ESET PROTECT

中小事業者向けガイド

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.

Copyright ©2023 by ESET, spol. s r.o.

ESET PROTECT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。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと遭わず、複製、検索システムへの保存、または転送が禁じられています。

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: 2023年/3月/19日

1 ヘルプ 1
2 概要 1
2.1 管理可能なESETエンドポイント製品 2
2.2 ESET PROTECT 10.0の新機能 2
3 ESET PROTECTコンポーネントとアーキテクチャ 3
4 システム要件 4
4.1 ハードウェア 4
4.2 OS 6
4.3 ネットワーク 8
4.4 ソフトウェア 8
5 ESET PROTECTサーバーのインストール 9
5.1 ESET PROTECTサーバーのオールインワインインストール 10
6 インストール後の手順 23
7 ESET Managementエージェントと ESETエンドポイント製品の展開 24
7.1 展開パッケージの作成 25
7.2 展開パッケージのインストール 29
7.3 他の展開方法 32
7.4 ESET Remote Deployment Tool 33
8 ESET PROTECT Webコンソール 36
8.1 ESET PROTECTガイド 38
8.2 ダッシュボード 39
8.3 コンピューター 40
8.4 グループ 42
8.5 検出 43
8.6 レポート 45
8.7 タスク 46
8.8 ポリシー 47
8.9 通知 48
8.10 ステータス概要 50
8.11 隔離 50
8.12 ライセンス管理 51
8.13 ユーザーと権限設定 53
8.14 証明書 54
9 ヘルプとサポート 55
10 エンドユーザーライセンス契約 55
11 プライバシーポリシー 61

ヘルプ

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、VA展開、およびSMBガイド。
- 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。

概要

このガイドは、最大250のWindows ESETエンドポイント製品を、ESET PROTECT 10で管理する小規模から中規模事業向けです

ESETセキュリティ製品の展開と使用に関する基本概念について説明します。

ESET PROTECT 10

ESET PROTECT10 (旧称ESMC)は、1つの中央の場所からネットワーク環境にあるクライアントワークステーション、サーバー、およびモバイルデバイスで、ESET製品を管理できるアプリケーションです。

ESET PROTECTのビルトインのタスク管理システムでは、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、新しい問題や検出に迅速に対応できます。

ESETPROTECT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のESET Endpoint Securityなど、ESETセキュリティソリューションが存在するかどうかによって異なります。

管理可能なESETエンドポイント製品

ESETエンドポイント製品は主に小規模事業、エンタープライズ環境のワークステーションで使用するために設計され、ESET PROTECTとともに使用できます。

ESET PROTECT 10は次のESETエンドポイント製品の展開、アクティベーション、または管理ができます。

管理可能 ESET PROTECT 10	製品のバージョン
ESET Endpoint Security for Windows	6.5+, 7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus for Windows	6.5+, 7.3, 8.x, 9.x, 10.x
ESET Endpoint Security for macOS	6. 10以降
ESET Endpoint Antivirus for macOS	6. 10以降
ESET Endpoint Antivirus for Linux	7.1, 8.x, 9.x
ESET Endpoint Security for Android	2.x

管理可能なESETセキュリティ製品の一覧も参照してください。

ESET PROTECT 10.0の新機能

拡張VDIサポート

VDI環境を設定するときに、コンピューターハードウェアフィンガープリントの識別情報だけでなく、コンピューターのFQDNでも、コンピュータIDを処理(新しいIDを作成し、既存のIDを更新)できます。詳細を見る

ダークテーマ

ESET PROTECTに追加された新しいダークテーマを試すことができます。コンソールユーザーは、この機能をユーザー設定で有効にできます。詳細を見る

SyslogのCEF形式

共通イベント形式でログをSyslogに送信できます。詳細を見る

その他の改善とユーザビリティの変更

詳細については、変更ログを参照してください。

ESET PROTECTコンポーネントとアーキテクチャ

ESETセキュリティソリューションポートフォリオ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。

- ESET PROTECTサーバー(クライアントコンピューターとの通信を制御)
- ESET PROTECT Webコンソール(ESET PROTECTサーバー用のブラウザーベースのユーザーインターフェイス)
- ESET Managementエージェント(クライアントコンピューターに展開ESET PROTECTサーバーと通信)

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のためインストールすることをお勧めします。

- ESET Bridge (HTTPプロキシ)
- RD Sensor (ネットワーク上の非管理コンピューターを検出可能)

証明書とESET PROTECTコンポーネント構造も参照してください。

サーバー

ESET PROTECTサーバー(エージェント経由)は実行アプリケーションで、ESET Managementエージェント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。

エージェント

エージェント(ESET Managementエージェント)はESET PROTECT の基本的な要素です。クライアントコンピューターは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にタスクを送信する場合、エージェントに送信され、エージェントがクライアントで実行中のESETエンドポイント製品にこのタスクを送信します。

Webコンソールへの接続

ESET PROTECT Webコンソールはブラウザー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。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を使用できます。

ESET Bridge (HTTPプロキシ)

ESET PROTECT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によってプッシュされたESET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 10.0以降ではESET BridgeがApache HTTP Proxyの代わりに導入されます。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。

Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) は、ネットワークでESET PROTECTに登録されていないコンピューターを検索します。このコンポーネントは新しいコンピューターを検索し、自動的にESET PROTECTに追加できます。

Rogue Detection Sensorがネットワーク上の新しいコンピューターを検索するには最大24時間かかることがあります。

新しく検出されたコンピューターは定義済みレポートに一覧表示されるため、簡単にESET Managementエージェントを展開し、特定の静的グループに割り当て、タスクとポリシーを使用して管理できます。

システム要件

ESET PROTECTをインストールする前に、すべてのハードウェア、オペレーティングシステム、ネットワーク、およびソフトウェア要件が満たされていることを確認してください。

ハードウェア

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IOPS[2]
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。

ℹ データベースとESET PROTECT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

OS

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。サポート対象のオペレーティングシステムの一覧も参照してください。

OS	サーバー	エージェント	RD Sensor	MDM
KB4493730およびKB4039648がインストールされているWindows Server 2008 R2 x64 SP1		✔	✔	
KB4493730およびKB4039648がインストールされているWindows Server 2008 R2 CORE x64		✔	✔	
KB4493730およびKB4039648がインストールされているWindows Storage Server 2008 R2 x64		✔	✔	
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
Windows Server 2012 x64	✔	✔	✔	✔
Windows Server 2012 CORE x64	✔	✔	✔	✔
Windows Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2012 R2 CORE x64	✔	✔	✔	✔
Windows Storage Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2016 x64	✔	✔	✔	✔
Windows Storage Server 2016 x64	✔	✔	✔	✔
Windows Server 2019 x64	✔	✔	✔	✔

OS	サーバー	エージェント	RD Sensor	MDM
Windows Server 2022 x64	✔	✔	✔	✔

OS	サーバー	エージェント	RD Sensor	MDM
最新のWindowsアップデート(KB4474419およびKB4490628以上)がインストールされているWindows 7 x86 SP1		✔	✔	
最新のWindowsアップデート(KB4474419およびKB4490628以上)がインストールされているWindows 7 x64 SP1		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64		✔	✔	
Windows 8.1 x86		✔	✔	
Windows 8.1 x64		✔	✔	
Windows 10 x86		✔	✔	
Windows 10 x64（すべての正式リリース）	*	✔	✔	*
ARMのWindows 10		✔		
Windows 11 x64, 21H2, と22H2	*	✔	✔	*
Windows 11 ARM		✔		

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)はサポート終了が予定されています。詳細クラウドMDMに移行することをお勧めします。

* 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。

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 2008Windows 7などの古いシステムの場合)。
- ESET PROTECTは、実行中のコンピューターWindows 7 (SPがない)、Widows VistaWindows XPの管理をサポートしません。
- 2020年3月24日以降ESETは、次のMicrosoft WindowsオペレーティングシステムにインストールされたESET PROTECT (サーバーおよびMDM)について、サポートと技術サポートの提供を正式に終了しますWindows 7Windows Server 2008 (すべてのバージョン)。

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。

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。

ESXiがなくても、サーバー以外のOSでESET PROTECT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。

ネットワーク

ESET PROTECTサーバーとESET PROTECT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)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で管理されるコンピューターはESET PROTECTサーバーと同じLANに接続し、同じActive Directoryドメインである必要があります。ESET PROTECTサーバーはクライアントコンピューターから表示可能である必要があります。また、クライアントコンピューターはESET PROTECTサーバーと通信し、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。

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。

ソフトウェア

WindowsにESET PROTECTサーバ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。

- 有効なライセンスが必要です。

- Microsoft .NET Framework 4をインストールする必要があります。**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。

- ESET PROTECT Webコンソールには、Java/OpenJDK（64ビット）が必要です。

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。

- ESET PROTECTは、Microsoft SQL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。Windows版のESET PROTECTオールインワンインストーラーに含まれるMicrosoft SQL Server Express 2019を使用することをお勧めします。既存のデータベースサーバーをESET PROTECTで使用する場合は、データベース要件を満たしていることを確認してください。

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

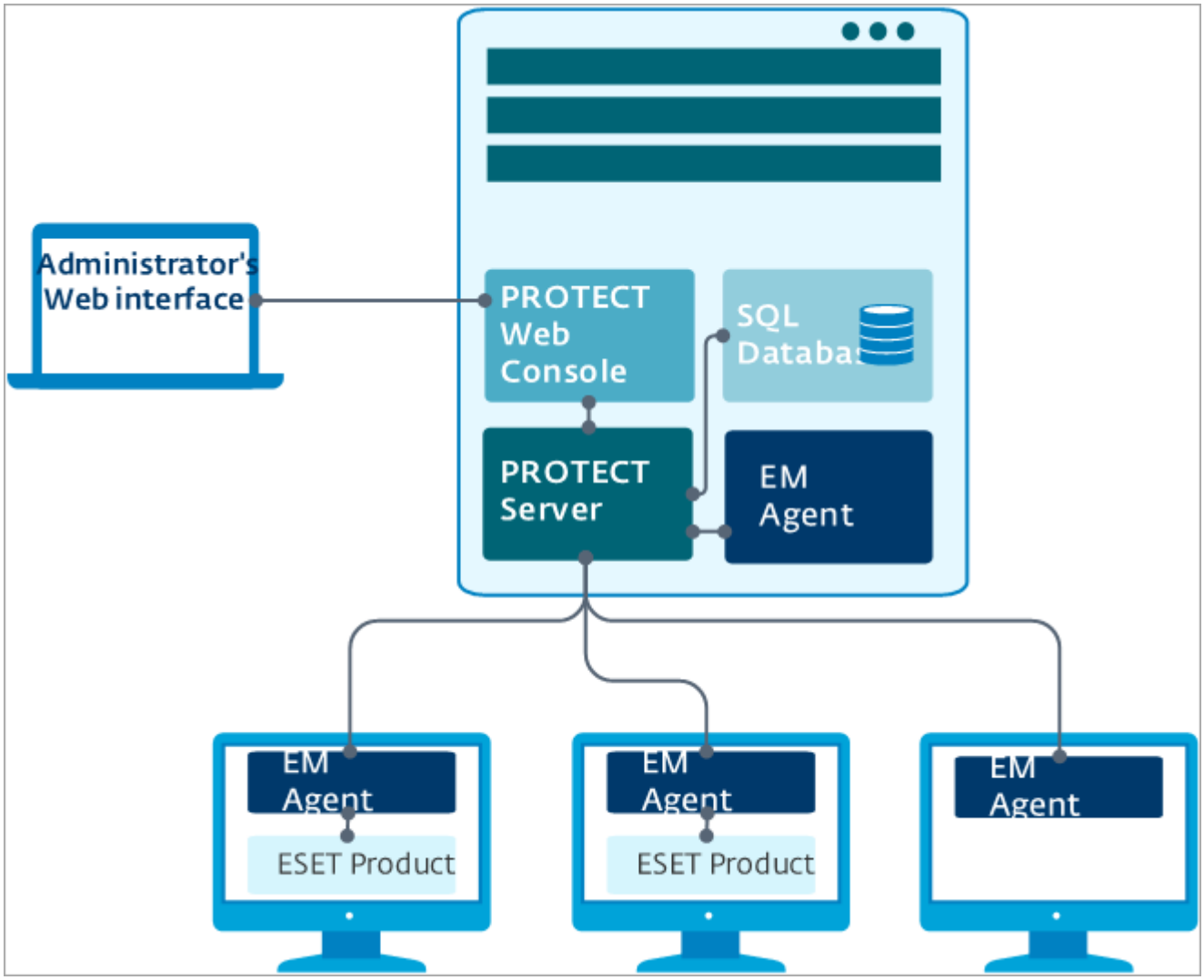
- Mozilla Firefox
- Microsoft Edge
- Google Chrome
- Safari
- Opera

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サーバーのインストール

ESET PROTECTコンポーネント構造

通常、小規模から中規模のネットワーク(1,000クライアント以下)を管理するにはESETPROTECTサーバーとすべてのコンポーネント(Webサーバー、データベースなど)がインストールされた1台のサーバーで十分です。1台のサーバーのインストールまたはスタンドアロンインストールとして考えることができます。すべての管理対象クライアントは、ESET PROTECTエージェント経由で直接ESET Managementサーバーに接続します。管理者は、ネットワーク上の任意のコンピュータからWebブラウザでESET PROTECT Webコンソールに接続したりESET PROTECTサーバーから直接Webコンソールを実行したりできます。



インストール

ESET PROTECTインストーラーは、さまざまなインストール方法をサポートするために、複数の形式で提供されています。

- Windowsでの小規模な展開には、オールインインワンインストーラーをお勧めします。
- ハイパーバイザーを使用する場合は、設定済みのESET PROTECT仮想アプライアンス(CentOSLinuxで実行)を展開することをお勧めします。Windowsでのインストールよりも展開がすばやく簡単です。

i 前のバージョンのESET PROTECTまたはESMC 7.xからアップグレードする場合は、次の手順に従います。

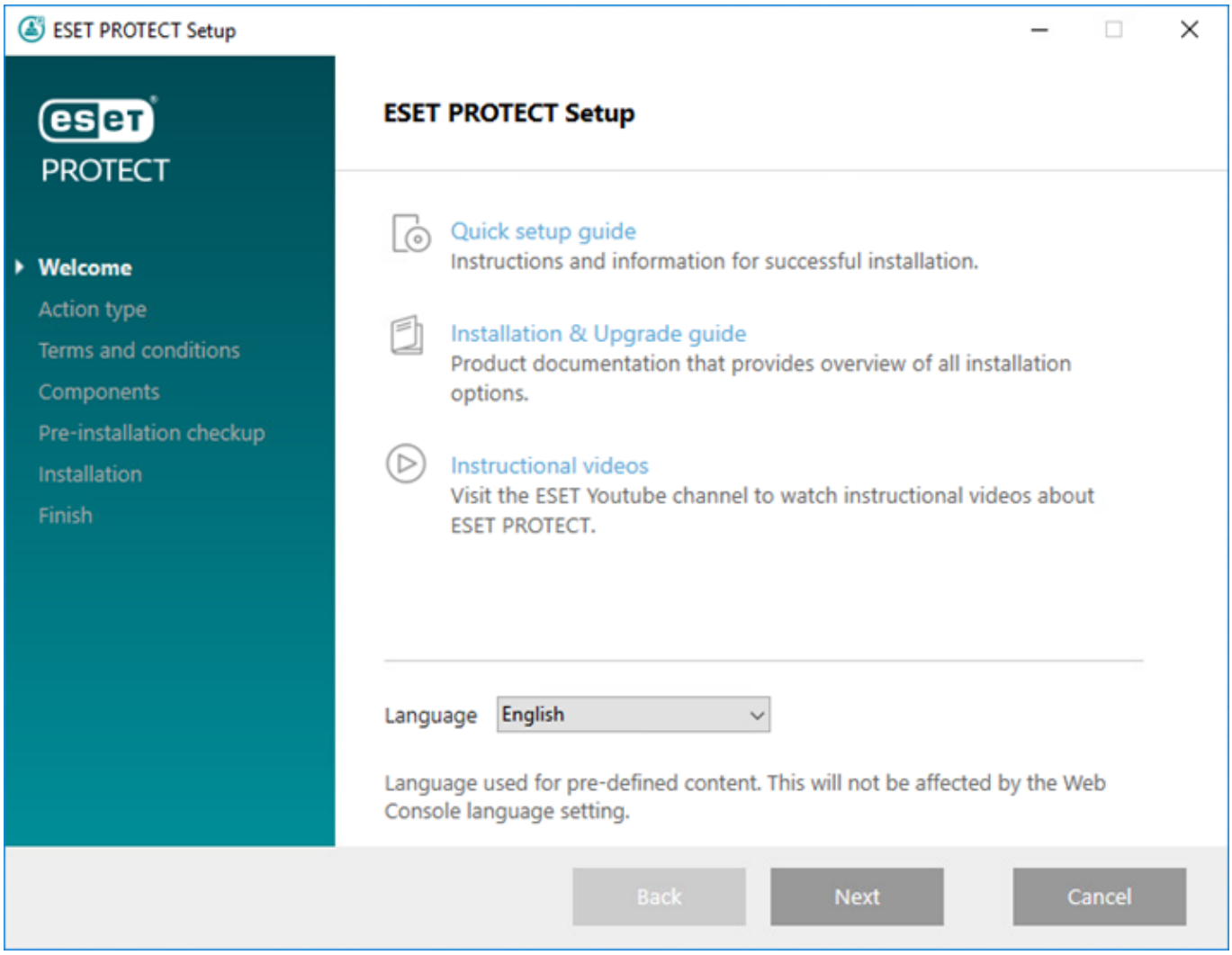
ESETPROTECTサーバーのオールインワインインストール

i
- 別の方法は、設定済みのESET PROTECT仮想アプライアンスを展開する方法です(ハイパーバイザーを使用する場合)。
- 前のバージョンのESET PROTECTまたはESMC 7.xからアップグレードする場合は、次の手順に従います。

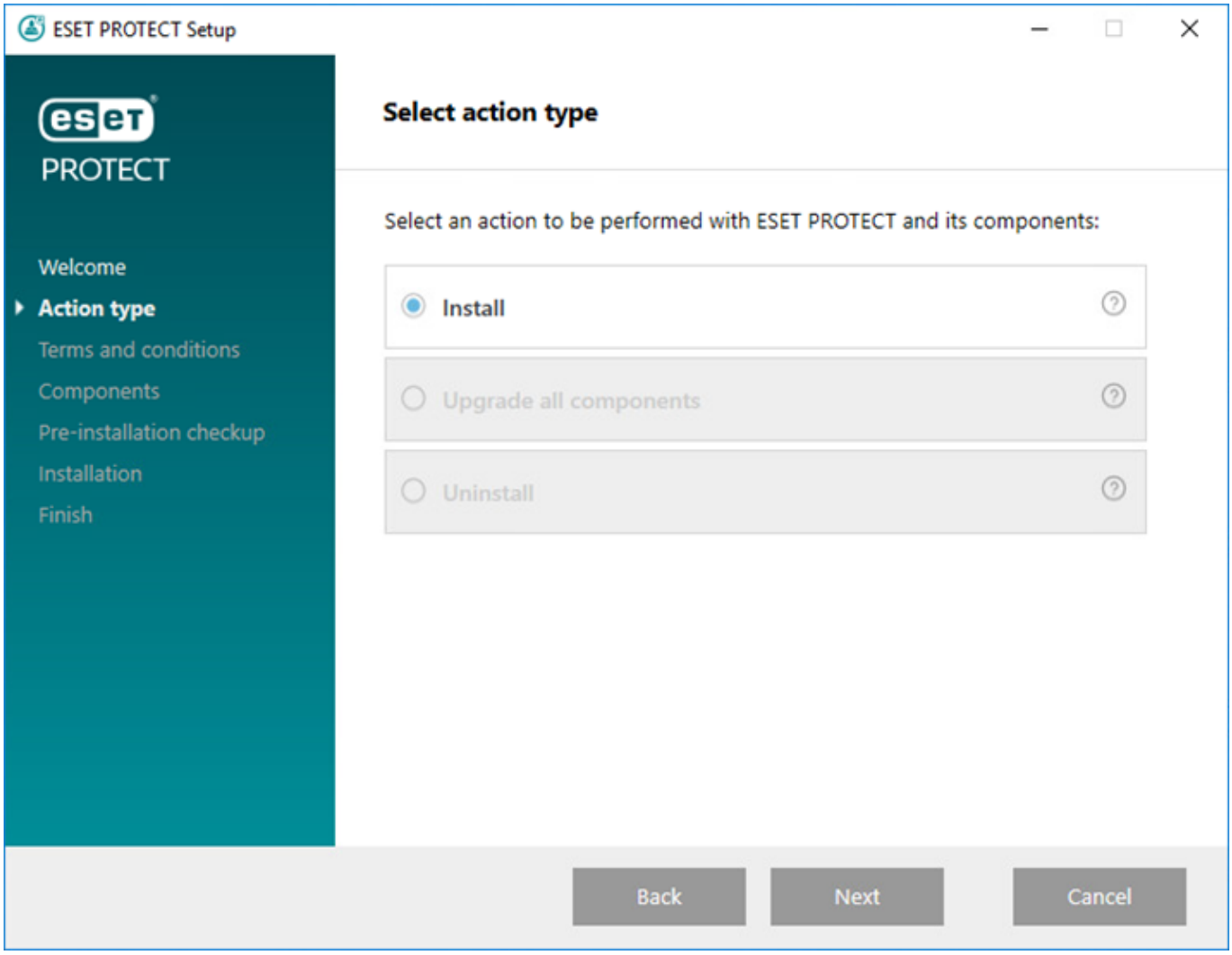
ESET PROTECTオールインワンインストーラーはWindowsオペレーティングシステムでのみ使用できます。

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 10.0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とESET Inspect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

