のサンプルパッケージ名は、ご使用のLinuxディストリビューションリポジトリパッケージとは異なる場合があります Linuxディストリビューションの既定のリポジトリには、サポートされている最新バーンのApache TomcatとJavaが含まれていない場合があります。

Linuxディストリビューション	ターミナルコマンド
DebianとUbuntuディストリビューション	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOSとRed Hatディストリビューション	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. */etc/tomcat9/server.xml*ファイルをバックアップの*server.xml*で置換します。

4. *server.xml*ファイルを開き、*keystoreFile*パスが正しいことを確認してください。

5. Apache TomcatのHTTPS接続が正しく設定されていることを確認してください。

エンタープライズソリューションまたは低パフォーマンス ステムの追加のWebコンソール設定も参照してください。

6.Javaをアップグレードした場合は、次の手順に従い、システムにインストールされた最新のJavaパッケージを使用するようにApache Tomcatを設定します。

a.Apache Tomcat設定フォルダーに移動します。

```
cd /usr/share/tomcat/conf/
```

b.テキストエディターで*tomcat.conf*ファイルを開きます。

```
nano tomcat.conf
```

c.JAVA_HOME変数で最新のインストールされたJavaパッケージへのパスを更新します(パスはシステムにインストールされたJavaパッケージによって異なります)。

```
JAVA_HOME="/usr/lib/jvm/jre-11-openjdk"
```

d.ファイルを保存して閉じます:**CTRL+X**を押してから、**Y**と**ENTER**を押します。

e.**tomcat**サービスを再起動します:

```
sudo systemctl restart tomcat
```

f.次のコマンドを実行し、Apache Tomcatで使用されるJavaパッケージを検証します。

```
sudo systemctl status tomcat
```

Apache Tomcatを新しいメジャーバージョン(Apache Tomcatバージョン7.xから9.x)にアップグレード後の手順
1.もう一度ESET PROTECT Webコンソールを展開します(ESET PROTECTWebコンソールインストール - Linuxを参照してください)
2.*%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*を再利用してESET PROTECT Webコンソールにカスタム設定を保持します。
Web コンソールとApache Tomcatアップグレードによって、オフラインヘルプファイルがクリアされます。古いバージョンのESET PROTECT On-Premのオフラインヘルプを使用していた場合は、アップグレード後にESET PROTECT On-Prem 11.0用に再作成して、最新のオフラインヘルプがESET PROTECT On-Premバージョンと一致するようにします。

移行、および再インストール手順

以下ではESET PROTECTサーバーと他のESET PROTECTコンポーネントの移行および再インストールのためのさまざまな手順について説明します。

- サーバー間でESET PROTECT On-Prem 11.0を移行または再インストールする

1つのESET PROTECTサーバーから新しいサーバーコンピューターに移行するには、すべての認証局とESET PROTECTサーバー証明書をエクスポート/バックアップします。そうしない場合ESET PROTECTコンポーネントのいずれも新しいESET PROTECTサーバーと通信できません。

- ESET PROTECTデータベース移行

- MDMの移行
- ESET PROTECTサーバーでIPアドレスまたはホスト名を変更します。

アップグレード手順を参照してください。

サーバー間の移行

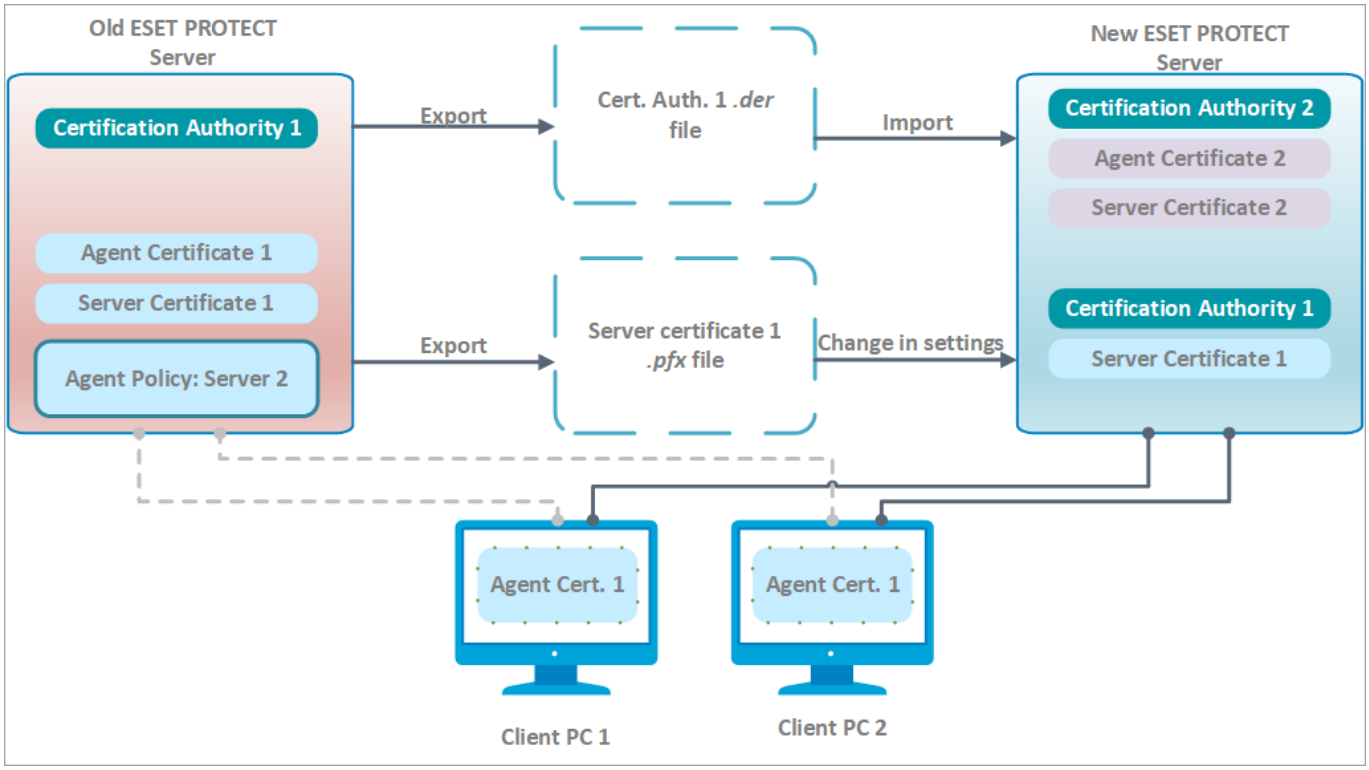
サーバー間でESET PROTECT On-Premを移行する方法は複数あります(これらのシナリオはESET PROTECTサーバーの再インストールで使用できます)。

- クリーンインストール – 同じIPアドレス – 新しいインストールは古いESET PROTECTサーバーの前のデータベースを使用せず、元のIPアドレスを保持します。
- クリーンインストール – 別IPアドレス(ナレッジベース記事) – 新しいインストールは古いESET PROTECTサーバーの前のデータベースを使用せず、異なるIPアドレスを使用します。
- 移行されたデータベース – 同じ/別のIPアドレス – 2つの類似したデータベースタイプ(MySQLからMySQL、またはMicrosoft SQLからMicrosoft SQL)、および近い2つのESET PROTECT On-Premバージョン間でのみデータベース移行を実行できます。

クリーンインストール – 同じIPアドレス

この手順の目的は、以前のデータベースを使用しないESET PROTECTサーバーの完全に新しいインスタンスをインストールすることです。この新しいESET PROTECTサーバーは前のサーバーと**同じIPアドレス**を使用しますが、古いESET PROTECTサーバーのデータベースを使用しません。

次の手順では、古いESET PROTECTサーバーがアクセス可能なWebコンソールで実行されている必要があります。古いESET PROTECTサーバーにアクセスできない場合
1. オールインパッケージインストーラー(Windows)を使用してESET PROTECTサーバ/MDMをインストールするか、別のインストール方法(Windows 手動インストールLinuxまたは仮想アプライアンス)を選択します。
2. ESET PROTECT Webコンソールに接続します。
3. ESET PROTECTインフラストラクチャにクライアントコンピューターを追加し、ESET Managementエージェントをローカルまたはリモートで展開します。



大きい画像を表示します

I. 現在の(古い)ESET PROTECTサーバー:

ESET Full Disk Encryptionで暗号化されたデバイスを管理する場合は、次の手順に従い、回復データの損失を防止してください。
1.移行の前: **ステータス概要 > 暗号化**に移動します。ここでは、現在**ESET Full Disk Encryption回復データ**を**エクスポート**できます。
2.移行の後: 新しい管理コンソールで**ESET Full Disk Encryption回復データ**を**インポート**します。
これらの手順を実行できない場合は、移行前に管理されたデバイスを復号する必要があります。
移行後ESET PROTECT Webコンソールから、管理されたデバイスを暗号化できます。

1. サーバー証明書を現在のESET PROTECTサーバーからエクスポートし、外部ストレージに保存します。

   • すべての認証局証明書をESET PROTECTサーバーからエクスポートし、*.der* ファイルとして各CA証明書を保存します。

   • サーバー証明書をESET PROTECTサーバーから*.pfx*ファイルにエクスポートします。エクスポートされた*.pfx*には、秘密鍵も含まれます。

2. ESET PROTECT Serverサービスを停止します。

3. ESET PROTECTサーバーコンピューターをオフにします。

まだ古いESET PROTECTサーバーをアンインストール/使用停止しないでください。

II. 新しいESET PROTECTサーバー:

同じIPアドレスで新しいESETPROTECTサーバーを使用するには、新しいESETPROTECTサーバーのネットワーク構成(**IPアドレス**、**FQDN**、**コンピューター名**、**DNSSRVレコード**)が古いESETPROTECTサーバーと一致することを確認してください。

1. オールインパッケージインストーラー(Windows)を使用してESET PROTECTサーバ/MDMをインストールするか、別のインストール方法 (Windows 手動インストールLinuxまたは仮想アプライアンス)を選択します。

2. ESET PROTECT Webコンソールに接続します。

3. 古いESET PROTECTサーバーからエクスポートしたすべてのCAをインポートします。このためには、公開鍵のインポートの手順に従います。

4. **詳細** > 設定でESET PROTECTサーバー証明書を変更し、古いESET PROTECTサーバーからサーバー証明書を使用します。

5. すべての必要なESETライセンスをESET PROTECT On-Premにインポートします。

6. 詳細についてはESET PROTECT Serverサービスを再起動します。ナレッジベース記事を参照してください。

1回または2回のエージェント接続間隔の後、クライアントコンピューターは、元のESETPROTECTエージェント証明書を使用して新しいESET Managementサーバーに接続する必要があります。これは、古いESET PROTECTサーバーからインポートされたCAによって認証されます。 クライアントが接続していない場合は、「ESET PROTECTサーバーのアップグレード/移行後の問題」を参照してください。

新しいクライアントを追加するときには、新しい認証局を使用して、エージェント証明書を署名します。これは、インポートされたCAを使用して新しいピア証明書を署名できないためです。移行されたクライアントコンピューターのESET Managementエージェントのみを認証できます。

III. 古いESET PROTECTサーバ/MDMアンインストール:

新しいESET PROTECTサーバーですべて正常に実行されたら、段階的な手順を使用して古いESET PROTECTサーバ/MDMを注意して使用停止します。

移行されたデータベース – 同じ/異なるIPアドレス

この手順の目標は、まったく新しいESET PROTECTサーバーのインスタンスをインストールし、**既存のクライアントコンピューターを含む既存のESET PROTECTデータベースを保持**することです。新しいESET PROTECTサーバーの**IPアドレスは古いサーバーと同じか異なり**、古いESET PROTECTサーバーのデータベースはインストール前に新しいサーバーコンピューターにインポートされます。

- データベースの移行は同じデータベースタイプ間でのみサポートされています(MySQLからMySQLまたはMicrosoft SQLからMicrosoft SQL)
- データベースを移行するときには、同じESET PROTECT On-Premバージョンのインスタンス間で移行する必要がありますESET PROTECTコンポーネントのバージョンを調べる手順については、ナレッジベース記事を参照してください。データベース移行を完了した後は、必要に応じて、アップグレードを実行し、最新バージョンのESET PROTECT On-Premを取得できます。

I. 現在の(古い)ESET PROTECTサーバー:

別のIPアドレスへの移行は上級ユーザー専用の手順です。新しいESET PROTECTサーバーの**IPアドレスが異なる**場合は、現在の(古い)ESET PROTECTサーバーで次の手順を実行します。
a)新しいESET PROTECTサーバー証明書新しいESET PROTECTサーバーの接続情報を含むを生成します。[**ホスト**]フィールドを既定値(アスタリスク)にすると、特定のDNSまたはIPアドレスに関連付けずに、この証明書の配布ができます。
b)ポリシーを作成し、新しいESET PROTECTサーバーとIPアドレスを定義して、すべてのコンピューターに割り当てます。ポリシーがすべてのクライアントコンピューターに配布されるまで待機します(新しいサーバー情報を受信すると、コンピューターはレポートを停止します)。

1. ESET PROTECT Serverサービスを停止します。

2. ESET PROTECTデータベースをエクスポート/バックアップします

3. 現在のESET PROTECTサーバーコンピューターをオフにします(新しいサーバーが別のIPアドレスの場合は任意)。

まだ古いESET PROTECTサーバーをアンインストール/使用停止しないでください。

II. 新しいESET PROTECTサーバー:

同じIPアドレスで新しいESETPROTECTサーバーを使用するには、新しいESETPROTECTサーバーのネットワーク構成(**IPアドレスFQDNコンピューター名、DNSSRVレコード**)が古いESETPROTECTサーバーと一致することを確認してください。

1. サポートされているESET PROTECTデータベースをインストール/起動します。

2. 古いESET PROTECTサーバーからESET PROTECTデータベースをインポート/復元します。

3. オールインパッケージインストーラー(Windows)を使用してESET PROTECTサーバ/MDMをインストールするか、別のインストール方法 (Windows 手動インストールLinuxまたは仮想アプライアンス)を選択しますESET PROTECTサーバーのインストール中にデータベース接続設定を指定します。

4. ESET PROTECT Webコンソールに接続します。

5. **詳細 > 設定 > 接続**に移動します。**証明書の変更 > 証明書リストを開く**をクリックして、古いESET PROTECTサーバーの**サーバー証明書**を選択して、**OK**を2回クリックします。

6. ESET PROTECT Serverサービスを再起動します。

7. ESET PROTECT Web コンソールにログインし、**コンピューター**をクリックします。

1回または2回のエージェント接続間隔の後、クライアントコンピューターは、元のESETPROTECTエージェント証明書を使用して、新しいESET Managementサーバーに接続します。 クライアントが接続していない場合は、「ESET PROTECTサーバーのアップグレード/移行後の問題」を参照してください。

III. 古いESET PROTECTサーバ/MDMアンインストール:

新しいESET PROTECTサーバーですべて正常に実行されたら、段階的な手順を使用して古いESET PROTECTサーバ/MDMを注意して使用停止します。

ESET PROTECTデータベース移行

これらの手順は、異なるSQL Serverインスタンス間でのESET PROTECTデータベース移行に適用されます(これは、異なるSQL Serverバージョンに移行する場合または別のコンピューター上でホストされたSQL Serverに移行する場合に適用されます)。