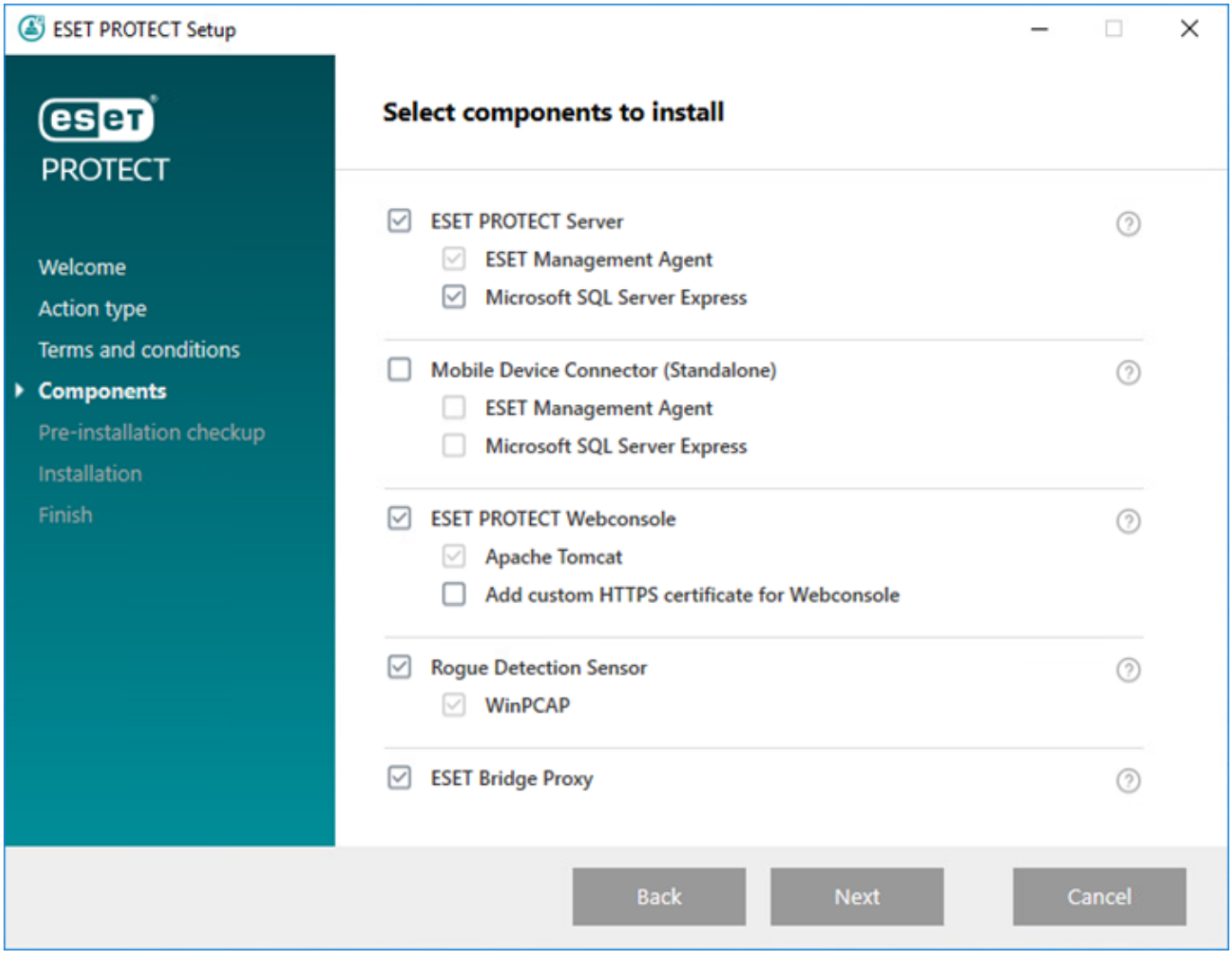
ESET Bridge Proxyオプションは、ローミングクライアントがない小規模または一元化されたネットワーク専用です。このオプションが選択されている場合、クライアントが既定でESET PROTECTサーバーと同じコンピューターにインストールされたプロキシ経由でESETとの通信をトンネルするようにインストーラーによって設定されます。クライアントとESET PROTECTサーバー間で直接ネットワーク可視がない場合は、この接続は動作しません。

- 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ESETPROTECT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。

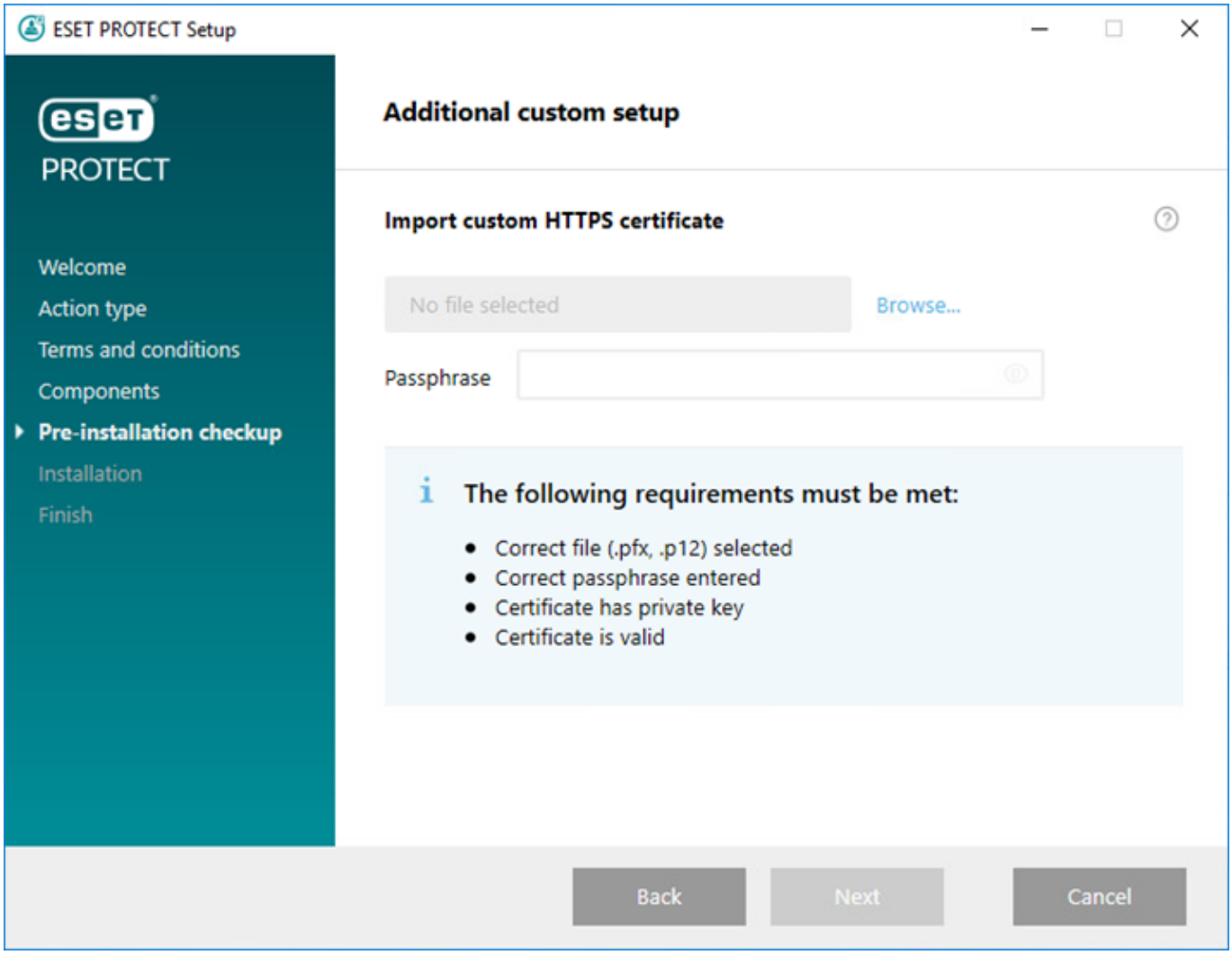
- 詳細については、ESET Bridge (HTTPプロキシ)とESET Bridge (HTTPプロキシ)、ミラーツール、および直接接続の違いを参照してください。

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**HTTP Proxy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。

HTTPプロキシホストは、ESETPROTECT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。



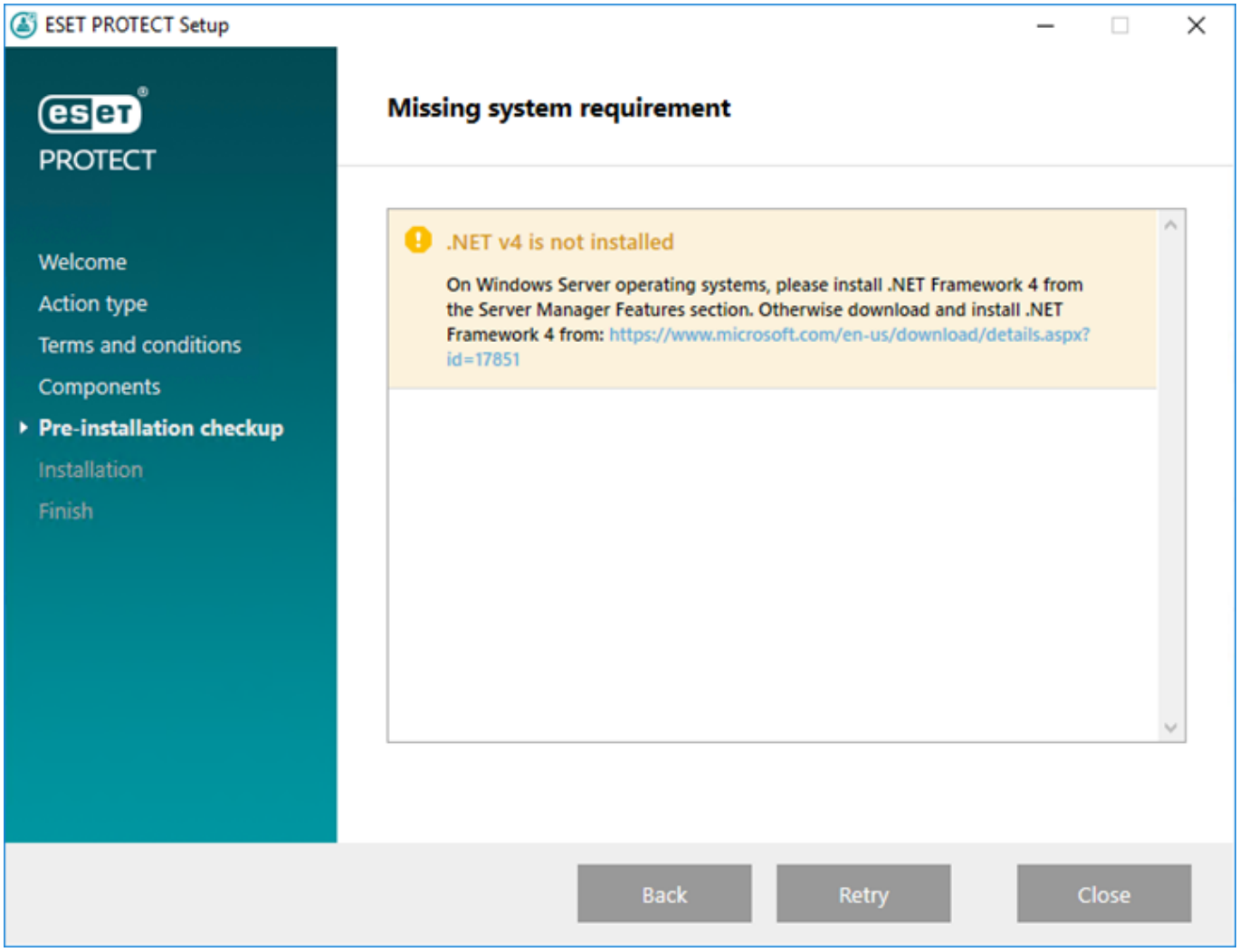
5. **Webコンソールのカスタム HTTPS証明書を追加**を選択した場合は、**参照**をクリックして、有効な証明書(*.pfx*またはp12ファイル)を選択し、**パスフレーズ**を入力(またはパスフレーズがない場合は空欄)します。インストーラーは、TomcatサーバーにWebコンソールアクセスの証明書をインストールします。**次へ**をクリックして続行します。



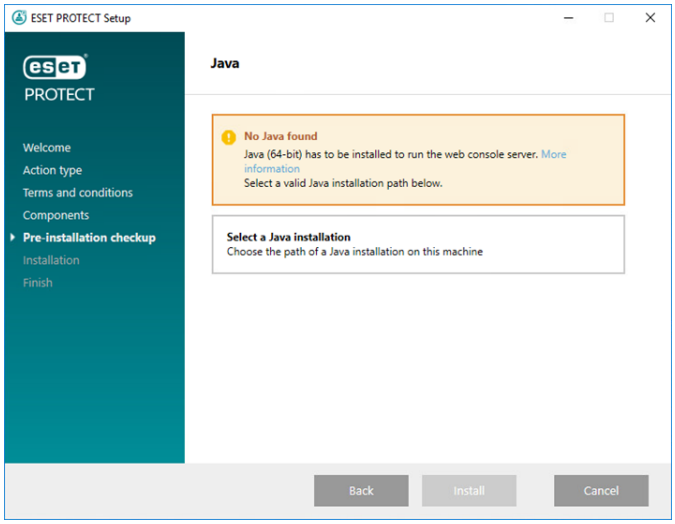
6. 前提条件チェック中にエラーが見つかった場合は、エラーを修正します。システムがすべての前提条件を満たしていることを確認します。

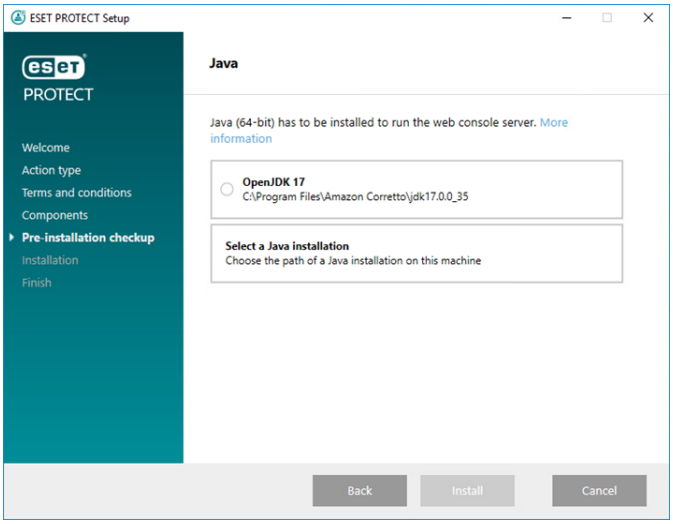
^ .NET v4がインストールされていません

.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。

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。

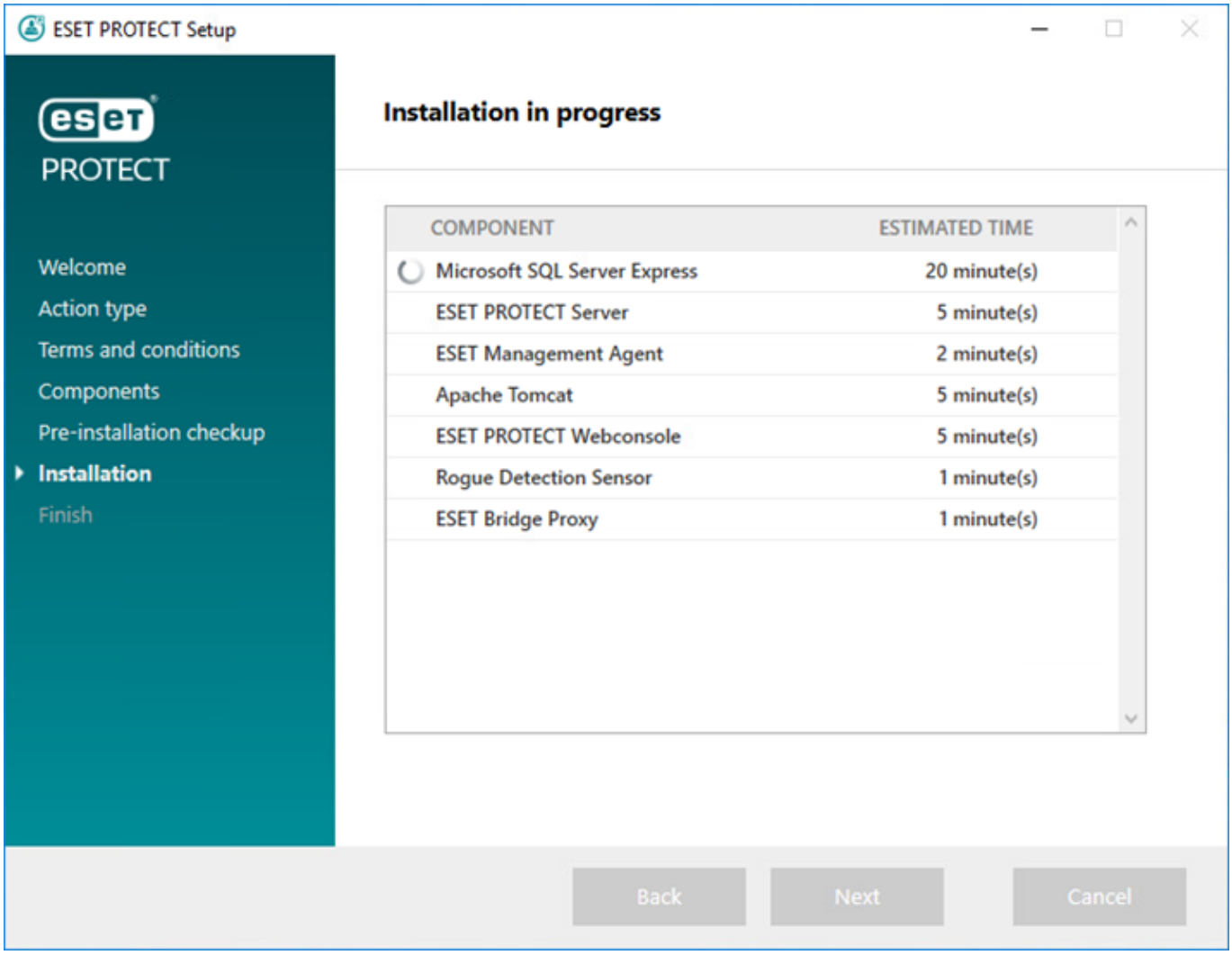
- ESET PROTECTとすべてのコンポーネントをインストールするには4,400 MB以上の空きディスク領域が必要です。

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。

直接アップグレードはサポートされていません。ERA 5.xからの移行またはERA 6.xからのアップグレードを参照してください。

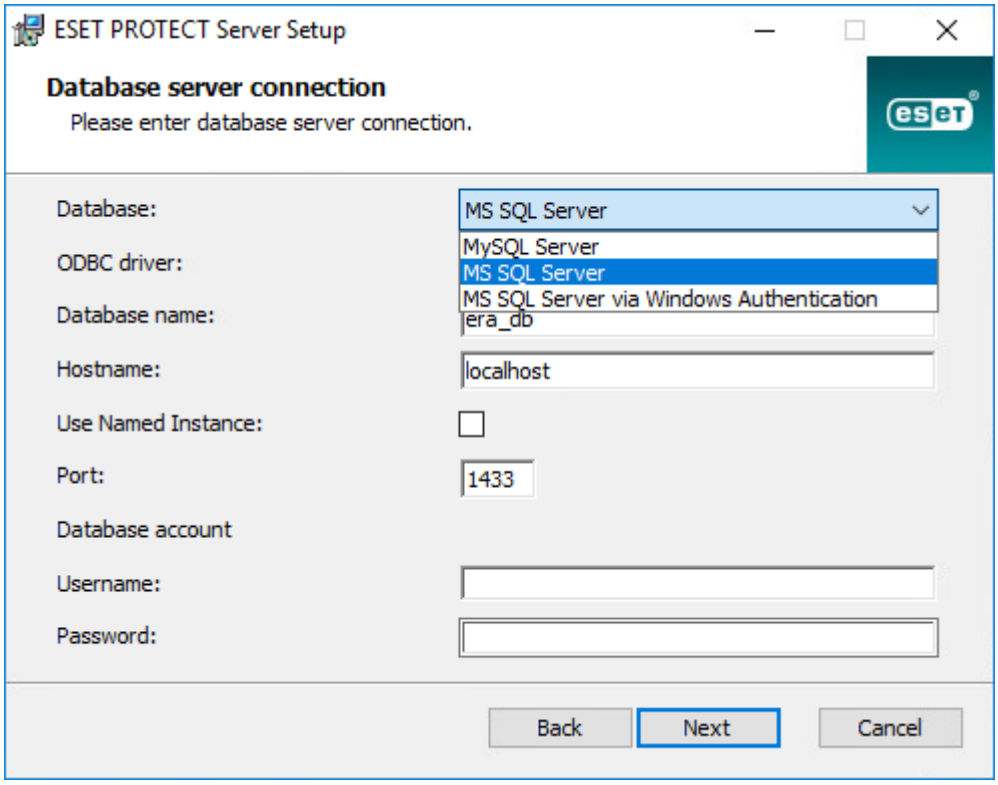
7. 前提条件チェックが完了し、環境がすべての要件を満たしたら、インストールが開始します。システムとネットワーク構成によっては、インストールに1時間以上かかる場合があります。