- Microsoft SQL Serverの移行処理
- MySQL Serverの移行処理

Microsoft SQL Serverの移行処理

この移行処理は**Microsof SQL Server**と**Microsoft SQL Server Express**で同じです。

詳細については、次のMicrosoftナレッジベース記事を参照してください。https://msdn.microsoft.com/en-us/library/ms189624.aspx

前提条件

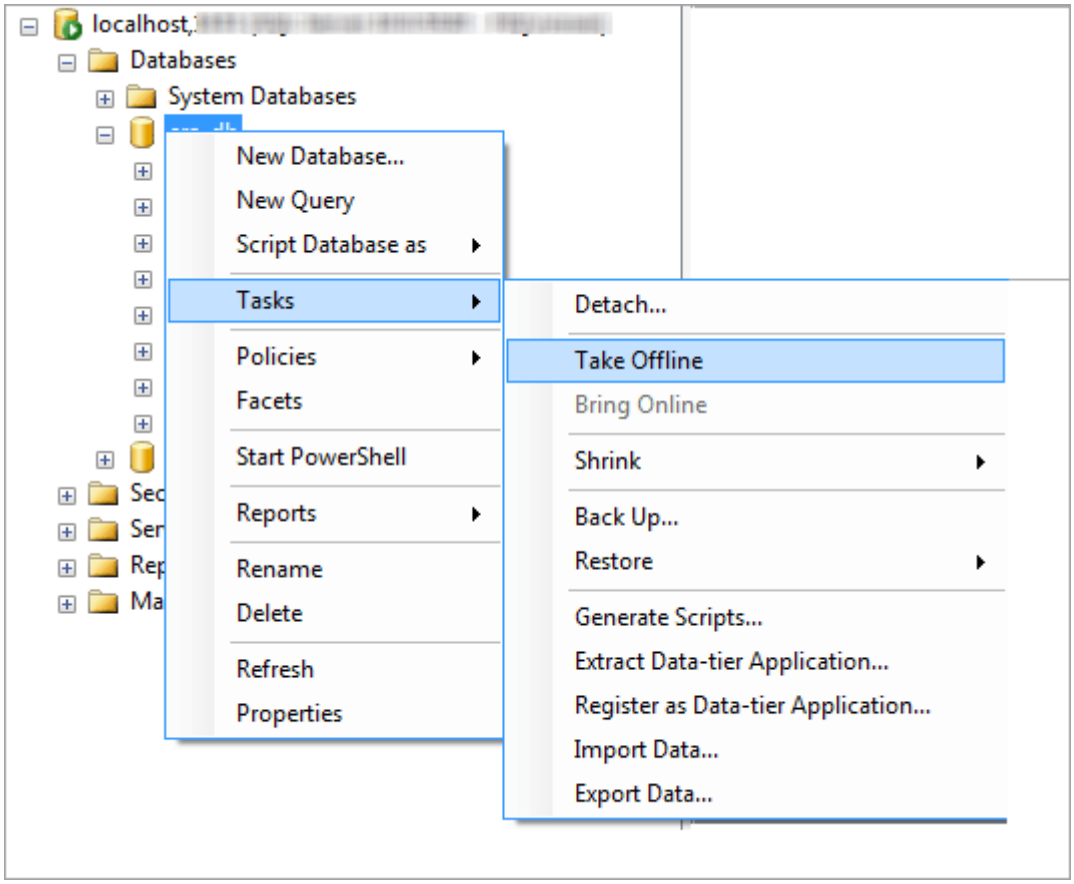
- ソースとターゲットのSQL Serverインスタンスをインストールする必要があります。これらは別のコンピューターでホストできます。
- ターゲットSQL Serverインスタンスはソースインスタンスと同じバージョン以上でなければなりません。ダウングレードはサポートされていません。
- **SQL Server Management Studio**をインストールする必要があります。SQL Serverインスタンスが別のコンピューターにある場合、両方に存在する必要があります。

SQL Server Management Studioを使用した移行

1. ESET PROTECT Serverサービス、またはESET PROTECT MDMサービスを停止します。

> 以下のすべての手順を完了してから、ESET PROTECTサーバーまたはESET PROTECT MDMを起動してください。

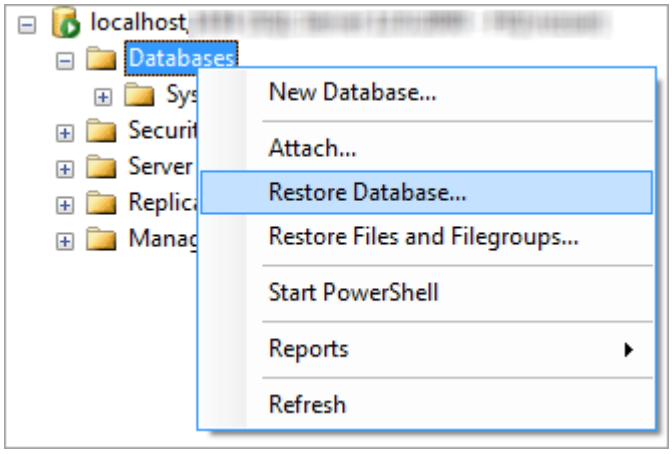
2. SQL Server Management Studio経由でソースSQL Serverインスタンスにログインします。
3. 移行するデータベースの完全データベースバックアップを作成します。新しいバックアップ名を指定することをお勧めします。そうでないと、バックアップセットが既に使用されている場合、新しいバックアップがそれに追加され、不必要に大きいバックアップファイルが作成されます。
4. ソースデータベースをオフラインにし、[**タスク**] > [**オフラインにする**]を選択します。



5. 手順3で作成したバックアップ(*.bak*)ファイルを、ターゲットSQL Serverインスタンスからアクセスできる場所にコピーします。データベースバックアップファイルのアクセス権を編集しなければならない場合があります。

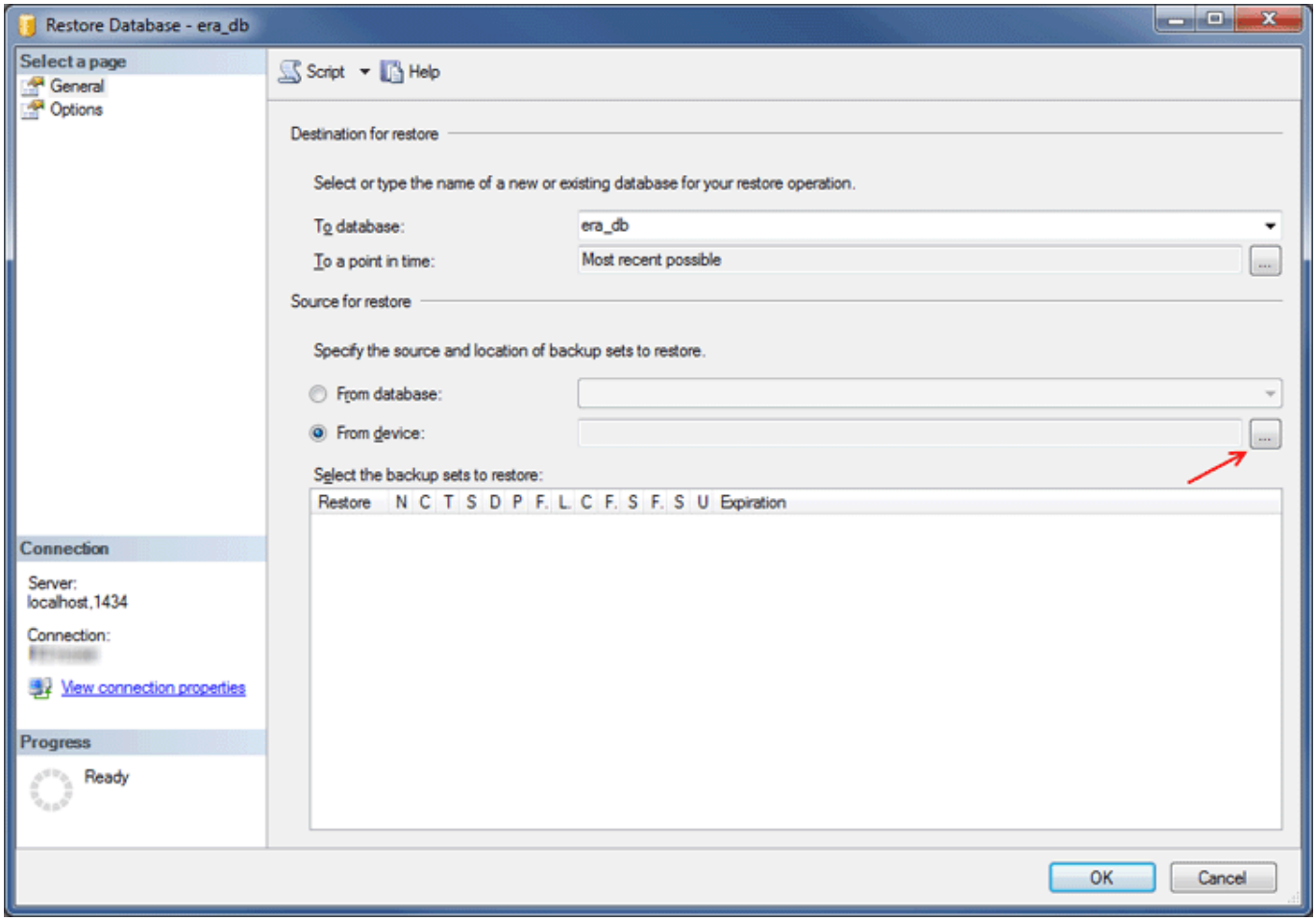
6. SQL Server Management Studioを使用してターゲットSQL Serverインスタンスにログインします。

7. ターゲットSQL Serverインスタンスでデータベースを復元します。



8. 新しいデータベースの名前を**[復元先]**データベースフィールドに入力します。古いデーターベースと同じ名前にすることもできます。

9. **[復元するバックアップセットのソースと場所を指定]**の下の[復元元デバイス]を選択し、[…]をクリックします。

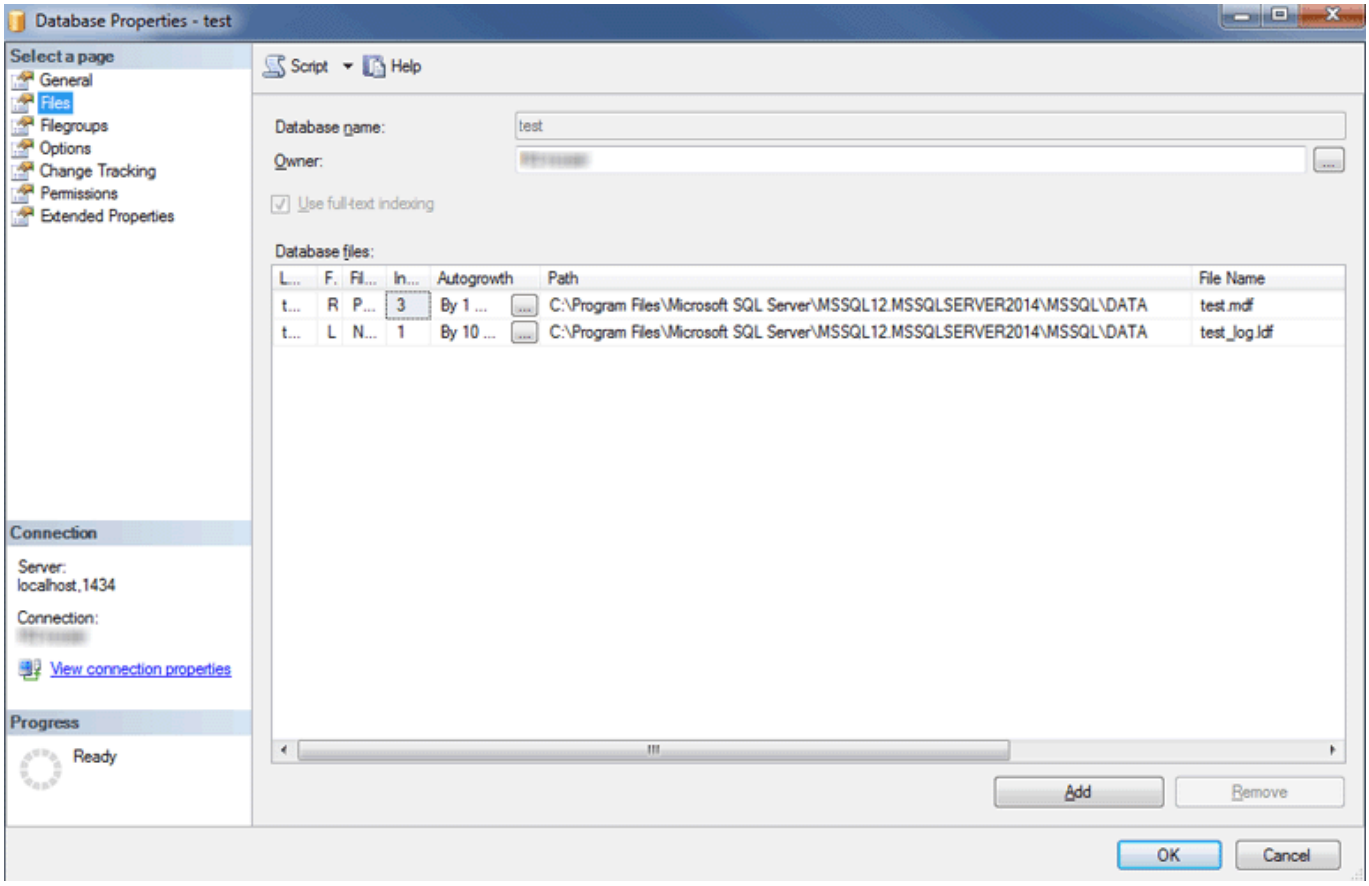


10. [追加]をクリックして、バックアップファイルに移動して開きます。

11. 復元する可能な最新のバックアップを選択します(バックアップセットには複数のバックアップが含まれることがあります)。

12. 復元ウィザードの[**オプション**]ページをクリックします。任意で、[**既存のデータベースを上書き**]を選択し、データベース(*.mdf*)とログ(*.ldf*)の復元先が正しいことを確認します。既定値を使用すると SQL Serverのパスが使用されます。このため、これらの値を確認してください。

- データベースファイルがターゲットSQL Serverインスタンスに保存されている場所がわからない場合は、既存のデータベースを右クリックし、[**プロパティ**]を選択し、[**ファイル**]タブをクリックします。データベースが保存されているディレクトリが、次の表の[**パス**]列に表示されます。