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

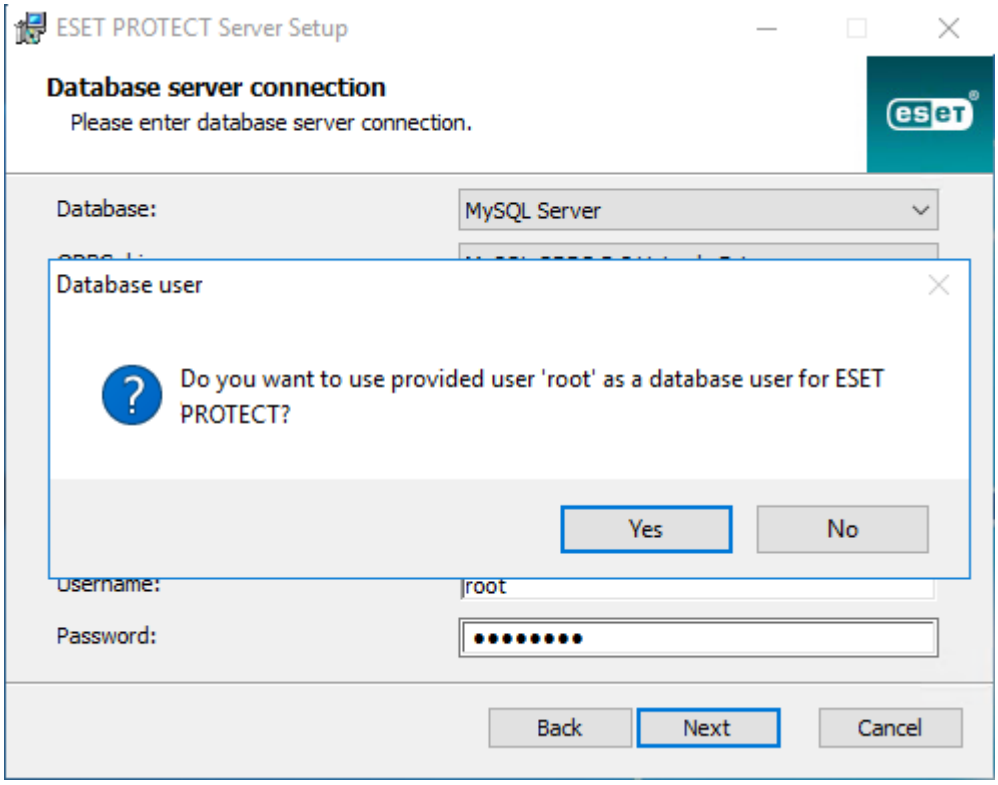


データベース名、**ホスト名**、**ポート**番号(この情報はMicrosoft SQL Server Configuration Managerで確認できます)と**データベース管理者アカウント**詳細情報(**ユーザー名**と**パスワード**)を該当するフィールドに入力し、[**次へ**]をクリックします。インストーラーは、データベース接続を検証します。既存のデータベース(前のESMC/ESET PROTECTインストール)がデータベースサーバーにある場合は、これが検出されます。**既存のデータベースを使用してアップグレードを適用**するか、**既存のデータベースを削除して新しいバージ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

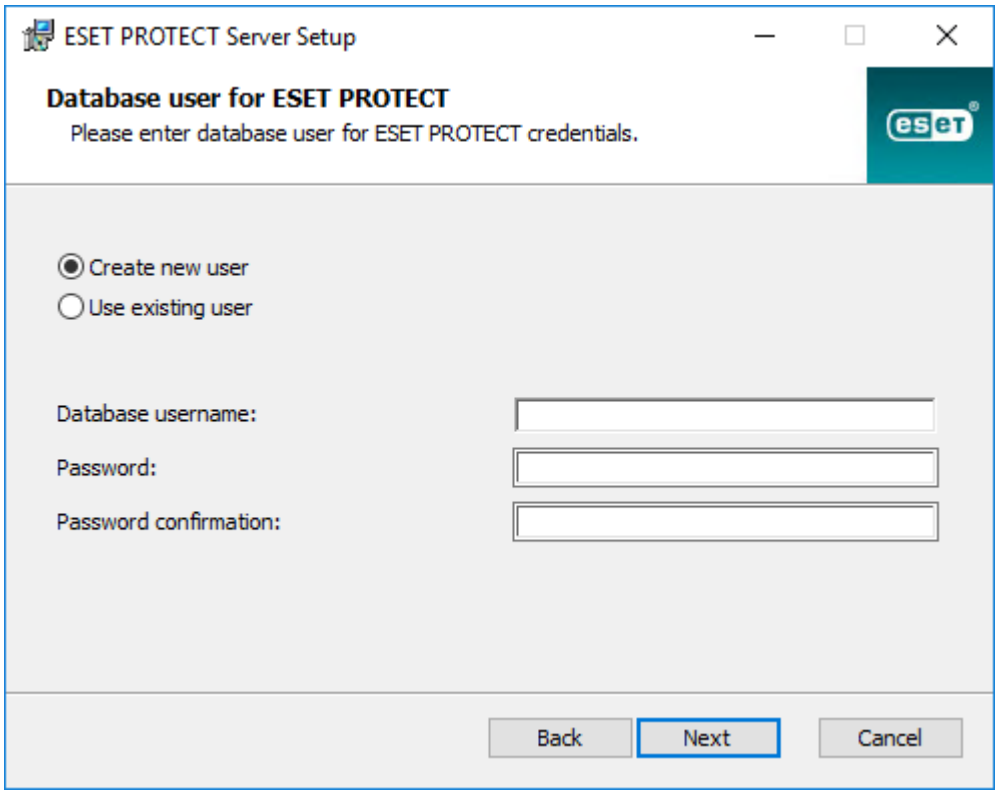
名前付きインスタンスを使用する - Microsoft SQLデータベースを使用している場合は、**名前付きインスタンスを使用する**チェックボックスを選択し、カスタムデータベースインスタンスを使用できます。*HOSTNAME\DB_INSTANCE*の形式で**ホスト名**フィールドで設定できます。(例: *192.168.0.10\ESMC7SQL*)。クラスタデータベースの場合、クラスタ名のみを使用します。このオプションを選択する場合、データベース接続ポートを変更できません。Microsoftの既定のポートが使用されます。フェールオーバークラスターにインストールされたMicrosoft SQL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

データー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。

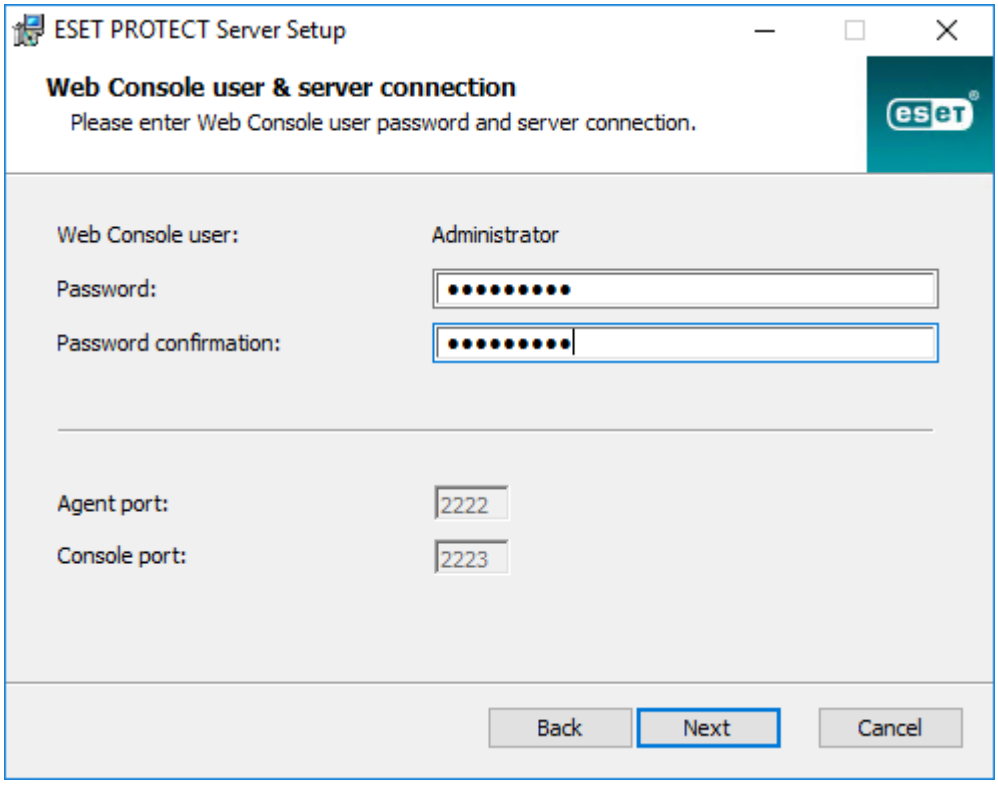
前のウィンドウで**SAアカウント**または**rootアカウント**を入力した場合は、**はい**をクリックし、SA/rootアカウントをESET PROTECTのデータベースユーザーとして使用し続けます。



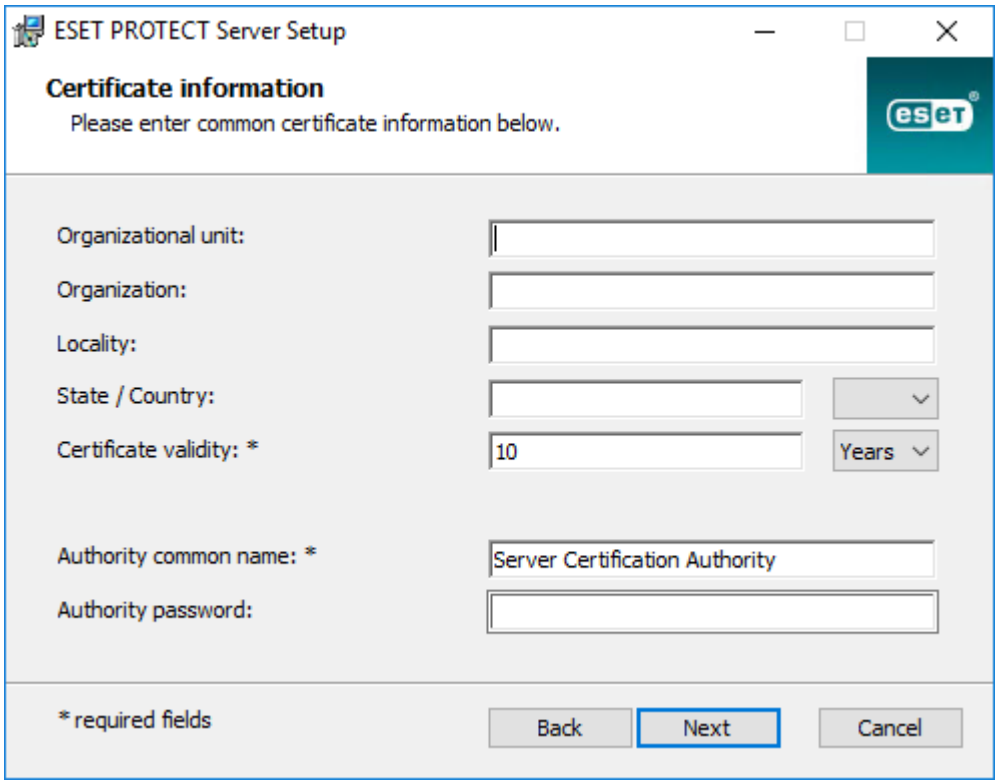
いいえをクリックする場合は、**新しいユーザーの作成**(まだ作成していない場合)または**既存のユーザーを使用する** (専用データベースユーザーアカウントがある場合)を選択する必要があります。



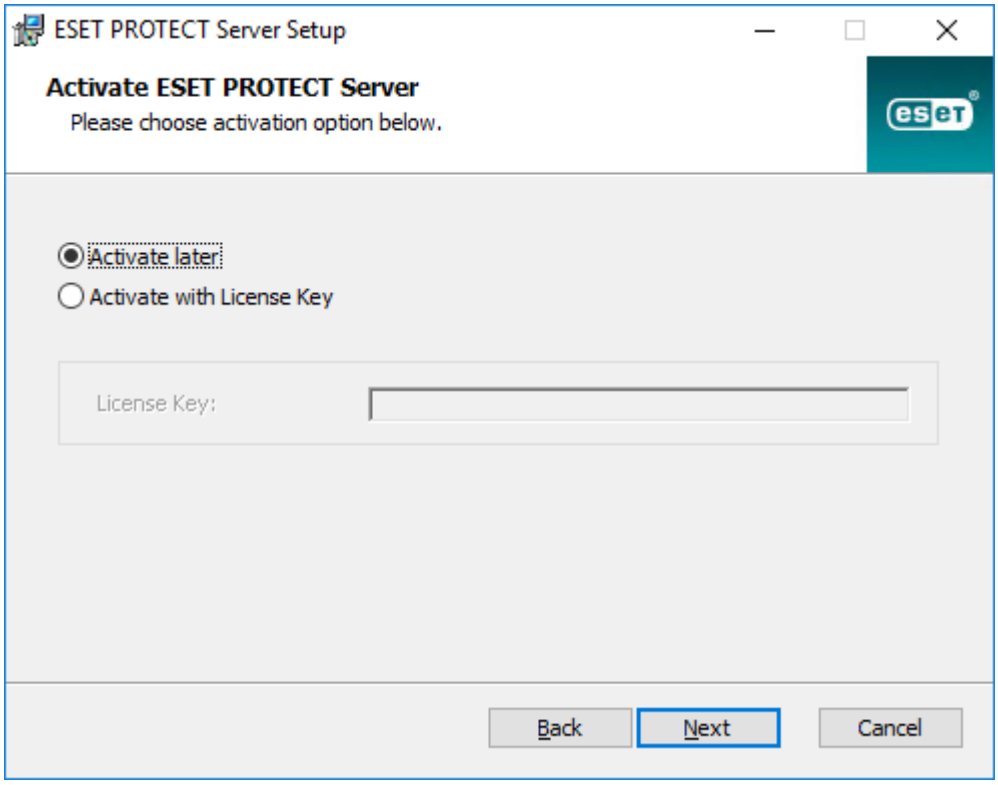
9. Webコンソール管理者アカウントのパスワードを入力するように指示されます。このパスワードはESET PROTECT Webコンソールにログインするときに使用するため重要です。**次へ**をクリックします。



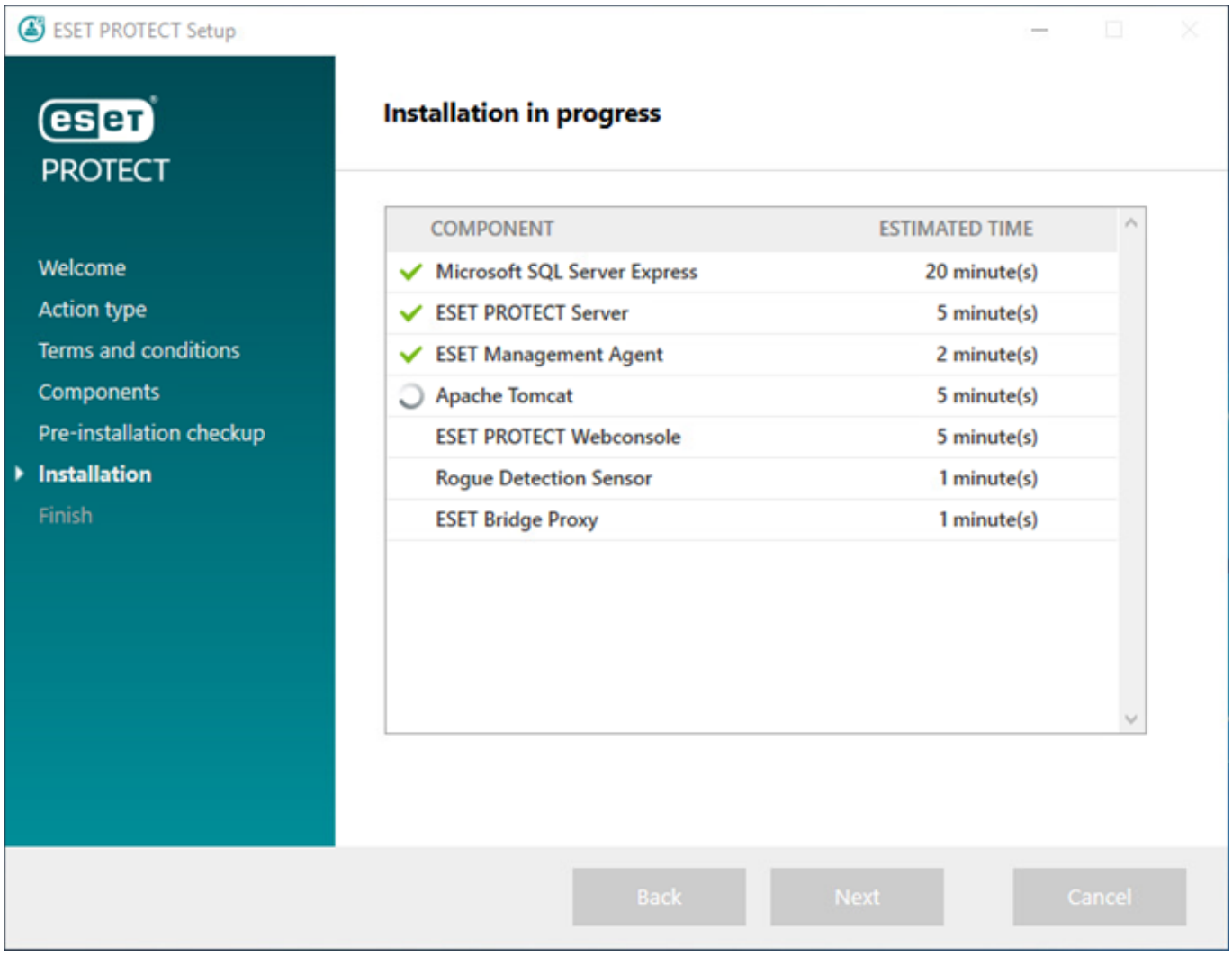
10. フィールドをそのままにするか、ESET Managementエージェントと ESET PROTECTサーバー証明書の詳細に表示する企業情報を入力できます。**認証パスワード**フィールドにパスワードを入力する場合は、必ず覚えておいてください。**次へ**をクリックします。



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。レガシーライセンス認証情報(ユーザー名とパスワード)を使用している場合は、認証情報をライセンスキーに変換します。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)。



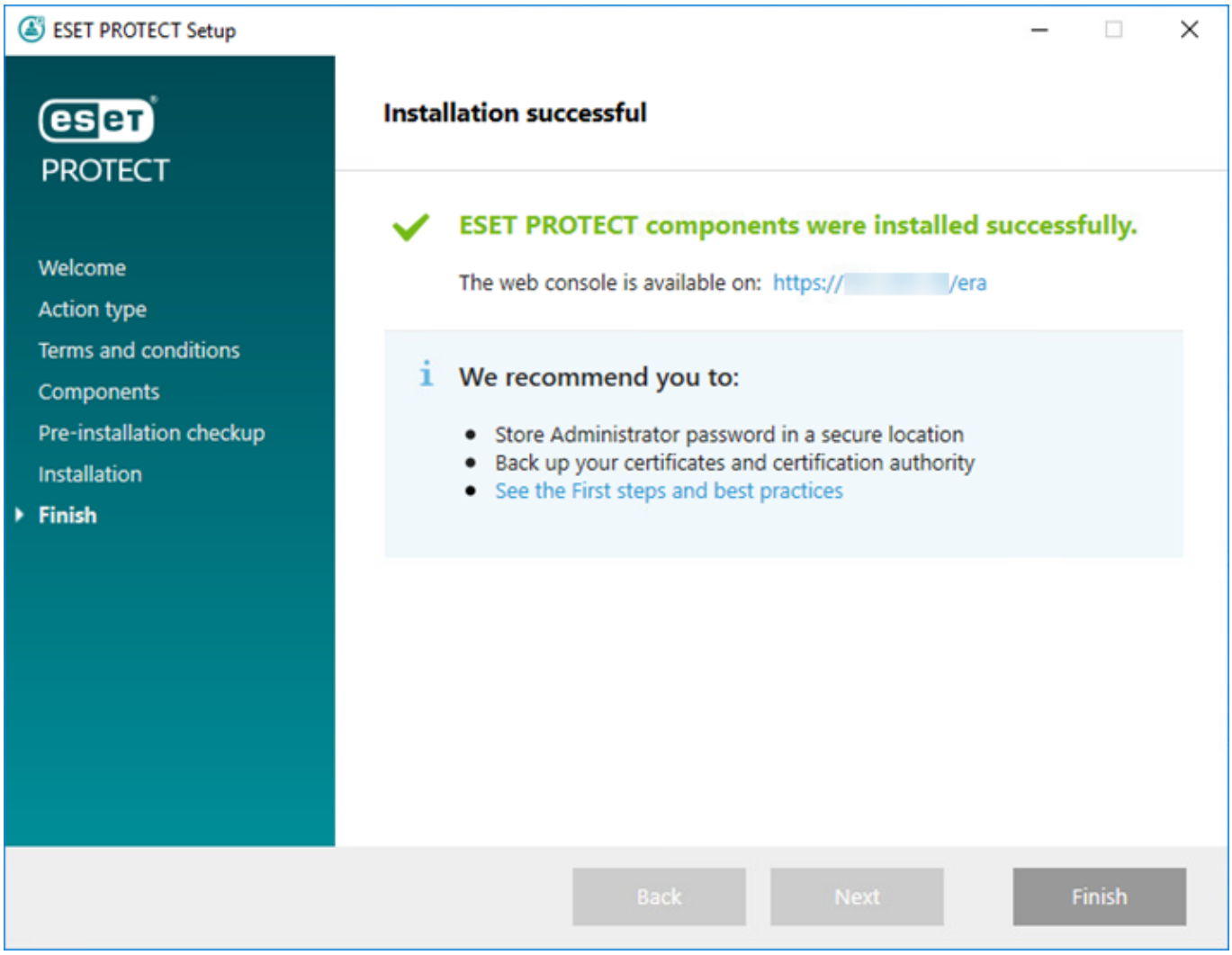
12. インストールの進行状況が表示されます。



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。

インストール後の手順

ESET PROTECTのインストール後、設定を開始できます。

ESET PROTECTサーバーを展開した後の最初の手順

1. ESET PROTECT Webコンソールに接続します。

2.ESET PROTECTガイドの手順をお読みください。

3.ライセンスを追加します。

4.ESET ManagementエージェントとESETエンドポイント製品をネットワークのクライアントコンピューターに展開します。

ステータス概要ではESET PROTECTの初期設定を行えます。

ESET PROTECTサーバーがサーバーにインストールされESETエンドポイントソリューションがクライアントにインストールされている場合は、ネットワークの管理を開始できますESET Endpoint 製品を管理する方法の詳細については、管理者ガイドを参照してください。

追加の推奨手順

- 通知とレポートを使用して、環境内のクライアントコンピューターのステータスを監視します。たとえば、特定のイベントに関する通知を受信したり、レポートを表示したり、ダウンロードしたりできます。

- SMTPサーバー接続を設定します。電子メールで通知またはレポートを受信する場合は、この設定は任意ですESET PROTECTサーバーを構成し、Syslogサーバーに通知を送信できます。

- 新しいESET PROTECT Webコンソールユーザーを作成します。

- ESET PROTECTデータをバックアップします

ESET ManagementエージェントとESETエンドポイント製品の展開

ESET PROTECTのインストールが成功した後にはESET ManagementエージェントとESETエンドポイント製品をネットワークのクライアントコンピューターに展開する必要があります。

展開の手順は次のとおりです。

1. 展開パッケージの作成
2. 展開パッケージのインストール

他の展開オプションも参照してください。大規模なネットワークでは、ESET Remote Deployment Toolを使用することをお勧めします。

展開パッケージの作成

複数の方法で、Windows版のエージェントおよびESETセキュリティ製品のインストーラーを作成できます。

- **クイックリンク > エージェントの展開 > Windows**
- **インストーラー > インストーラーの作成**

Windows > インストーラーのダウンロードまたはESET Remote Deployment Toolの使用をクリックします。

インストーラーパッケージは*.exe*ファイルで、Microsoft Windowsでのみ有効です。

1.配布 – 選択**インストーラーのダウンロードまたはESET Remote Deployment Toolの使用**

別のインストーラータイプを選択した場合は、該当する手順に従います。
- エージェントの最初の展開(エージェントスクリプトインストーラー)
- 展開のためにGPOまたはSCCMを使用

2.コンポーネント – 次のオプションからチェックボックスを選択します。

- **Management Agent - パッケージの内容**で他の項目を選択しない場合は、ESET Managementエージェントだけがインストーラーに含まれます。後からクライアントコンピューターにESETセキュリティ製品をインストールするか、クライアントコンピューターに既にESETセキュリティ製品がインストールされている場合に、このオプションを選択します。
- **セキュリティ製品** - ESETセキュリティ製品とESET Managementエージェントを含みます。クライアントコンピューターにESETセキュリティ製品がインストールされてなくESET Managementエージェントでインストールする場合に、このオプションを選択します。
- **フルディスク暗号化** – 暗号化オプションは、アクティブなESET Full Disk Encryptionライセンスでのみ表示されます。
- **ESET Inspectコネクター** – インストーラーにESET Inspectコネクターが含まれます。

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.親グループ – エージェントインストール後にWebコンソールがコンピューターを配置ESET PROTECTする親グループを選択します。インストーラーが展開された後にデバイスが割り当てられる、既存のグループを選択するか、新しい静的グループを作成できます。親グループを選択すると、グループに適用されているすべてのポリシーがインストーラーに追加されます。

5.サーバーホスト名(任意) - ESET PROTECTサーバーのホスト名またはIPアドレスを入力します。必要に応じて、**ポート**番号を指定(既定は2222)します。

6.ピア証明書:

• **ESET PROTECT証明書** – エージェントインストールおよびESET PROTECT認証局のピア証明書が自動的に選択されます。別の証明書を使用する場合は、**ESET PROTECT証明書説明**をクリックし、使用可能な証明書のドロップダウンメニューから選択します。

• **カスタム証明書** – 認証でカスタム証明書を使用する場合は、**カスタム証明書 > 選択**をクリックして.pfx証明書ををアップロードし、エージェントのインストール時にそれを選択します。詳細については、証明書を参照してください。

証明書パスフレーズ - ESET PROTECTサーバーインストール中にパスフレーズを指定した場合(認証局を作成した手順)、またはカスタム証明書とパスフレーズを使用する場合は、必要に応じて、証明書パスフレーズを入力します。そうでない場合は、**証明書パスフレーズ**フィールドは空欄にします。

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。

証明書パスフレーズはインストーラーに埋め込まれているため、抽出できます。

7. その他の設定をカスタマイズ

• **インストーラー名**と**説明**(任意)を入力します。

• **コンポーネントインストール - 常に最新バージョンの製品とコンポーネントをインストールする**チェックボックスをオンにすると、インストーラーは常に、インターネットに接続されているデバイスに、選択した最新バージョンの製品とコンポーネントをインストールします。デバイスがインターネットに接続していない場合、このウィザードの次の手順で選択したバージョンがインストールされます。このインストーラーを長い期間使用する場合は、この設定を選択して、最新バージョンの製品とコンポーネントを必ず確実にインストールすることをお勧めします。

• **タグを選択**をクリックして、タグを割り当てます。

• **初期構成(任意)** – このオプションを使用して、設定ポリシーをESET Managementエージェントに適用します。 **エージェント設定**の下の**選択**をクリックして、使用可能なポリシーのリストから選択します。 定義済みのポリシーのいずれも適さない場合は、新しいポリシーを作成するか、既存のポリシーをカスタマイズできます。

• HTTPプロキシ(ESET Bridgeの使用が推奨されます)を使用する場合は、**HTTPプロキシ設定を有効にする**チェックボックスを選択し、プロキシ設定(**ホスト**、**ポート**、**ユーザー名**、**パスワード**)を指定して、プロキシ経由でインストーラーをダウンロードします。またESET Managementエージェント接続をプロキシに設定し、ESET Managementエージェントと ESET PROTECTサーバーとの間の通信転送を可能にします。 **ホスト**フィールドは、HTTPプロキシが実行されているコンピューターのアドレスです。ESET Bridgeは既定でポート3128を使用します。必要に応じて、別のポートを設定できます。HTTPプロキシ設定でも同じポートを設定してください(ESET Bridgeポリシーを参照)。

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。

このフォールバックオプションを許可する場合は、**HTTPプロキシが使用不可能な場合は直接接続を使用する**を有効にします。

8. **完了**または**製品設定**をクリックします。

9. セキュリティ製品

a.選択済みのESETセキュリティ製品をクリックし、詳細を変更します。

o別の互換性があるESETセキュリティ製品を選択します。

o **言語**ドロップダウンメニューから言語を選択します。

o**詳細**チェックボックスをオンにします。 既定では、最新のバージョンがあらかじめ選択されています(推奨)。前のバージョンを選択できます。

> 製品インストールファイルが表示されない場合は、必ずリポジトリを**AUTOSELECT**に設定してください。詳細については、設定の**詳細設定**セクションを参照してください。

b. 設定の横のチェックボックスをオンにし、インストーラーで有効に設定します。

oESET LiveGrid®フィードバックシステムを有効にする(推奨)

o望ましくない可能性のあるアプリケーションの検出を有効にする-ナレッジベース記事で詳細をお読みください。

oインストール中に保護設定を変更することを許可 – このチェックボックスをオフにすることをお勧めします。

c.[**アプリケーションエンドユーザー使用許諾契約の条項に同意し、プライバシーポリシーを承諾する**]の横のチェックボックスを選択します。ESET製品のエンドユーザーライセンス契約(EULA)利用規約、およびプライバシーポリシー

d.**その他の設定をカスタマイズ**:

o使用可能なライセンスのリストから該当する製品ライセンスを選択します。 ライセンスはインストール中にESETセキュリティ製品をアクティベーションします。 使用可能なライセンスリストには、有効期限切れおよび使用超過のライセンス(**エラー**または**古い**状態のライセンス)が表示されません。 ライセンスがない場合は、ライセンスなしでESETセキュリティ製品をインストールし、後から製品をアクティベーションできます。 ライセンス管理で説明されている方法のいずれかを選択して、ライセンスを追加できます。ライセンスの追加と削除は、ホームグループが**すべて**に設定され、ライセンスに対する**書き込み**権限がある管理者にのみ制限されています。

o**設定** - 任意で、インストール中にESET Security製品に適用する**ポリシー**を選択できます。

o**ESET AV リムーバーを実行** – ターゲットデバイスの他のウイルス対策プログラムをアンインストールするか、完全に削除する場合は、チェックボックスをオンにします。

手順2でFull Disk EncryptionまたはESET Inspectコネクターを選択した場合は、設定を変更することもできます。

フルディスク暗号化

a.あらかじめ選択された**ESET Full Disk Encryption**をクリックして、詳細を変更します。

o **言語**ドロップダウンメニューから言語を選択します。

o**詳細**チェックボックスをオンにします。 既定では、最新のバージョンがあらかじめ選択されています(推奨)。前のバージョンを選択できます。

b.**[アプリケーションエンドユーザー使用許諾契約の条項に同意し、プライバシーポリシーを承諾する]**の横のチェックボックスを選択します。ESET製品のエンドユーザーライセンス契約(EULA)利用規約、およびプライバシーポリシー

c.**設定** – インストール中にESET Full Disk Encryptionで適用されるポリシーを選択します。

d.**その他の設定をカスタマイズ**:

o使用可能なライセンスのリストから該当する製品ライセンスを選択します。 ライセンスはインストール中にESETセキュリティ製品をアクティベーションします。 使用可能なライセンスリストには、有効期限切れおよび使用超過のライセンス(**エラー**または**古い**状態のライセンス)が表示されません。 ライセンスがない場合は、ライセンスなしでESETセキュリティ製品をインストールし、後から製品をアクティベーションできます。 ライセンス管理で説明されている方法のいずれかを選択して、ライセンスを追加できます。ライセンスの追加と削除は、ホームグループが**すべて**に設定され、ライセンスに対する**書き込み**権限がある管理者にのみ制限されています。

ESET Inspect Connector

ESET Inspectコネクター要件:
- ESET Inspectコネクターをアクティベーションするには**ESET Inspect**ライセンスが必要です。
- 互換性があるESETセキュリティ製品が管理されたコンピューターにインストールされている。

a.あらかじめ選択された**ESET Inspectコネクター**をクリックして、詳細を変更します。

o **言語**ドロップダウンメニューから言語を選択します。

o**詳細**チェックボックスをオンにします。 既定では、最新のバージョンがあらかじめ選択されています(推奨)。前のバージョンを選択できます。

b.**[アプリケーションエンドユーザー使用許諾契約の条項に同意し、プライバシーポリシーを承諾する]**の横のチェックボックスを選択します。ESET製品のエンドユーザーライセンス契約(EULA)利用規約、およびプライバシーポリシー

c.**その他の設定をカスタマイズ**:

o使用可能なライセンスのリストから該当する製品ライセンスを選択します。 ライセンスはインストール中にESETセキュリティ製品をアクティベーションします。 使用可能なライセンスリストには、有効期限切れおよび使用超過のライセンス(**エラー**または**古い**状態のライセンス)が表示されません。 ライセンスがない場合は、ライセンスなしでESETセキュリティ製品をインストールし、後から製品をアクティベーションできます。 ライセンス管理で説明されている方法のいずれかを選択して、ライセンスを追加できます。ライセンスの追加と削除は、ホームグループが**すべて**に設定され、ライセンスに対する**書き込み**権限がある管理者にのみ制限されています。

o**設定 - 選択**をクリックして既存のESET Inspectコネクターポリシーを選択するか、**作成**をクリッ

クして新しいESET Inspectコネクターポリシーを作成します。インストーラーは、ESET Inspectコネクターインストール中にポリシー設定を適用します。

- ESET Inspect**サーバーホスト名**と、ESET Inspectサーバーインストール中に指定された接続**ポート**を入力します(既定のポートは8093です)。
- ESET Inspectサーバーに接続するための**認証局**を選択します。

10. [**完了**]をクリックします。

11. 生成されたオールインインインインストールパッケージをダウンロードします。展開するバージョンを選択します。

- **32ビット**（例*PROTECT_Installer_x86_en_US.exe*）
- **64ビット**（例*PROTECT_Installer_x64_en_US.exe*）
- **ARM64**: *PROTECT_Installer_arm64.exe*）をダウンロード - x86またはx64バージョンのESET Managementエージェントまたは ESETセキュリティ製品はWindows ARM64にインストールできません。

> リポジトリ(ESETリポジトリまたはカスタムリポジトリミラー)からダウンロードされたすべてのデータは、ESETによってデジタル署名されます。ESET PROTECTサーバーはファイルハッシュとPGP署名を検証します。ESETPROTECTサーバーはローカルでオールインインインインストーラーを生成します。このため、オールインワンインストーラーはデジタル署名されていません。インストーラーのダウンロード中にWebブラウザー警告が生成され、オペレーティングシステムアラートが生成される場合があります。また、未署名のインストーラーがブロックされるシステムではインストールが防止される場合があります。

12. オールインワンインストーラーパッケージを作成およびダウンロードした後、ESET Managementエージェントを展開するための2つのオプションがあります。

- クライアントコンピューターでローカル クライアントコンピューターでインストールパッケージファイルを実行します。 デバイスにESET Managementエージェントと ESETセキュリティ製品をインストールし、ESET PROTECTにデバイスを接続します。ESET PROTECTで作成されたESET Endpoint Antivirus/Securityインストーラー 8.1以降 は仮想デスクトップとWindows 10マルチセッションモードのWindows 10 Enterpriseをサポートします。 段階的な手順については、セットアップウィザードを参照してください。 サイレントモードでインストールパッケージを実行し、セットアップウィザードウィンドウを非表示にできます。
- ESETリモート展開ツールを使用して、同時に複数のクライアントコンピューターにESET Managementエージェントを展開します。

展開パッケージのインストール

ESET PROTECTでこのインストーラーパッケージを作成できます。

インストーラーパッケージはESET Managementエージェントをインストールします。パッケージは次のコンポーネントもインストールできます(インストーラーパッケージの作成中に選択した場合)。

- ESETセキュリティ製品(エンドポイントまたはサーバー)
- ESET Full Disk Encryption
- ESET Inspect Connector

- インストールパッケージは*.exe*ファイルの形式であり、Windowsオペレーティングシステムでのみ有効です。
- ESETセキュリティ製品またはESET Managementエージェントが既にインストールされているクライアントコンピューターでインストーラーを実行する場合は、インストーラーのバージョンにアップグレードされます。
- ビルトイン管理者アカウントまたはドメイン管理者アカウント(ビルトイン管理者アカウントが無効な場合)の下でインストーラーを実行する必要があります。 その他のユーザーには、管理者グループのメンバーでない限り、十分なアクセス権が与えられません。 したがって、ビルトインの管理者アカウントを使用する必要があり、ローカルまたはドメイン管理者以外のユーザーアカウントでは、インストールを正常に完了することができません。
- リポジトリ(ESETリポジトリまたはカスタムリポジトリミラー)からダウンロードされたすべてのデータはESETによってデジタル署名されています。ESET PROTECTサーバーはファイルハッシュとPGP署名を検証します。ESET PROTECTサーバーはオールインワンインストーラーをローカルで生成します。このため、オールインワンインストーラーはデジタル署名されていません。インストーラーのダウンロード中にWebブラウザー警告が生成され、オペレーティングシステムアラートが生成される場合があります。また、未署名のインストーラーがブロックされるシステムではインストールが防止される場合があります。
- 機密データ(証明書パスフレーズなど)は、インストーラーに埋め込まれているため、抽出できます。
- ESET PROTECT 8.1以降で作成されたESET Endpoint Antivirus/Securityインストーラーは、Windows 10 Enterprise for Virtual DesktopsおよびWindows 10マルチセッションモードをサポートします。

インストール処理

- ダイアログを表示せずにインストーラーを実行する場合は、サイレントインストール手順に従ってください。
- インストール中にエラーが発生した場合、一般的なインストールエラーについては、トラブルシューティングセクションを参照してください。

1. インストーラーパッケージを実行します。

ESETセキュリティ製品をインストールする前に、必ずコンピューターからサードパーティセキュリティ製品をアンインストールしてください。

- インストールパッケージの作成時に**ESET AV Remover**を含める場合は、**ESET AV Remover**によって、サードパーティのセキュリティソフトウェアをアンインストールまたは完全に削除できます。

a)**互換性がないセキュリティ製品をアンインストールする**チェックボックスをオンにすると、コンピューターで実行中であるかインストールされているサードパーティのセキュリティソフトウェアが削除/アンインストールされます。サポートされているソフトウェアの一覧を確認してください。

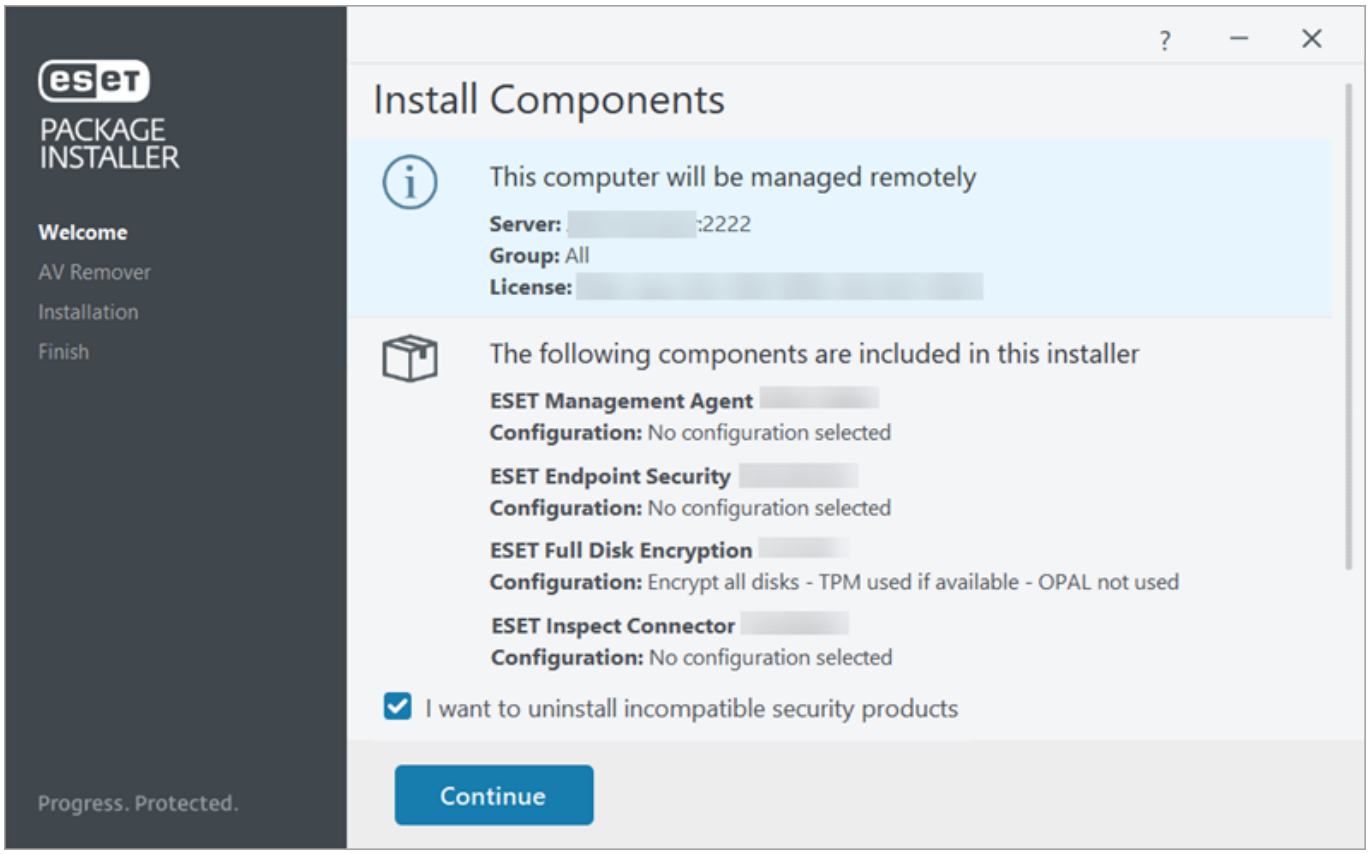
b)**続行**をクリックします。

c)インストールされているアプリケーションを検査した後、削除するアプリケーションの横のチェックボックスをオンにして、**削除**をクリックします。詳細についてはESET AV Removerに

関するナレッジベース記事を参照してください。

d)ESET AV Removerによってサードパーティセキュリティソフトウェアがアンインストールされた後、またはアプリケーションを何も削除しない場合は、**インストールの続行**をクリックします。

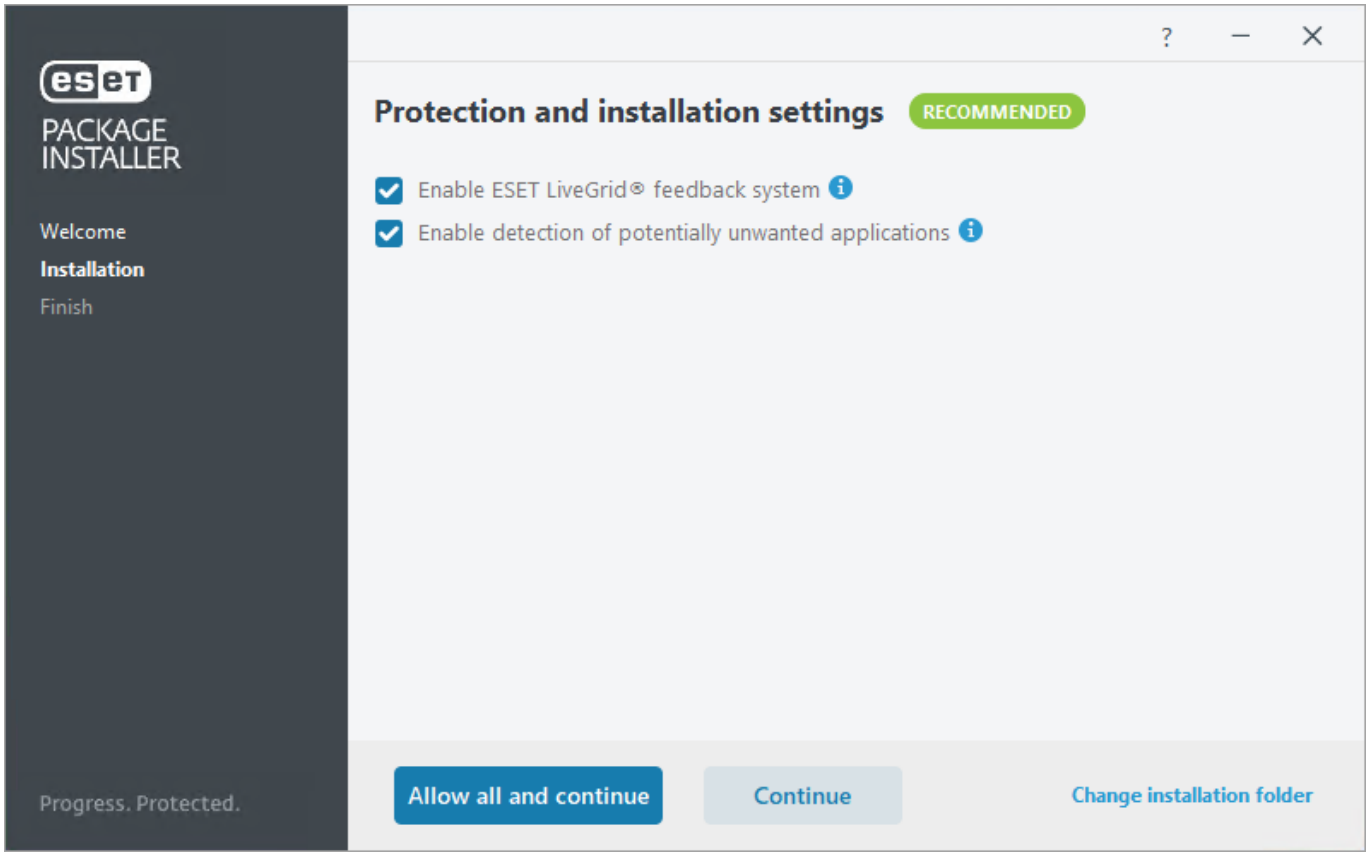
- ローカルコンピューターでサードパーティセキュリティ製品を使用していない場合は、**続行**をクリックします。