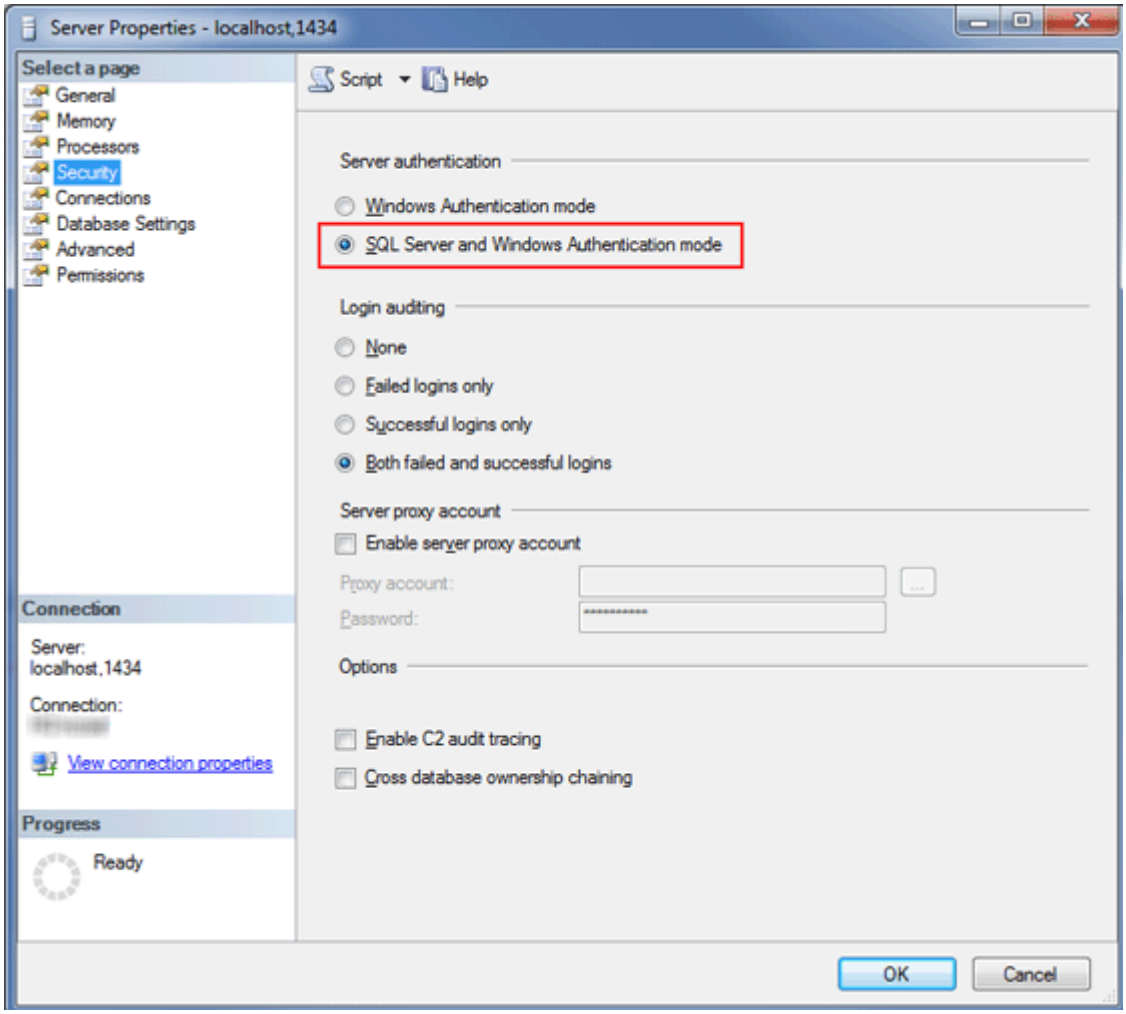


13. 復元ウィザードウィンドウで**[OK]**をクリックします。

14. **era_db**データベースを右クリックし、**新しいクエリ**を選択して、次のクエリを実行し、**tbl_authentication_certificate**テーブルの内容を削除します(そうしないと、エージェントが新しいサーバーに接続できない場合があります)。