2.

oESET LiveGrid®フィードバックシステムを有効にする(推奨)

o望ましくない可能性のあるアプリケーションの検出を有効にする-ナレッジベース記事で詳細をお読みください。



3. インストールが完了したら、**完了**をクリックしますESET Security製品が自動的に開きます。クライアントコンピューターで状態ログ(*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html*この場所は既定で非表示)を確認し、ESET Managementエージェントが正常に動作していることを確かめます。インストールされたESET Managementエージェントで問題がある場合(ESET PROTECTサーバーに接続していないなど)は、エージェント接続のトラブルシューティングを参照してください。

トラブルシューティング

インストール中にエラーが発生した場合、一般的なインストールエラーについては、トラブルシューティングセクションを参照してください。

他の展開方法

ESET Managementエージェントと ESETエンドポイント製品は、個別に複数の方法で展開できます。

ESET Managementエージェントの展開

ローカル展開:

- オールインインインストーラー – このパッケージにはESET Managementエージェントと ESETセキュリティ製品が含まれます。
- エージェントスクリプトインストーラー
- ESET Webサイトからエージェントをダウンロードし、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使用します。

リモート展開(大規模なネットワークの場合に推奨):

- ESET Remote Deployment Tool - オールインワンインストーラーをリモートで展開します。
- グループポリシーオブジェクト(GPO)
- エージェント展開サーバータスク

ESETエンドポイント製品の展開

ESET Managementエージェントが展開された後、次の2つの方法でESET PROTECTから直接ESETエンドポイント製品をインストールできます。

- ソフトウェアインストールタスクの使用
- 標準のESET製品インストールを使用してローカルで実行する

ESET Remote Deployment Tool

ESET Remote Deployment Toolは、ESET PROTECT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□ESETManagement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あるESET Managementエージェントに展開するためのものです。

ESETリモート展開ツールの前提条件

リモート展開の場合、すべてのクライアントコンピューターがインターネットに接続していることを確認します。

WindowsでESET Remote Deployment toolを使用するには、次の要件を満たす必要があります。

- ESET PROTECTサーバーおよびESET PROTECT Webコンソールがインストールされている(サーバーコンピューター上)。
- 適切なポートを開く必要があります。 Windows OSのターゲットコンピューターにESET Managementエージェントをリモート展開するときに使用されるポートを参照してください。
- インストールパッケージの名前には、文字列"x86"または"x64"を含める必要があります。それ以外の場合は、展開が動作しません。
- バンドル(オールインワン)インストーラーパッケージを作成し、ローカルドライブにダウンロードする必要があります。
- オールインワンインストーラーを作成する権限が必要です。

さまざまな理由により、展開が失敗する場合があります。 展開の問題がある場合は、トラブルシューティングの章またはESET Managementエージェント展開の検証済みシナリオ例を参照してください。

クライアントコンピューターでESET Managementエージェントを展開するには、次の手順に従います。

1. ESET WebサイトからESET Remote Deployment Toolをダウンロードします。

2. すべての前提条件が満たされていることを確認してください。

3. クライアントコンピューターでESET Remote Deployment toolを実行します。

4. **コンピューターを手動で追加**を選択します。ホスト名またはIPアドレスのリストを手動で入力する必要があります。

5. ホスト名またはIPアドレスを入力し、**次へ**をクリックします。各IPアドレスまたはホスト名は新しい行に入力する必要があります。

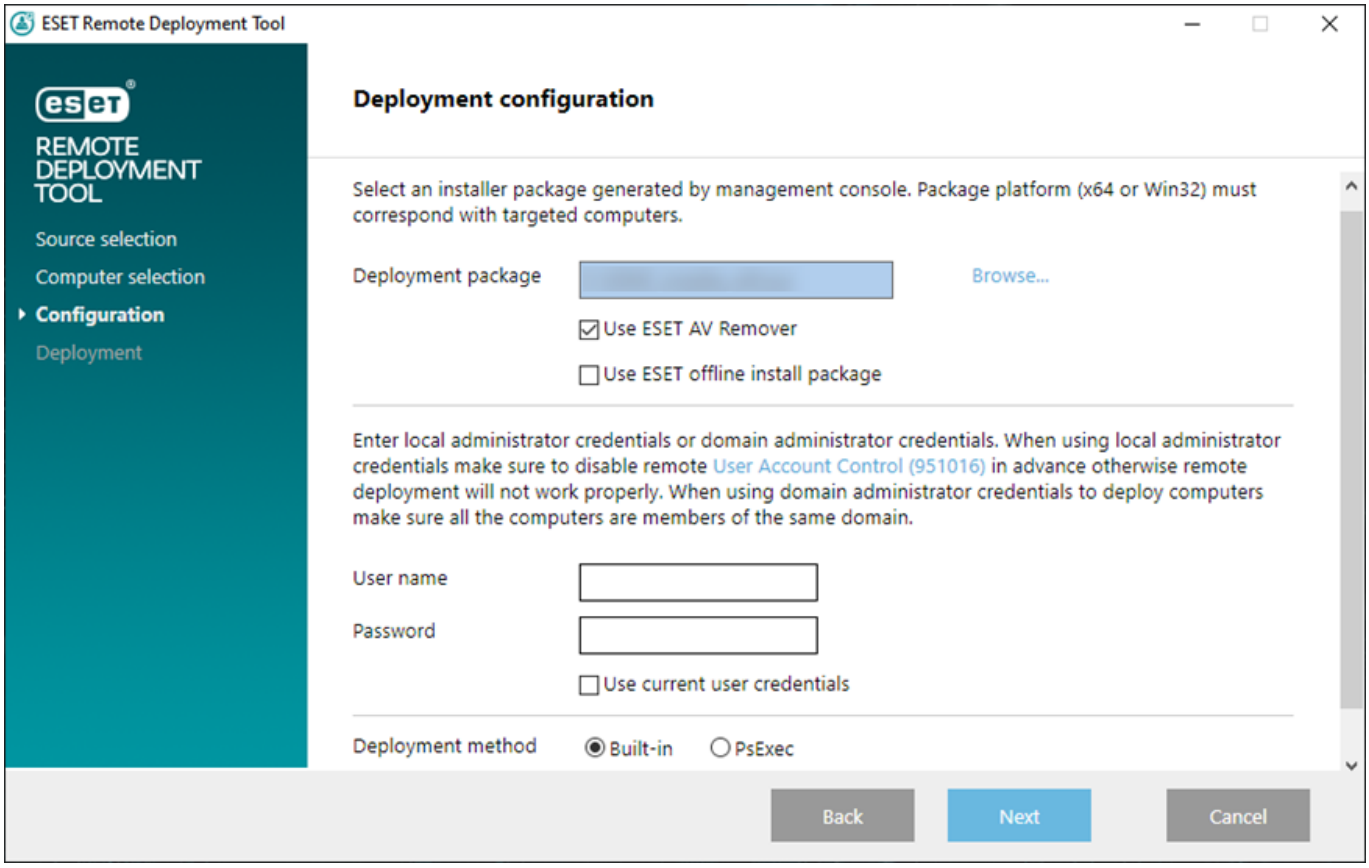
すべての選択されたコンピューターが同じプラットフォームであることを確認します(64ビットまたは32ビットOS)。

6. リモート展開に選択したコンピューターが表示されます。すべてのコンピューターが追加されていることを確認し、[**次へ**]をクリックします。

7. **参照**をクリックし、ESET PROTECTまたはESET PROTECT Cloud Webコンソールで作成されたバンドルインストーラーパッケージを選択します。ESET PROTECT Live Installer(のみESET PROTECT Cloud)ライブインストーラーから作成された**ESETオフラインインストールパッケージ**(*.dat*ファイル)を使用することもできます。ローカルコンピューターに他のセキュリティアプリケーションをインストールしない場合は、[**ESET AV Removerを使用する**]チェックボックスをオフにします。ESET AV Removerは特定のアプリケーションを削除できます。

8.ターゲットコンピューターのログイン資格情報を入力します。コンピューターがドメインのメンバーである場合は、**ドメイン管理者資格情報**を入力します。**ローカル管理者資格情報**でログインする場合は、ターゲットコンピューターでリモートUACを無効にする必要があります。任意で、[**現在のユーザー資格情報を使用する**]の横のチェックボックスを選択できます。ログイン資格情報が自動的に入力されます。

9. **展開方法**が使用され、リモートコンピューターでプログラムを実行します。**ビルトイン**方法はWindowsエラーメッセージをサポートする既定の設定です。**PsExec**はサードパーティツールであり、ビルトイン方法の代替方法です。これらのオプションのいずれかを選択し、[**次へ**]をクリックします。



PsExecを選択した場合、ツールが**PsExec**エンドユーザーライセンス契約に同意できないため、展開が失敗します。展開を正常に実行するには、コマンドラインを開き、**PsExec**コマンドを手動で実行します。

10. インストールが開始すると、「成功」が表示されます。**[完了]**をクリックし、展開を完了します。展開が失敗する場合は、**ステータス**列で**詳細**をクリックし、詳細を表示します。失敗したコンピューターのリストをエクスポートできます。**[失敗したコンピューターのエクスポート]**フィールドの横の**[参照]**をクリックし、リストを保存する*.txt*ファイルを選択し、**[失敗したコンピューターのエクスポート]**をクリックします。



クライアントコンピューターのステータスログ *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*をチェックし、ESET Managementエージェントが正常に動作していることを確認できます。

ESET Remote Deployment ToolでESET Managementエージェントを展開する他の方法

- Active Directory - Active Directory資格情報を指定します。このオプションにはESET PROTECT を後からインポートするためのActive Directory構造のエクスポートがあります。

- ネットワークの検査 - IP範囲を入力し、ネットワークのコンピューターを検査します。
- リストのインポート – ホスト名またはIPアドレスのリストを入力します。

トラブルシューティング

さまざまな理由により、展開が失敗する場合があります。 展開の問題がある場合は、トラブルシューティングの章またはESET Managementエージェント展開の検証済みシナリオ例を参照してください。

ESET PROTECT Webコンソール

ESET PROTECT Webコンソールにログインします

- ローカルWindowsサーバー(Webコンソールをホストするコンピューター):

スタート > すべてのプログラム > ESET > ESET PROTECT Web コンソールをクリックします。

- Webサーバーにインターネット接続できる場所から、以下の形式でURLを入力します(yourservernameの部分はWebサーバーの実際の名前またはIPアドレスに置き換えます)。https://yourservername/era/

既定のWebブラウザーでログイン画面が開きますSSL証明書警告が表示される場合は、証明書例外をWebブラウザーに追加します。

サポートされているWebブラウザーを使用してESET PROTECT Webコンソールに接続します。

Webコンソールに初めてログインするときには、ESET PROTECTガイドが表示されESET Managementエージェントをネットワークのコンピューターに展開できます。

ESET PROTECT Webコンソールユーザーインターフェース

ESET PROTECT Webコンソールユーザーインターフェースは、次の複数の部分で構成されています。

- ESET PROTECT Webコンソールの上部にある**検索**ツールを使用できます。
- **クイックリンク**をクリックすると、最もよく使用されるWebコンソールアクションの一部を実行できます。
- ESET PROTECTを使用しているときにヘルプが必要な場合は、右上端の**ヘルプ**アイコンをクリックし、**<Current topic> - ヘルプ**をクリックします。現在のページの該当するヘルプウィンドウが表示されます。
- 右上には、現在のユーザーとユーザーセッションタイムアウトカウントダウンのが表示されます。[**ログアウト**]をクリックすると、いつでもログアウトできます。ユーザーの操作がなく、セッションがタイムアウトした場合は、もう一度ログインする必要があります。

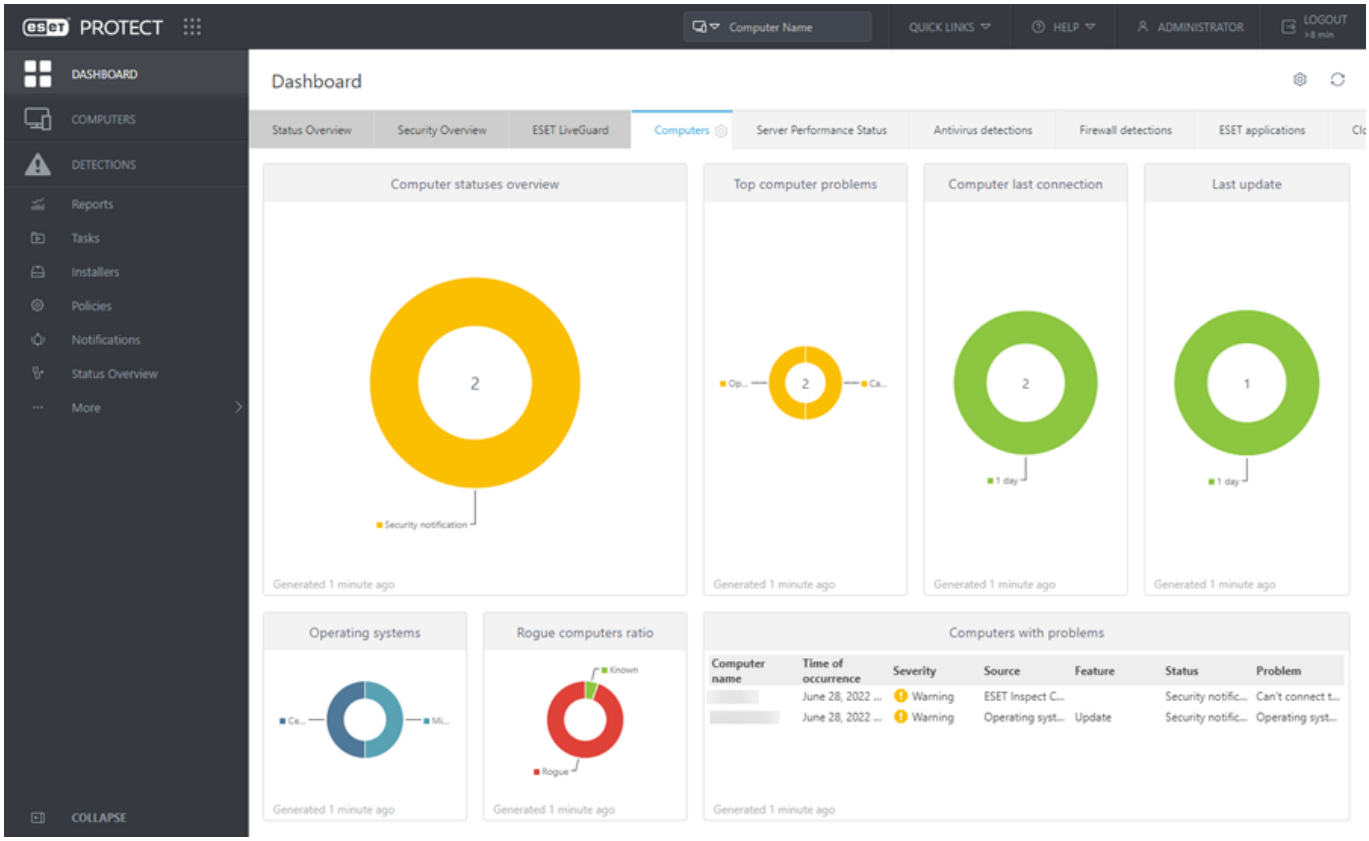
• Webコンソールの左側のメインメニューには、管理者がクライアントセキュリティソリューションとESETPROTECTサーバー設定を管理するために使用できるツールが表示されます。**詳細**の下のツールを使用すると、ネットワーク環境を設定し、メンテナンスのニーズを最小化できます。また、通知とダッシュボードを設定し、常にネットワークステータスを監視することができます。 をクリックすると、画面の左側にメニューが開きます。**折りたたむ**をクリックすると、折りたたむことができます。

• 画面の左上ESET PROTECTの名前の横には、製品ナビゲーションアイコンが表示されESET PROTECTとその他の製品(ESET InspectESET Business AccountESET MSP Administrator)を操作できます。

• アイコンは常にコンテキストメニューを示します。

• **[更新]**をクリックすると、表示情報を再読み込み/更新します。

• ページの下のボタンは、各セクションと機能で固有であり、該当する章で詳述します。



次のトピックでは、メインメニュー項目について説明します。

- ダッシュボード
- コンピューターとグループ
- 検出
- レポート
- タスク
- ポリシー
- 通知
- ステータス概要

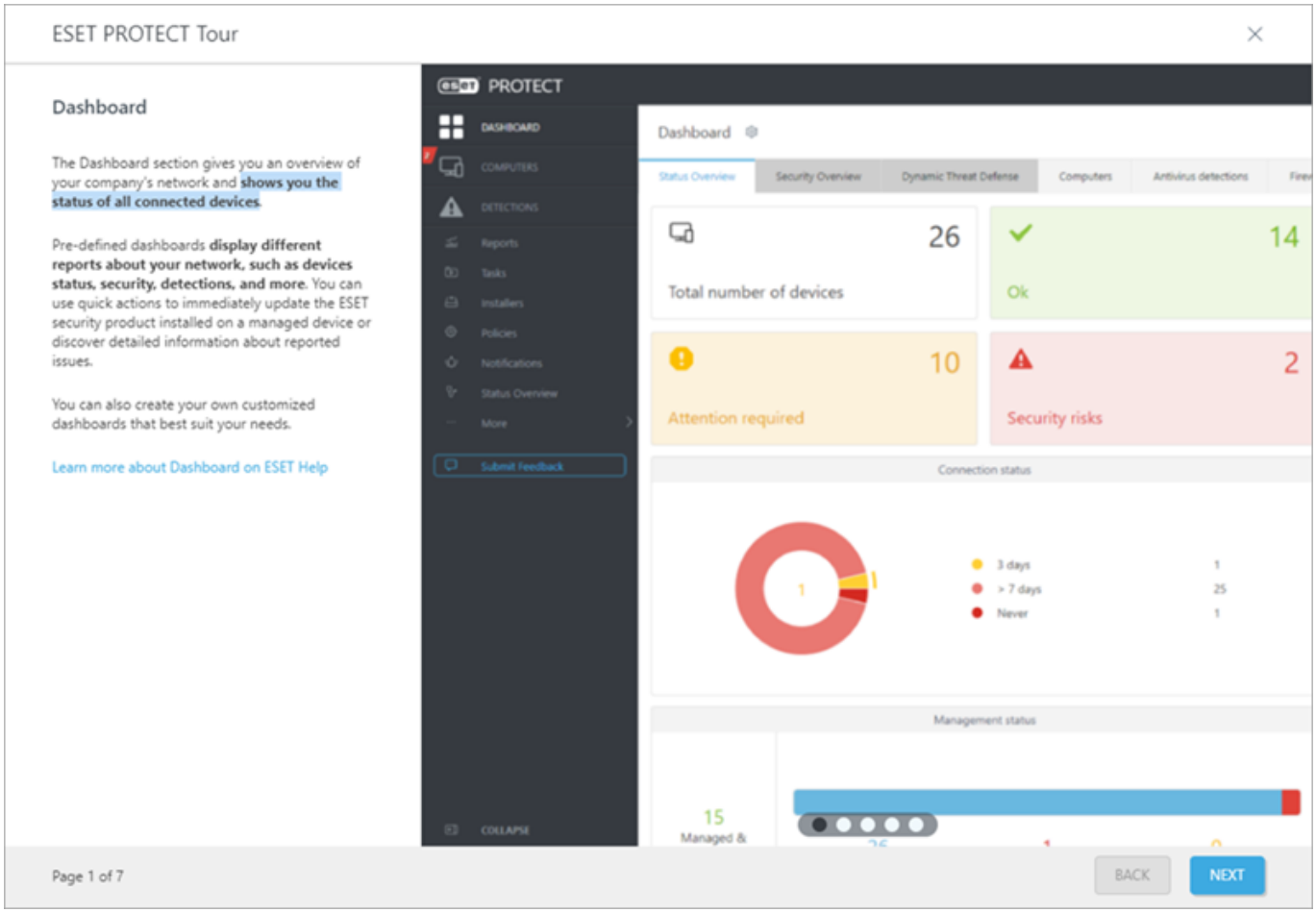
··· **その他** > 除外
··· **詳細** > 隔離
··· **詳細** > ユーザーと権限設定
··· **詳細** > ライセンス管理
··· **詳細** > 証明書

ESET PROTECTガイド

初めてWebコンソールにログインすると、**ESET PROTECTガイド**が表示されます。

このウィザードでは、重要なESET PROTECT Webコンソールセクション、ESET Managementエージェント、およびESETセキュリティ製品の基本的な説明を提供します。ダッシュボード、コンピューター、検出、タスク、ポリシー、通知、自動製品アップデートについてお読みください。

ESET PROTECTガイドの最後のステップで**デバイスの保護**をクリックし、ネットワークのコンピューターにESET Managementエージェントを展開します。ウィザードを使用せずにエージェントインストーラーを作成するには、**インストーラー** > **インストーラーの作成**をクリックします。



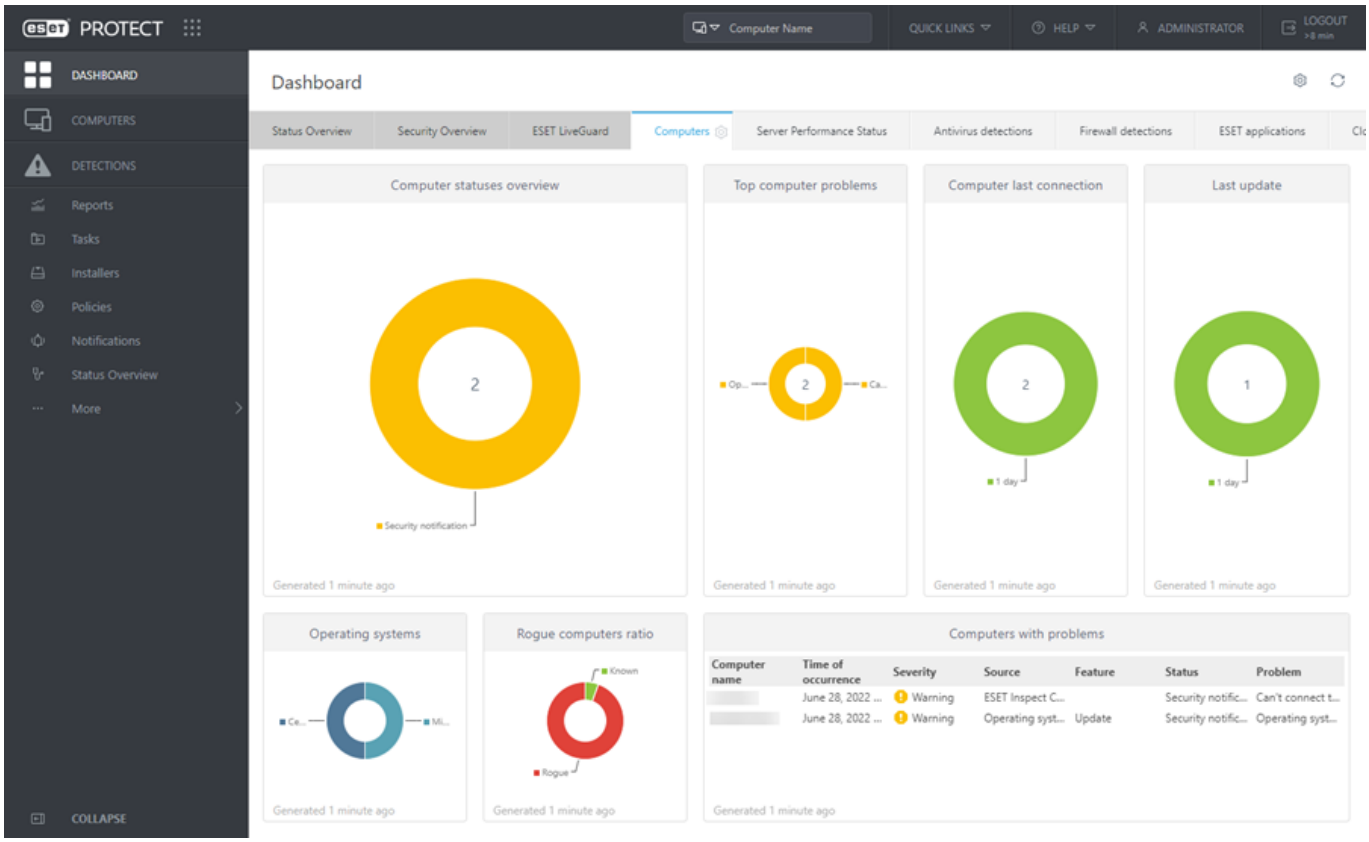
ESET PROTECTガイドを使用しない場合は、**X**をクリックします。ESET PROTECT Webコンソールが開きます。次回ESET PROTECT Webコンソールにログインするときには、**ESET PROTECTガイド**は表示されません。

ESET PROTECTガイドを再表示するには、**ヘルプ** > **ESET PROTECTガイド**をクリックします。

ESET PROTECT Webコンソールに初めてログインした後はESET PROTECTがインストールされているコンピューターで、オペレーティングシステムアップデートクライアントタスクを実行することをお勧めします。

ダッシュボード

ダッシュボードは、既定画面となっており、ユーザーがESET PROTECT Webコンソールにログインした後、表示されます。ネットワークに関する定義済みレポートが表示されます。トップメニューバーのタブを使用して、ダッシュボード間を切り替えることができます。各ダッシュボードは、さまざまなレポートで構成されています。



レポートの追加、既存ダッシュボードの変更、サイズ変更、移動および再調整して、ダッシュボードをカスタマイズできます(**ステータス概要**、**セキュリティ概要**、**ESET LiveGuard**を除く)。この柔軟性により、ESET PROTECTとそのオブジェクトの包括的な概要(コンピューター、グループ、タスク、ポリシー、ユーザーなど)を作成できます。

ESET PROTECTには、4つのダッシュボードがあらかじめ設定されています。

- **概要** - ESET PROTECTネットワークに関する主要な情報が表示される基本ダッシュボードウィンドウ。このダッシュボードは修正できません。
- **セキュリティ概要** – 重要度、検出方法、解決ステータス、インシデントがある上位10のコンピューター/ユーザーなど、過去7日間に報告された未解決の検出の概要を示します。このダッシュボードは修正できません。
- **ESET LiveGuard** - ESET LiveGuard Advancedを使用している場合は、便利なESET LiveGuard Advancedレポートの概要をここで確認できます。
- **コンピューター** – このダッシュボードでは、保護の状態、オペレーティングシステム、アップ

デートの状態など、クライアントマシンの概要を説明しています。

• **サーバーパフォーマンス状態** – このダッシュボードでは、サーバーの負荷、問題のあるクライアントCPU負荷、データベース接続などESET PROTECTサーバー自体に関する情報を表示することができます。

• **ウイルス対策検出** – ここでは、未解決の検出、直近の7日間または30日間における検出など、クライアントセキュリティ製品のウイルス対策モジュールからのレポートを表示することができます。

• **ファイアウォール検出**脅威 – 重要度、レポート時間などに応じた、接続中のクライアントのファイアウォールイベント。

• **ESET アプリケーション** – このダッシュボードでは、インストール済みのESETアプリケーションの情報を確認できます。

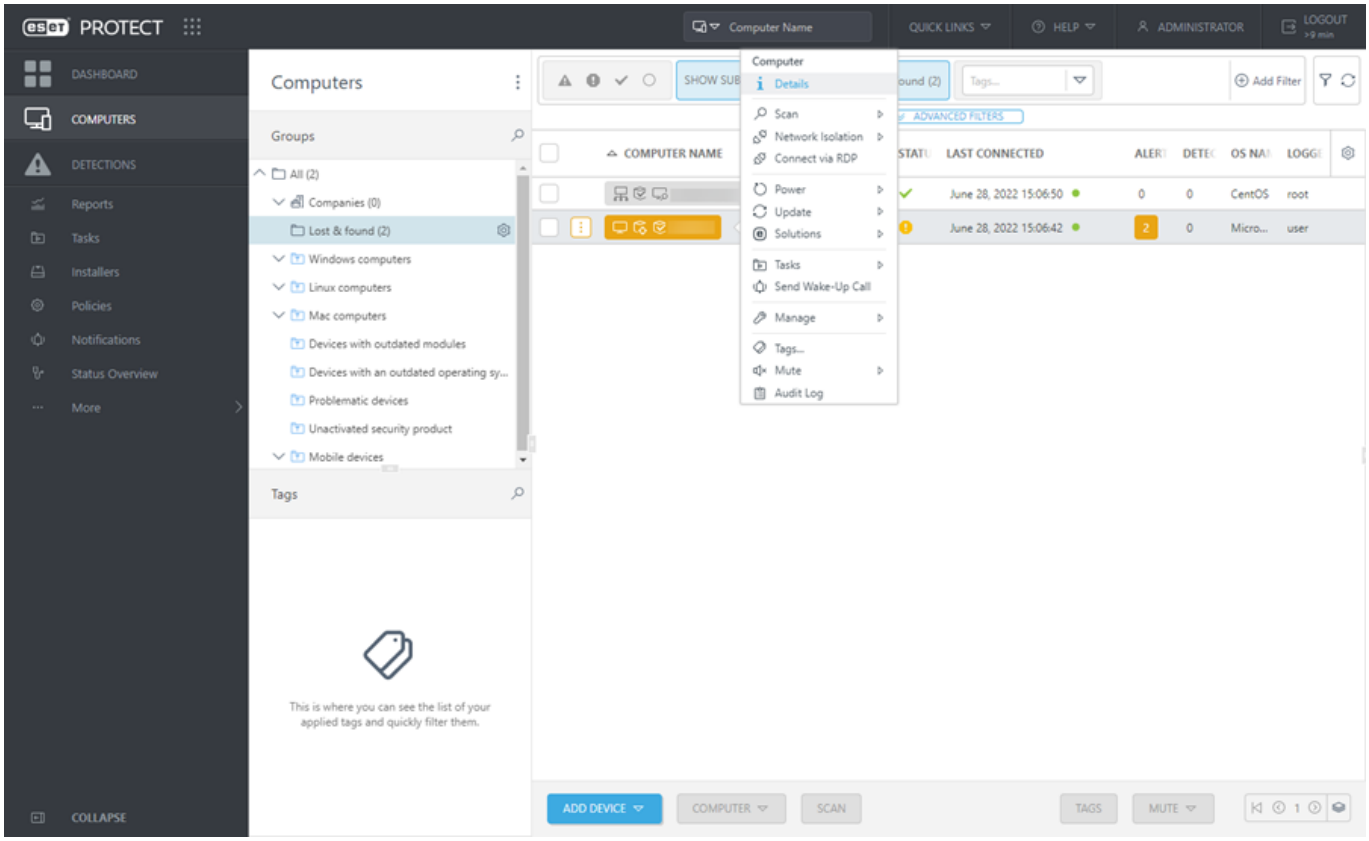
• **クラウドベースの保護** – このダッシュボードでは、クラウドベースの保護レポートの概要(ESET LiveGrid®とESET LiveGuard Advanced (適切なライセンスがある場合))が表示されます。

コンピューター

ESET PROTECTから接続可能なすべてのクライアントコンピューターは**コンピューター**に表示され、グループ別に表示されます。(左側のウィンドウの)リストからグループをクリックすると、右側のペインで該当するグループのメンバー(クライアント)が表示されます。クライアントをドラッグアンドドロップすると、グループ間で移動できます。

コンピューターの管理

デバイスをクリックすると、そのデバイスで使用できるアクションの新しいメニューが開きます。デバイスの横のチェックボックスを選択し、下のバーの**コンピューター**をクリックします。**コンピューター**メニューには、デバイスのタイプに応じてさまざまなオプションが表示されます。



コンピューターのフィルタリング

リストに特定のコンピューターが表示されずESET PROTECTインフラストラクチャ内にあることがわかっている場合には、すべてのフィルターがオフになっていることを確認してください。

ページの上部にあるフィルターを使用してクライアント(コンピューター)をフィルタリングできます。

- **サブグループの表示**チェックボックスをオンにすると、現在選択されているグループのサブグループが表示されます。
- **フィルターの追加**をクリックすると、使用可能なフィルタリング条件が表示されます。定義済みフィルターもいくつか用意されており、すばやくアクセスできます。
- **フィルターの追加 > 製品カテゴリ**をクリックして、使用可能なカテゴリから選択できます。

  o**すべてのデバイス** – フィルタリングなしですべてのクライアントコンピューターが表示されます。表示を絞り込む場合は、上記すべてのフィルタオプションの組み合わせを使用します。

  o**ESET保護中**—ESET製品で保護されたクライアントが表示されます。

  o**ESET PROTECT**— エージェントRD SensorESET Bridge (HTTPプロキシ)などの個別のESET PROTECTコンポーネントが表示されます。

  o**その他** – 選択した製品(Shared Local Cache仮想セキュリティアプライアンスESET Inspect)を実行するクライアントコンピューターのみが表示されます。

- ステータスアイコンを使用すると、検出された問題の重要度別にクライアントをフィルタリングできます(エラーは赤、警告は黄、通知は緑、管理されていないコンピューターは灰色)。ステータスアイコンは、特定のクライアントコンピューターと、インストールされているESETソリューションの現在の状態を表します。異なる重要度のステータスアイコンを非表示または表示し、ステー

タス別にネットワークのクライアントを評価できます。たとえば、警告のあるコンピューターだけを表示するには、黄色のアイコンのみをオンにします(残りのアイコンをオフにする必要があります)。警告とエラーの両方を確認するには、赤および黄のステータスアイコンをオンにします。管理対象外のコンピューター(ESET Managementエージェントまたは ESETセキュリティ製品がインストールされていないネットワーク上のクライアント)は通常、**紛失**静的グループに表示されます。

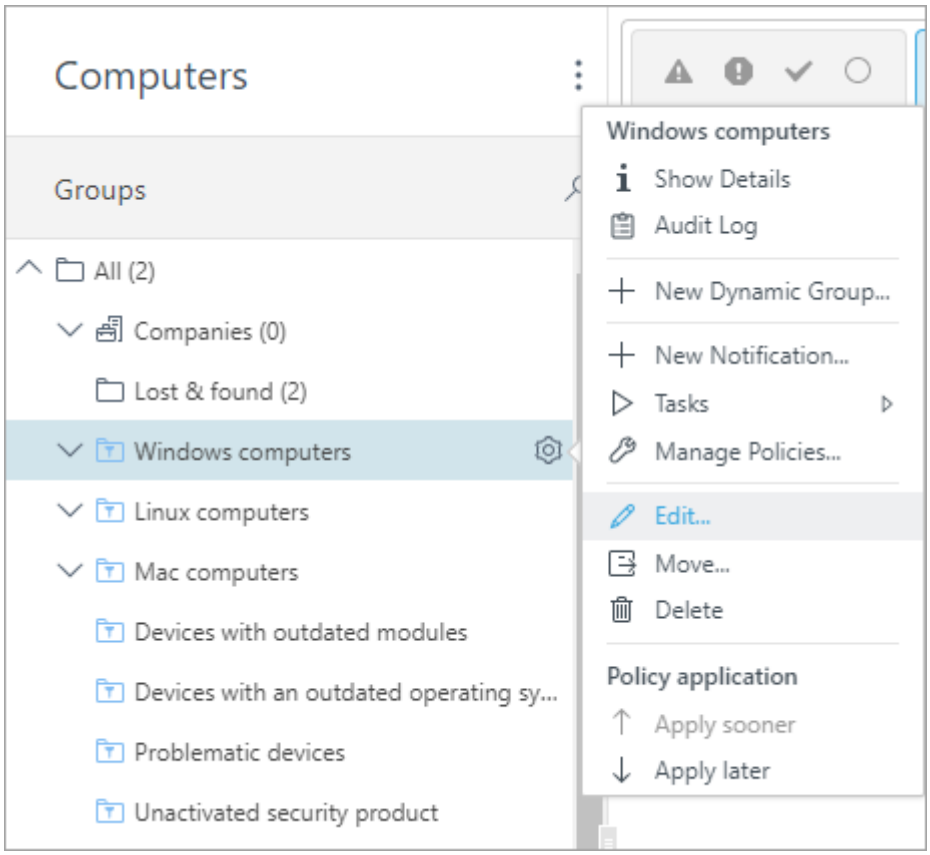
- **コンピューター**画面には、展開可能なフィルターパネルとして、**詳細フィルター**が表示されます。多数のコンピューターをフィルタリングする場合は、詳細フィルターによって、管理可能な結果数を返すフィルター値が表示され、適切なデバイスをすばやく検索できます。
- 列の見出しをクリックすると、属性別にコンピューターを並べ替えることができます。

前回の接続には、管理されたデバイスの前回の接続日時が表示されます。緑の点は、コンピューターが10分以内に接続されていることを示します。**前回の接続**列情報はハイライトされ、コンピューターが接続していないことを示します。

- o黄色(エラー) – コンピューターは2～14日接続されていません。
- o赤(警告) – コンピューターは14日以上接続されていません。

グループ

コンピューターからグループを管理できます。グループでは、ネットワークのエンドポイントを整理し、体系的にポリシーとタスクを割り当てることができます。この設定はすべてのグループメンバーに適用されます。グループメンバーのコンピューターは、右側のウィンドウに一覧表示されます。グループ名の横の歯車アイコンをクリックして、使用可能なグループアクションとグループ詳細を表示します。



グループには、静的グループと動的グループの2種類があります。

静的グループ

- 静的グループは選択されたクライアントコンピューターと他のオブジェクトのグループになります。
- すべてのモバイルおよびコンピューターデバイスは静的グループにあります。
- 静的グループに属するエンドポイントは手動で選択できます。
- オブジェクトは1つの静的グループにだけ属することができます。
- 静的グループはESET PROTECTセキュリティモデルで重要な役割を担います。
- ESET Business AccountまたはESET MSP Administratorからライセンスをインポートする場合、ESET Business Account会社構造（サイトを含む）またはESET MSP Administrator構造が静的グループツリーに表示されます。

動的グループ

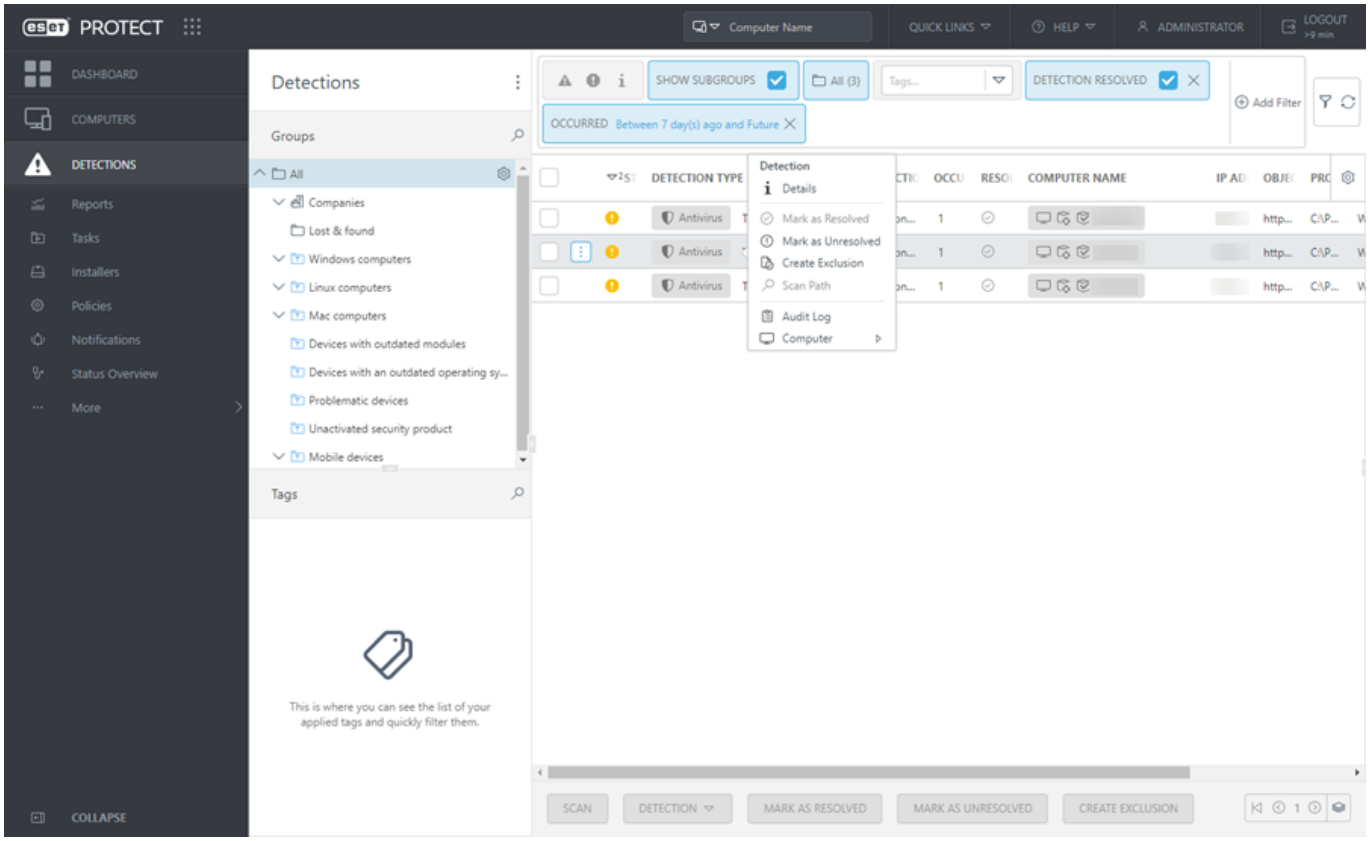
- 動的グループは、コンピューターをフィルタリングするルールを設定できるカスタムフィルターとして考えることができます。
- 動的グループはテンプレートに基づき、テンプレートで定義された条件を満たすエンドポイントが自動的に含まれます。
- クライアントデバイスが条件を満たしていない場合、自動的に動的グループから削除されます。
- コンピューターは、同時に複数の動的グループに属したりか、どの動的グループにも属さなかったりすることができます。

ナレッジベース記事には、静的グループへのコンピューターの追加、新しい動的グループテンプレートの作成、およびグループへのポリシーの割り当ての方法が記載されています。

グループのグループに関する詳細を参照してください。

検出

検出レポートにアクセスするには、左側のWebコンソールメニューの**検出**をクリックします。**検出**パネルは、ネットワークのコンピューターで見つかったすべての検出の概要が表示されます。