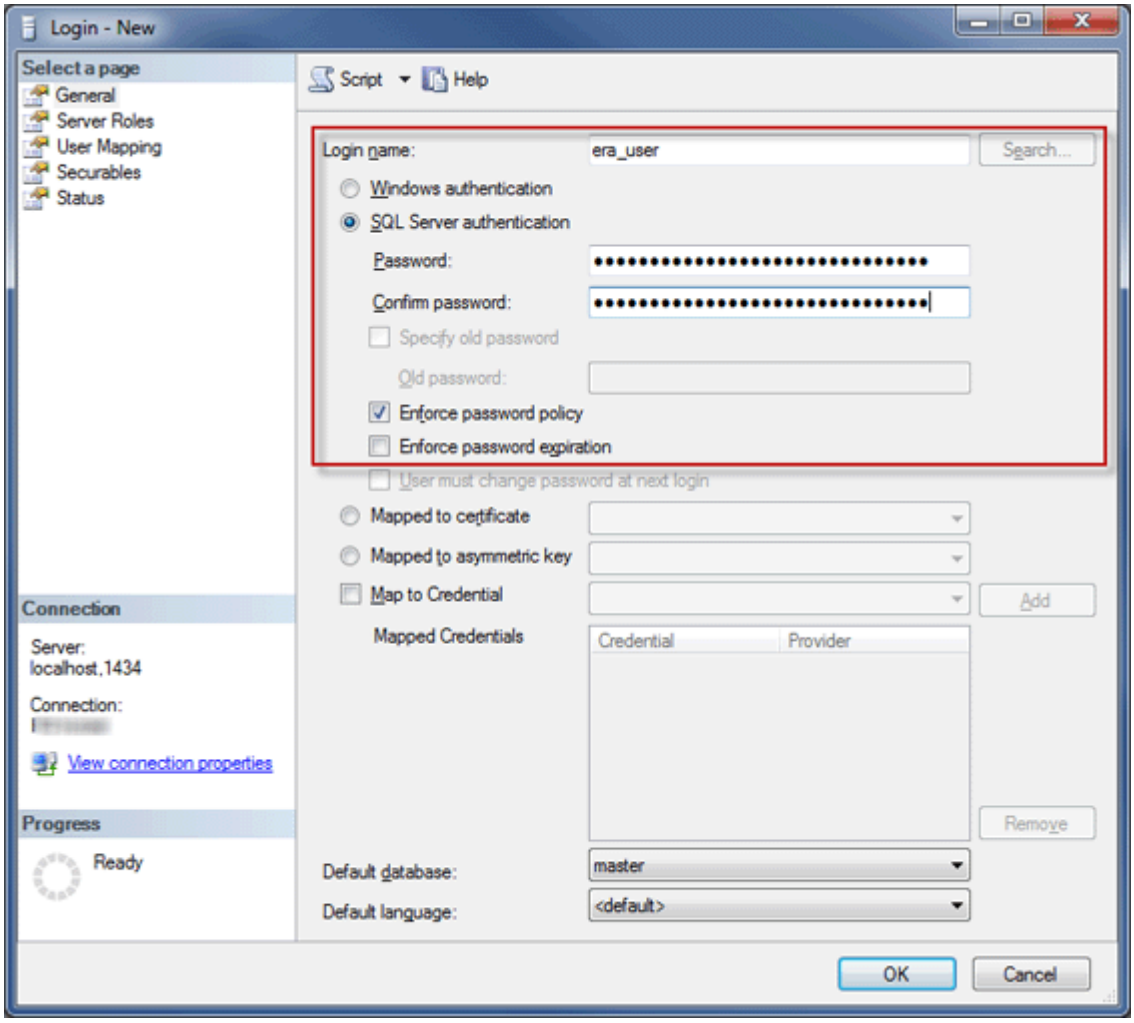
```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. 新しいデータベースサーバーで**SQL Server認証が有効**になっていることを確認します。サーバーを右クリックし、**[プロパティ]**をクリックします。**[セキュリティ]**に移動して、**SQL Server とWindows認証モード**が選択されていることを確認します。

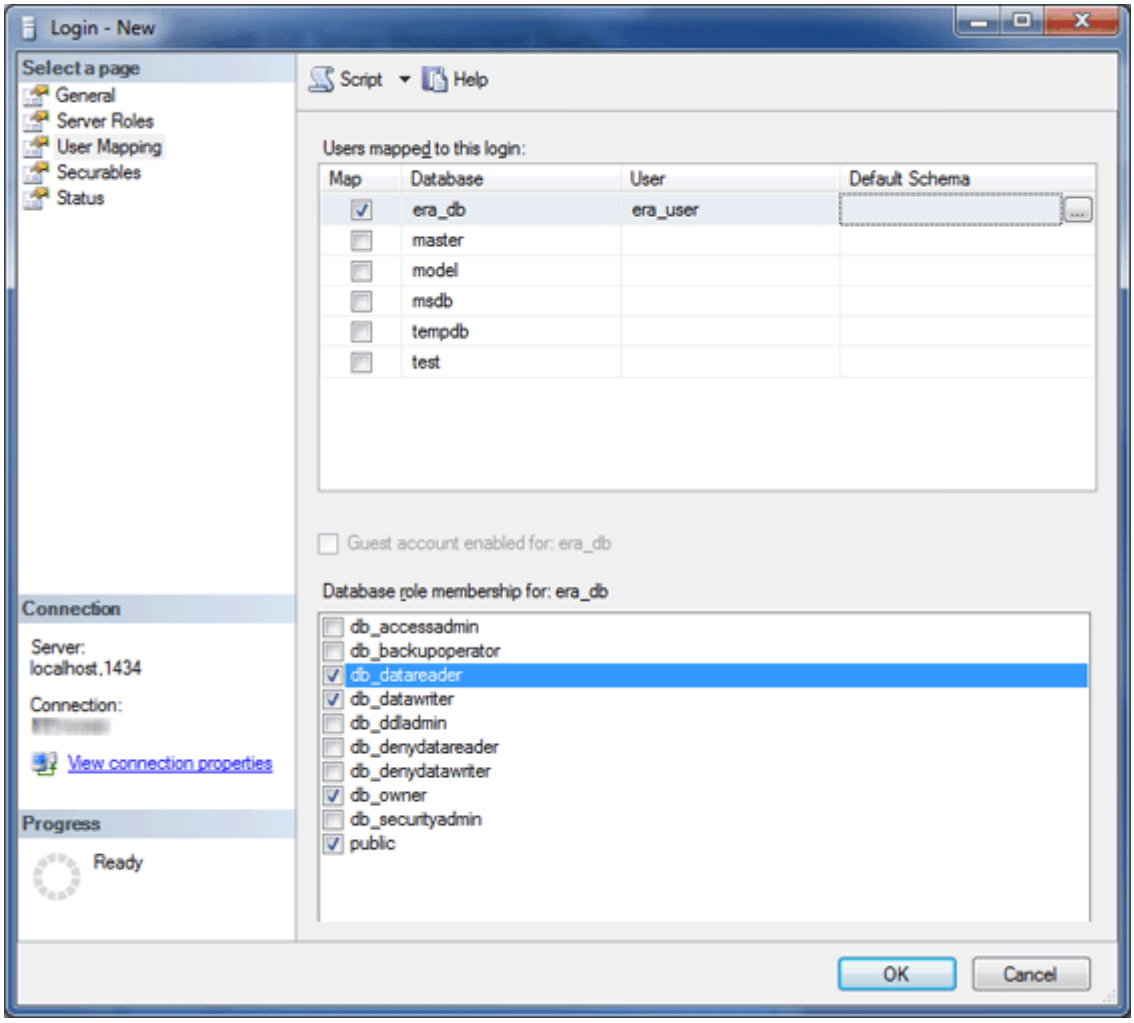


16. SQL Server認証を使用してターゲットSQL Serverで**新しいSQL Serverログイン**(ESET PROTECTサーバ/ESET PROTECT MDM)を作成し、復元されたデータベースのユーザーにログインをマッピングします。

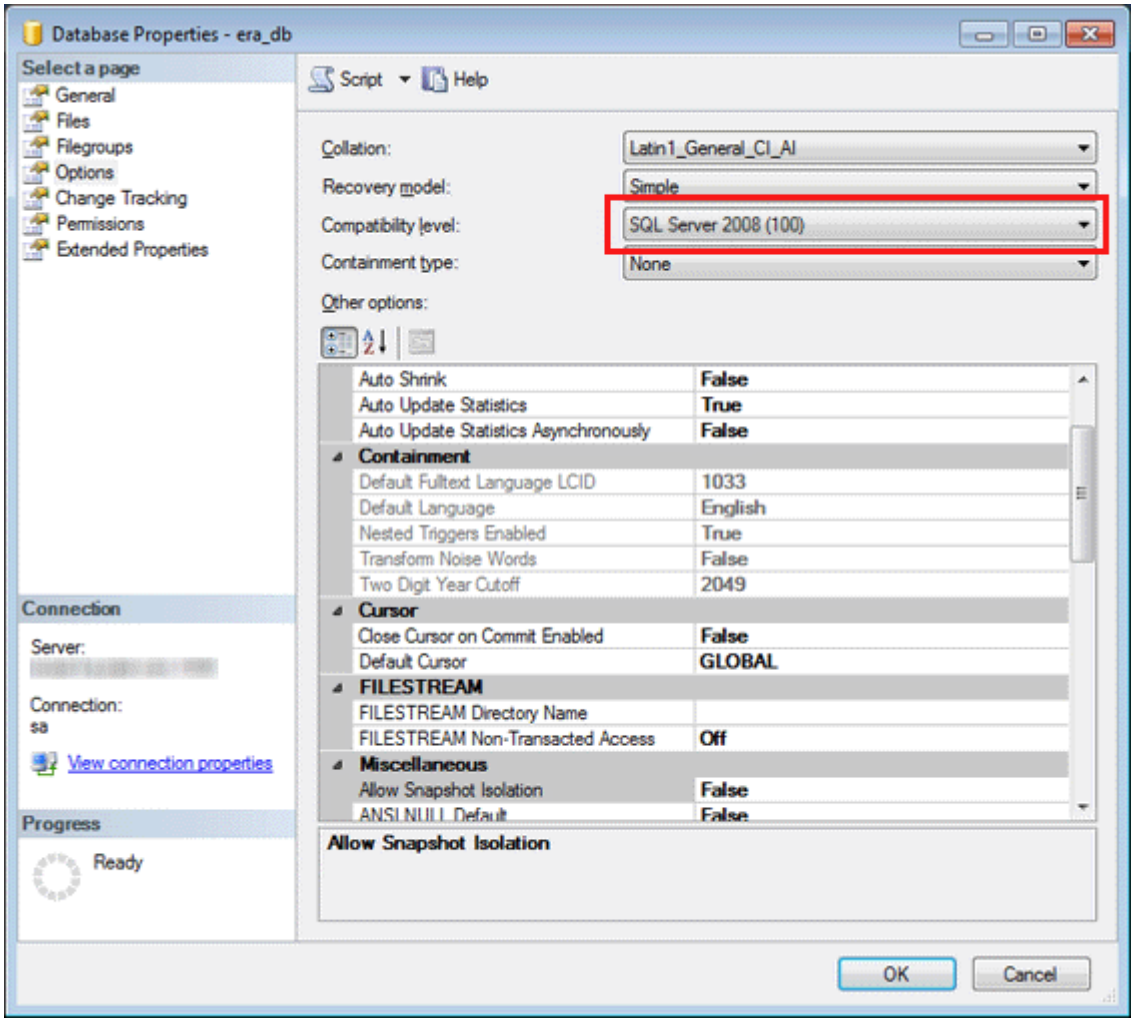
- パスワードの有効期限を適用しないでください。
- ユーザー名の推奨文字:小文字のASCII文字、数字、アンダースコア「_」
- パスワードの推奨文字:大文字と小文字のASCII文字、数字、スペース、特殊文字を含むASCII文字のみ
- 非ASCII文字、波括弧{}または@は使用しないでください。
- 上記の文字に関する推奨事項に従わない場合、データベース接続の問題が発生する可能性があるか、データベース接続文字列の修正中に後から特殊文字をエスケープする必要があります。文字のエスケープルールはこのマニュアルの対象外です。



17. ターゲットデータベースのユーザーにログインをマッピングします。**ユーザーマッピング**タブで、データベースユーザーに次のロールがあることを確認します。**db_datareader**、**db_datawriter**、**db_owner**

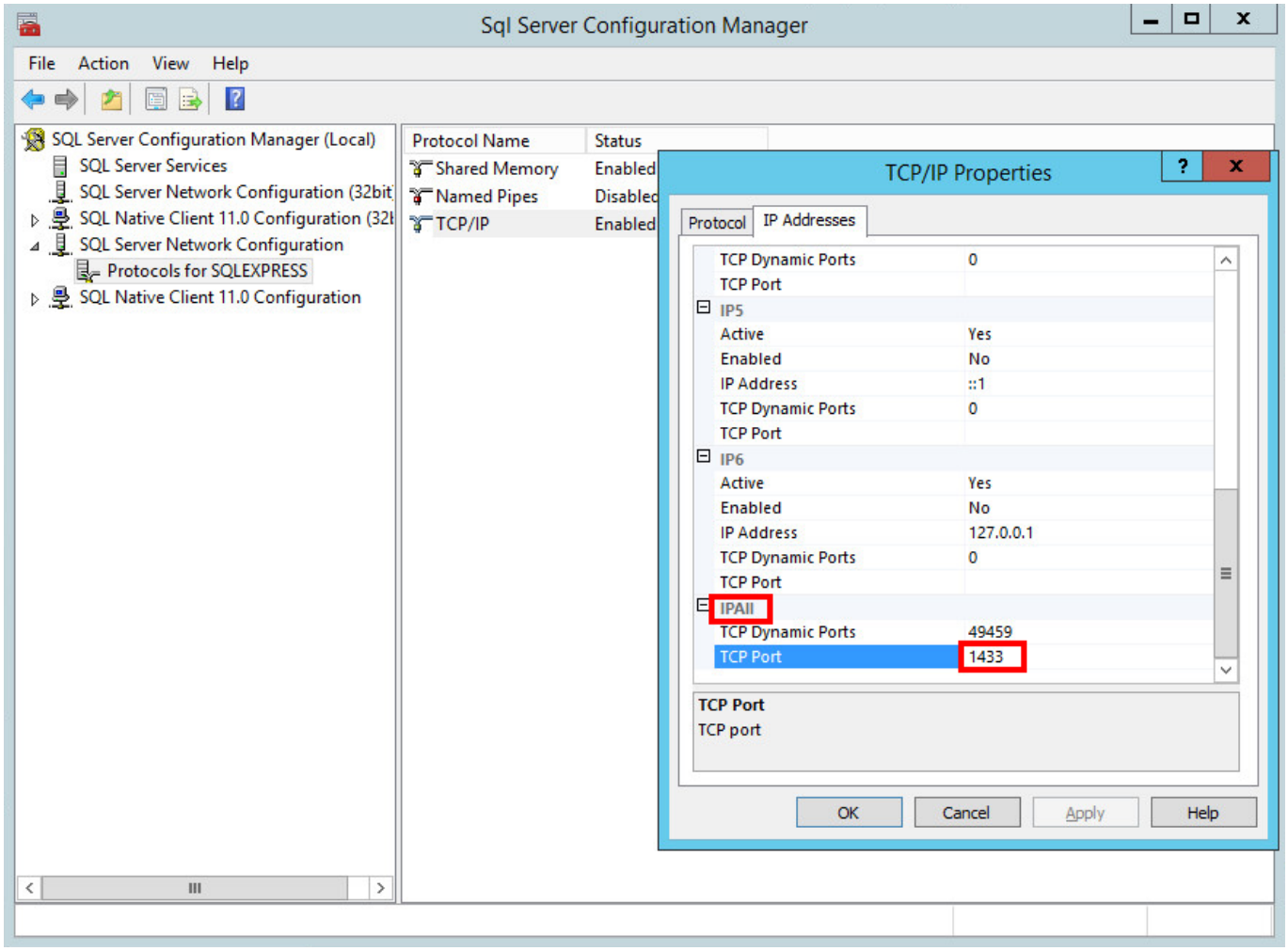


18. 最新のデータベースサーバー機能を有効にするには、復元されたデータベースの**互換レベル**を最新に変更します。新しいデータベースを右クリックし、データベース**プロパティ**を開きます。



SQL Server Management Studioは、使用中のバージョンよりも後の互換レベルを定義できません。たとえばSQL Server Management Studio 2014は、SQL Server 2019の互換レベルを設定できません。

19. db_instance_name(例: SQLEXPRESSまたはMSSQLSERVER)の**TCP/IP**接続プロトコルが**有効**で、TCP/IP**ポート**が**1433**に設定されていることを確認します。このためには、**Sql Server Configuration Manager**を開き、**SQL Serverネットワーク構成** > **db_instance_nameのプロトコル**に移動し、**TCP/IP**を右クリックして、**有効**を選択します。次に、**TCP/IP**をダブルクリックし、**プロトコル**タブに切り替え、**IPAll**まで下にスクロールし、**TCPポート**フィールドに1433と入力します。**OK**をクリックし、**SQL Server**サービスを再起動します。



20. ESET PROTECTサーバーまたはMDMをデータベースに接続します

MySQL Serverの移行処理

前提条件

- ソースとターゲットのSQL Serverインスタンスをインストールする必要があります。これらは別のコンピューターでホストできます。

- MySQLツールは、1台以上のコンピューター(`mysqldump`とmysqlクライアント)で使用できる必要があります。

便利なリンク

- https://dev.mysql.com/doc/refman/8.0/en/copying-databases.html
- https://dev.mysql.com/doc/refman/8.0/en/mysqldump.html
- https://dev.mysql.com/doc/refman/8.0/en/mysql.html

移行処理

次のコマンド、構成ファイル、またはSQL文では、必ず次の項目を置換してください。
- **SRCHOST**をソースデータベースサーバーのアドレスに変更する
- **SRCROOTLOGIN**をソースMySQLサーバールートユーザーログインに変更する
- **SRCDBNAME**をバックアップするソースESET PROTECTデータベースの名前に変更する
- **BACKUPFILE**をバックアップが保存されるファイルへのパスに変更する
- **TARGETROOTLOGIN**をターゲットMySQLサーバールートユーザーログインに変更する
- **TARGETHOST**をターゲットデータベースサーバーのアドレスに変更する
- **TARGETDBNAME**をターゲットESET PROTECTデータベースの名前に変更する(移行後)
- **TARGETLOGIN**をターゲットデータベースサーバー上の新しいESET PROTECTデータベースユーザーのログイン名に変更する
- **TARGETPASSWD**をターゲットデータベースサーバー上の新しいESETPROTECTデータベースユーザーのパスワードに変更する

コマンドラインで次のSQL文を実行する必要はありません。GUIツールが使用できる場合は、既に知っているアプリケーションを使用できます。

1. ESET PROTECTサーバー/MDMサービスを停止します。

2. ソースESET PROTECTデータベースの完全データベースバックアップ(移行するデータベース)を作成する:

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. ターゲットMySQLサーバー上に空のデータベースを準備する:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

Linuxシステムでは、引用符の「″」の代わりにアポストロフィ文字「’」を使用してください。

4. ターゲットMySQLサーバーのデータベースを以前に準備された空のデータベースに復元する:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. ターゲットMySQLサーバー上にESET PROTECTデータベースユーザーを作成する:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

TARGETLOGINの推奨文字:

- 小文字のASCII文字、数字、アンダースコア「_」

TARGETPASSWDの推奨文字:

- 大文字と小文字のASCII文字、数字、スペース、特殊文字を含むASCII文字のみ

- 非ASCII文字、波括弧{}または@は使用しないでください。

上記の文字に関する推奨事項に従わない場合、データベース接続の問題が発生する可能性があるか、データベース接続文字列の修正中に後から特殊文字をエスケープする必要があります。文字のエスケープルールはこのマニュアルの対象外です。

6. ターゲットMySQLサーバー上のESET PROTECTデータベースユーザーに適切なアクセス権を付与する:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

Linuxシステムでは、引用符の「″」の代わりにアポストロフィ文字「'」を使用してください。

7. **tbl_authentication_certificate**テーブルの内容を削除します(そうでない場合、エージェントが新しいサーバーに接続できない場合があります)。

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. ESET PROTECTサーバーまたはMDMをデータベースに接続します

ESET PROTECTサーバーまたはMDMをデータベースに接続する

ESET PROTECTサーバーまたはESET PROTECT MDMがインストールされているコンピューターで次の手順を実行して、データベースに接続します。

1. ESET PROTECT Server/MDMサービスを停止します。

2. *startupconfiguration.ini*を探します。

   - Windows:

サーバー:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

   - Linux:

サーバー:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. ESET PROTECTサーバ/MDMのデータベース接続文字列を*startupconfiguration.ini*に変更します

    oを新しいデータベースサーバーのアドレスとポートを設定します。

    oを新しいESET PROTECTユーザー名とパスワードを接続文字列に設定します。

最終的な結果は次のようになります。

- Microsoft SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

上記の設定では常に置換してください。
- **TARGETHOST**をターゲットデータベースサーバーのアドレスに変更する
- **TARGETDBNAME**をターゲットESET PROTECTデータベースの名前に変更する(移行後)
- **TARGETLOGIN**をターゲットデータベースサーバー上の新しいESET PROTECTデータベースユーザーのログイン名に変更する
- **TARGETPASSWD**をターゲットデータベースサーバー上の新しいESETPROTECTデータベースユーザーのパスワードに変更する

4. ESET PROTECTサーバーまたはESET PROTECT MDMを起動し、サービスが正しく実行されていることを確認します。

MDMの移行

ESETPROTECTモバイルデバイス管理/コネクタ(MDM/MDC)コンポーネント(オンプレミスのみ)は、2024年1月にサポートが終了します。詳細クラウドMDMに移行することをお勧めします。

サーバー間でモバイルデバイス管理(オンプレミス)を移行するには、次の手順に従います。

サーバー間のモバイルデバイス管理の移行(オンプレミス)

この手順の目標は、既存のESET PROTECT MDMのインスタンスを移行し、登録されたモバイルデバイスを含む、**既存のESET PROTECT MDMデータベース**を保持することです。移行されたESET PROTECT MDMの**IPアドレス/ホスト名は古いESET PROTECT MDMと同じ**で、古いESET PROTECT MDMのデータベースはインストール前に新しいMDMホストにインポートされます。

- データベースの移行は同じデータベースタイプ間でのみサポートされています(MySQLからMySQLまたはMicrosoft SQLからMicrosoft SQL)
- データベースを移行するときには、同じESET PROTECT On-Premバージョンのインスタンス間で移行する必要があります。ESET PROTECTコンポーネントのバージョンを調べる手順については、ナレッジベース記事を参照してください。データベース移行を完了した後は、必要に応じて、アップグレードを実行し、最新バージョンのESET PROTECT On-Premを取得できます。

I. 現在の古いESET PROTECT MDMサーバー:

1. MDM構成のバックアップを作成します。

   a)**コンピューター**で、MDMサーバーをクリックし、**詳細**を選択します。

   b)**設定 > 設定の要求**をクリックします。要求された設定が作成されるまで、しばらく(エージェント接続間隔による)待つ必要がある場合があります。

   c)**ESET PROTECT Mobile Device Connector**をクリックし、**設定を開く**を選択します。

   d)設定から外部ストレージに次の項目をエクスポートします。

   - MDMサーバーの正確なホスト名。
   - ピア証明書 – エクスポートされた*.pfx*ファイルには秘密鍵も含まれます。

   LinuxでESET PROTECT MDMサーバーを実行している場合は、MDM設定ポリシーからHTTPS証明書をエクスポートする必要があります。
   I.**HTTPS証明書**の横の**表示**をクリックします。
   II. **ダウンロード**をクリックしてPFX形式でHTTPS証明書をダウンロードします。

   e)存在する場合は、次の証明書とトークンもエクスポートします。

   - 登録プロファイル署名証明書。
   - APNS証明書(APNS証明書とAPNS秘密鍵の両方をエクスポート)。
   - Apple Business Manager (ABM) 認証トークン。

2. ESET PROTECT MDMサービスを停止します。
3. ESET PROTECT MDMデータベースをエクスポート/バックアップします
4. 現在のESET PROTECT MDMコンピュータをオフにします。

まだ古いESET PROTECT MDMをアンインストール/使用停止しないでください。

II. 新しいESET PROTECT MDMサーバー:

新しいESET PROTECT MDMサーバーのネットワーク構成(古いMDMサーバーの構成からエクスポートしたホスト名)が古いESET PROTECT MDMと一致することを確認してください。

1. サポートされているESET PROTECT MDMデータベースをインストール/起動します。

2. 古いESET PROTECT MDMからESET PROTECT MDMデータベースをインポート/復元します。

3. オールインパッケージインストーラー(Windows)を使用してESET PROTECTサーバ/MDMをインストールするか、別のインストール方法(Windows 手動インストールLinuxまたは仮想アプライアンス)を選択しますESET PROTECT MDMのインストール中にデータベース接続設定を指定します。

LinuxにESET PROTECT MDMをインストールするときには、バックアップからHTTPS証明書を使用します。

4. ESET PROTECT Webコンソールに接続します。

5. ESET PROTECT MDMサービスを再起動します。