グループを参照し、特定のグループのメンバーの検出を確認できます。ビューはフィルタリングできます。既定では、最後の7日間のすべての検出タイプが表示されます。脅威は**脅威**セクションまたは特定のクライアントの詳細の下で**解決済みに設定**できます。

検出が時間および他の条件によって集約され、解決を簡素化します。24時間を経過した検出は、毎日午前0時に自動的に集計されます。**解決済み**列でX/Y (解決済みのアイテム/合計アイテム数)によって、集約された検出を特定できます。検出詳細の**発生**タブには、集約された検出が一覧表示されます。

隔離された検出は、⋯ **その他** > 隔離にあります。

除外

検出で選択したアイテムを将来の検出から除外できます。検出をクリックして、**除外の作成**をクリックします。**ウイルス対策**検出と**ファイアウォール**検出 – IDSルールのみを除外できます。除外を作成して、その他のコンピューターとグループに適用できます。

> ⚠ 除外は注意して使用してください。コンピューターが感染するおそれがあります。

⋯ **その他** > **除外**セクションには、すべての作成された除外が含まれ、表示がわかりやすくなり、管理が簡素化されます。

アーカイブ内の検出

アーカイブで1つ以上の検出が見つかった場合、アーカイブ内の各検出が**検出**で報告されます。

> ⚠ 検出を含むアーカイブファイルを除外しても、検出は除外されません。アーカイブ内の個々の検出を除外する必要があります。アーカイブに含まれるファイルの最大ファイルサイズは3 GBです。

除外された検出は、別のアーカイブまたはアーカイブされていない場合でも検出されなくなります。

ランサムウェアシールド

ESETビジネス製品(バージョン7以降)には、**ランサムウェアシールド**があります。この新しいセキュリティ機能は、HIPSの一部であり、コンピューターをランサムウェアから保護します。ランサムウェアがクライアントコンピューターで検出されると ESET PROTECT Webコンソールの**検出**に検出詳細が表示されます。ランサムウェア検出のみをフィルタリングするには、**フィルターの追加 > スキャナー > ランサムウェア対策スキャナー**のをクリックします。ランサムウェア保護の詳細については、ESET用語集を参照してください。

ESETビジネス製品の**ポリシー**設定を使用して ESET PROTECT Webコンソールから**ランサムウェアシールド**をリモート設定できます。

- **ランサムウェア保護を有効にする** - ESETビジネス製品は、ランサムウェアのように動作するすべての不審なアプリケーションを自動的にブロックします。

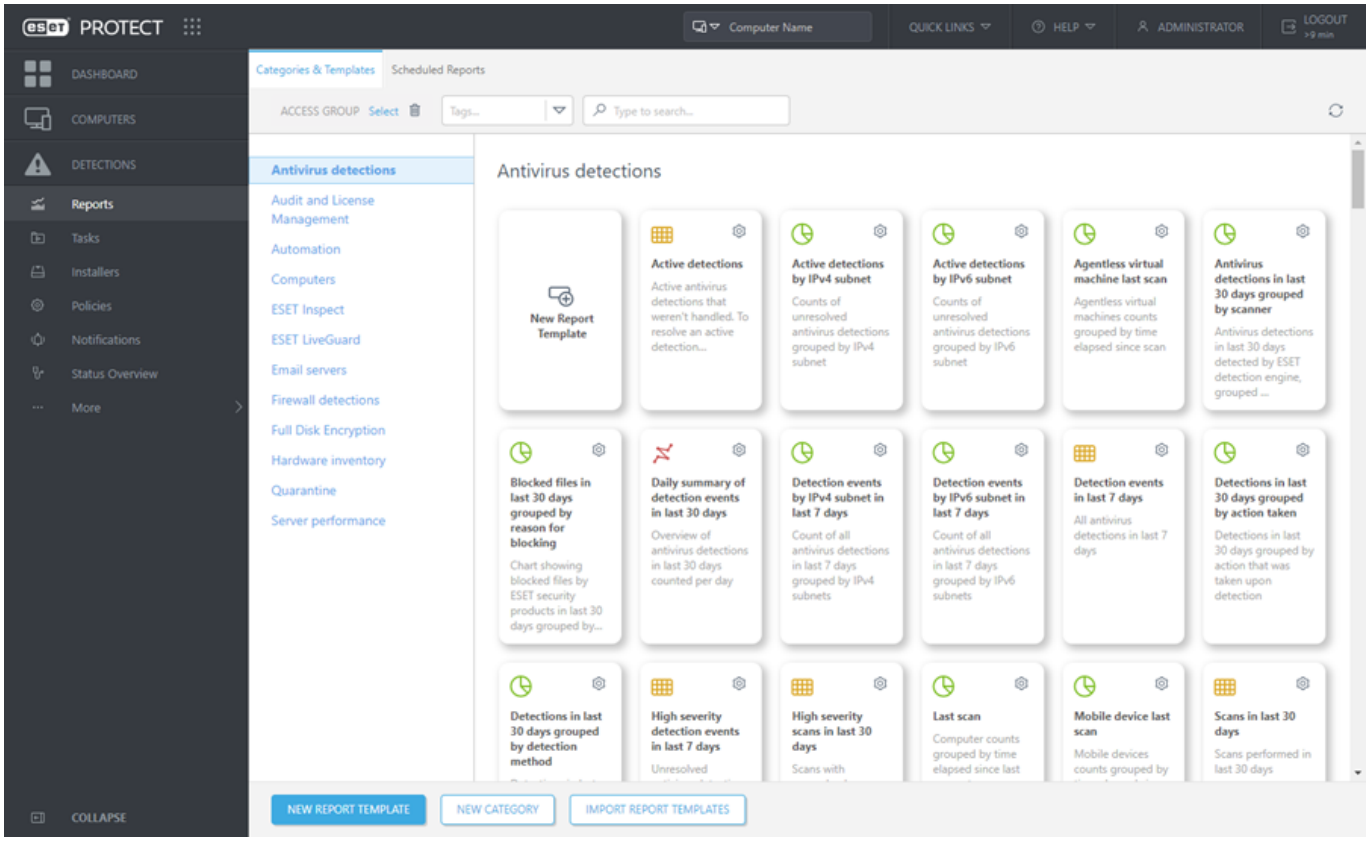
- **監査モードを有効にする** – 監査モードを有効にすると、ランサムウェア保護によって特定された検出はESET PROTECT Webコンソールで報告されますが、セキュリティ製品によってブロックされません。 管理者は、報告された検出をブロックするか、除外の作成を選択して、除外するかを決定できます。 このポリシー設定は、ESET PROTECT Webコンソールでのみ使用できます。

既定では、ランサムウェアシールドは、合法的なアプリケーションを含め、潜在的なランサムウェアの動作をしているすべてのアプリケーションをブロックします。新しい管理されたコンピューターでは、少しの間、**監査モードを有効にする**を推奨します。このようにすると、動作に基づいてランサムウェアとして検出される合法的なアプリケーション(誤検出)を除外できます。永久的に監査モードを使用することは推奨されません。監査モードを有効にすると、管理されたコンピューターのランサムウェアが自動的にブロックされないためです。

レポート

レポートを使用すると、簡単にデータベースからデータにアクセスしてフィルタリングできます。レポートにはカテゴリがあります。各カテゴリには短い説明があります。

レポートにアクセスするには、左のWebコンソールメニューで**レポート**をクリックし、任意のレポートテンプレート(説明、アクションのタイル)を選択し、(歯車アイコン) > **今すぐ生成**をクリックします。



既定では、すべてのレポートテンプレートは管理者のみがアクセスできます。他のユーザーは、十分な権限が割り当てられているか、テンプレートが別の場所に移動されないかぎり、これらのテンプレートを参照または使用できません。

電子メールでレポートを受信するには、SMTPサーバー接続を正しく設定する必要があります。

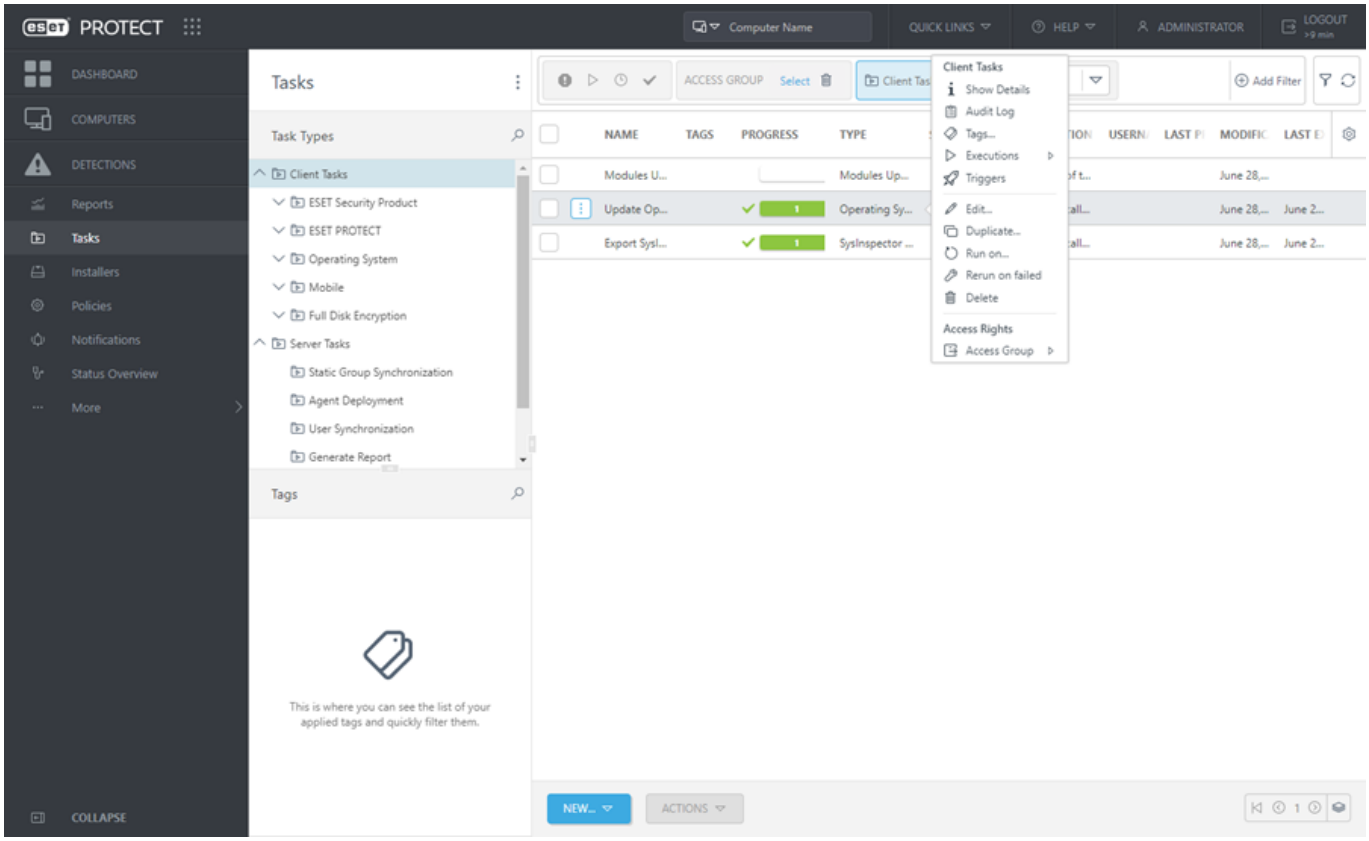
ESET PROTECTで自動レポートを設定するための段階的な手順については🖻ESETナレッジベース記事を参照してください。

タスク

タスクを使用して🖻ESET PROTECTサーバー、クライアントコンピューター、およびESET製品を管理できます。タスクは日常的なジョブを自動化できます。個別のコンピューターとグループをタスクのターゲットにできます。

タスクでは、個別のクライアントまたはクライアントのグループに特定の手順を割り当てることができます。

タスクウィンドウの他に、コンピューターのコンテキストメニューからタスクを作成できます。実行されたタスクのステータスを表示するには、**タスク**をクリックし、タスクが正常に完了したかどうかを確認します。



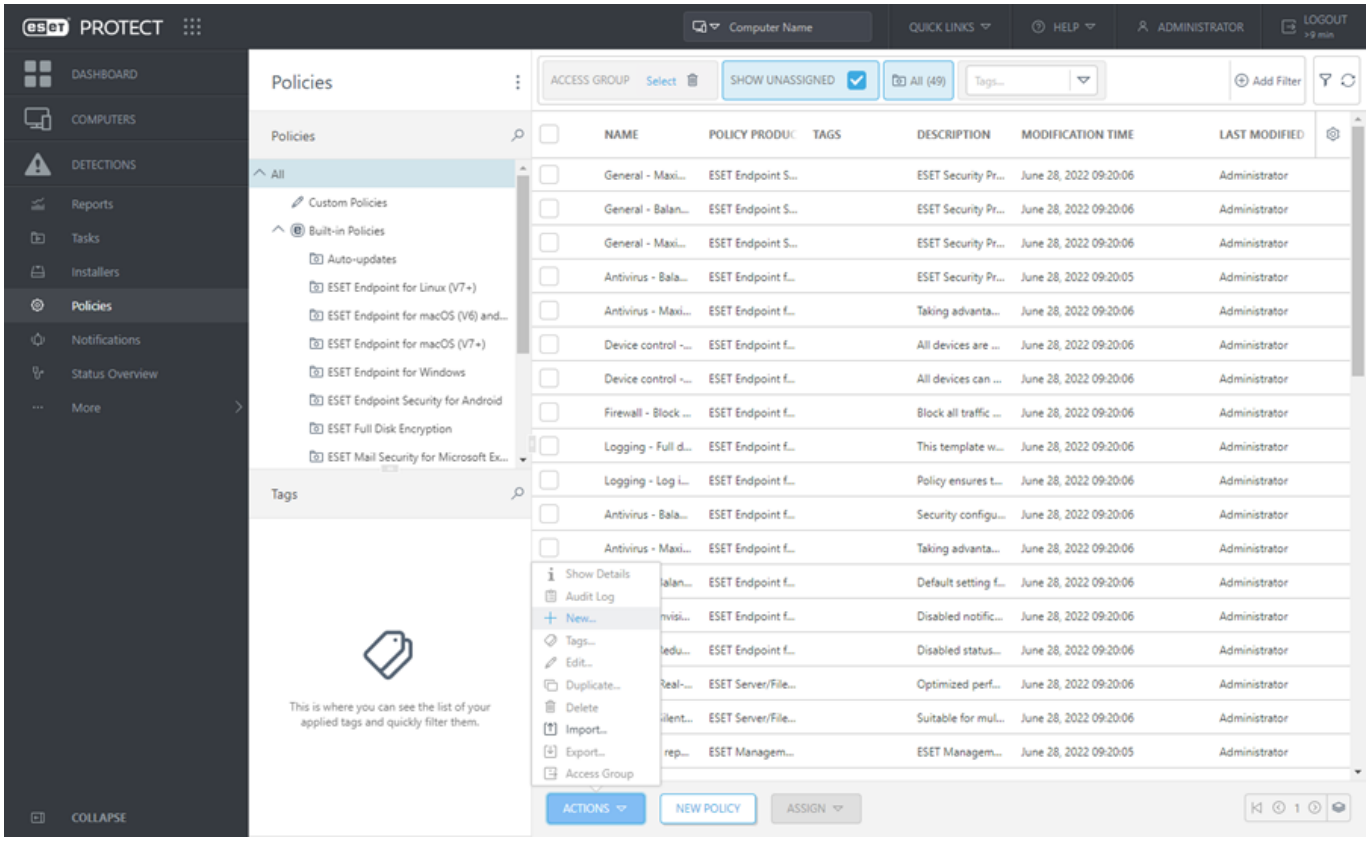
新しいタスクの作成、割り当て、およびスケジュール方法については🔗ESET PROTECT管理者ガイドのタスクセクションを参照してください。

ESETナレッジベースには、次のような特定のタスクを設定する手順の例があります。

- ESET PROTECTでクライアントコンピューターにウェイクアップコールを送信し、すぐにタスクを実行する🔗
- ESET PROTECTでクライアントコンピューターのエージェント接続間隔を変更する🔗
- ソフトウェアインストールクライアントタスクを使用して🔗ESETエンドポイント製品を展開またはアップグレードする🔗
- ESET PROTECTをActive Directoryと同期する🔗

ポリシー

ポリシーを使用して、クライアントコンピューターを管理できます。ポリシーは、クライアントコンピューターで実行されるESET製品に適用できる設定ルールのセットで、各クライアントのESET製品を手動で設定しないようにできます。個別のコンピューターとグループに直接ポリシーを適用できます。また、複数のポリシーをコンピューターまたはグループに割り当てることができます。



ESETナレッジベース記事の手順に従い、新しいポリシーを作成し、グループに割り当てます。

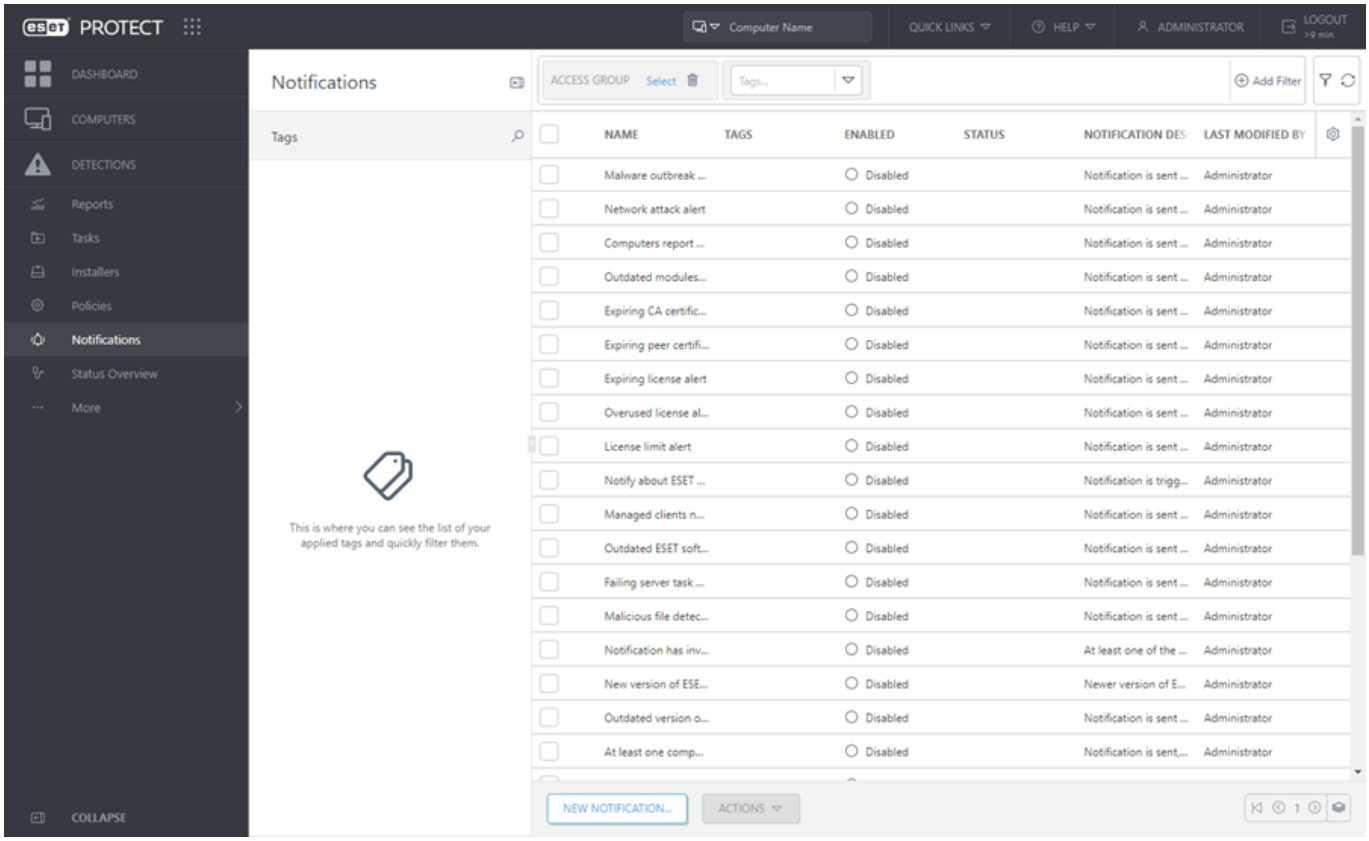
ポリシーは、静的グループの配置順に適用されます。このルールは、動的グループでは有効ではありません。動的グループでは、子動的グループが最初に走査され、グループツリーの上にある影響が大きいポリシーを適用し、サブグループに対して特定のポリシーを適用できます。

> グループツリーの上位にあるグループには、より汎用的なポリシー(アップデートサーバーなど)を割り当てることをお勧めします。下位のグループツリーには、より具体的なポリシー(デバイスコントロール設定など)を割り当ててください。

ポリシーの管理と適用、およびポリシー削除ルールの詳細については🖻ESET PROTECT管理者ガイドのポリシーセクションを参照してください。

通知

報告された検出、古いエンドポイントなどの特定のイベントに基づいて、自動通知を設定できます。通知の設定と管理の詳細については🖻ESET PROTECT管理者ガイドの通知セクションまたはナレッジベース記事を参照してください。



電子メールで通知を受信するには□SMTPサーバー接続を正しく設定する必要があります。

ESET PROTECTは電子メールレポートと通知を自動的に送信できます。**SMTPサーバーを使用する**を有効にし、**詳細 > 設定 >詳細設定SMTPサーバー**に移動し、次の項目を指定します。

- **ホスト** - SMTPサーバーのホスト名またはIPアドレス。

- **ポート** - SMTPは既定で25番ポートを使用しますが□SMTPサーバーが別のポートを使用する場合は変更できます。

- **ユーザー名** - SMTPサーバーで認証が必要な場合は、SMTPユーザーアカウント名(ドメインを含むと動作しないため含めないでください)を指定します。

- **パスワード** - SMTPユーザーアカウントに関連付けられたパスワード。

- **接続セキュリティタイプ** – 接続タイプを指定します。既定値は**保護しない**ですが□SMTPサーバーが安全な接続を許可する場合は、TLSまたはSTARTTLSを選択します。接続をより安全にする場合は、STARTTLSまたはSSL/TLS拡張を使用してください。暗号化通信用に別のポートが使用されます。

- **認証タイプ** – 既定値は**認証なし**に設定されます。ただし、ドロップダウンリストから該当する認証タイプ(ログイン□CRAM-MD5□CRAM-SHA1□SCRAM-SHA1□NTLM□自動など)を選択できます。

- **送信者アドレス** – 通知メールのヘッダーに表示される送信者アドレスを指定します

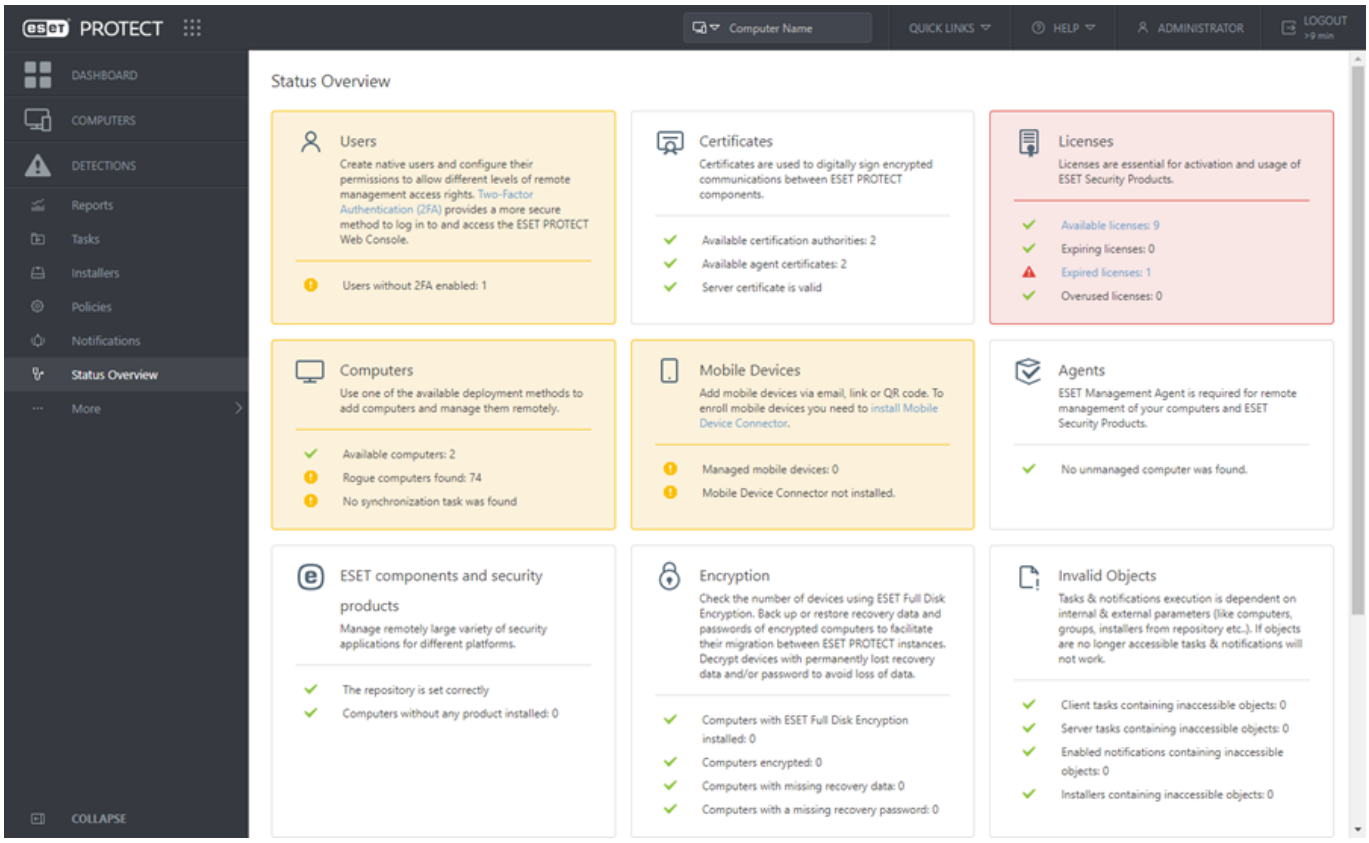
- **SMTPサーバーのテスト** - SMTP設定が正しいことを確認します。**テスト電子メールの送信**をクリックすると、ウィンドウが開きます。受信者の電子メールアドレスを入力すると、テストメールメッセージがSMTPサーバー経由でこのアドレスに送信されます。受信者のメールボックスを確認し、テスト電子メールが配信されたことを確認します。

ステータス概要

ESET PROTECTサーバーは定期的な診断チェックを実行します。

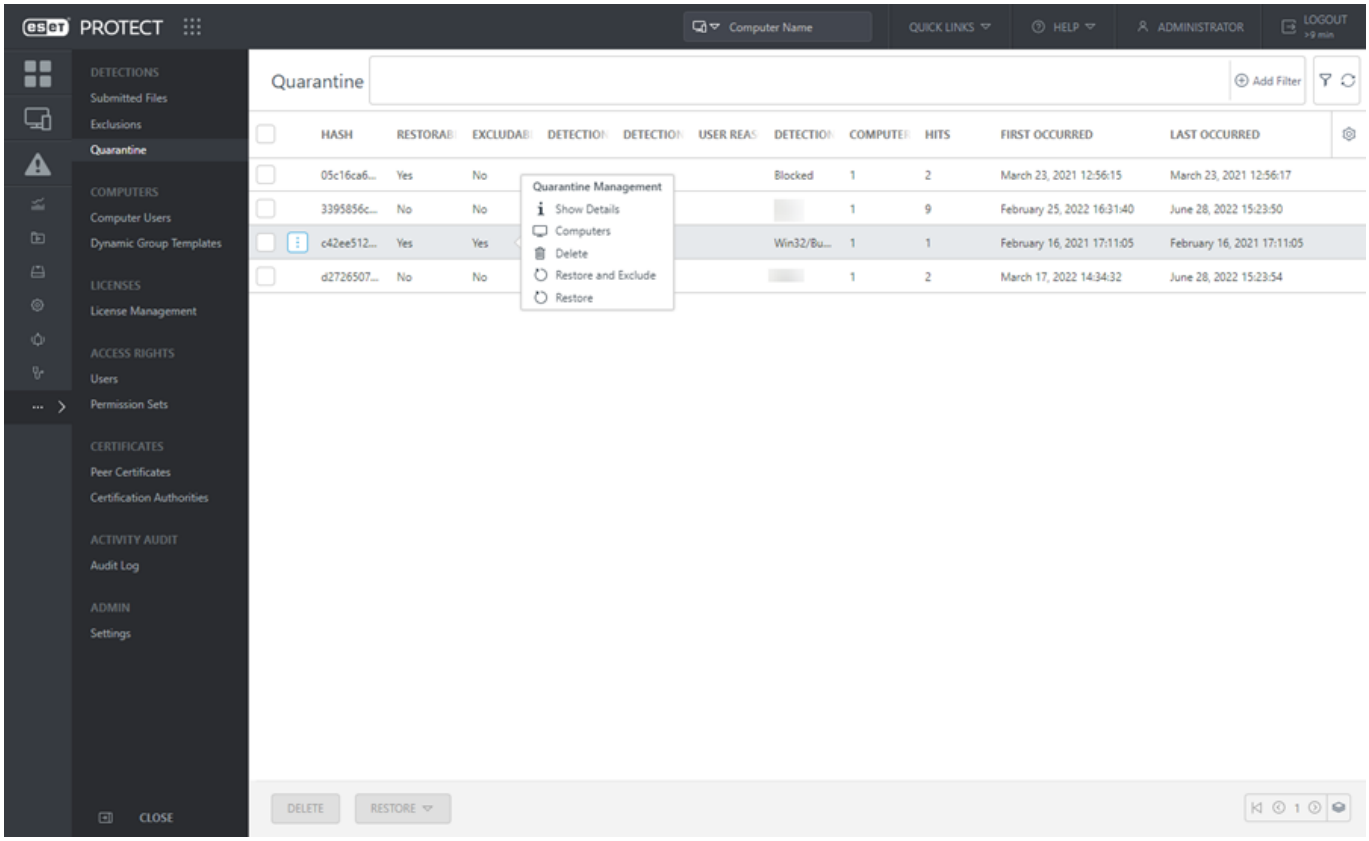
1.**ステータス概要**をクリックし、ESET PROTECTに関する詳細なステータス情報を表示します。**ステータス概要**を使用して、使用統計情報とESET PROTECTの一般的なステータスを表示します。また、ESET PROTECTの初期設定にも使用できます。

2.セクションタイルをクリックし、アクションのある右側のタスクバーを表示します。



隔離

隔離セクションは、Webコンソールの ⋯ **詳細** > **隔離**に表示されます。このセクションには、クライアントデバイスで隔離されたすべてのファイルが表示されます。



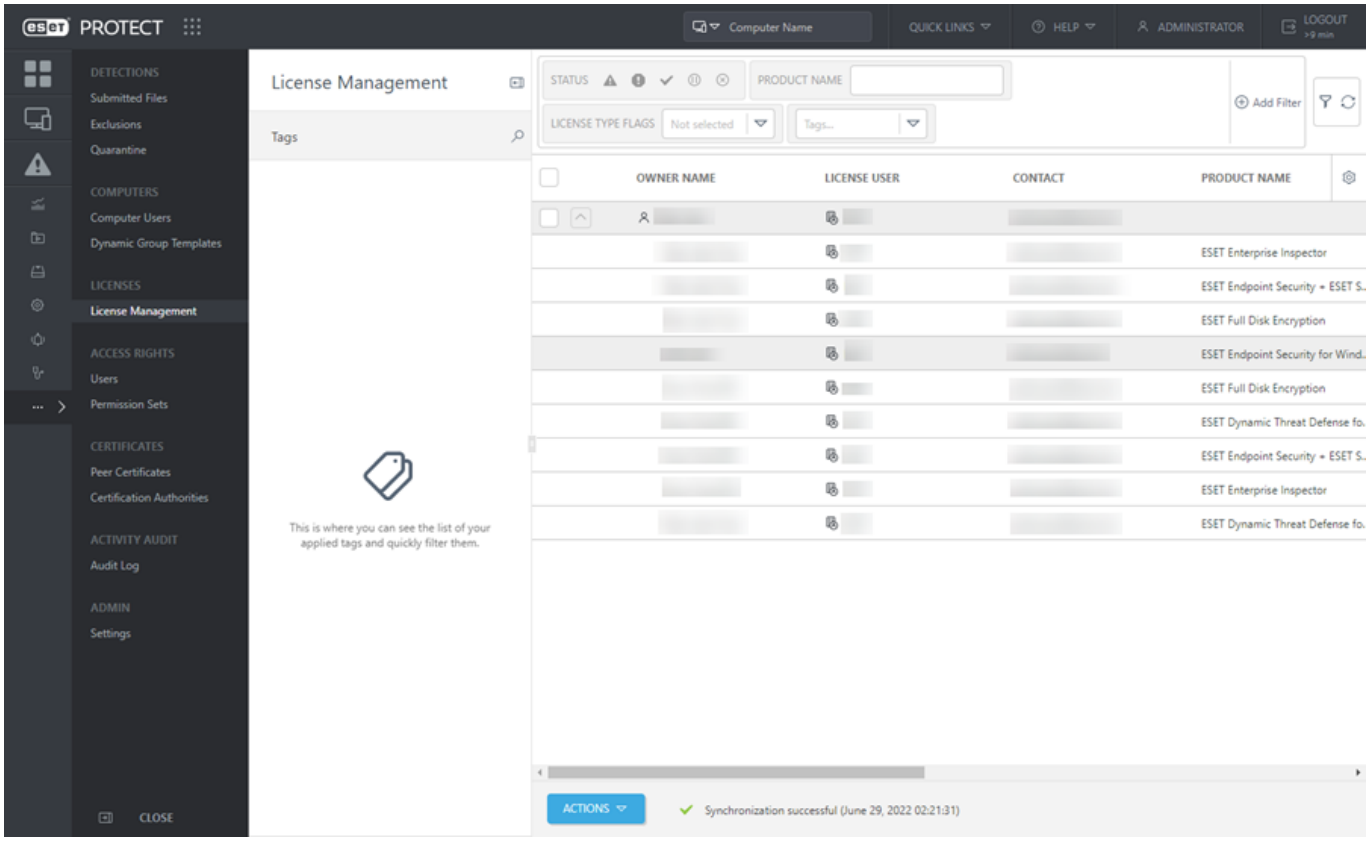
ファイルを駆除できない場合、ファイルの削除が安全でも推奨もされない場合、あるいはESET製品で誤検出された場合、ファイルを隔離してください。

クライアントデバイスで見つかったすべての検出が隔離に移動されるわけではありません。隔離されない検出:
- 削除できない検出
- 動作に基づき不審ではあるものの、マルウェアとして特定されない検出。たとえば、PUA

隔離管理に関するESETナレッジベース記事も参照してください。

ライセンス管理

⋯ **詳細** > **ライセンス管理**をクリックします。



新しいライセンスキーをESET PROTECTに追加するには：

1. ⋯ **詳細** > **ライセンス管理**をクリックして、**アクション** > **ライセンスの追加**をクリックします。

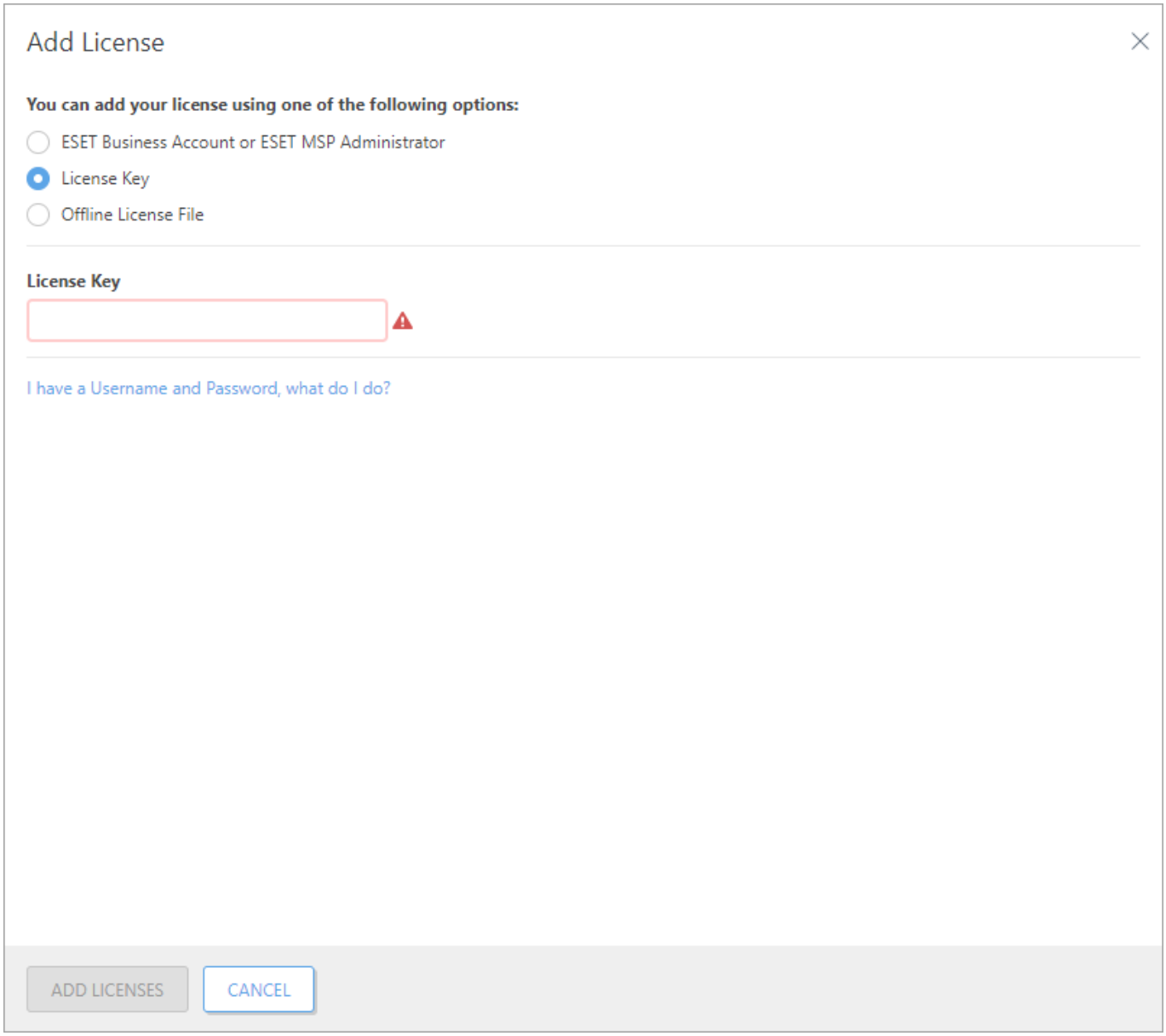
2.新しいライセンスを追加するのに使用する方法を選択します。

a.**ESET Business Account または ESET MSP Administrator** - ESET Business Accountまたは ESET MSP Administratorアカウントのライセンスを ESET PROTECT Web コンソールと同期します。サイト間でのライセンスシートの分配など ESET Business Accountの構造全体をインポートできます。

b.**製品認証キー** - ESET製品をアクティベーションし、ライセンス所有者を特定するために使用される一意の文字列 ESETセキュリティソリューションを購入したときに受け取ったライセンスキーを**製品認証キー**フィールドに入力するか、コピーして貼り付けます。

c.**オフラインライセンスファイル** - ESET Business Accountでオフラインライセンスを作成およびダウンロードする手順を参照してください

3.**ライセンスの追加**をクリックします。



ESET PROTECTは、サブスクリプションライセンスの管理をサポートします。ESET Business Account、ESET MSP Administratorまたは製品認証キーを使用して、ライセンスを追加できます。**有効期間**列の**ライセンス管理**の下、または**コンピューター** > 詳細をクリックすると、サブスクリプションの有効期限を確認できます。

ユーザーと権限設定

ESET PROTECT セキュリティモデル

セキュリティモデルの主な用語:

用語	説明
ホームグループ	ホームグループでは、ユーザーが作成するすべてのオブジェクト(デバイス、タスク、テンプレートなど)が自動的に保存されます。各ユーザーには1つのホームグループだけを持つ必要があります。

用語	説明
オブジェクト	各オブジェクト(コンピューター、タスク、ポリシー、レポート、通知)は静的グループに属します。オブジェクトへのアクセスは、ユーザーではなくグループごとに行われます（グループごとにアクセスを提供すると、たとえば、1人のユーザーが休暇中の場合など、複数のユーザーに簡単に対応できます）。
アクセスグループ	アクセスグループは、ユーザーがアクセス権に基づいてオブジェクトの場所をフィルタリングできる静的グループです。
管理者	管理者はホームグループ**すべて**に属し、グループに対するフル権限設定があるユーザーです。
アクセス権	オブジェクトにアクセスするかタスクを実行する権限が権限設定で割り当てられます。
権限設定	権限設定は、ESET PROTECT Webコンソールにアクセスするユーザーの権限です。権限設定は、ユーザーがESET PROTECT Webコンソールで表示または実行できる操作を定義します。ユーザーには複数の権限設定を割り当てることができます。権限設定は定義された静的グループのオブジェクトにのみ適用されます。
機能	機能はオブジェクトまたはアクションの1つのタイプです。一般的に、機能には次の値があります。**読み取り**、**書き込み**、または**使用**。アクセスグループに適用される機能の組み合わせは権限設定と言います。

詳細についてはESET PROTECT管理ガイドのアクセス権を参照してください。

新しいESET PROTECT Webコンソールユーザーを作成します。

新しいESET PROTECT設定には、最初に唯一のユーザーである既定の**管理者**(ホームグループ**すべて**に属し、すべてにアクセスできるユーザー)があります。

ESETは既定の管理者ユーザーアカウントを使用することをお勧めしません。別の管理者アカウントを作成してください。また、必要な権限に基づいて、よりアクセス権が制限された追加のユーザーを作成できます。

証明書

証明書

証明書はESET PROTECTの基本的な要素でESET PROTECTコンポーネントとESET PROTECTサーバー間の安全な通信と、ESET PROTECT Webコンソールの安全な接続を確立するための機能です。 ⋯ **詳細** > **ピア証明書**ではESET PROTECT証明書を管理できます。

ESET PROTECTインストール中に自動的に生成される証明書を使用できます。

認証局

認証局はネットワークから配布された証明書を合法化します。エンタープライズ設定では、公開鍵は、クライアントソフトウェアとESET PROTECTサーバーを自動的に関連付け、ESET製品のリモートインストールを有効にします。 ⋯ **詳細** > **認証局**ではESET PROTECT認証局を管理できます。

すべてのピア証明書は有効で、同じ認証局によって署名されることでコンポーネントが正常に通信できることを保証する必要があります。

証明書と認証局の詳細については、ESETナレッジベース記事またはオンラインヘルプをお読みください。

ヘルプとサポート

ESETは常にESET PROTECTおよびESETエンドポイント製品のアップデートと改善に努めています。

- oESET ナレッジベースは、サポート記事を検索できるリポジトリで、問題の解決と質問への回答を目的としています。
- oESETユーザーフォーラムはESETスタッフによって監視され、ESETユーザーは発生している問題を共有し、解決を検索できます。
- oESETナレッジベースビデオチャンネルには、ESET製品の一般的な手順を説明するビデオがあります。
- oESET製品機能とアップグレードに関する最新のお知らせについては、ESETサポートニュースとカスタマーアドバイザリーをご覧ください。
- o問題を解決したり、質問への回答が見つからない場合は、いつでも、ESETカスタマーサポートに問題を報告できます。

また、詳細については、ESET PROTECTインストールガイド（アップグレード、移行、トラブルシューティングなど）、管理者ガイド (ESET PROTECT WebコンソールでESET PROTECTを管理する)、および仮想アプライアンスガイド (ハイパーバイザーのESET PROTECT)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-ROM、DVD、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ー（「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ー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