管理されたモバイルデバイスは、元の証明書を使用して、新しいESET PROTECT MDMサーバーに接続します。

III. 古いESET PROTECTサーバ/MDMアンインストール:

新しいESET PROTECTサーバーですべて正常に実行されたら、段階的な手順を使用して古いESET PROTECTサーバ/MDMを注意して使用停止します。

移行後のESET PROTECTサーバIPアドレスまたはホスト名の変更

ESET PROTECTサーバーのIPアドレスまたはホスト名を変更するには、次の手順を実行します。

1. ESET PROTECTサーバー証明書に特定のIPアドレスまたはホスト名が含まれる場合は、新しいサーバー証明書を作成し、切り替え先の新しいIPアドレスまたはホスト名を含めます。ただし、サーバー証明書のホストフィールドにワイルドカード*がある場合は、**手順2に進みます**。そうでない場合は、カンマ区切りの新しいIPアドレスとホスト名を追加する新しいサーバー証明書を作成し、前のIPアドレスとホスト名も含めます。

2. ESET PROTECTサーバー認証局を使用して、新しいサーバー証明書を署名します。

3. クライアント接続を新しいIPアドレスまたはホスト名(IPアドレスを推奨)に変更するポリシーを作成しますが、古いIPアドレスまたはホスト名への2番目の(代替)接続を含めESET Managementエージェントが両方のサーバーに接続できるようにします。詳細については、「ESET Managementエージェントが新しいESET PROTECTサーバーに接続するためのポリシーの作成」を参照してください。

4. このポリシーをクライアントコンピューターに追加しESET Managementエージェントがレプリケーションできるようにします。ポリシーによりクライアントは新しいサーバー(実行中ではないサー

バー)にリダイレクトしますがESET Managementエージェントは代替サーバー情報を使用して、元のIPアドレスに接続します。

5. [その他] > [設定]で新しいサーバー証明書を設定します。

6. ESET PROTECT Serverサービスを再起動し、IPアドレスまたはホスト名を変更します。

ESET PROTECTサーバーアドレスを変更するための図に基づいた手順については、ナレッジベース記事を参照してください。

ESET PROTECTサーバーとそのコンポーネントのアンインストール

ESET PROTECTサーバーとコンポーネントをアンインストールするには、以下の章のいずれかを選択してください。

- ESET Managementエージェントのアンインストール
- Windows - ESET PROTECTサーバーとそのコンポーネントのアンインストール
- Linux - ESET PROTECTコンポーネントのアップグレード、再インストール、またはアンインストール
- macOS - ESET Managementエージェントおよび ESET Endpoint製品のアンインストール
- 別のサーバーへの移行後に古いESET PROTECT/MDMサーバーを使用停止する

ESET Managementエージェントのアンインストール

ESET Managementエージェントは複数の方法でアンインストールできます。

ESET PROTECT Webコンソールを使用したリモートアンインストール

1. ESET PROTECT Webコンソールにログインします。

2. **コンピューター**ペインからESET Managementエージェントを削除するコンピューターを選択し、**[新しいタスク]**をクリックします。

あるいは、対応するチェックボックスをオンにして複数のコンピューターを選択し、**コンピューター > タスク > 新しいタスク**をクリックします。

3. タスク**名**を入力します。

4. [**タスクカテゴリ**]ドロップダウンメニューから[**ESET PROTECT On-Prem**]を選択します。

5. **タスク**ドロップダウンメニューから、管理の停止(ESET ManagementAgentのアンインストール)を選択します。

クライアントコンピューターからESET Managementエージェントをアンインストールすると、デバイスはESET PROTECT On-Premで管理されなくなります。
• ESET Managementエージェントをアンインストールした後に、ESETセキュリティ製品の一部の設定が残る場合があります。
• ESET Managementエージェントがパスワードで保護されている場合は、アンインストール、修復、またはアップグレード(変更あり)を行うには、パスワードを入力する必要があります。 デバイスを管理から削除する前に、ポリシーを使用して、保持する一部の設定（パスワード保護など）を既定の設定にリセットすることをお勧めします。
• エージェントで実行中のすべてのタスクは破棄されます。データレプリケーションによっては、このタスクの**実行中**/**完了**/**失敗**実行ステータスが、ESET PROTECT Webコンソールに正確に表示されない場合があります。
• エージェントがアンインストールされた後、統合されたEGUIまたはeShellからセキュリティ製品を管理できます。

6. タスク**概要**を確認し、[**完了**]をクリックします。

7. [トリガーの作成]をクリックして、このクライアントタスクが実行される日時と**ターゲット**を指定します。

ローカルアンインストール - Windows

LinuxまたはmacOSでのESET Managementエージェントのローカルアンインストールの手順も参照してください。
エージェントアンインストールのトラブルシューティングについては、ESET Managementエージェントアンインストールのトラブルシューティングを参照してください。

1. ESET Managementエージェントを削除するエンドポイントコンピューターに接続します(RDP経由など)。

2. [**コントロールパネル**] > [**プログラムと機能**]に移動し、[**ESET Managementエージェント**]をダブルクリックします。

3. [**次へ**] > [**削除**]をクリックして、アンインストール手順に従います。

ESETManagementエージェントのポリシーを使用してパスワードを設定した場合は、次のオプションがあります。
• アンインストール中にパスワードを入力する必要があります。
• ESET Managementエージェントをアンインストールする前に先にポリシーの割り当てを解除します。
• 既存のパスワード保護されたエージェントの上にESET Managementエージェントを再展開します(ナレッジベース記事)。

Windows - ESET PROTECTサーバーとそのコンポーネントのアンインストール

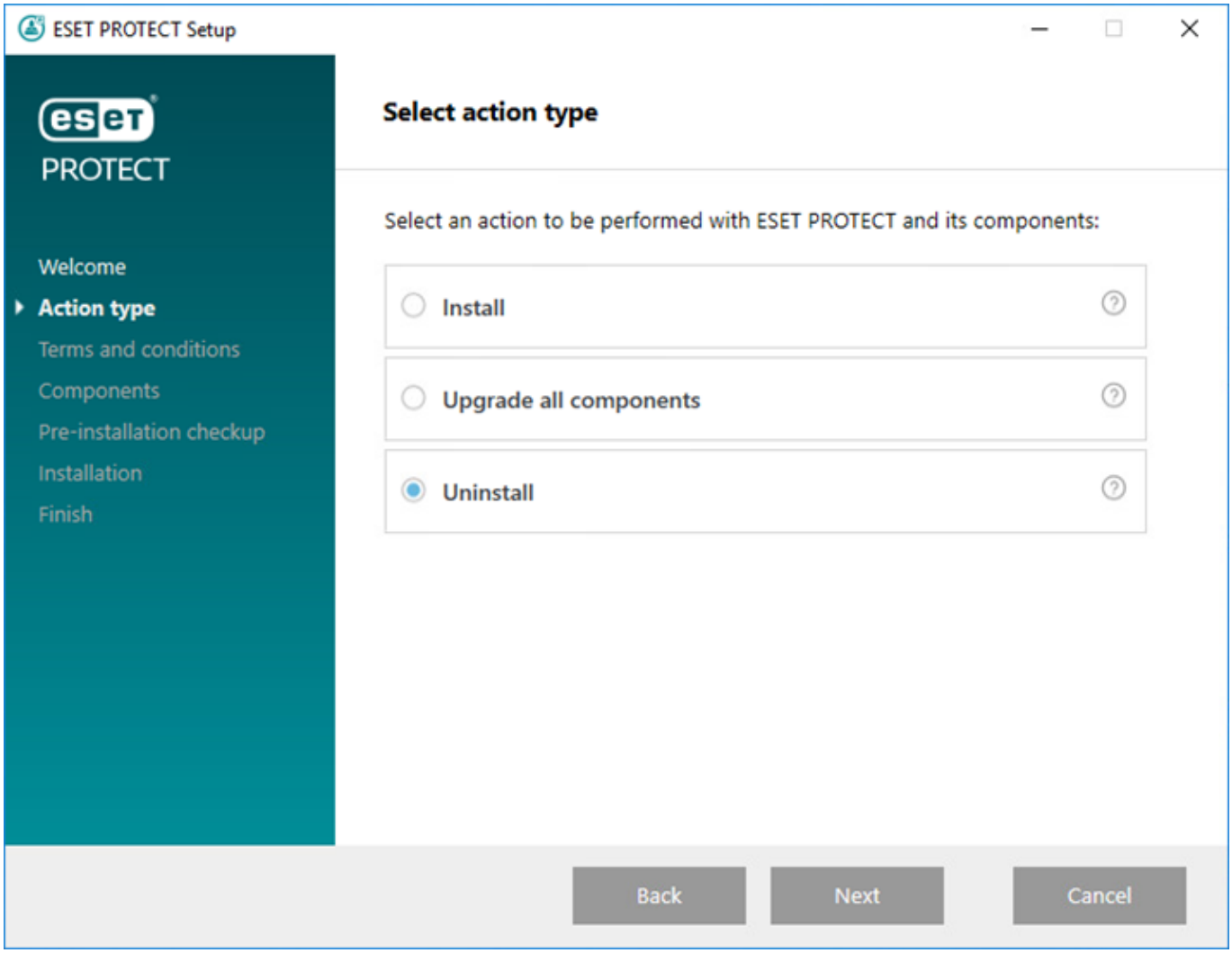
ESET PROTECT On-Premをアンインストールする前に、管理されたコンピューターでエージェントをアンインストールします
モバイルデバイスコネクターをアンインストールする前に、MDM iOSライセンス機能をお読みください。

次の手順に従い、WindowsでESET PROTECTサーバーとそのコンポーネントをアンインストールします。

1. ESET PROTECTオールインワンインストーラーをダウンロードして、パッケージを解凍します。

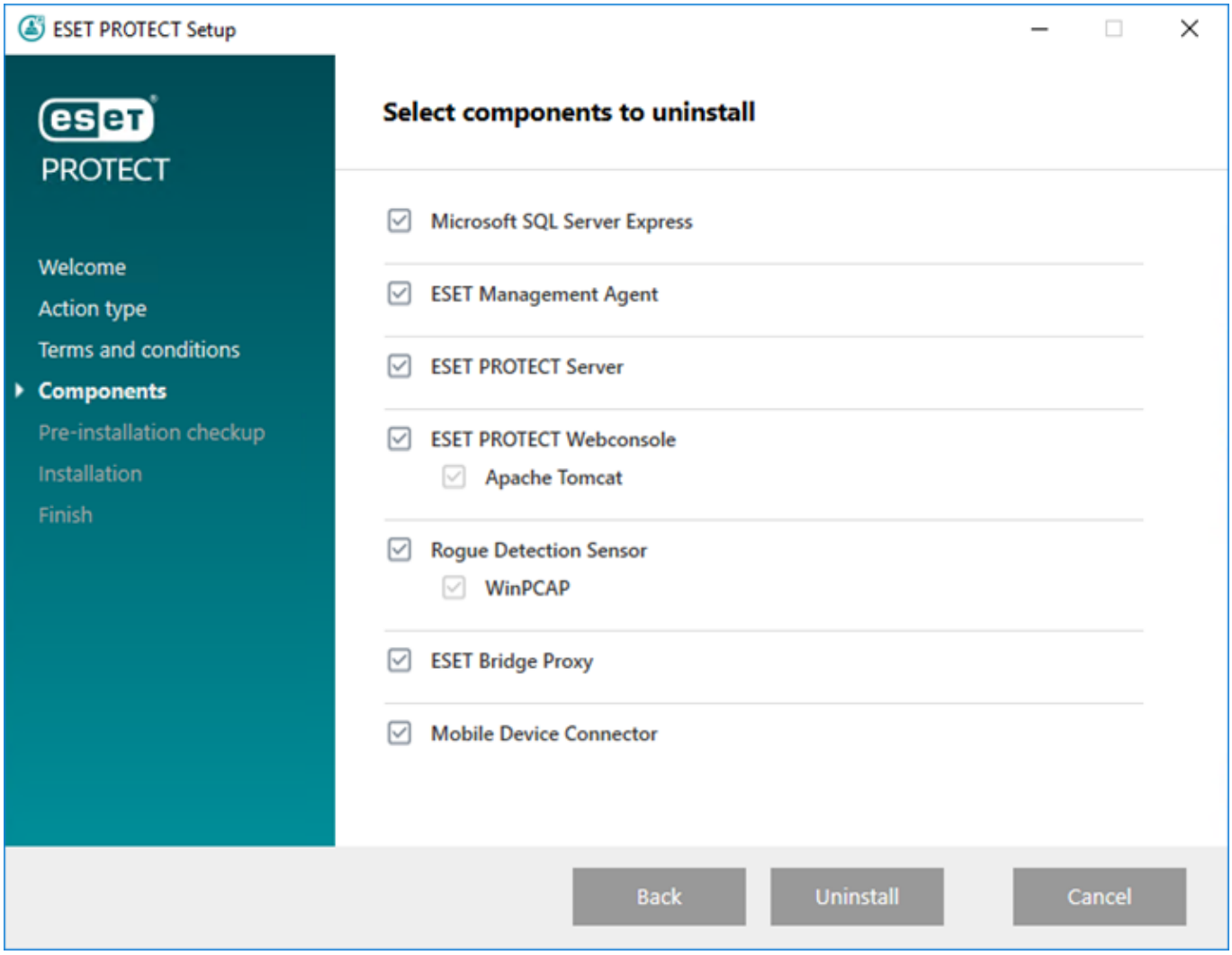
2. *Setup.exe*を実行します。ドロップダウンメニューから**の言語**を選択できます。**Next**(次へ)をクリックします。

3. **アンインストール**を選択して、**次へ**をクリックします。



4. EULAに同意し、[**次へ**]をクリックします。

5. アンインストールするコンポーネントを選択し、[**アンインストール**]をクリックします。



6. 特定のコンポーネントの削除を完了するには、コンピューターの再起動が必要な場合があります。

> 別のサーバーへの移行後に古いESET PROTECT On-Prem/MDMサーバーを使用停止するも参照してください。

Linux - ESET PROTECTコンポーネントのアップグレード、再インストール、またはアンインストール

新しいバージョンを再インストールまたはアップグレードする場合は、インストールスクリプトをもう一度実行します。

コンポーネント(この場合はESET PROTECTサーバー)をアンインストールするには、次のように`--uninstall`パラメータを使用してインストーラを実行します。

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

他のコンポーネントをアンインストールする場合は、コマンドで適切なパッケージ名を使用します。ESET Managementエージェントの場合:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

構成およびデータベースファイルはアンインストール中に削除されます。データベースファイルを保持するには、データベースのSQLダンプを作成するか、`--keep-database`パラメータを使用します。

アンインストール後に次の点を確認します。

- サービス`eraserver`が削除されていること。
- フォルダ`/etc/opt/eset/RemoteAdministrator/Server/`が削除されていること。

データの復元が必要になる場合に備えて、アンインストールを実行する前に、データベースダンプバックアップを作成することをお勧めします。
エージェントの再インストールの詳細については、関連する章を参照してください。
エージェントアンインストールのトラブルシューティングについては、ESET Managementエージェントアンインストールのトラブルシューティングを参照してください。

macOS - ESET ManagementエージェントおよびESET Endpoint製品のアンインストール

ESET ManagementエージェントおよびESET Endpoint製品をローカルでアンインストールするかESET PROTECT On-Premを使用してリモートでアンインストールします。

ESET ManagementエージェントおよびESET Endpoint製品のローカルアンインストールの詳細な手順については、ナレッジベース記事を参照してください。

ESET Endpoint製品をリモートでアンインストールする場合は、必ずESET Managementエージェントをアンインストールする前にアンインストールしてください。

ESET Managementエージェントをローカルでアンインストールする

1. **Finder**をクリックして、新しい**Finder**ウィンドウを開きます。
2. **アプリケーション** > **Ctrl**を押したまま、**ESET Managementエージェント**をクリックし、コンテキストメニューから**パッケージコンテンツを表示**を選択します。
3. **コンテンツ** > **スクリプト**に移動し、**Uninstaller.command**をダブルクリックして、アンインストーラーを実行します。
4. パスワードの入力を求められたら、管理者パスワードを入力し、**Enter**キーを押します。
5. ESET Managementエージェントがアンインストールされると、**処理完了**のメッセージが表示されます。

ターミナル経由でESET Managementエージェントをローカルでアンインストールする

1. **検索** > **アプリケーション** > **ユーティリティ** > **ターミナル**を開きます。
2. 次のコードを入力し、**Enterキー**を押します。

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. パスワードの入力を求められたら、管理者パスワードを入力し、**Enter**キーを押します。

4. ESET Managementエージェントがアンインストールされると、**処理完了**のメッセージが表示されます。

ESET Managementを使用してESET PROTECT On-Premエージェントをリモートでアンインストールする

コンピューターで、macOSコンピューターをクリックし、**削除**を選択しますESET Managementエージェントをアンインストールし、コンピューターを管理から削除します。

エージェントアンインストールのトラブルシューティングについては、ESET Managementエージェントアンインストールのトラブルシューティングを参照してください。

ESET Endpoint製品をローカルでアンインストールする

1. **Finder**をクリックして、新しい**Finder**ウィンドウを開きます。

2. **アプリケーション** > **Ctrl**を押したまま、**ESET Endpoint Security**または**ESET Endpoint Antivirus**をクリックし、コンテキストメニューから**パッケージの内容を表示**を選択します。

3. **コンテンツ** > **ヘルパー**に移動し、**Uninstaller.app**をダブルクリックして、アンインストーラーを実行します。

4. **アンインストール**をクリックします。

5. パスワードの入力を求められたら、管理者パスワードを入力し、**OK**をクリックします。

6. ESET Endpoint SecurityまたはESET Endpoint Antivirusが正常にアンインストールされると、**アンインストール成功**のメッセージが表示されます。**[閉じる]をクリックしますし**

ターミナル経由でESET Endpoint製品をローカルでアンインストールする

1. **検索** > **アプリケーション** > **ユーティリティ** > **ターミナル**を開きます。

2. 次のコードを入力し、**Enterキー**を押します。

- アンインストールESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- アンインストールESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
```

```
Contents/Scripts/uninstall.sh
```

3. パスワードの入力を求められたら、管理者パスワードを入力し、**Enter**キーを押します。

4. ESET Endpoint製品がアンインストールされると、**処理完了**のメッセージが表示されます。

ESET PROTECT On-Premを使用してESET Endpoint製品をリモートでアンインストールする

ESET Managementを使用してESET PROTECT On-Premエージェントをリモートでアンインストールするには、次のオプションのいずれかを使用できます。

- **コンピューター**で、macOSコンピューターをクリックし、**詳細 > インストールされたアプリケーション > ESET Endpoint Security**または**ESET Endpoint Antivirus**を選択して、**アンインストール**ボタンをクリックします。
- ソフトウェアアンインストールタスクを使用します。

別のサーバーへの移行後に古いESET PROTECT/MDMサーバーを使用停止する

新しいESET PROTECTサーバ/MDMが実行中であり、クライアントコンピュータとモバイルデバイスが新しいESET PROTECT On-Premに正しく接続されていることを確認します。

別のサーバーにへの移行後に、古いESET PROTECTサーバ/MDMを使用停止するときに2つのオプションがあります。

I.サーバーコンピューターのOSを保持し、再利用する

1. 古いESET PROTECT Serverサービスを停止します

2. (DROP DATABASE) 古いESET PROTECTサーバーデータベースインスタンス(Microsoft SQLまたはMySQL)を削除します。

データベースを新しいESET PROTECTサーバーに移行した場合は、アンインストールする前に、古いESET PROTECTサーバーで必ずデータベースを削除し、新しいESET PROTECTサーバーデータベースからライセンスの関連付けが解除(削除)されないようにしてください。

3. 古い ESET PROTECT On-Prem /MDMサーバーとそのすべてのコンポーネント(ESET Managementエージェント、Rogue Detection Sensor、MDMなどを含む)をアンインストールします。

   - ESET PROTECT On-Premのアンインストール—Windows
   - ESET PROTECT On-Premのアンインストール - Linux

データベースに依存する他のソフトウェアがある場合は、データベースをアンインストールしないでください。

4. アンインストール後にサーバーのオペレーティングシステムの再起動を計画します。

II.サーバーコンピューターを保持する

ESET PROTECT On-Prem/MDMを削除する最も簡単な方法は、インストールされているディスクをフォーマットすることです。

⚠ これによりOSを含むディスクのすべての項目が消去されます。

トラブルシューティング

ESET PROTECT On-Premは複雑な製品で、複数の他社ツールを使用し、多くのOSプラットフォームをサポートしているため、トラブルシューティングが必要な問題が発生することがあります。

ESETマニュアルでは、複数のESET PROTECT On-Premのトラブルシューティング方法を説明しています。ESET PROTECT On-Premに関する一般的な問題の解決については、一般的なインストールの問題に対する回答を参照してください。ESETビジネス製品の既知の問題を参照してください。

問題を解決できない場合

- 各ESET PROTECTコンポーネントにはログファイルがあり、詳細レベルを設定できます。ログを確認し、発生している問題を説明できるエラーを特定します。
- 各コンポーネントのログの詳細レベルはポリシーで設定されます > **トレースログの詳細レベル** – ログの詳細を設定して収集されログに記録する情報のレベル、**トレース**（情報）から**クリティカル**（最重要情報）までを決定することができます。 ポリシーを有効にするには、デバイスに適用する必要があります。

  oESET Managementエージェントポリシー *trace.log*で詳細なESET Managementエージェントロギングを有効にするには*trace.log*と同じフォルダに拡張子なしでダミーファイルの*traceAll*を作成し、コンピューターを再起動します(ESET Managementエージェントサービスを再起動します)。

  oESET Bridgeポリシー

  oESET Mobile Device Connectorポリシー – ポリシーを有効にするには、デバイスに適用する必要があります。MDMトラブルシューティングも参照してください。

  oESET PROTECTサーバーのログの詳細レベルは設定にあります。

- 問題を解決できない場合は、ESETセキュリティフォーラムを使用して、発生しうる問題の情報をESETコミュニティに相談できます。
- ESETテクニカルサポートに問い合わせるときには、ESET Log Collectorまたは診断ツールを使用してログファイルを収集するように求められる場合があります。問題を迅速に解決するために、サポートに問い合わせるときにはログを添付することを強くお勧めします。

オフライン環境でのESET PROTECTコンポーネントのアップグレード

次の手順に従い、インターネットに接続していないESET PROTECTコンポーネントとESETエンドポイント製品をアップグレードします。

オフライン環境でのコンポーネントアップグレードタスクは、次の条件を満たしている場合に使用できます。
• 利用可能なオフラインリポジトリがあること。
• ESET Managementエージェントのリポジトリの場所は、アクセス可能な場所が指定されたポリシーを使用して設定されます。

まずESET PROTECTサーバーとWebコンソールのアップグレードを実行します。

1. サーバーで実行されているESET管理コンソールのバージョンを確認します。

2. ESETダウンロードサイトから、最新のWindows版オールインワンインストーラーまたは最新のLinux版スタンドアロンESET PROTECTコンポーネントインストーラーをダウンロードします。

3. まずESET PROTECTサーバーとESET PROTECT Webコンソールのアップグレードを実行します。

   • Windows - オールインワンインストーラーを使用したアップグレード

   • Linux - 手動コンポーネントベースアップグレード

Web コンソールとApache Tomcatアップグレードによって、オフラインヘルプファイルがクリアされます。古いバージョンのESET PROTECT On-Premのオフラインヘルプを使用していた場合は、アップグレード後にESET PROTECT On-Prem 11.0用に再作成して、最新のオフラインヘルプがESET PROTECT On-Premバージョンと一致するようにします。

ESETエンドポイント製品のオフラインアップグレードを続行します

1. クライアントにインストールされているESET製品を確認しますESET PROTECT Webコンソールを開き、**[ダッシュボード] > [ESETアプリケーション]**に移動します。

2. 最新バージョンのESETエンドポイント製品がインストールされているのを確認します。

3. ESETダウンロードサイトからオフラインインストール中に設定されたローカルリポジトリへインストーラーをダウンロードします。

4. ESET PROTECT Webコンソールからソフトウェアインストールタスクを実行します。

一般的なインストールの問題の解決方法

解決するエラーメッセージのセクションを展開します。

ESET PROTECTサーバー

ESET PROTECTサーバーサービスが起動しない

破損したインストール

- レジストリキーが見つからない、ファイルが見つからない、またはファイル権限が無効である可能性があります。
- ESETオールインワンインストーラーには固有のログファイルがあります。コンポーネントを手動でインストールするときには、MSIロギング方法を使用します。

リスニングポートが既に使用されている(通常は2222および2223)

OSに合ったコマンドを使用します。

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

データベースが実行中ではない/データベースに接続できない

- Microsoft SQL Server:ポート1443がデータベースサーバーとの接続で使用可能であることを確認するか、SQL Server Management Studioにログインします。
- MySQL:ポート3306がデータベースサーバーとの接続で使用可能であることを確認するか、データベースインターフェイス(たとえばMySQL コマンドラインインターフェイスまたは`phpmyadmin`を使用)にログインします。

破損したデータベース

複数のSQLエラーがESET PROTECTサーバーログファイルに表示されます。バックアップからデータベースを復元することをお勧めします。バックアップが存在しない場合は、ESET PROTECT On-Premを再インストールします。

不十分なシステムリソース(RAM、ディスク領域)

実行中のプロセスとシステムパフォーマンスを確認します。

- Windowsユーザー:タスクマネージャーまたはイベントビューアーを実行し、情報を確認します。
- Linuxユーザー:次のコマンドのいずれかを実行します。

`df -h`(ディスク領域情報の確認)
`cat /proc/meminfo`(メモリ領域情報の確認)
`dmesg` (Linuxシステム正常性の確認)

ESET PROTECTサーバーインストール中のODBCコネクターの問題

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

マルチスレッドをサポートするODBCドライバーバージョンを再インストールするか、ODBC構成セクションに従い*odbcinst.ini*を再構成します。

ESET PROTECTサーバーインストール中のデータベース接続エラー

ESET PROTECTサーバーのインストールが次の汎用エラーメッセージで終了します。

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

インストールログからのエラーメッセージ

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group
value 100663296 is too low.
```

データベースドライバーの構成がODBC構成セクションで示す内容と一致していることを確認します。

ESET Managementエージェント

ESET Managementエージェントアンインストールのトラブルシューティング

• ESET Managementエージェントのログファイルを確認します。
• ESET アンインストーラーまたは標準以外の方法(ファイルの削除、ESET Managementエージェントサービス、レジストリエントリの削除など)によってESET Managementエージェントをアンインストールできます。同じコンピューターにESETエンドポイント保護がある場合は、自己防衛が有効なため、この方法はできません。
•メッセージ「データベースをアップグレードできません。最初に製品を削除してください」がエージェントアンインストール - ESET Managementエージェントの修復中に表示される
1.[コントロールパネル] > [プログラムと機能]をクリックし、**[ESET Managementエージェント]**をダブルクリックします。
2.[次へ] > [修復]をクリックして、手順に従います。
ESET Managementエージェントをアンインストールするすべての方法については、アンインストールセクションを参照してください。

エージェントインストール中にエラーコード1603が発生しました

このエラーは、インストーラーファイルがローカルディスクにない場合に発生することがあります。この問題を修正するには、インストーラーファイルをローカルディレクトリにコピーし、インストールを再実行します。ファイルが既に存在する場合、またはエラーが解決しない場合は、ナレッジベースの手順に従ってください。

Linuxでのエージェントインストール中にエラーメッセージが表示される

エラーメッセージ

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

このエラーの考えられる原因は、インストールコマンドのファイル名が正しくありません。コンソールは大文字と小文字を区別します。たとえば、`Agent.pfx`は`agent.pfx`と同じではありません。

エージェントESET ManagementはESET PROTECTサーバーに接続できません

エージェント接続のトラブルシューティングとナレッジベース記事を参照してください。

エージェントスクリプトインストーラーがコード30で終了しました

カスタムインストーラーの場所でエージェントスクリプトインストーラーを使用しているため、スクリプトを正常に編集できませんでした。ヘルプページを確認し、再試行してください。

Webコンソールへの接続

ESET BridgeHTTPプロキシ

ESET Rogue Detector Sensor

なぜ次のエラーメッセージがESET Rogue Detectorのtrace.logに継続的に出力されるのですか。

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:
The system cannot find the device specified. (20)
```

これはWinPcapの問題です。ESET Rogue Detector Sensorサービスを停止し、最新バージョンのWinPcap (4.1.0以上)を再インストールし、ESET Rogue Detector Sensor サービスを再開します。

Linux

CentOS LinuxでlibQtWebKit依存関係が見つからない

次のエラーが表示されます。

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

ナレッジベース記事の手順に従います。

CentOS 7のESET PROTECTサーバーインストールが失敗しました

次のエラーが表示されます。

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

この問題は環境/ロケール設定が原因であると考えられます。サーバーインストーラースクリプトの前に次のコマンドを実行すると解決されます。

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

エラーコード -2068052081がMicrosoft SQL Serverインストール中に発生する。

コンピューターを再起動して、もう一度セットアップを実行します。問題が解決しない場合は、SQL Server Native Clientをアンインストールし、もう一度インストールを実行します。問題が解決しない場合は、すべてのMicrosoft SQL Server製品をアンインストールし、コンピューターを再起動してから、もう一度インストールを実行します。

エラーコード -2067922943がMicrosoft SQL Serverインストール中に発生する。

システムがESET PROTECT On-Premのデータベース要件を満たしていることを確認します。

エラーコード -2067922934がMicrosoft SQL Serverインストール中に発生する。

正しいユーザーアカウント権限があることを確認します。

Webコンソールに「データを読み込めませんでした」と表示される。

Microsoft SQL Serverはトランザクションログ用に可能な限り多くのディスク領域を使用しようとします。これをクリーンアップする場合は、公式のMicrosoft社のWebサイトをご覧ください。

エラーコード -2067919934がMicrosoft SQL Serverインストール中に発生する。

すべての前の手順が正常に完了したことを確認します。このエラーはシステムファイルの誤った設定が原因です。コンピューターを再起動して、もう一度インストールを実行します。

ログファイル

ESET PROTECTコンポーネントはロギングを実行します。ESET PROTECTコンポーネントは特定のイベントに関する情報をログファイルに書き込みます。ログファイルの場所はコンポーネントによって異なります。次にログファイルの場所の一覧を示します。

Windows

ESET PROTECTコンポーネント	ログファイルの場所
ESET PROTECTサーバー	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

ESET PROTECTコンポーネント	ログファイルの場所
ESET Managementエージェント	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* エージェント接続のトラブルシューティングも参照してください。
ESET PROTECT Webコンソールおよび Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* https://tomcat.apache.org/tomcat-9.0-doc/logging.htmlも参照してください。
モバイルデバイスコネクター	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* MDMトラブルシューティングも参照してください。
Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
ESET Bridge(HTTPプロキシ)	ESET Bridgeオンラインヘルプを参照してください。

*C:\ProgramData*は既定では非表示です。フォルダーを表示するには：
1.**スタート > コントロールパネル > フォルダーオプション > 表示**に移動します。
2.**非表示のファイル、フォルダー、ドライブを表示する**を選択し、**OK**をクリックします。

Linux

ESET PROTECTコンポーネント	ログファイルの場所
ESET PROTECTサーバー	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Managementエージェント	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
モバイルデバイスコネクター	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* MDMトラブルシューティングも参照してください。
ESET Bridge(HTTPプロキシ)	ESET Bridgeオンラインヘルプを参照してください。
ESET PROTECT Webコンソールおよび Apache Tomcat	*/var/log/tomcat/* https://tomcat.apache.org/tomcat-9.0-doc/logging.htmlも参照してください。
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

ESET PROTECT仮想アプライアンス

ESET PROTECTコンポーネント	ログファイルの場所
ESET PROTECT VA設定	*/root/appliance-configuration-log.txt*
ESET PROTECTサーバー	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Bridge(HTTPプロキシ)	ESET Bridgeオンラインヘルプを参照してください。

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

診断ツール

診断ツールはすべてのESET PROTECTコンポーネントに含まれています。製品コンポーネントの問題を解決することを目的に、テクニカルサポートエージェントや開発者が使用可能なログを収集して圧縮する

ために使用されます。

診断ツールの場所

Windows

フォルダー*C:\Program Files\ESET\RemoteAdministrator\[product]* **Diagnostic.exe**

Linux

サーバーの次のディレクトリ:*/opt/eset/RemoteAdministrator/[product]/***Diagnostic[product]**実行ファイルがあります。(1単語、たとえば**DiagnosticServer**、**DiagnosticAgent**)

使用方法(Linux)

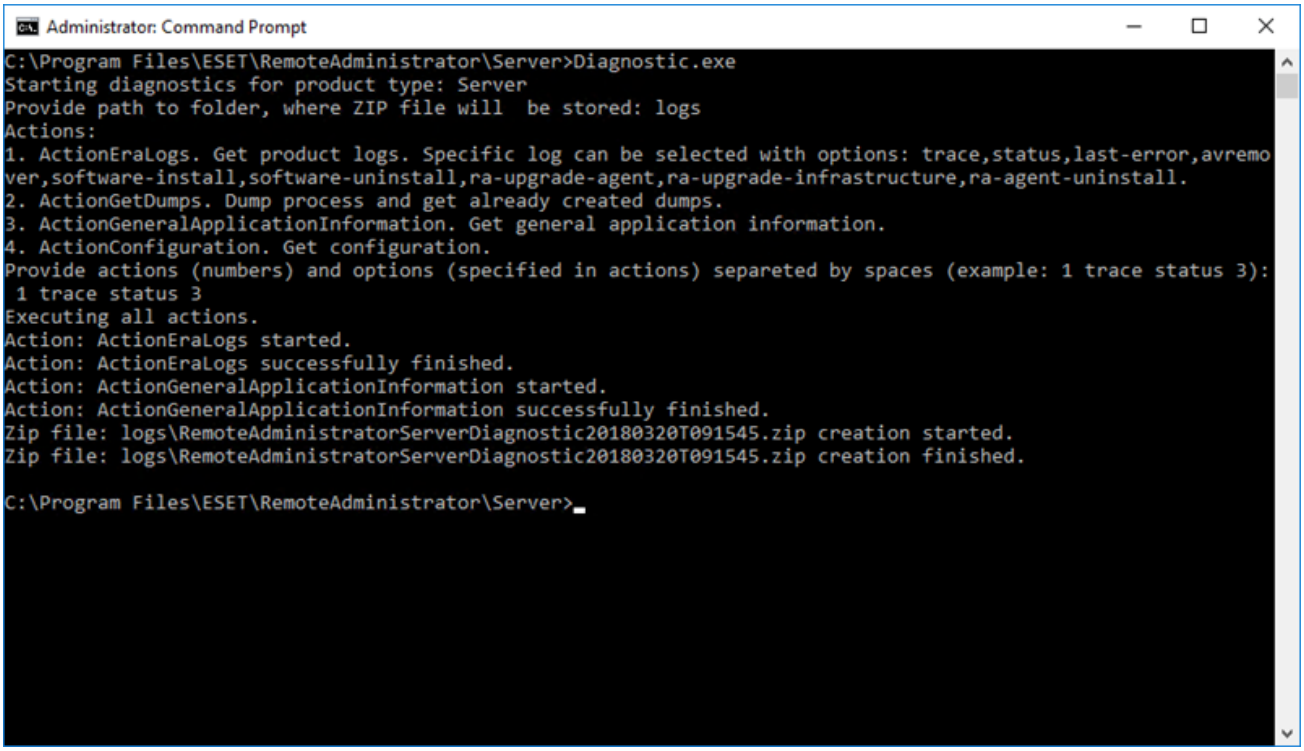
ターミナルでrootとして診断実行ファイルを実行し、画面に表示される手順に従います。

使用方法(Windows)

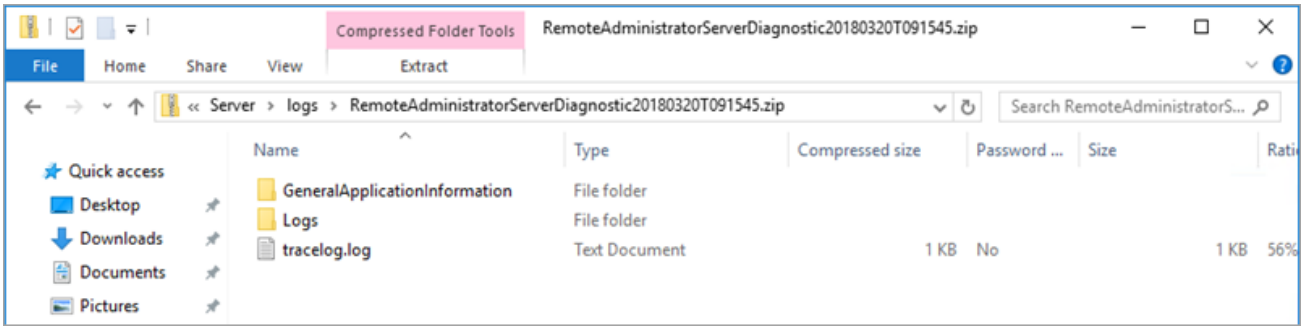
1. コマンドプロンプトを使用してツールを実行します。

2. 保存するログファイルの場所(この例では"logs")を入力し、**Enter**を押します。

3. 収集する情報を入力します(この例では`1 trace status 3`)。詳細については、以下の「**アクション**」を参照してください。



4. 完了したら、診断ツールの場所の「**logs**」ディレクトリに*.zip*ファイルで圧縮されたログファイルが作成されます。



アクション

- **ActionEraLogs** – すべてのログの保存中に作成されるログフォルダ。特定のログのみを指定するには、スペースを使用して、各ログを区切ります。

- **ActionGetDumps** – 新しいフォルダが作成されます。処理ダンプファイルは一般的に、問題が検出された場合に作成されます。重大な問題が検出された場合、ダンプファイルはシステムによって作成されます。手動で確認するには%temp%フォルダ(Windows)または/tmp/フォルダ(Linux)に移動し、dmpファイルを挿入します。

> コンポーネントサービス(Agent、Server、RD Sensor)が実行中でなければなりません。

- **ActionGeneralApplicationInformation** - GeneralApplicationInformationフォルダーが作成され、中には*GeneralApplicationInformation.txt*があります。ファイルには、製品名および現在インストールされている製品のバージョンなどのテキスト情報があります。

- **ActionConfiguration** – ファイルstorage.luaが保存される設定フォルダーが作成されます。

ESET PROTECTサーバーのアップグレード/移行後の問題

インストールの破損または不明なログファイルエラーにより、ESET PROTECT Severサービスを起動できない場合は、以下の手順で修復処理を実行します。

> 修復処理を開始する前に、データベースサーバーバックアップを実行することをお勧めします。

1. **[スタート] > [コントロールパネル] > [プログラムと機能]**に移動し、**ESET PROTECTサーバー**をダブルクリックします。

2. **修復**を選択し、**次へ**をクリックします。

3. 既存のデータベース接続設定を再利用し、**次へ**をクリックします。確認を求められたら、**はいをクリックします**。データベース接続情報は次の場所から確認できます。*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. **既にデータベースに保存されている管理者パスワードを使用する**を選択し、**次へ**をクリックします。

5. **既存の証明書を保持する**を選択し、**次へ**をクリックします。

6. 有効な製品認証キーでESET PROTECTサーバーをアクティベーションするか、**後でアクティベーション**(詳細な手順については*ライセンス管理*を参照)を選択し、**次へ**をクリックします。

7. **修復**をクリックします。

8. Webコンソールに接続し、問題がないかどうかを確認します。

他のトラブルシューティングシナリオ

ESET PROTECTサーバーが実行されていないが、データベースバックアップがある

1. データベースバックアップを復元します。

2. 新しいコンピューターは、前のインストールと同じIPアドレスまたはホスト名を使用し、エージェントが接続していることを確認します。

3. ESET PROTECTサーバーを修復し、復元したデータベースを使用します。

ESET PROTECTサーバーが実行されていないが、エクスポートされたサーバー証明書と認証局がある

1. 新しいコンピューターは、前のインストールと同じIPアドレスまたはホスト名を使用し、エージェントが接続していることを確認します。

2. バックアップ証明書を使用してESET PROTECTサーバーを修復します(修復時に**ファイルから証明書を読み込む**を選択し、手順に従います)。

ESET PROTECTサーバーが実行されておらず、データベースバックアップもESET PROTECTサーバー証明書と認証局もない

1. ESET PROTECTサーバーを修復します。

2. 次の方法のいずれかでESET Managementエージェントを修復します。

   - エージェントインストーラースクリプト
   - リモート展開(ターゲットコンピューターのファイアウォールを無効にする必要があります)
   - 手動エージェントコンポーネントインストーラー

MSIロギング

エージェントなどESET ManagementESET PROTECTコンポーネントをWindowsに正常にインストールできない場合に有用です。

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT On-Prem API

ESET PROTECT ServerApi (*ServerApi.dll*) はアプリケーションプログラミングインターフェイスで、ニーズや仕様を満たすためのカスタムアプリケーションを作成する一連の機能とツールです。ServerApiを使用すると、ESET PROTECTの管理、レポートの生成と受信など、通常はESET PROTECT On-Prem Webコンソール経由で実行するカスタムインターフェイス、機能、処理をアプリケーションで実装できます。

C言語の詳細と例および使用可能なJSONメッセージの一覧については、次のオンラインヘルプを参照してください。

ESET PROTECT On-Prem 11.0 API

FAQ

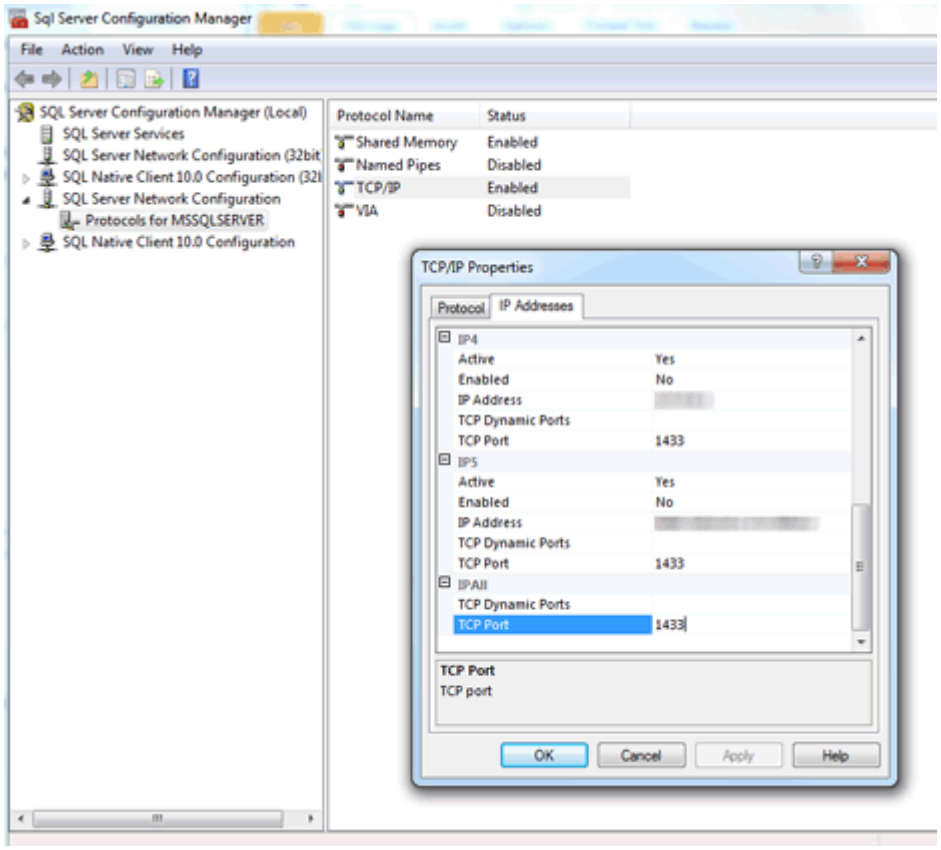
なぜJavaをサーバーにインストールするのですか。セキュリティリスクにはなりませんか。セキュリティ会社とセキュリティフレームワークの大半は、コンピューター、特にサーバーからJavaをアンインストールすることを推奨しています。

ESET PROTECT Webコンソールが機能するには、Java/OpenJDKが必要です。JavaはWebベースのコンソールの業界標準であり、主要なWebコンソールはすべてJavaとWebサーバ(Apache Tomcat)を使用して処理を実行しています。Javaはマルチプラットフォームのwebサーバーをサポートするために必要です。セキュリティの理由で、専用コンピューターにWebサーバーをインストールすることもできます。

⚠ 2019年1月以降、ビジネス、商業、本番利用向けのOracle JAVA SE 8公開アップデートには、商業ライセンスが必要です。JAVA SEサブスクリプションを購入しない場合は、別の無料の製品に移行できます。サポートされたバージョンのJDKを参照してください。

SQL Severが使用するポートはどのように決定するのですか。

SQL Serverで使用されるポートを決定する方法は複数あります。SQL Server Configuration Managerを使用すると、最も正確な結果が得られます。SQL Server Configuration Managerでこの情報を検索する場所の例については、以下の図を参照してください。



SQL Server Express (ESET PROTECT On-Premパッケージに含まれる)をWindows Server 2012にインストールした後、標準SQLポートがリスニングしていないようです。既定の1433以外のポートでリスニングしている可能性があります。

どのようにしてMySQLを設定し大きいパケットサイズを許可するのですか。

WindowsまたはLinuxについてはMySQLインストールと構成を参照してください。

SQLを自分でインストールする場合、どのようにESET PROTECT On-Prem

その必要はありません。データベースは*Server.msi*インストーラーによって作成されますESET PROTECTインストーラーによっては作成されません。手順の簡素化を目的に、ESET PROTECTインストーラーにはSQL Serverをインストールし、*Server.msi*インストーラーによってデータベースが作成される手順が含まれています。

ESET PROTECT On-Premインストーラーは、適切な接続詳細と資格情報がある場合、既存のMicrosoft SQL Serverインストールで新しいデータベースを作成できますか。インストーラーでサポートされるSQL serverのバージョンが異なる（2014、2019など）場合に便利です。

データベースは、*Server.msi*によって作成されます。個別にインストールされたSQL Serverインスタンス上にESET PROTECTデータベースを自分で作成できます。サポート対象のMicrosoft SQL Serverのバージョンは2014以降です。

ESET PROTECT On-Prem 11.0オールインワンインストーラーでは、既定でMicrosoft SQL Server Express 2019がインストールされます。

- 古いWindowsエディション（サーバー2012またはSBS 2011）を使用している場合は、Microsoft SQL Server Express 2014が既定でインストールされます。

- インストーラーはデータベース認証（*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*に保存）のランダムなパスワードを自動的に生成します。

Microsoft SQL Server Expressには各関係データベース10 GBのサイズ制限があります。次の環境ではMicrosoft SQL Server Expressの使用は推奨されません。
- エンタープライズ環境または大規模ネットワーク。
- ESET PROTECT On-PremとESET Inspect On-Premを使用する場合。

既存のSQL ServerにインストールしているSQL Serverはビルトインの Windows認証モードを既定で使用するべきですか。

いいえ。Windows認証モードはSQL Serverで無効にでき、唯一のログイン方法は、SQL Server認証（ユーザー名とパスワードの入力）を使用することです。ESET PROTECTサーバーのインストール中には、混合モード認証(SQLサーバー認証およびWindows認証）が必要です。SQLServerを手動でインストールする場合は、ルートパスワードを作成し、安全な場所に後から使用できるように保存することをお勧めします（ルートユーザー名は「sa」で、セキュリティ管理者を表します）。ルートパスワードは、ESET PROTECTサーバーのアップグレード時に必要になる場合があります。ESET PROTECTサーバーをインストールした後に、Windows認証を設定できます。

MySQLの代わりにMariaDBを使用できますか。

いいえ。MariaDBはサポートされていません。 必ずサポートされているバージョンのMySQL ServerとODBCコネクターをインストールしてください。 MySQLインストールおよび構成を参照してください。

ESET PROTECT On-Premインストーラーによって(http://www.microsoft.com/en-us/download/details.aspx?id=17851)にリダイレクトされるためMicrosoft .NET Framework 4をインストールする必要がありますがWindows Server 2012 R2 SP1の新規インストールでは動作しませんでした。

このインストーラーは、Windows Server 2012のセキュリティポリシーのためWindows Server 2012では使用できませんMicrosoft .NET Frameworkは、**ロールと機能の追加ウィザード**でインストールする必要があります。

SQL Serverインストールが実行中かどうかを判断するのは非常に困難です。インストールに10分以上かかる場合は、どのように実行されている処理を判断できるのでしょうか。

SQL serverインストールは、ごくまれにですが、最大で1時間かかる場合があります。インストール時間はシステム性能によって異なります。

どのようにしてWebコンソールの管理者パスワードのリセット(セットアップ中に入力)ができるのでしょうか。

パスワードをリセットするには、サーバーインストーラを実行し、[**修復**]を選択します。データベースの作成中にWindows認証を使用していない場合は、ESET PROTECTデータベースにアクセスするためにパスワードが必要な場合があります。

- 一部の修復オプションは保存されているデータを削除する可能性があるため注意してください。
- パスワードリセットを実行すると、2FAが無効になります。.

ESETPROTECTOn-Premに追加するコンピューターのリストが入ったファイルをインポートするときには、どのようなファイル形式にする必要がありますか。

次の行のような形式になります。

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX

すべてがルートグループの必要な名前です。

Apache Tomcatの代わりにIISを使用できますか。別のHTTPサーバーは使用できますか。

IISはHTTPサーバーです。Webコンソールでは、Javaサーブレットコンテナ(Apache Tomcatなど)を実行する必要があります。HTTPサーバーは不十分です。IISをJavaサーブレットコンテナに変更する解決策がありますが、一般的にこの方法はサポートされません。

ESETは異なる製品のApache Tomcatを使用しています。

ESET PROTECT On-Premにはコマンドラインインターフェイスがありますか。

はい。ESET PROTECT On-Prem ServerApiがあります。

ドメインコントローラーにESET PROTECT On-Premをインストールできますか。

ドメインコントローラーにはSQL Serverをインストールしないでください(たとえば、Windows SBS / Essentials)。別のサーバーにESET PROTECT On-Premをインストールするか、インストール中にSQL Server Expressコンポーネントを選択しない(この場合、既存のSQL ServerまたはMySQLを使用してESET PROTECTデータベースを実行する必要があります)ことをお勧めします。

ESET PROTECTサーバーインストールは、SQLがシステムにインストール済みであるかどうかを検出しますか。インストール済みの場合は

どうなりますか MySQLは検出されますか。

インストールウィザードを使用し、SQL Expressのインストールを選択した場合は、ESET PROTECT On-Premはシステムで実行中のSQLがあるかどうかを確認します。システムでSQLが実行中の場合は、既存のSQLをアンインストールする通知が表示されます。この後に、インストールを再実行するかSQL ExpressなしでESET PROTECT On-PremをインストールしますESET PROTECT On-Premのデータベース要件を参照してください。

リリースバージョンと関連付けられたESET PROTECTコンポーネントはどこにありますか。

詳細については、ナレッジ記事を参照してください

ESET PROTECT On-Premから最新バージョンへのアップグレードはどのように実行するのですか。

アップグレード手順を参照してください。

インターネット接続なしでシステムを更新するにはどのようにするのですか。

ESETアップデートサーバー(アップデートファイルがキャッシュされる場所)に接続可能なコンピューターにインストールされたESET Bridge HTTPプロキシを使用し、エンドポイントがローカルネットワーク上のHTTPプロキシを参照するようにします。サーバーがインターネットに接続していない場合は、コンピューターでエンドポイント製品のミラー機能を有効にしUSBドライブを使用してアップデートファイルをこのコンピューターに配信し、アップデートサーバーとしてこれを使用するように他のすべてのオフラインコンピューターを構成します。

オフラインインストールの実行方法については、次の手順に従いますを参照してください。

SQL Serverが自動的に初期ESET PROTECTインストールによって設定さ

れている場合ESET PROTECT On-Premサーバーを再インストールし、既存のSQL Serverに接続するにはどうすればよいですか。

元のESET PROTECTサーバーをインストールしたユーザーアカウント(ドメイン管理者のアカウントなど)の新しいESET PROTECTサーバーのインスタンスをインストールしている場合は、**[Windows認証経由でMS SQL Server]**を使用できます。

Linux上でActive Directory同期の問題が発生した場合どのように修正するのですか。

ドメイン名がすべて大文字(`administrator@test.local`ではなく`administrator@TEST.LOCAL`)で入力されていることを確認します。

リポジトリの代わりに、独自のネットワークリソース(SMB共有など)を使用する方法はありますか。

パッケージがある直接URLを指定するように選択できます。ファイル共有を使用している場合は、file://の後にファイルへの完全ネットワークパスを続けて指定します。たとえば、

file://\\eraserver\install\ees_nt64_ENU.msi

どのようにしてパスワードをリセットまたは変更するのですか。

管理者アカウントは、個別の管理者のアカウントを作成する場合にのみ使用することをお勧めします。管理者アカウントが作成されたら、管理者パスワードを保存し、管理者アカウントは使用しないでください。この方法では、パスワードリセット/アカウント詳細でのみ管理者アカウントを使用できます。

ビルトインのESET PROTECT On-Prem管理者アカウントのパスワードをリセットする方法:

1. **[プログラムと機能]**を開き(appwiz.cpl)ESET PROTECTサーバーを見つけ、右クリックします。
2. コンテキストメニューから**[変更]**をクリックします。
3. **[修復]**を選択します。
4. データベース接続の詳細を指定します。
5. **[既存のデータベースを使用]**を選択して、アップグレードを適用します。

6.[**データベースに既に保存されているパスワードを使用**]オプションがオフになっていることを確認し、新しいパスワードを入力します。

7.新しいパスワードでESET PROTECT Webコンソールにログインします。

任意のアカウント機能に基づいて特定のアクセス権を持つその他のアカウントを作成することを強くお勧めします。

ESET PROTECTサーバーとESET PROTECT Webコンソールポートはどのように変更するのですか。

Webサーバー構成でポートを変更し、新しいポートへのWebサーバー接続を許可する必要があります。手順は次のとおりです。

1. Webサーバーをシャットダウンします

2. Webサーバー構成でポートを修正します。

   a)ファイル*webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*を開きます

   b)新しいポート番号を設定します(例:`server_port=44591`)

3. Webサーバーを再起動します。

オールインワンインストーラーを使用して ERA5.x/6.xまたはESMC7.xを直接ESET PROTECT On-Prem 11.0にアップグレードできますか。

ESET PROTECT On-Prem 9.0以降から直接ESET PROTECT On-Prem 11.0にアップグレードできます。サポート終了バージョン7.2–8.xからの直接アップグレードはテストされておらず、サポートされていません。

ERA 5.x/6.xまたはESMC 7.0/7.1をお持ちの場合ESET PROTECT On-Prem11.0への直接アップグレードはサポートされていませんESET PROTECT On-Prem11.0のクリーンインストールを実行してください。

ESET PROTECT On-Premでエラーメッセージまたは問題が発生します。どうすればよいですか。

トラブルシューティングFAQを参照してください。

エンドユーザーライセンス契約

発効日：2021年10月19日

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。**本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、**プライバシーポリシー**に同意したことになります。**

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（「本契約」）は、Einsteinova 24, 85101 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o.（ESETまたは「供給者」）と、自然人または法人であるお客様（「お客様」または「エンドユーザー」）との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意し、プライバシーポリシーを承諾するものとします。本契約の規定またはプライバシーポリシーに同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの供給者にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.ソフトウェア。(i)本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明（「ドキュメント」）(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート（該当する場合）を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.インストール、コンピューター、およびライセンスキー。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコン

ピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.**ライセンス**。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します（以下「ライセンス」とします）。

a) **インストールおよび使用。**お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(i) 本ソフトウェアがインストールされている1台のコンピューターを意味します(ii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下MUAとします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) **Home/Business Edition**本ソフトウェアのHome Editionバージョンは、家庭および家族での利用に限定された個人または非商業環境でのみ使用されるものとします。本ソフトウェアを商業環境、またはメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) **ライセンス契約の期間。**お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) **OEMソフトウェア。**OEMに分類されたソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア。**再販不可品NFRまたは試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除。**ライセンス契約は，その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機

能を使用する権利を取り消す権利があるものとします。

4.**データ収集機能およびインターネット接続要件。**本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。本ソフトウェアの機能、ならびに本ソフトウェアの更新およびアップグレードの目的で、インターネットへの接続および該当するデータ収集が必要です。供給者には、本ソフトウェアのアップデートまたはアップグレード(「アップデート」)を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていないかぎり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

アップデートの提供には、サービス終了ポリシ(EOLポリシー」)が適用される場合があります。https://go.eset.com/eol_businessをご覧ください。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、アップデートが提供されません。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.**エンドユーザの権利行使**。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.**権利の制限。**お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを

使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび / またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.**権利の留保**。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.**複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー**。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、賃借、サブライセンス付与、貸与、または譲渡することはできません。

10.**本契約の開始と解除。**本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本ソフトウェアおよび本ソフトウェアの機能を使用するお客様の権利にはEOLポリシーが適用される場合があります。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、本ソフトウェアを使用するお客様の権利が失効します。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.**エンドユーザーの表明**。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.**さらなる義務の否定**。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセン

サーに対して課す義務はありません。

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアのインストール、本ソフトウェアの使用、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事者の法的権利を損なうものではありません。

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、テクニカルサポートが提供されません。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび / またはESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび / またはESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポートの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16.**ライセンスの譲渡**。本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合、(i) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず、(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され、(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17.**正規ソフトウェアの証明。**エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます。(i)供給者または供給者が指定した第三者が発行するライセンス証明書、(ii)締結されている場合、書面によるライセンス契約、(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18.**公共団体および米国政府に対するライセンス**。米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19.**輸出管理規制**

a)お客様は、直接的または間接的に、ESETまたはESETの持ち株会社、ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件を課すすべての法律。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策。

(上記第i項および第ii項で参照される法律、ならびに「貿易管理法」)。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i.ESETが、合理的な意見において、ユーザーが本契約の第19 a)条の条項に違反したか違反する可能性が高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果として ESETが、合理的な意見において、本契約の義務の継続的な履行によって ESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為(あるいは行為または不作為に同意すること)を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20.**通知**。すべての通知、ならびに本ソフトウェアおよびドキュメントの返却は、本契約の第22条に従い、本契約、プライバシーポリシ EOLポリシー、ドキュメントの変更をお客様に通知するESETの権利を損なうことなく ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic宛てに送付する必要があります ESETは、電子メールや、本ソフトウェア経由でのアプリ内通知を送信したり Webサイトにコミュニケーションを投稿したりする場合があります。お客様は、規約、特別な規約、プライバシーポリシーの変更、契約の提案/承諾、またはキャンペーンへの招待、通知または他の法的な通知に関するコミュニケーションを含め、電子的な形式でESETから法的な通知を受信することに同意します。適用される法律で特に別のコミュニケーションの形態が義務付けられている場合を除き、かかる電子的なコミュニケーションは書面を受け取った場合と同義に見なされるものとします。

21.**準拠法**。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22.**一般条項**。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約は英語で締結されました。便宜上またはその他の目的で、本契約書の翻訳が用意されている場合、または本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。

ESETは、(i) 本ソフトウェアまたはESETの事業の方法に関する変更を反映する (ii) 法律、規制、セキュリティの理由から (iii) 悪用または被害を防止するため、関連するドキュメントを更新することで、いつでも、本ソフトウェアを変更し、本契約、付録、補遺、プライバシーポリシ EOLポリシー、ドキュメントまたはその一部を改訂する権利を留保します。これらの条項の改訂は、電子メール、アプリ内通知、または他の電子的な手段で通知されます。お客様が本契約の変更の提案に同意しない場合は、変更の通知を受領してから30日以内にアカウントまたは影響を受ける購入済みのサービスを解約できます。この期限内に本契約を解約しない場合は、提案された変更が承認されたと見なされ、変更の通知を受け取っ

た日時点でお客様側で変更が有効になります。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

契約書の補遺

供給者への情報の転送。供給者への情報の転送には、次のように追加の条項が適用されます。

本ソフトウェアには、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報、管理されたデバイスの情報(「情報」)を含む、データを収集する機能が含まれ、これらの情報を供給者に送信します。情報には、管理されたデバイスに関するデータ（ランダムまたは誤って取得された個人データを含む）が含まれます。本ソフトウェアでこの機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合があります。

ソフトウェアでは、管理されたコンピューターにコンポーネントをインストールする必要があります。これにより、管理されたコンピューターとリモート管理ソフトウェア間の情報の転送が可能になります。転送される情報には、管理されているコンピューターのハードウェアおよびソフトウェア情報、リモート管理ソフトウェアからの管理手順などの管理データが含まれます。管理されたコンピューターから転送されるデータの他のコンテンツは、管理されたコンピューターにインストールされたソフトウェアの設定によって決定されるものとします。管理ソフトウェアからの手順の内容は、リモート管理ソフトウェアの設定によって決定されます。

EULAID: EULA-PRODUCT-PROTECT; 3537.0

プライバシーポリシー

データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic 商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:31333532) (ESET または「当社」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の事項を通知する目的でのみ、本プライバシーポリシーを発行しています。

- 個人データの処理、
- データの機密保持、
- データの主体の権利。

個人データの処理

製品に実装されたESETが提供するサービスは、エンドユーザーライセンス契約(EULA)の条項に従って提供されますが、項目によっては特定の注意が必要になる場合があります ESETは、サービスの提供に関連するデータ収集の詳細について、お客様に説明します ESETは、アップデート/アップグレードサービス ESET LiveGrid® データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。すべてを機能させるために ESETは次の情報を収集する必要があります。

- ESET Security製品の管理には ESET Security製品がインストールされている管理されたコンピューターに関連する、シートIDおよび名前、製品名、ライセンス情報、アクティベーションと有効期限情報、ハードウェアおよびソフトウェア情報などが必要であり、ローカルで保存されます ESETへの自動送信なしで、機能およびサービスの管理と監視を支援するために、管理されているESET Security製品とデバ

イスのアクティビティに関連するログが収集され、提供されます。

• ESET製品がインストールされているプラットフォーム、ハードウェアフィンガープリント、インストールID、クラッシュダンプ、ライセンスID、IPアドレス、MACアドレス、管理されているデバイスを含むこともある製品の構成設定などの製品の動作と機能に関する情報といった、インストールプロセスに関する情報。

• ライセンスIDおよび名前、姓、住所、電子メールアドレスなどの個人データといったライセンス情報は、請求目的、ライセンスの正当性の検証、サービスの提供のために必要です。

• サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。生成されたログファイルやダンプファイルなど、サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

• ESETのサービスの使用に関するデータは、セッションの終了時まで完全に匿名です。セッションの終了後は、個人を特定できる情報は保存されません。

データの機密保持

ESETは、販売、サービス、サポートネットワークの一部として、関連会社またはパートナー経由で、世界中で事業を展開している会社です。ESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じます。ESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合があります。ESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

ESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)
- 個人データの消去を要求する権利、
- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および

- データ移植性の権利。

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk