

ESET PROTECT

管理ガイド

[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。](#)

Copyright ©2024 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問わず、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: 2024年/4月/12日

1 ヘルプ	1
1.1 アイコン凡例	2
1.2 オフラインヘルプ	4
2 ESET PROTECTの概要	7
2.1 ESET PROTECTの新機能	8
2.2 サポート対象のWebブラウザとESETセキュリティ製品および言語	9
2.3 自動製品アップデート	12
3 ESET PROTECTの基本操作	15
3.1 ESET PROTECT Webコンソールを開く	16
3.2 ESET PROTECT Webコンソール	18
3.2 ログイン画面	21
3.2 セットアップウィザードの使用	23
3.2 ユーザー設定	27
3.2 フィルターとレイアウトのカスタマイズ	28
3.2 タグ	31
3.2 CSVのインポート	34
3.2 トラブルシューティング - Webコンソール	35
3.3 ESET PROTECTからエンドポイント製品を管理する方法	37
3.4 ESETプッシュ通知サービス	39
4 VDI複製、ハードウェア検出	39
4.1 複製の質問の解決	43
4.2 ハードウェアID	46
4.3 複製のためのマスター	46
5 ESET Management エージェント展開	48
5.1 Active Directory同期を使用してコンピューターを追加する	49
5.2 新しいデバイスを手動で追加する	50
5.3 RD Sensorを使用してコンピューターを追加する	52
5.3 ESET Rogue Detection Sensorポリシー設定	54
5.4 ローカル展開	55
5.4 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する	56
5.4 エージェントライブインストーラーの作成 - Windows/Linux/macOS	59
5.4 WebサイトからERA エージェントをダウンロード	67
5.5 リモート展開	67
5.5 GPOとSCCMを使用したエージェント展開	68
5.5 展開手順 - SCCM	70
5.5 ESET Remote Deployment Tool	86
5.5 ESETリモート展開ツールの前提条件	87
5.5 Active Directoryからコンピューターを選択	87
5.5 ローカルネットワークのコンピューターを検査	90
5.5 コンピューターのリストのインポート	92
5.5 コンピューターを手動で追加	94
5.5 ESET Remote Deployment Tool - トラブルシューティング	96
5.6 エージェント保護	97
5.7 ESET Managementエージェント設定	98
5.7 ESET Managementエージェント接続間隔のポリシーの作成	100
5.7 新しいESET Managementサーバーに接続するためのESET PROTECTエージェントのポリシーを作成する	104
5.7 ポリシーを作成してESET Managementエージェントパスワード保護を有効にする	108
5.8 ESET Managementエージェント自動アップグレード	110
5.9 トラブルシューティング - エージェント接続	111
5.10 トラブルシューティング - エージェント展開	112

5.11 ESET Managementエージェント展開のシナリオ例	115
5.11 ドメインに参加していない対象へのESET Managementエージェントの展開シナリオ例	115
5.11 ドメインに参加している対象へのESET Managementエージェントの展開シナリオ例	117
6 ESET PROTECT メインメニュー	118
6.1 ダッシュボード	119
6.1 ドリルダウン	122
6.2 コンピューター	123
6.2 コンピューター詳細	125
6.2 コンピュータープレビュー	131
6.2 コンピューターを管理から削除する	131
6.2 グループ	133
6.2 グループアクション	133
6.2 グループ詳細	135
6.2 静的グループ	136
6.2 新しい静的グループを作成します	136
6.2 Active Directoryからのクライアントのインポート	138
6.2 静的グループのエクスポート	138
6.2 静的グループのインポート	139
6.2 動的グループ	140
6.2 新しい動的グループの作成	141
6.2 静的または動的グループの移動	143
6.2 グループへのクライアントタスクの割り当て	145
6.2 グループへのポリシーの割り当て	146
6.3 検出	147
6.3 検出の管理	149
6.3 検出プレビュー	151
6.3 除外の作成	152
6.3 除外と互換性のあるESETセキュリティ製品	154
6.3 ランサムウェアシールド	154
6.3 ESET Enterprise Inspector	155
6.4 レポート	156
6.4 新しいレポートテンプレートの作成	159
6.4 レポートの作成	162
6.4 レポートのスケジュール	162
6.4 古いアプリケーション	164
6.4 SysInspectorログビューア	164
6.4 ハードウェアインベントリ	165
6.4 監査ログレポート	167
6.5 タスク	167
6.5 クライアントタスク	170
6.5 クライアントタスクトリガー	171
6.5 グループまたはコンピューターへのクライアントタスクの割り当て	173
6.5 アンチセフトアクション	175
6.5 診断	177
6.5 メッセージの表示	179
6.5 ネットワークからのコンピューターの隔離を終了	180
6.5 ESETアプリケーション設定のエクスポート	181
6.5 コンピューターをネットワークから隔離する	182
6.5 モジュールアップデート	183
6.5 モジュールアップデートロールバック	184
6.5 オンデマンド検査	185

6.5 オペレーティングシステムアップデート	187
6.5 隔離管理	188
6.5 製品のアクティベーション	190
6.5 クローンされたエージェントのリセット	191
6.5 Rogue Detection Sensorデータベースリセット	192
6.5 コマンドの実行	193
6.5 SysInspectorスクリプトの実行	194
6.5 ESET PROTECT コンポーネントのアップグレード	195
6.5 EDTDにファイルを送信	197
6.5 サーバー検査	197
6.5 コンピューターをシャットダウンする	198
6.5 ソフトウェアインストール	199
6.5 Safeticaソフトウェア	203
6.5 ソフトウェアアンインストール	204
6.5 管理の停止(ESET Managementエージェントのアンインストール)	206
6.5 SysInspectorログ要求(Windowsのみ)	207
6.5 隔離ファイルのアップロード	208
6.5 サーバータスク	209
6.5 エージェント展開	211
6.5 接続していないコンピューターの削除	213
6.5 レポートの作成	214
6.5 コンピューター名の変更	216
6.5 静的グループの同期	218
6.5 同期モード - Active Directory/Open Directory/LDAP	218
6.5 同期モード - MS Windowsネットワーク	222
6.5 同期モード - VMware	223
6.5 静的グループ同期 - Linuxコンピュータ	225
6.5 ユーザー同期	226
6.5 タスクトリガータイプ	229
6.5 CRON式間隔	230
6.5 詳細設定 - 調整	233
6.5 調整例	237
6.5 タスク概要	239
6.5 進捗状況のインジケータ	241
6.5 ステータスアイコン	242
6.5 タスク詳細	242
6.6 インストーラー	244
6.7 ポリシー	247
6.7 ポリシーウィザード	249
6.7 フラグ	250
6.7 ポリシーの管理	251
6.7 ポリシーがクライアントに適用される方法	252
6.7 グループの順序	253
6.7 ポリシーの列挙	255
6.7 ポリシーのマージ	256
6.7 ポリシーの統合シナリオの例	258
6.7 ESET PROTECTからの製品の構成	262
6.7 グループへのポリシーの割り当て	262
6.7 クライアントへのポリシーの割り当て	264
6.7 上書きモードを使用する方法	265
6.8 通知	267

6.8 通知の管理	269
6.8 管理されたコンピューターまたはグループのイベント	270
6.8 サーバーステータス変更	271
6.8 動的グループ変更	272
6.8 配布	273
6.8 SNMPトラップサービスの構成方法	275
6.9 ステータス概要	276
6.10 詳細	278
6.10 ファイルを提出	279
6.10 除外	280
6.10 隔離	283
6.10 コンピューターユーザー	285
6.10 新しいユーザーの追加	286
6.10 ユーザーの編集	287
6.10 新しいユーザーグループの作成	290
6.10 動的グループテンプレート	291
6.10 新しい動的グループテンプレート	292
6.10 動的グループテンプレートのルール	293
6.10 演算子	293
6.10 ルールと論理接続	294
6.10 テンプレートルール評価	296
6.10 動的グループテンプレート - 例	298
6.10 動的グループ - セキュリティ製品がインストールされている	299
6.10 動的グループ - 特定のソフトウェアバージョンがインストールされている	299
6.10 動的グループ - 特定のバージョンのソフトウェアがインストールされていない	300
6.10 動的グループ - 特定のバージョンのソフトウェアがインストールされてなく、他のバージョンが存在する	301
6.10 動的グループ - コンピュータが特定のサブネットにある	301
6.10 動的グループ - インストールされ、アクティベーションされていないバージョンのサーバーセキュリティ製品	302
6.10 ESET PROTECTを自動化する方法	302
6.10 ライセンス管理	304
6.10 ESET Business AccountまたはESET MSP Administrator	308
6.10 ライセンスの追加 - ライセンスキー	309
6.10 オフラインアクティベーション	310
6.10 アクセス権	313
6.10 ユーザー	314
6.10 ネイティブユーザーの作成	318
6.10 ユーザーアクションとユーザー詳細	319
6.10 ユーザーパスワードの変更	321
6.10 マッピングされたユーザー	322
6.10 権限設定をユーザーに割り当てる	324
6.10 二要素認証	326
6.10 権限設定	327
6.10 権限設定の管理	329
6.10 権限の一覧	331
6.10 証明書	336
6.10 ピア証明書	337
6.10 新しい証明書の作成	339
6.10 ピア証明書のエクスポート	340
6.10 APN/ABM証明書	341
6.10 取り消しを表示	343
6.10 新しいESET PROTECTサーバー証明書の設定	344

6.10 ESET PROTECTのカスタム証明書	346
6.10 ESET PROTECTでのカスタム証明書の使用方法	359
6.10 期限切れの証明書 - 報告と置換	360
6.10 認証局	361
6.10 新しい認証機関の作成	362
6.10 公開鍵のエクスポート	364
6.10 公開鍵のインポート	365
6.10 サーバー設定	365
6.10 高度なセキュリティ	371
6.10 SMTPサーバー	372
6.10 検出されたコンピューターを自動的に組み合わせる	373
6.10 監査ログ	374
6.10 ログをSyslogにエクスポートする	375
6.10 Syslogサーバー	375
6.10 LEEF形式にエクスポートされたイベント	376
6.10 JSON形式にエクスポートされたイベント	377
7 モバイルデバイス管理	384
7.1 MDM設定	386
7.2 デバイス登録	387
7.2 Androidデバイス登録	390
7.2 デバイス所有者としてのAndroidデバイス登録	398
7.2 iOSデバイス登録	404
7.2 ABMを使用したiOSデバイス登録	408
7.2 電子メールで登録	412
7.2 リンクまたはQRコードで個別に登録	414
7.2 デバイス所有者としての個別の登録	416
7.2 iOS MDMのポリシーの作成 - Exchange ActiveSyncアカウント	418
7.2 MDCのポリシーを作成してiOS登録でAPN/ABMを有効にする	424
7.2 iOSおよびWi-Fi接続で制限を適用するポリシーの作成	429
7.2 MDM構成プロファイル	432
7.2 OSアップデート管理	433
7.3 MDMトラブルシューティング	434
8 マネージドサービスプロバイダー向けESET PROTECT	435
8.1 MSPユーザー向けESET PROTECTの新機能	438
8.2 MSPの展開処理	440
8.2 エージェントのローカル展開	441
8.2 エージェントのリモート展開	441
8.3 MSPライセンス	442
8.4 MSPアカウントのインポート	444
8.5 MSP顧客設定の開始	446
8.6 MSP顧客設定のスキップ	449
8.7 カスタムインストーラーの作成	450
8.8 MSPユーザー	453
8.8 カスタムMSPユーザーの作成	456
8.9 MSPオブジェクトのタグ付け	457
8.10 MSPステータス概要	458
8.11 会社の削除	460
9 アップデートESET PROTECT	462
10 FAQ	464
11 ESET PROTECTについて	468

12 エンドユーザーライセンス契約	468
13 プライバシーポリシー	474

ヘルプ

この管理者ガイドの目的は、ESET PROTECTの理解を深め、その使用方法を説明することです。

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。

i 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。




















































アイコン凡例

ESET PROTECT Web コンソールで使用されるアイコンと説明を示します。一部のアイコンは、アクション、項目タイプ、または現在の状態を示します。ほとんどのアイコンは3色のいずれかで表示され、要素を使用できるかどうかを示します。


















 既定のアイコン - 使用可能なアクション

 青のアイコン - マウスポインターを置いたときにハイライトされる要素

 灰色のアイコン - 使用できないアクション



ステータスアイコン	説明
  	詳細を表示 - クライアントデバイスの 詳細情報
  	新規追加 - 新しいデバイスを追加します 新しいタスク - 新しいタスクを追加します 新しい通知 - 新しい通知を追加します 新しい静的/動的グループ - 新しいグループを追加します
  	編集 - 作成したタスク、通知、レポートテンプレート、グループ、ポリシーを編集できます。
  	複製 - 選択した既存のポリシーに基づいて、新しいポリシーを作成できます。複製には新しい名前が必要です。
  	移動 - コンピューター、ポリシー、静的または動的グループ。 アクセス グループ - 項目を別の静的グループに移動します。
  	削除 - 選択したクライアント、グループなどを完全に削除します。
  	複数の項目名の変更 - 複数の項目を選択する場合は、リストで1つずつ名前を変更するか Regex 検索を使用して、同時に複数の項目を置換できます。
  	検査 - このオプションを使用すると、検出を報告したクライアントで、 オンデマンド検査 が実行されます。
  	アップデート>モジュールのアップデート - このオプションを使用すると、 モジュールアップデート タスク(アップデートを手動でトリガー)が実行されます。 アップデート>ESET製品のアップデート - 選択したデバイスにインストールされているESET製品をアップデートします。 アップデート>オペレーティングシステムのアップデート - 選択したデバイスのオペレーティングシステムを更新します。
  	監査ログ - 選択した項目の 監査ログ を表示します。
  	モバイルデバイスのタスクを実行します。
  	再登録 - 電子メールでモバイルデバイスを追加 ウィンドウが開きます。
  	ロック解除 - デバイスのロックが解除されます。
  	ロック - 不審なアクティビティが検出されるか、デバイスが紛失に設定されると、デバイスがロックされます。
  	検索 - モバイルデバイスのGPS座標を要求する場合。
  	警報/紛失モード - リモートで大音量の警報音をトリガーします。デバイスがミュートに設定されていても、警報音が作動します。
  	初期設定リセット - デバイ스에保存されているすべてのデータが完全に消去されます。

ステータスアイコン	説明
	再起動 - コンピューターを選択し、 再起動 をクリックすると、デバイスが再起動します。 復元 - 隔離された ファイルを元の場所に復元します。
	シャットダウン - コンピューターを選択し、 再起動>シャットダウン をクリックすると、デバイスがシャットダウンします。 製品のアクティベーション解除
	タスクの実行 - タスクを選択し、このタスクのトリガーと 調整 (任意)を設定します。このタスクは、タスク設定に従って、キューに追加されます。このオプションは、使用可能なタスクのリストから選択した既存の タスク をただちにトリガーします。
	最後に使用したタスク - 最後に使用したタスクを表示します。 タスクをクリックすると、もう一度実行します。
	ユーザーの割り当て - ユーザーをデバイスに割り当てます。 コンピューターユーザー でユーザーを管理できます。
	ポリシーの管理 - ポリシー を、グループだけではなく、直接クライアント(複数のクライアント)にも割り当てることができます。このオプションを選択すると、選択したクライアントにポリシーを割り当てます。
	ウェイクアップコールの送信 - ESET PROTECTサーバーは、 EPNS 経由でクライアントコンピューターでESET Managementエージェントとの即時複製を実行します。これはESET ManagementエージェントがESET PROTECTサーバーに接続するときに、定期間隔を待機しない場合に便利です。例えば、クライアントでただちに クライアントタスク を実行する場合や、 ポリシー をただちに適用する場合に便利です。
	エージェントの展開 - このオプションを使用すると、 新しいサーバータスク を作成できます。
	ネットワークから隔離する
	ネットワーク隔離を終了
	接続 - リモートデスクトッププロトコル経由で対象デバイスに接続できる .rdp ファイルを生成してダウンロードします。
	ミュート - コンピュータを選択し、 [ミュート] をクリックすると、このクライアントのエージェントはESET PROTECTへの報告を停止します。情報の集約だけが行われます。ミュートアイコンは、 [ミュート] 列のコンピューター名の横に表示されます。 [ミュート解除] をクリックしてミュートを無効にしたら、ミュートされたコンピューターがもう一度報告しESET PROTECTとクライアント間の通信が復元されます。
	無効にする - 設定または選択を無効にするか、削除します。
	割り当て - ポリシーをクライアントまたはグループに割り当てます。
	インポート - インポートする レポート / ポリシー / 公開鍵 を選択します。
	エクスポート - エクスポートする レポート / ポリシー / ピア証明書 を選択します。
	タグ : タグ を編集します(割り当て、割り当て解除、作成、削除)。
	静的グループ
	動的グループ
	ポリシーフラグ を適用しません
	ポリシーフラグ を適用します
	ポリシーフラグ を強制します
	トリガー - 選択したクライアントタスクの トリガー のリストを表示します。
	デスクトップ

ステータス アイコン	説明
	モバイル
	サーバー
	ファイルサーバー
	メールサーバー
	ゲートウェイサーバー
	コラボレーションサーバー
	ESET Management エージェント
	モバイルデバイスコネクタ
	Rogue Detection Sensor
	ESET PROTECT サーバー
	Enterprise Inspector エージェント
	Enterprise Inspector サーバー
	ウイルス対策検出タイプ。 検出 ですべての検出タイプを参照してください。
	暗号化を有効にする - 選択したコンピュータで ESET Full Disk Encryption を有効にします。
	コンピュータの ESET Full Disk Encryption が有効になっています。
	EDTD を有効にする - ESET Dynamic Threat Defense を アクティベーションして有効にします 


オフラインヘルプ

ESET PROTECT のオフラインヘルプは既定でインストールされません。オフライン(インターネットに断続的または常時接続できない場合)でも使用できる ESET PROTECT ヘルプが必要な場合は、次の手順を実行して、オフラインヘルプを追加します。


i 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  ESMC または古いバージョンの ESET PROTECT 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 9.0 用に再作成します。これにより  ESET PROTECT のバージョンに一致する最新のオフラインヘルプがあることが保証されます。

言語コードをクリックし、任意の言語で ESET PROTECT のオフラインヘルプをダウンロードします。複数の言語でオフラインヘルプをインストールすることもできます。

[Windows のオフラインヘルプセットアップ手順](#)

1. 言語コードをクリックし、任意の言語で ESET PROTECT のオフラインヘルプをダウンロードして、.zip ファイルをダウンロードします。
2. .zip ファイルを保存します(USB フラッシュドライブなど)。
3. 次の場所で ESET PROTECT Web コンソールを実行するコンピュータで新しいフォルダーの *help* を作成します。%ProgramFiles%\Apache Software Foundation\[Tomcat フォルダ - 4. .zip ファイルを *help* フォルダーにコピーします。

5. `.zip` ファイルの内容を展開します。たとえば、`en-US.zip`を同じ名前のフォルダーに展開します。この場合は**en-US**です。フォルダー構造は次のようになります。`%ProgramFiles%\Apache Software Foundation\[Tomcat folder]\webapps\era\webconsole\help\en-US`

ESET PROTECT Webコンソールを開き、言語を選択してログインできます。右上にある  **ヘルプ** をクリックし、**現在のトピック - ヘルプ** をクリックするたびに ESET PROTECT オフラインヘルプが開きます。


 上記の手順に従い、必要に応じて、複数の言語でオフラインヘルプを追加できます。



ESET PROTECT Webコンソールにアクセスするコンピューターまたはモバイルデバイスがインターネットに接続していない場合は、ESET PROTECT Webコンソールの設定を変更し、オンラインヘルプではなく、**強制的にESET PROTECTオフラインヘルプ**が既定で開くようにする必要があります。このためには、表の下の手順に従います。

Linuxのオフラインヘルプセットアップ手順

1. 言語コードをクリックし、任意の言語でESET PROTECTのオフラインヘルプをダウンロードして、`.tar`ファイルをダウンロードします。
2. `.tar`ファイルを保存します(USBフラッシュドライブなど)。
3. ターミナルを開き、`/usr/share/tomcat/webapps/era/webconsole`に移動します。
4. `mkdir help`コマンドを実行して、新しいフォルダーの**help**を作成します。
5. `help`フォルダーで、`.tar`ファイルと同じ名前の新しい言語フォルダーを作成します。例：英語の場合は`mkdir en-US`コマンドを実行します。
6. `.tar`ファイルを言語フォルダー(例：`/usr/share/tomcat/webapps/era/webconsole/help/en-US`)にコピーして展開します。たとえば、`tar -xvf en-US.tar`コマンドを実行します。

ESET PROTECT Webコンソールを開き、言語を選択してログインできます。右上にある  **ヘルプ** をクリックし、**現在のトピック - ヘルプ** をクリックするたびに ESET PROTECT オフラインヘルプが開きます。

前のバージョンからの移行(ESMC 7.5など)の後にオフラインヘルプを更新するには、既存のヘルプフォルダーを削除(`...webapps\era\webconsole\help`)し、上記の手順3で同じ場所に新規作成します。フォルダーを置換した後、標準とおり続行します。

 上記の手順に従い、必要に応じて、複数の言語でオフラインヘルプを追加できます。




ESET PROTECT Webコンソールにアクセスするコンピューターまたはモバイルデバイスがインターネットに接続していない場合は、ESET PROTECT Webコンソールの設定を変更し、オンラインヘルプではなく、**強制的にESET PROTECTオフラインヘルプ**が既定で開くようにする必要があります。このためには、表の下の手順に従います。

サポートされている言語	オフラインHTMLヘルプ .zip	オフラインHTMLヘルプ .tar
英語	en-US.zip	en-US.tar
アラビア語	ar-EG.zip	ar-EG.tar
簡体中国語	zh-CN.zip	zh-CN.tar
繁体中国語	zh-TW.zip	zh-TW.tar

サポートされている言語	オフラインHTMLヘルプ .zip	オフラインHTMLヘルプ .tar
クロアチア語	hr-HR.zip	hr-HR.tar
チェコ語	cs-CZ.zip	cs-CZ.tar
フランス語	fr-FR.zip	fr-FR.tar
フランス語(カナダ)	fr-CA.zip	fr-CA.tar
ドイツ語	de-DE.zip	de-DE.tar
ギリシャ語	el-GR.zip	el-GR.tar
イタリア語	it-IT.zip	it-IT.tar
日本語	ja-JP.zip	ja-JP.tar
韓国語	ko-KR.zip	ko-KR.tar
ポーランド語	pl-PL.zip	pl-PL.tar
ポルトガル語(ブラジル)	pt-BR.zip	pt-BR.tar
ロシア語	ru-RU.zip	ru-RU.tar
スペイン語	es-ES.zip	es-ES.tar
スペイン語(ラテンアメリカ)	es-CL.zip	es-CL.tar
スロバキア語	sk-SK.zip	sk-SK.tar
トルコ語	tr-TR.zip	tr-TR.tar
ウクライナ語	uk-UA.zip	uk-UA.tar


Windowsでオフラインヘルプ施行

1. テキストエディターでC:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.propertiesを開きます。
2. help_show_online=true行を見つけ、この設定値をfalseに変更して保存します。
3. コマンドラインからサービス内のTomcatサービスを再起動します。

右上にある  ヘルプをクリックし、現在のトピック - ヘルプをクリックするたびにESET PROTECTオフラインヘルプが開きます。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。

Linuxでオフラインヘルプ施行

1. /usr/share/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties設定ファイルをテキストエディター(nanoなど)で開きます
2. help_show_online=true行を見つけ、この設定値をfalseに変更して保存します。
3. tomcatサービスを停止し、tomcat stopコマンドを実行します。
4. tomcatサービスを開始し、tomcat startコマンドを実行します。

右上にある  ヘルプをクリックし、現在のトピック - ヘルプをクリックするたびにESET PROTECTオフ

ラインヘルプが開きます。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。

ESET PROTECTの概要

ESET PROTECT バージョン9.0をご利用いただき、誠にありがとうございます。ESET PROTECTは、ネットワーク環境のワークステーション、サーバー、およびモバイルデバイス上のESET製品を1か所から管理できます。ESET PROTECT Webコンソールを使用すると、ESETソリューションを展開し、タスクを管理し、セキュリティポリシーを施行し、システムステータスを監視して、リモートコンピューターの問題または検出にすばやく対応します。[ESET PROTECTアーキテクチャおよびインフラストラクチャ要素の概要](#)、[ESET PROTECT Webコンソールの基本操作](#)、および[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](#)を参照してください。

ESET PROTECTには次のコンポーネントがあります。

- [ESET PROTECTサーバー](#) - ESET PROTECTサーバーはWindowsとLinuxにインストールでき、仮想アプリケーションス作为一项として提供しています。エージェントとの通信を処理し、アプリケーションデータを収集して、データベースに保存します。
- [ESET PROTECT Webコンソール](#) - ESET PROTECT Webコンソールは、環境内のクライアントコンピューターを管理できる主要なインターフェイスです。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。ESET PROTECTサーバーをインストールすると、Webブラウザを使用してWebコンソールにアクセスできます。インターネットからWebサーバーにアクセスする場合は、インターネットに接続しているすべての場所とデバイスからESET PROTECTを使用できます。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。
- [ESET Managementエージェント](#) - ESET ManagementエージェントはESET PROTECTクライアントコンピューターにESET PROTECTエージェントをインストールし、コンピューターとサーバー間の通信を確立する必要があります。これはクライアントコンピューターにあり、複数のセキュリティシナリオを保存できるためESET Managementエージェントを使用すると、新しい検出への対応時間が大幅に短くなります。ESET PROTECT Webコンソールを使用すると、Active Directory経由または[ESET Rogue Detection Sensor](#)によって特定された非管理コンピューターに[ESET Managementエージェントを展開](#)できます。必要に応じて、クライアントコンピューターに[手動でESET Managementエージェントをインストール](#)することもできます。
- [Rogue Detection Sensor](#) - ESET PROTECT Rogue Detection (RD) Sensorは、ネットワークに存在する管理されていないコンピューターを検出し、その情報をESET PROTECTサーバーに送信します。これによって、簡単に新しいクライアントコンピューターを安全なネットワークに追加できます。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。
- [HTTP Apache Proxy](#) - ESET PROTECT と組み合わせて使用できるサービスで、
 - クライアントコンピューターにアップデートを配布し、ESET Managementエージェントにインストールパッケージを配布します。
 - ESET Managementエージェントからサーバーへ通信を転送 ESET PROTECT します。
- [モバイルデバイスコネクタ](#) - ESET PROTECTは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)を管理し、ESET Endpoint Security for Androidを管理できます。

- [ESET PROTECT仮想アプライアンス](#) – 仮想環境でESET PROTECT を実行する場合は、VAを使用できます。
- [ミラーツール](#) – オフラインモジュールアップデートが必要です。クライアントコンピューターがインターネットに接続しない場合、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。
- [ESET Remote Deployment Tool](#) – このツールではESET PROTECT Webコンソールで作成されたオールインワンパッケージを展開できます。ネットワーク上のコンピューターにESET ManagementエージェントとESET製品を配布するための便利な方法です。
- [ESET Business Account](#) - ESETビジネス製品の新しいライセンスポータルでは、ライセンスを管理できます。製品のアクティベート手順については、このマニュアルの[ESET Business Account](#)セクションを参照するかESET Business Accountの使用法の詳細についてはESET Business Account[ユーザーガイド](#)を参照してください。「[レガシーライセンス資格情報の変換](#)」セクションを参照してください。
- [ESET Enterprise Inspector](#) – 包括的なエンドポイント検出および応答システムであり、インシデント検出、インシデント管理と応答、データ収集、危険検出の指標、特異性の検出、動作検出、ポリシー違反などの機能があります。

ESET PROTECTの新機能

詳細からワンクリック

コンピューター詳細や検出詳細の確認が、かつてないほど簡単かつすばやく行えるようになりました。コンピューターセクションでコンピューター名をクリックするだけで、詳細情報のサイドパネルが表示されます。 [詳細を見る](#) [検出]セクションで検出タイプをクリックした場合にも同じようにサイドパネルが表示されています。 [詳細を見る](#)

新しい概要ダッシュボード EDTD

新しいダッシュボードが導入されESET Dynamic Threat Defenseに関連する有用な情報と統計を確認できます。 [詳細を見る](#)

自動製品アップデート

操作をより簡単にするためにESETは、11月にリリースされる次のESET Endpoint Security/Antivirus v9で、セキュリティ製品(当面はWindowsエンドポイント製品)の自動アップデートとすぐに使えるイネーブルメントを導入します。自動アップデートを使用すると、簡単にネットワークのESET製品を常に最新の状態に維持することができます。 [詳細を見る](#)

ブルートフォース攻撃保護の管理

Windowsエンドポイント製品v9では、新しいセキュリティ機能が導入され、資格情報を推測されてリモート接続を確立されてしまう危険性からデバイスが保護されます。コンソールから直接ポリシーを使用してこの機能を簡単に設定できます。ブロックされるべきではない項目がブロックされたときには検出セクションから除外を作成できます。

ESET Full Disk Encryption 改善点

ESET Full Disk Encryptionモジュールのアップデートを簡単に自動化することで、貴重な時間を節約できます。また、定義済みのパスワードとキーボードマップを使用してインストーラーを展開し、暗号化を開始するオプションも追加されました。さらに重要な点として、ユーザーインターフェースが改善され、現在インストールされているESET Full Disk Encryptionモジュールが表示されるようになりました。

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。

サポート対象のWebブラウザとESETセキュリティ製品および言語

ESET PROTECT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](#)と[Linux](#)と[macOS](#)

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

Webブラウザ
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ブラウザを常に最新の状態にすることをお勧めします。
- Internet Explorerを使用するとESET PROTECT WebコンソールでサポートされていないWebブラウザを使用していることが通知されます。

ESET PROTECT 9.0で管理可能な最新バージョンのESET製品

製品	製品のバージョン
ESET Endpoint Security for Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus for Windows	7.x, 8.x, 9.x
ESET Endpoint Security for macOS	6.8+
ESET Endpoint Antivirus for macOS	6.8+
ESET Endpoint Security for Android	2.x
ESET Server Security for Windows	8.x
ESET File Security for Microsoft Windows Server	7.x

製品	製品のバージョン
ESET File Security for Microsoft Azure	7.x
ESET Mail Security for Microsoft Exchange Server	7.x, 8.x, 9.x
ESET Security for Microsoft SharePoint Server	7.x, 8.x, 9.x
ESET Mail Security for IBM Domino Server	7.x, 8.x, 9.x
ESET File Security for Linux	7.x, 8.x
ESET Server Security for Linux	8.1+
ESET Endpoint Antivirus for Linux	7.x, 8.x, 9.x
ESET Dynamic Threat Defense	
ESET Enterprise Inspector Agent	1.6
ESET Full Disk Encryption for Windows	
ESET Full Disk Encryption for macOS	

ESET PROTECT9.0 で管理可能なその他のバージョンのESET製品:

製品	製品のバージョン
ESET Endpoint Security for Windows	6.5+
ESET Endpoint Antivirus for Windows	6.5+
ESET File Security for Microsoft Windows Server	6.5
ESET File Security for Microsoft Azure	6.5
ESET Mail Security for Microsoft Exchange Server	6.5
ESET Mail Security for IBM Lotus Domino	6.5
ESET Security for Microsoft SharePoint Server	6.5
ESET Mail Security for Linux/FreeBSD*	4.5.x
ESET File Security for Linux/FreeBSD*	4.5.x
ESET Gateway Security for Linux/FreeBSD*	4.5.x

* ESET Management エージェント9を使用してこの製品を管理することはできません。製品を管理するにはESET Management エージェント8.1以前を使用します。

i 次の表よりも前のESETセキュリティ製品のバージョンは、ESET PROTECT9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。

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製品	利用可能なバージョン
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 Dynamic Threat Defense	
ESET Enterprise Inspector (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
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。

自動製品アップデート

ESET PROTECTバージョン9.0には管理されたコンピューターでESETセキュリティ製品が最新バージョンに更新するための新機能が導入されています。

自動製品のアップデートは、新規ESET PROTECT9.0インストールで自動的に有効にされます。

- 自動アップデート機能を使用するには、有効なESETセキュリティ製品が必要です。[自動アップデートをサポートするESETビジネス製品](#)の一覧を参照してください。
- ポリシーを使用して[自動アップデートを構成](#)できます。
- 最初の自動アップデートは、最初にリリースされた9.xビルドの将来のバージョン(例: 9.1、またはxxxxが最初の9.xビルドよりも上位の場合は9.0.xxxx.y)に実行されます。アップデートの安定性を保証するために、新しいESETセキュリティ製品バージョンのグローバルリリース後に、遅れてから自動製品のアップデートが配布されます。その間に、Webコンソールで、ESETセキュリティ製品が最新ではないと報告される場合があります。
- 他のESETセキュリティ製品では自動アップデートがサポートされていませんESETは今後この機能を追加する予定です。

以下のオプションのいずれかを実行して、ネットワークのESETセキュリティ製品を自動アップデートをサポートするバージョンにアップグレードします。

• ダッシュボード>ステータス概要>製品バージョンステータスで[ワンクリックアクション](#)を使用して、棒グラフを選択し、インストールされているESET製品のアップデートを選択します。

i • コンピューターですべての静的グループの横の歯車アイコンをクリックして、タスク>アップデート>ESET製品のアップデートを選択します。

• [ソフトウェアインストールクライアントタスク](#)を使用します。

• ESET PROTECT 8.xまたはESMC 7.xからアップグレードした場合は、自動製品のアップデートウィンドウで[ワンクリックアップグレード](#)を使用できます。

ESETセキュリティ製品を最新バージョンにアップグレードするには、次の2つの方法があります。

- [ソフトウェアインストールクライアントタスク](#)
- 自動アップデート機能

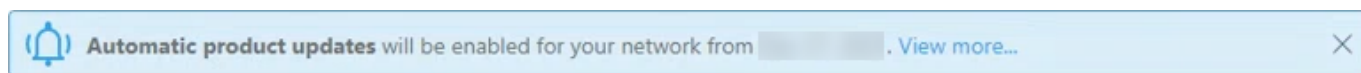
ソフトウェアインストールクライアントタスクと自動アップデート機能の違い:

	アップグレード処理	アップグレード後に再起動	今後のアップグレード
ソフトウェアインストールクライアントタスク	アップグレード処理にはESETセキュリティ製品の再インストールが含まれます。	ESETセキュリティ製品のアップグレードでは、セキュリティの理由からコンピューターを即時に再起動する必要があります(アップグレードされたESETセキュリティ製品の完全な機能を保証するため)。	手動-管理者は、ソフトウェアインストールクライアントタスクを実行して、今後の各アップグレードを開始する必要があります。 上記の使用可能なオプション を参照してください。

	アップグレード処理	アップグレード後に再起動	今後のアップグレード
自動アップデート	アップグレード処理にはESETセキュリティ製品の再インストールは含まれません。	ESETセキュリティ製品のアップグレードではコンピュータの再起動が必要ですが、ただちに再起動しなくてもかまいません。アップグレードは、次のコンピュータの再起動後に実行されますESET PROTECT管理者は、選択したコンピュータの再起動チェックボックスを使用して、 コンピュータクライアントのシャットダウンタスク を使用して、コンピュータのアップグレードを施行し、Webコンソールからリモートで再起動できます。	自動 - 新しいバージョンがリリースされたときに、 サポートされているESETセキュリティ製品の自動アップデート を実行します(安定性の理由によりアップデートは遅れて実行されます)。

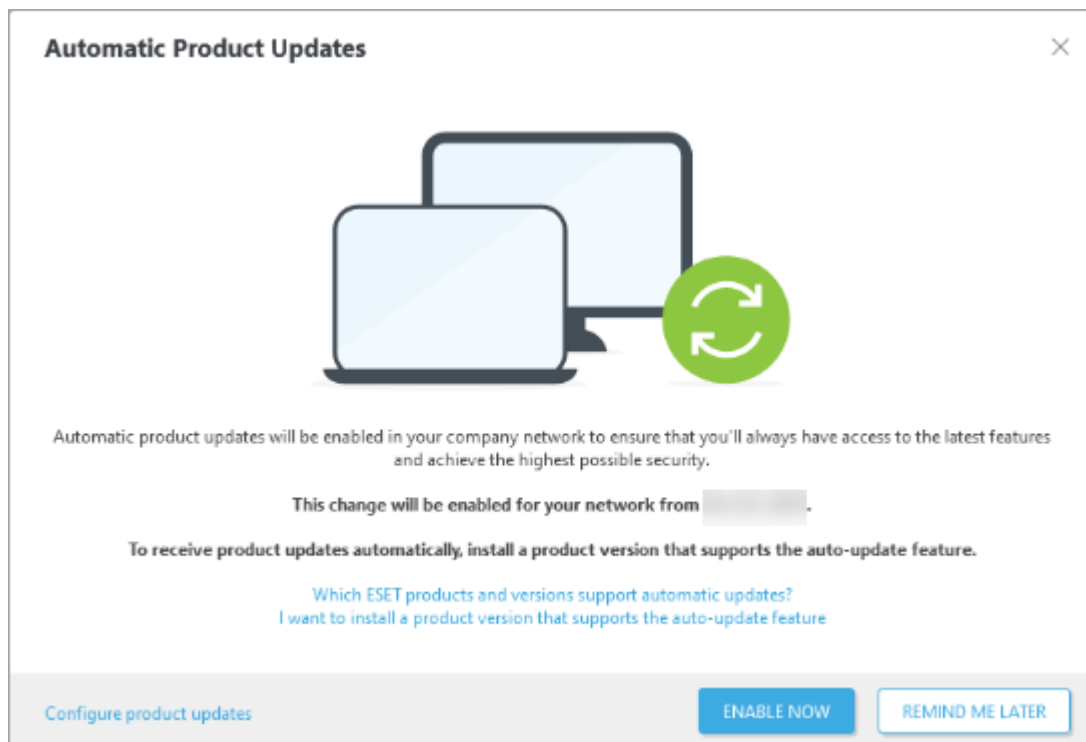
アップグレードESET PROTECT8.x または ESMC 7.x

ESET PROTECT 8.xまたはESMC 7.xからESET PROTECT 9.0にアップグレードした場合Webコンソールには自動製品のアップデート通知が表示されます。



自動製品のアップデートは、すべての管理されたコンピュータ(すべての[静的グループ](#))で、通知が表示された日から60日間自動的に有効にされます。[自動アップデートを無効にする](#)と、通知が表示されなくなります。

詳細をクリックすると、自動製品のアップデートを設定し、**自動製品のアップデート**ウィンドウが表示されます。



すべての管理されたコンピュータ(すべての静的グループ)でただちに自動アップデートを有効にするには、**今すぐ有効にする**をクリックします。

製品のアップデートの設定をクリックして、[自動アップデートポリシーを設定](#)します。

自動製品のアップデートウィンドウで自動アップデート機能をサポートする製品バージョンをインストールをクリックします。ESET PROTECTでワンクリックアップグレードオプション([ソフトウェアインストールクライアントタスク](#))が表示されます。

自動製品のアップデートの設定

[互換性があるESETセキュリティ製品](#)とすべての静的グループを既定の対象としてカバーする自動アップデート機能ポリシーを使用して、自動アップデートを設定できます。

ビルトインの自動アップデートポリシーターゲットを変更します。

ESET PROTECT Webコンソールで、ポリシーをクリックして、ビルトインポリシーを展開し、ポリシーをクリックします。割り当ての変更をクリックして、ターゲットを調整し、完了をクリックします。

自動アップデートを設定する:

新しい自動アップデートポリシーを作成して、自動アップデートを設定します。

1. ESET PROTECT Webコンソールで、ポリシー>新しいポリシー>設定をクリックします。
2. ドロップダウンメニューから自動アップデートを選択し、ポリシー設定を構成します。
 - 自動アップデート - 既定では自動アップデートが有効です。



自動アップデートを無効にするには、自動アップデートスライダーバーをオフにします。[自動アップデートのオプトアウト](#)も参照してください。

- アップデートを停止 - 自動アップデートを停止するESETセキュリティ製品バージョンを任意で設定できます。

o リポジトリから選択をクリックし、バージョンを選択します。

o バージョンを入力 - ワイルドカードとして*を使用できます。例: 9.* / 9.0.* / 9.0.2028.*




たとえば、9.0.*と入力する場合は、マイナーバージョン9.0からのすべてのホットフィックスがインストールされます。



この設定は、設定されたバージョンまたは自動アップデート設定状態に関係なく、自動的にインストールされた[セキュリティと安定性のアップデート](#)には適用されません。

3. 割り当てをクリックして、ポリシーターゲット(グループまたは個別のコンピューター)を選択します。

 ビルトインの自動アップデートポリシーによって自分で作成した自動アップデートポリシー設定が上書きされないことを確認してください。[クライアントのポリシーの適用](#)の詳細をお読みください。

4. [完了]をクリックします。

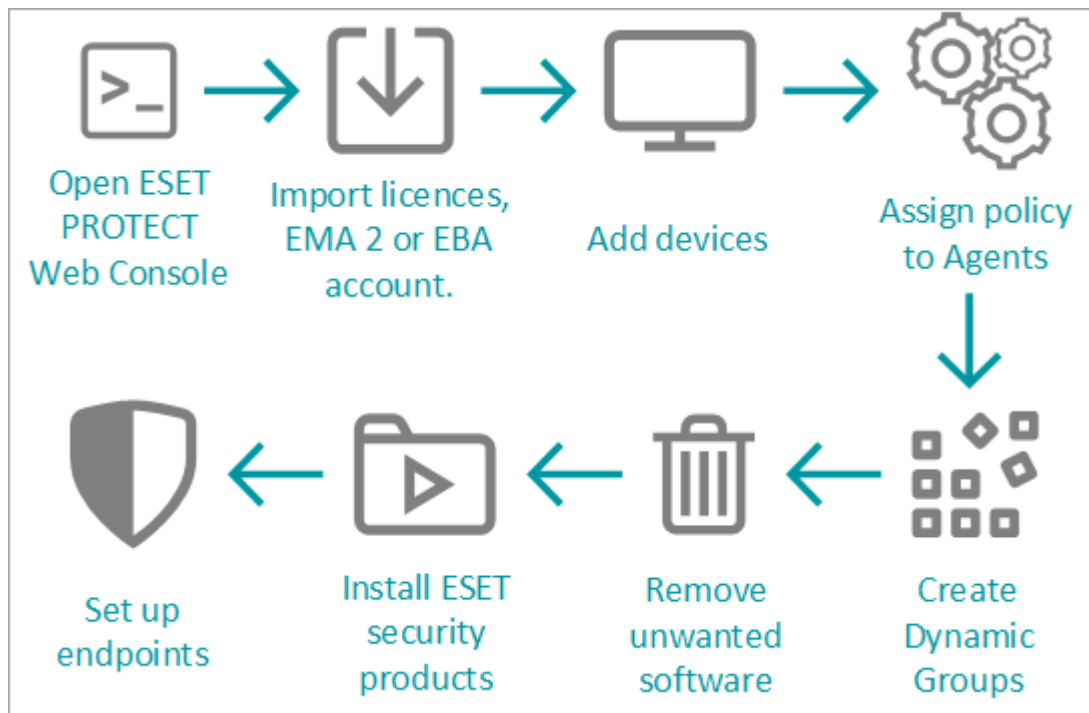
ESET PROTECTの基本操作

ESET PROTECTは、ESET PROTECT Web コンソールから設定および管理できます。正常に[ESET PROTECT](#)をインストールまたは[ESET PROTECT VAを展開](#)した後に、ESET PROTECT Webコンソールを使用してESET PROTECTサーバーに接続できます。

ESET PROTECTをインストールしたら、構成の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. ブラウザーで[ESET PROTECT Webコンソールを開き](#)、ログインします。
2. [ライセンス](#)をESET PROTECTに追加します。
3. [ネットワークのクライアントコンピューター](#)、サーバー、モバイルデバイスをESET PROTECT構造に追加します。
4. [ビルトインポリシーアプリケーションレポートを割り当て](#) - すべてのインストールされているアプリケーションをすべてのコンピューターに報告します。
5. ESETホーム製品がインストールされているコンピューターで、[動的グループを作成](#)します。
6. [ソフトウェアアンインストール](#)タスクを使用して、サードパーティのウイルス対策アプリケーションを削除します。
7. [ソフトウェアインストール](#)タスクを使用してESETセキュリティ製品をインストールします([オールインワンインストーラー](#)を使用してエージェントをインストールしていない場合)。
8. 推奨設定のポリシーを、ESETセキュリティ製品がインストールされている各コンピューターに[割り当て](#)ます。たとえばESET EndpointがインストールされたWindowsコンピューターの場合は、ビルトインポリシーウイルス対策 - 最大限のセキュリティ - 推奨を割り当てます。[ESET PROTECTからエンドポイント製品を管理する方法](#)を参照してください。



追加の推奨手順

- [ESET PROTECT Web コンソールに慣れる](#) ことをお勧めします。これは ESET セキュリティ製品を管理するために使用するインターフェイスであるためです。
- インストール中には、既定の管理者アカウントを作成します。管理者アカウントの資格情報を安全な場所に保存し、[新しいアカウント](#)を作成して、クライアントを管理し、[権限](#)を設定することをお勧めします。



標準ユーザーアカウントとして、既定の ESET PROTECT **管理者** アカウントを使用することは推奨されません。このアカウントは、通常のユーザーアカウントに問題が発生した場合や、ロックアウトされた場合にバックアップとして使用されます。このような問題を修正するために管理者アカウントでログインします。

- [通知](#)と[レポート](#)を使用し、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、特定のイベントが発生したことを通知したり、レポートの表示やダウンロードができます。
- [データベースを定期的にバックアップ](#)し、データ損失を防止してください。
- [サーバー認証局](#)と[ピア証明書](#)のエクスポートをお勧めします。ESET PROTECT サーバーを再インストールする必要がある場合は、元の ESET PROTECT サーバーからエクスポートした CA とピア証明書を使用できます。ESET Management エージェントをクライアントコンピューターに再インストールする必要はありません。

ESET PROTECT Web コンソールを開く

ESET PROTECT Web コンソールは ESET PROTECT サーバーと通信するメインインターフェイスです。すべての ESET セキュリティソリューションを管理できる一元的な場所であるコントロールパネルと考えることができます。それは、インターネットに接続しているあらゆる場所とデバイスから [ブラウザ](#) を使用してアクセスできる Web ベースのインターフェイスです。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 PROTECT Webコンソールを開くには複数の方法があります。

- ローカルサーバー([Web コンソール](#)をホストするコンピューター)で、以下のURLをWebブラウザに入力します。

<https://localhost/era/>

- 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。

<https://yourservername/era/>

yourservername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てください。

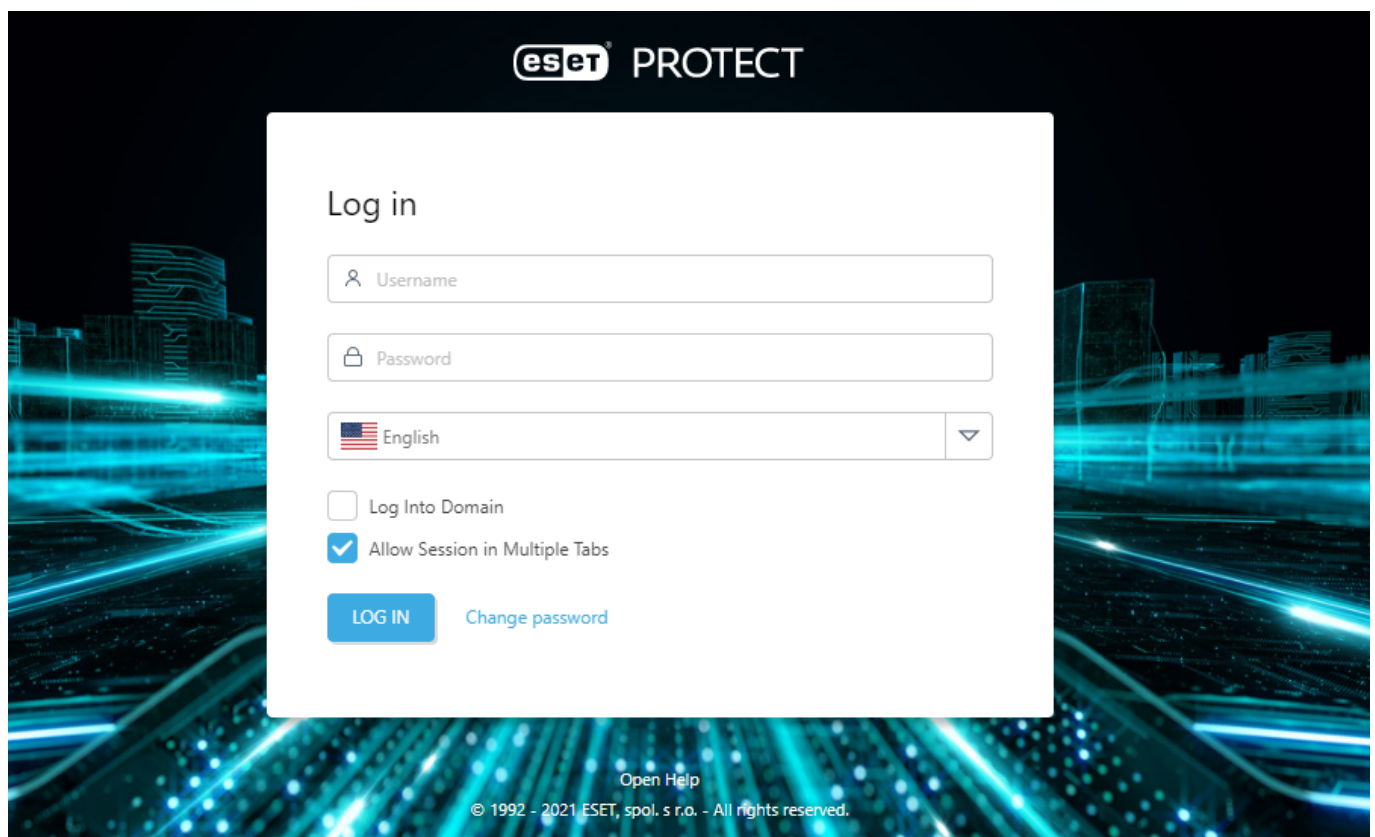
- ESET PROTECT仮想アプライアンスにログインするには、以下のURLを使用します。

[https://\[IPアドレス\]/](https://[IPアドレス]/)

[IPアドレス]の部分は、ESET PROTECT VMのIPアドレスを指定します。

- ローカルサーバ(Webコンソールをホストするコンピューター)で、[スタート]>[すべてのプログラム]>[ESET]>ESET PROTECT>[ESET PROTECT Web コンソール]をクリックします。既定のWebブラウザでログイン画面が開きます。これはESET PROTECT仮想アプライアンスには適用されません。

Webサーバ(ESET PROTECT Webコンソールを実行している)が起動している場合、次のログイン画面が表示されます。

The image shows the ESET PROTECT Web Console login interface. At the top, the 'eset PROTECT' logo is displayed. Below it, the title 'Log in' is centered. The login form contains several fields: a 'Username' field with a user icon, a 'Password' field with a lock icon, and a language dropdown menu currently set to 'English' with a US flag icon. Below these fields are two checkboxes: 'Log Into Domain' (unchecked) and 'Allow Session in Multiple Tabs' (checked). At the bottom of the form are two buttons: a blue 'LOG IN' button and a 'Change password' link. The background of the page features a dark, abstract design with glowing blue lines and dots, suggesting a digital or network environment. At the very bottom, there is a small 'Open Help' link and a copyright notice: '© 1992 - 2021 ESET, spol. s r.o. - All rights reserved.'







これが初めてのログインの場合、[インストール処理](#)中に入力した認証情報を入力してください。既定のWebコンソールユーザーは**Administrator**です。この画面の詳細については、[Webコンソールログイン画面](#)を参照してください。

i ログインできないか、ログインの試行でエラーメッセージが発生する場合は、[Webコンソールの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。

ESET PROTECT Webコンソール



ESET PROTECT WebコンソールはESET PROTECTサーバーと通信するメインインターフェイスです。すべてのESETセキュリティソリューションを管理できる一元的な場所であるコントロールパネルと考えることができます。それは、インターネットに接続しているあらゆる場所とデバイスからWebブラウザ([サポート対象のWebブラウザ](#)を参照)を使用してアクセスできるWebベースのインターフェイスです。初めてWebコンソールにログインするときには、[スタートアップウィザード](#)が表示されます。

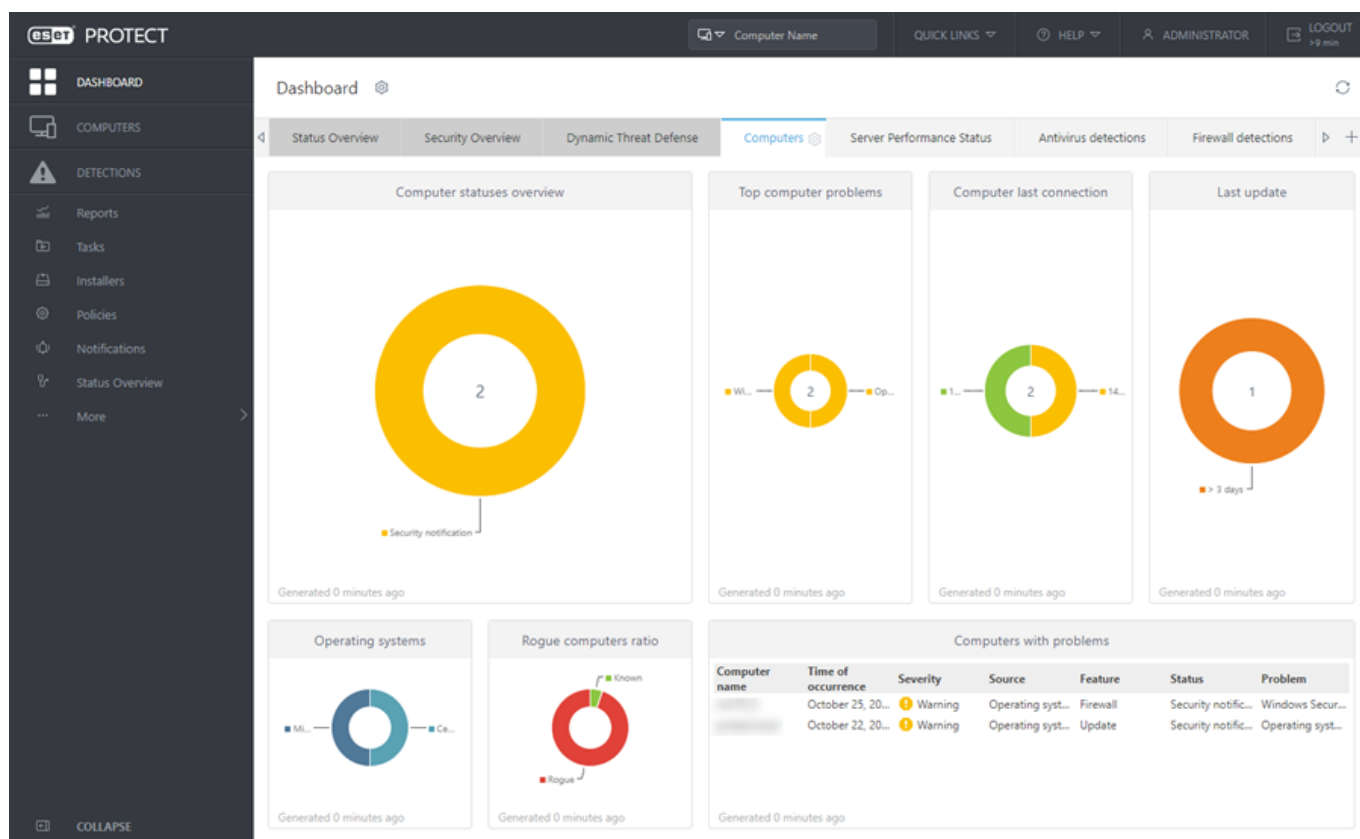
ESET PROTECT Webコンソールの標準レイアウト:

- 現在のユーザーは常に右上に表示されます。ここでは、セッションのタイムアウトがカウントダウンされます。**[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すると、ユーザーはもう一度ログインする必要があります。[ユーザー設定](#)を変更するにはESET PROTECT Webコンソールの右上端のユーザー名をクリックします。
- ウィザードを使用している場合を除き、左側には常に[メインメニュー](#)があります。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。
- 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、**現在のトピック - 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。
- ESET PROTECT Webコンソールの上部では、**簡易検索**ツールを使用できます。アイコンをクリックし、検索対象を選択します。
 - **コンピューター名**  **説明**、および**IPアドレス-クライアント名**  **コンピューター説明**  **IPv4/IPv6アドレス**、または**グループ名**を入力して、**Enter**を押します。結果が表示される[コンピューターセクション](#)にリダイレクトされます。
 - **検出名** - 結果が表示される[検出](#)セクションにリダイレクトされます。
 - **ユーザー名** - インポートされたADユーザーを検索できます。結果は[コンピューターユーザー](#)セクションに表示されます。
- クイックリンクボタンをクリックし、メニューを表示します。

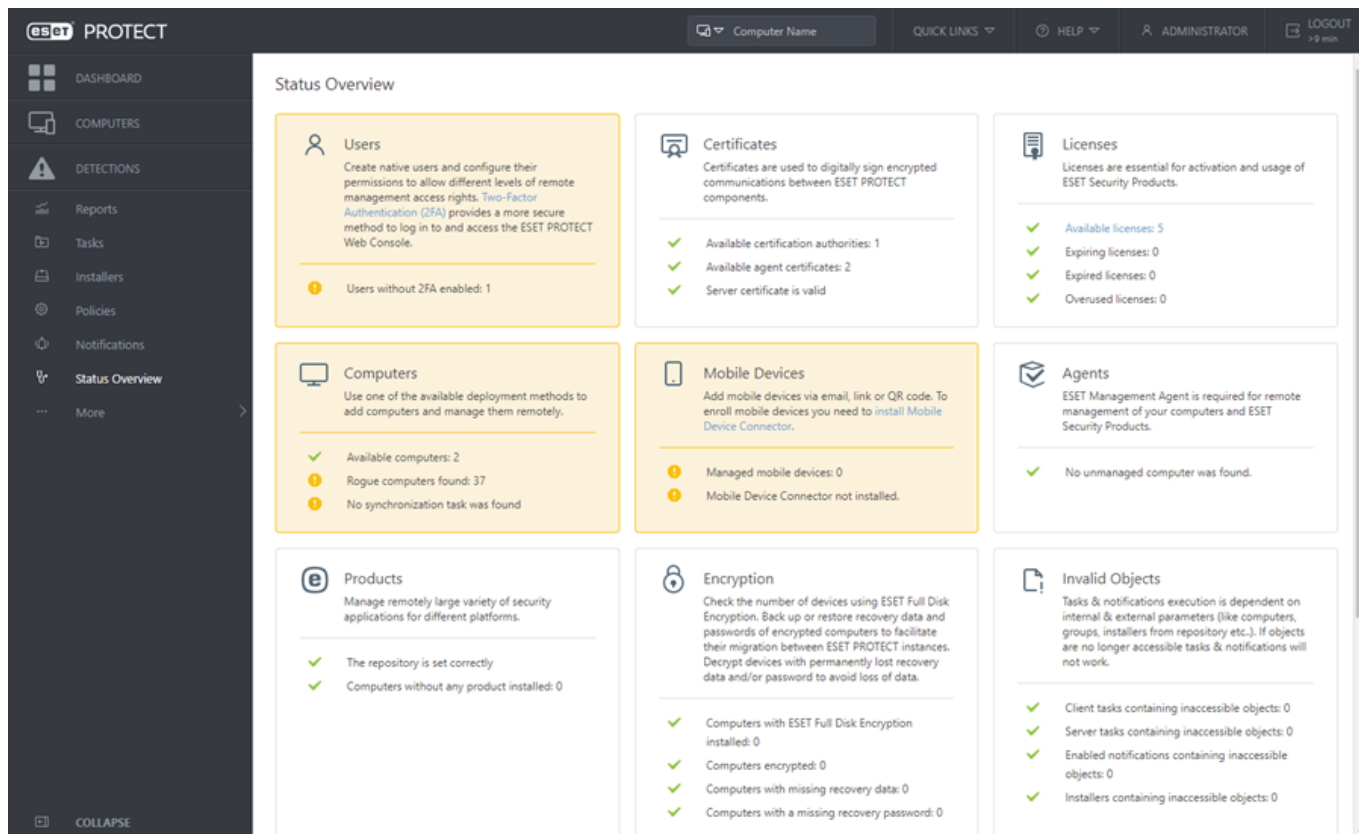
クイックリンク
コンピューターのセットアップ
• コンピューターの追加
• モバイルデバイスの追加
• 他の展開オプション
• コンピューターユーザーの追加
コンピューターの管理
• クライアントタスクの作成
• 新しいポリシーの作成

クイックリンク
<ul style="list-style-type: none"> • ポリシーの割り当て
ステータスの確認
<ul style="list-style-type: none"> • レポートの作成

-  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。
- ESET PROTECT ロゴをクリックすると、[ダッシュボード](#) 画面が開きます。

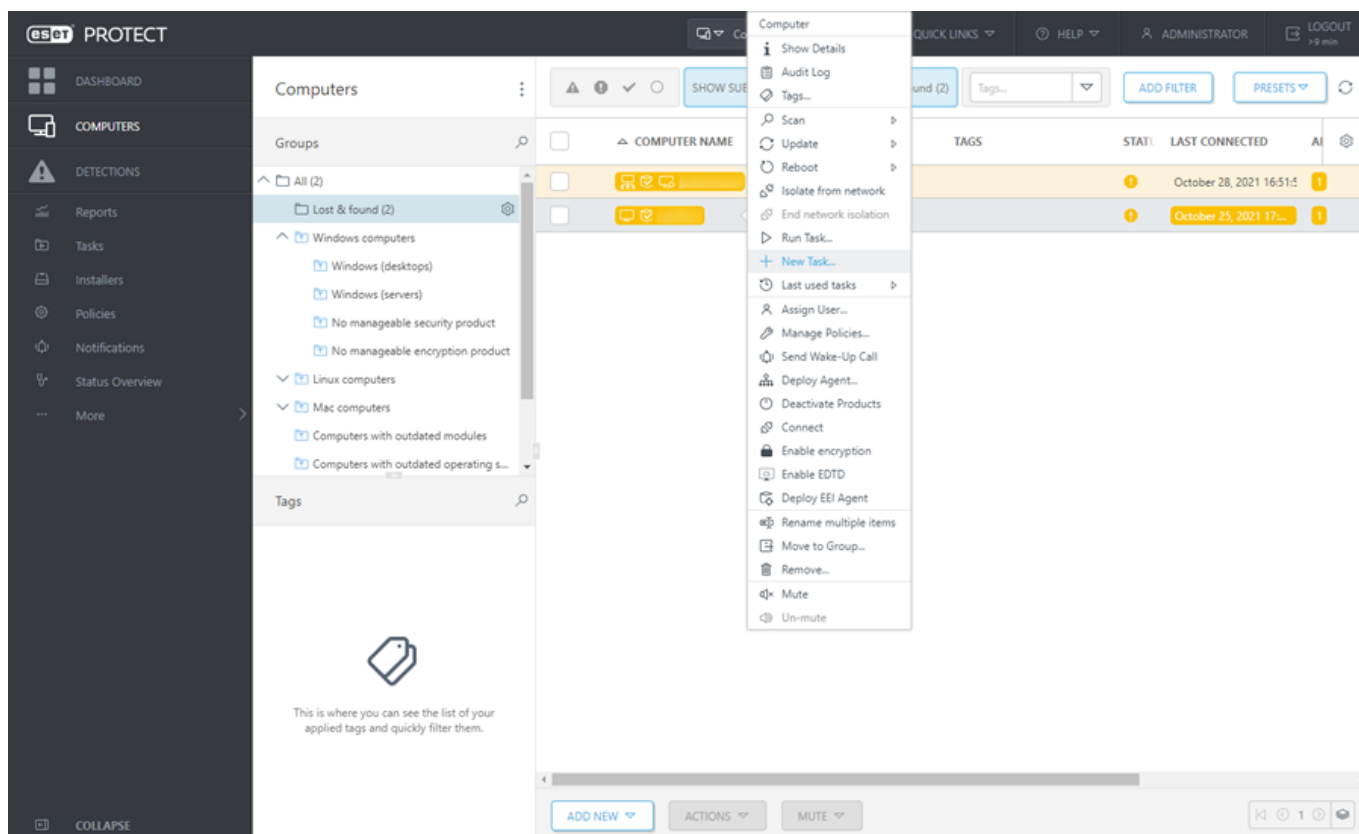


[ステータス概要](#)にはESET PROTECTを最大限に活用する方法が表示されます。ここでは推奨手順が案内されます。



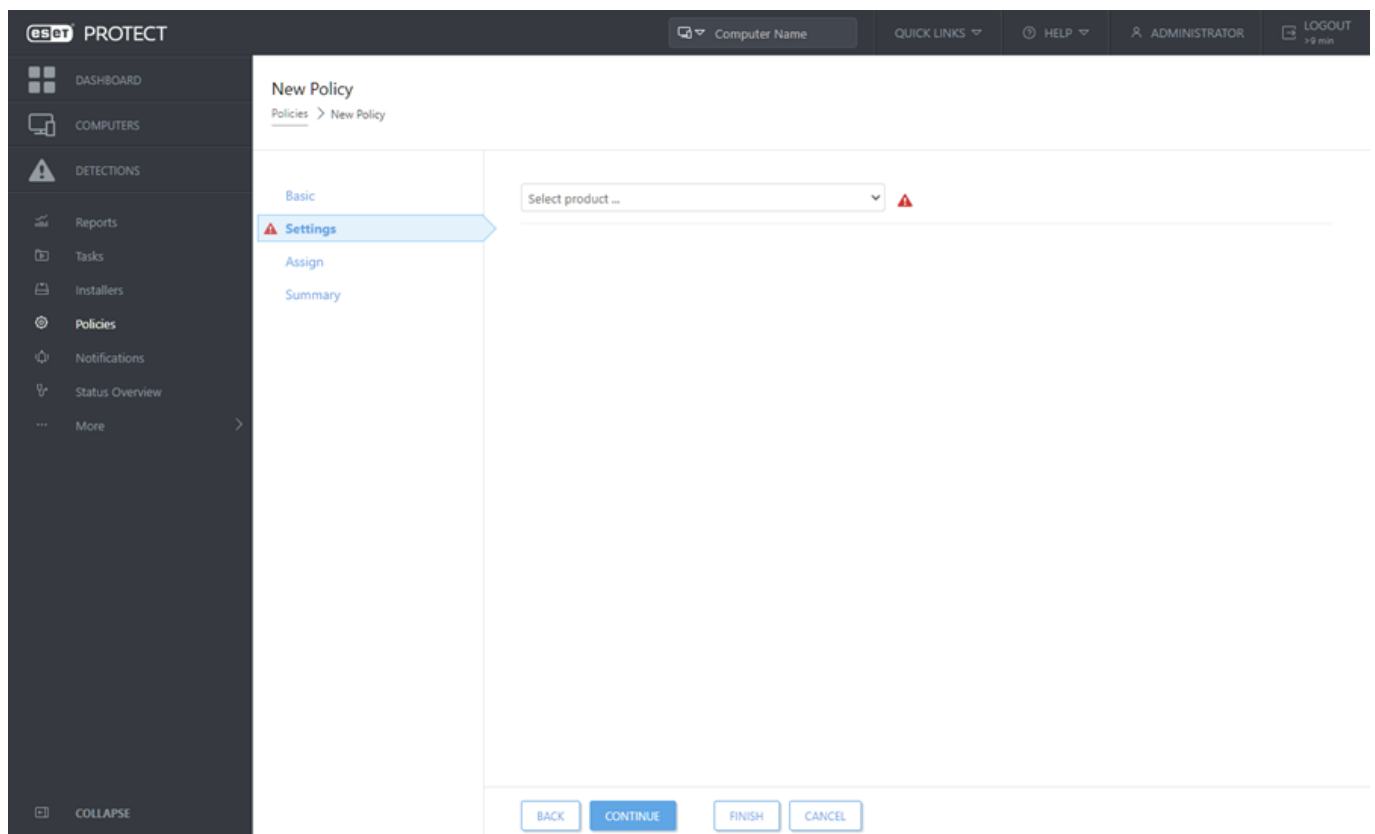
ツリーの画面には固有のコントロールがあります。ツリーは左側にあり、その下にアクションがあります。ツリーの項目をクリックすると、その項目のオプションが表示されます。

表では、行単位で個別にユニットを管理でき、複数行を選択した場合はグループ単位で管理できます。行をクリックすると、その行の単位のオプションを表示されます。表のデータは [フィルタリングおよび並べ替え](#) できます。



ESET PROTECTのオブジェクトはウィザードを使用して編集できます。すべてのウィザードには次の動作があります。

- 手順は上から下に垂直に表示されます。
- いつでも任意の手順に戻れます。
- 必須設定の場合、常に、セクションと該当する設定の横に赤色のエクスクラメーションマークが表示されます。
- 新しいフィールドにカーソルを動かすと、無効な入力フィールドにマークが表示されます。無効な入力データを含むウィザードの手順も同様にマークが表示されます。
- すべての入力データが正しくなるまで、[完了]は使用できません。



ログイン画面

ユーザーがWebコンソールにログインするには、ログイン認証情報(ユーザー名とパスワード)が必要です。また、ドメインユーザーとしてログインすることもできます。この場合、[ドメインユーザーとしてログイン]の横のチェックボックスをオンにします(ドメインユーザーは[マッピングされたドメイングループ](#)に関係していません)。ログイン形式は、ドメインタイプによって異なります。

Windows Active Directory: DOMAIN\username

LinuxおよびESET PROTECT仮想アプライアンスLDAP: username@FULL.DOMAIN.NAME

i ログインできないか、ログインの試行でエラーメッセージが発生する場合は、問題を解決するための提案について、[Webコンソールの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。

言語を選択するには、現在選択されている言語の横のドロップダウン矢印をクリックします。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。

i 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のインストール中に作成され、言語は変更できません。

複数のタブでセッションを許可する- Webコンソールを単一のブラウザーの複数のタブで開くことができます。

- チェックボックスがオンの場合、1つのブラウザーで開いているWebコンソールセッションの各タブが同じセッションに接続されます。新しいタブが開いている場合、同じ設定で接続されたすべての他のタブがこの新しいセッションに接続します。セッションがタブのいずれかでログアウトすると、他のすべてのタブもログアウトします。
- チェックボックスがオフの場合、各新しいタブは新しい独立したESET PROTECT Webコンソールセッションを開きます。

パスワードの変更/別のアカウントを使用する - パスワードを変更したり、もう一度ログイン画面に戻ることができます。

セッション管理とセキュリティ対策:

ログインIPアドレスのロックアウト

同じIPアドレスからログインの試みが10回失敗すると(たとえば、正しくない資格情報)、このIPアドレスからのさらなるログインの試みは一時的にブロックされます。これは次のエラーメッセージで示されます。 **ログインできませんでした:ユーザーはブロックされました。後でもう一度試してください。** 10分後に、正しい資格情報を使用してログインしてください。 ログイン試行のIPアドレス禁止は、既存のセッションには影響しません。

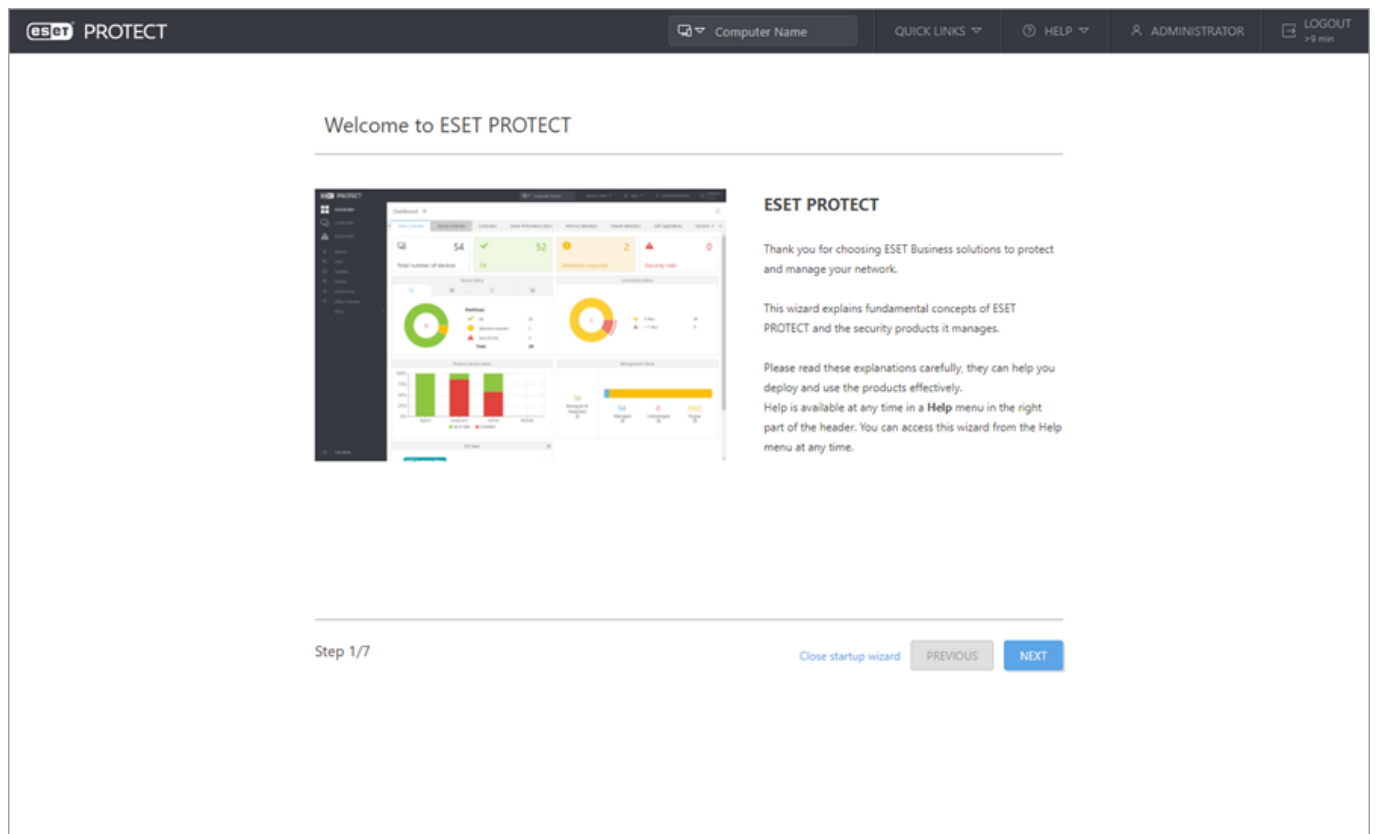
正しくないセッションIDアドレスのロックアウト

同じIPアドレスから無効なセッションIDを15回使用すると、このIPアドレスからの今後のすべての接続が約15分間ブロックされます。期限切れのセッションIDはカウントされません。期限切れのセッションIDがブラウザにある場合は、攻撃とみなされません。15分間のIPアドレスの禁止はすべてのアクション(有効な要求を含む)に適用されます。Webコンソール(tomcatサービス)を再起動すると、禁止を解除できます。

セットアップウィザードの使用

Webコンソールに初めてログインするときにはESET PROTECTのスタートアップウィザードが表示され、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。

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。[コンピューター](#)、[タスク](#)、[ポリシー](#)、および[ESET Managementエージェント](#)について説明します。



ウィザードを使用しない場合は、**スタートアップウィザードを閉じる**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、ウィザードが表示されません。スタートアップウィザードを再表示するには、**ヘルプ>スタートアップウィザード**をクリックします。

スタートアップウィザードの最後のステップの**展開**では、オールインワンインストーラーパッケージ(ESET ManagementエージェントとESETセキュリティ製品を含む)を作成できます。ウィザードを使用せずに[オールインワンエージェントインストーラーを作成](#)するには、**クイックリンクセクション**で**他の展開オプション**をクリックします。

Computer Name
QUICK LINKS
HELP
ADMINISTRATOR
LOGOUT > 9 min

Deployment

Create an installer for Endpoint deployment

The installer file contains all necessary components (ESET Management Agent, ESET security product) with the necessary configuration and license. Run the installer with admin privileges on computers that are to be managed with ESET PROTECT.

After successful installation, the computers appear in the **Lost & found** Static group in the **Computers** section.

For more deployment options, use the **Quick links** option **Other Deployment Options**.

Choose license

[Add license](#)

Product
ESET Endpoint Security; version for windows (WINDOWS); language en_US

Language
English

☐ I accept the [End User License Agreement](#) and acknowledge the [Privacy Policy](#).

Protection settings

The ESET LiveGrid® feedback system
☒ Enable The ESET LiveGrid® feedback system (recommended)

Detection of Potentially Unwanted Applications
☒ Enable detection of potentially unwanted applications
☐ Do not define the Protection settings right now. The end-user will be able to define them during installation. (not recommended)

Product improvement program
☒ Participate in product improvement program

Advanced
☐ Show advanced settings

Full Disk Encryption
☐ Show ESET Full Disk Encryption settings

Enterprise Inspector Agent
☐ Show ESET Enterprise Inspector Agent settings

CREATE INSTALLER

Step 7/7
Close startup wizard
PREVIOUS
NEXT

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。

インストーラーパッケージを作成する場合、ユーザーアカウントに **エージェント展開** の権限が割り当てられている必要があります。ユーザーアカウントにこの権限がない場合、スタートアップウィザードは **展開** 手順なしで表示され、ユーザーはインストーラーパッケージを作成できません。

次の手順に従い、インストーラーパッケージを作成します。

1. **ライセンス**（任意） - [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。既に [ライセンス管理](#) に既存のライセンスがある場合は、使用するライセンスを選択し、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。ライセンスがない場合は、ライセンスなしでインストーラーを作成し、[製品を後からアクティベーション](#) 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、そのグループのライセンスに対する **書き込み** 権限がある管理者にのみ許可されています。

2. **製品** - ESET Management エージェントと一緒にインストールする ESET セキュリティ製品を選択します。

i 製品インストールファイルが表示されない場合は、リポジトリが **AUTOSELECT** に設定されていることを確認します。詳細については、[サーバー設定](#) の **詳細設定** セクションを参照してください。

3. **言語** - ESET セキュリティ製品インストーラーの言語バージョンを選択します。

4. **[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。詳細については、[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](#)を参照してください。

5. **保護設定** – 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。

インストーラーでこれらの保護設定を定義せず、後からポリシーで設定する場合は、**今すぐ保護設定を定義しない**チェックボックスをオンにします。

6. クラッシュレポートと匿名のテレメトリデータ(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に送信することに同意しない場合は、**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フにします。チェックボックスがオンの場合、テレメトリデータとクラッシュレポートがESETに送信されます。

7. **詳細設定を表示**チェックボックスを選択した場合は、次の操作ができます。

- **ESET AV Remover** – 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。
- **エージェント証明書**を選択し、必要に応じて、**証明書パスフレーズ**を入力します。たとえば、ESET PROTECTのインストール中にパスフレーズを指定した場合、またはパスフレーズ付きのカスタム証明書を使用する場合です。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。

- HTTPプロキシを使用する場合は、**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。HTTPプロキシは既定でポート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。



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す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. **完全ディスク暗号化** – 暗号化オプションは、有効な[ESET Full Disk Encryption](#)ライセンスでのみ表示されます。

9. **Enterprise Inspector**エージェント - ESET Enterprise Inspectorエージェントをインストーラーに含めます。このオプションは、ESET Enterprise Inspectorライセンスがある場合にのみ表示されます。

 [ESET Enterprise Inspectorエージェント設定を表示](#)

ESET Enterprise Inspectorエージェント要件:

- ESET Enterprise InspectorエージェントをアクティベーションするにはESET Enterprise Inspector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。

1. **ライセンス (任意)** - インストール中にESET Enterprise InspectorエージェントをアクティベーションするESET Enterprise Inspectorライセンスを選択することをお勧めします。ライセンスなしでインストーラーを作成する場合は、後からESET Enterprise Inspectorエージェントをアクティベーションできます。
2. **製品/バージョン** - ESET Enterprise Inspectorエージェントのバージョンを選択します。最新の使用可能なバージョンがあらかじめ選択されています。
3. **設定ポリシー (任意)** - 既存のESET Enterprise Inspectorエージェントポリシーを選択し、ESET Enterprise Inspectorエージェントインストール中にポリシー設定を適用します。
4. **[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。詳細については、[ESET製品のエンドユーザーライセンス契約\(EULA\)と利用規約、およびプライバシーポリシー](#)を参照してください。
5. ESET Enterprise Inspectorサーバーホスト名と、ESET Enterprise Inspector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)。
6. ESET Enterprise Inspectorサーバーに接続するための**認証局**を選択します。
10. **インストーラーの作成**をクリックします。
11. 生成されたオールインワ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。

o32ビットバージョンをダウンロード(例: *PROTECT_Installer_x86_en_US.exe*)

o64ビットバージョンをダウンロード(例: *PROTECT_Installer_x64_en_US.exe*)

oARM64バージョン(例: *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。ESET PROTECTサーバーはローカルでオールインワ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. 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。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。

i 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。

ユーザー設定

このセクションでは、ユーザー設定をカスタマイズできます。ESET PROTECT Webコンソールの右上端にある**ユーザーアカウント**(ログアウト ボタンの横)をクリックし、すべてのアクティブなユーザーを表示します。異なるWebブラウザー、コンピューター、またはモバイルデバイスから同時にESET PROTECT Webコンソールにログインできます。すべてのセッションがここに表示されます。

i ユーザー設定は、現在ログインしているユーザーにのみ適用されます。各ユーザーは、ESET PROTECT Webコンソールで任意の時間設定を使用できます。ユーザー固有の時間設定は、ESET PROTECT Webコンソールにアクセスする場所に関係なく、そのユーザーに適用されます。

時間設定

すべての情報は、UTC (世界協定時間) 標準を使用してESET PROTECTに内部的に格納されます。UTC時間は、ESET PROTECT Webコンソールによって使用されるタイムゾーンに自動的に変換されます(夏時間を考慮)。ESET PROTECT WebコンソールにはESET PROTECT Webコンソールが実行されているシステムのローカル時間(内部UTC時間ではない)が表示されます。必要に応じて、この設定を上書きしESET PROTECT Webコンソールに表示される時間を手動で設定できます(必要な場合)。

既定の**ブラウザーローカル時刻**を使用設定を無効にする場合は、**手動選択**オプションを選択してから、コンソールタイムゾーンを手動で指定し、夏時間を使用するかどうかを決定します。

! The changes will be applied after the next login.

Time Settings

☐ Use Browser Local Time

☒ Select manually

UTC+01:00 ☒ Daylight saving time

SAVE TIME SETTINGS

! 場合によっては、別のタイムゾーンを使用するオプションが使用可能になります。トリガーを設定するときにはESET PROTECT Webコンソールのタイムゾーンが既定で使用されます。**サーバーのローカル時刻を使用**チェックボックス選択するとESETPROTECTコンソールタイムゾーンではなく、サーバーのローカルタイムゾーンを使用してトリガーを設定できます。

Use Server Local Time

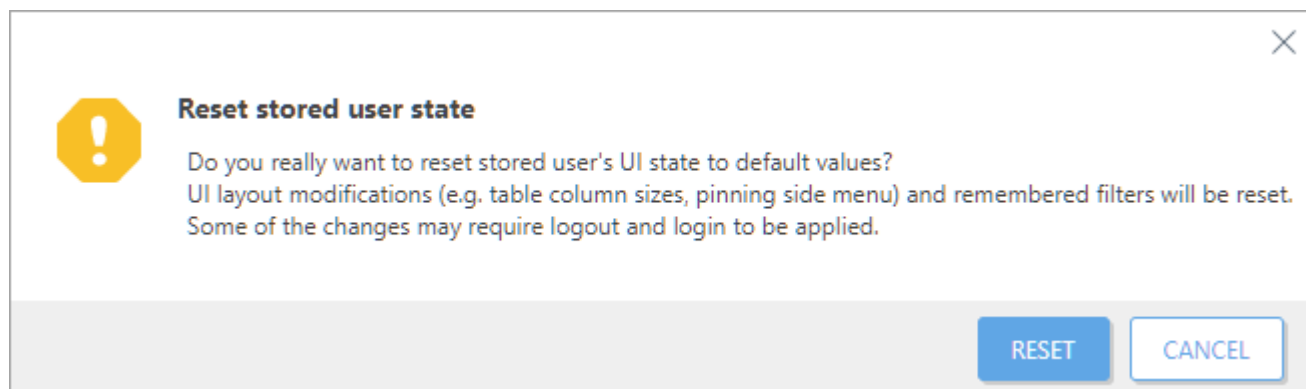


時間設定の保存をクリックして、変更を確認します。

保存されたユーザー状態

保存されたユーザーのUI状態を既定の設定にリセットするには、**保存されたユーザー状態のリセット**を

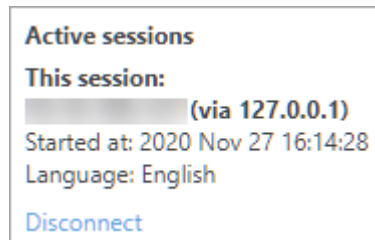
クリックします。これには、[スタートアップウィザード](#)、テーブル列サイズ、推奨フィルター、固定されたサイドメニューなどがあります。



アクティブなセッション

現在のユーザーのすべてのアクティブなセッションの情報は以下のとおりです。

- ユーザーがESET PROTECT Webコンソールに接続するクライアントコンピューターまたはデバイスのIPアドレスとESET PROTECT Webコンソールを実行するWebサーバーのIPアドレスが括弧で囲まれて表示されます。ESET PROTECT WebコンソールがESET PROTECTサーバーと同じコンピューターで実行されている場合は、127.0.0.1経由が表示されます。
- ユーザーがログインした日時。
- ESET PROTECT Webコンソールで選択した言語。



現在のセッションはこのセッションと表示されます。アクティブなセッションを切断する場合は、切断をクリックします。







フィルターとレイアウトのカスタマイズ

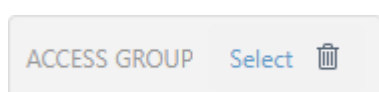
ESET PROTECT Webコンソールでは、複数の方法で、メイン画面に表示される項目のレイアウト(コンピュータータスクなど)をカスタマイズできます。

フィルターとフィルタープリセットの追加

フィルタリング条件を追加するには、**フィルターの追加**をクリックし、リストから項目を選択します。検索文字列を入力するか、フィルターフィールドでドロップダウンメニューから項目を選択して、**Enter**を押します。アクティブなフィルターは青でハイライト表示されます。

フィルターをユーザープロファイルに保存し、将来再利用することができます。プリセットの下で、次のオプションを使用できます：


フィルターセット	保存したフィルター。クリックすると適用します。適用されたフィルターは、  チェックマークが付いています。 表示される列、並べ替え、およびページ制御を含める を選択すると、これらのパラメーターがプリセットに保存されます。
 フィルターセットの保存	現在のフィルター設定を新しいプリセットとして保存します。プリセットが保存された後は、プリセットでフィルター設定を編集できません。
 フィルターセットの管理	既存のプリセットを削除または名前を変更します。 保存 をクリックして、プリセットの変更を適用します。
 フィルター値をクリア	クリックすると、現在の値のみを選択したフィルターから削除します。保存されたプリセットは変更されません。
*  フィルターを削除	クリックすると、選択したフィルターを削除します。保存されたプリセットは変更されません。
*  未使用のフィルターを削除	値がないフィルターフィールドを削除します。








アクセスグループフィルターボタンでは、ユーザーが静的グループを選択し、属するグループに応じて、[表示されるオブジェクトをフィルタリング](#)できます。



[タグ](#)を使用して、表示される項目をフィルタリングできます。

サイドパネルレイアウト


セクション名の横の  アイコンをクリックし、コンテキストメニューを使用してサイドパネルのレイアウトを調整します(使用可能なオプションは、現在のレイアウトによって異なる場合があります)。

-  サイドパネルを非表示
-  サイドパネルを表示
-  グループ
-  グループとタグ
-  タグ

グループが表示されている場合は、次のオプションのいずれかも選択できます。

-  すべて展開
-  すべて折りたたみ


メインテーブルの管理

列を並べ替えるには、列名の横の  アイコンにカーソルを置き、列をドラッグします。以下の**列の編集**も参照してください。


1つの列で並べ替えるには、列ヘッダーをクリックして、選択した列のデータに基づいて表の行を並べ替えます。

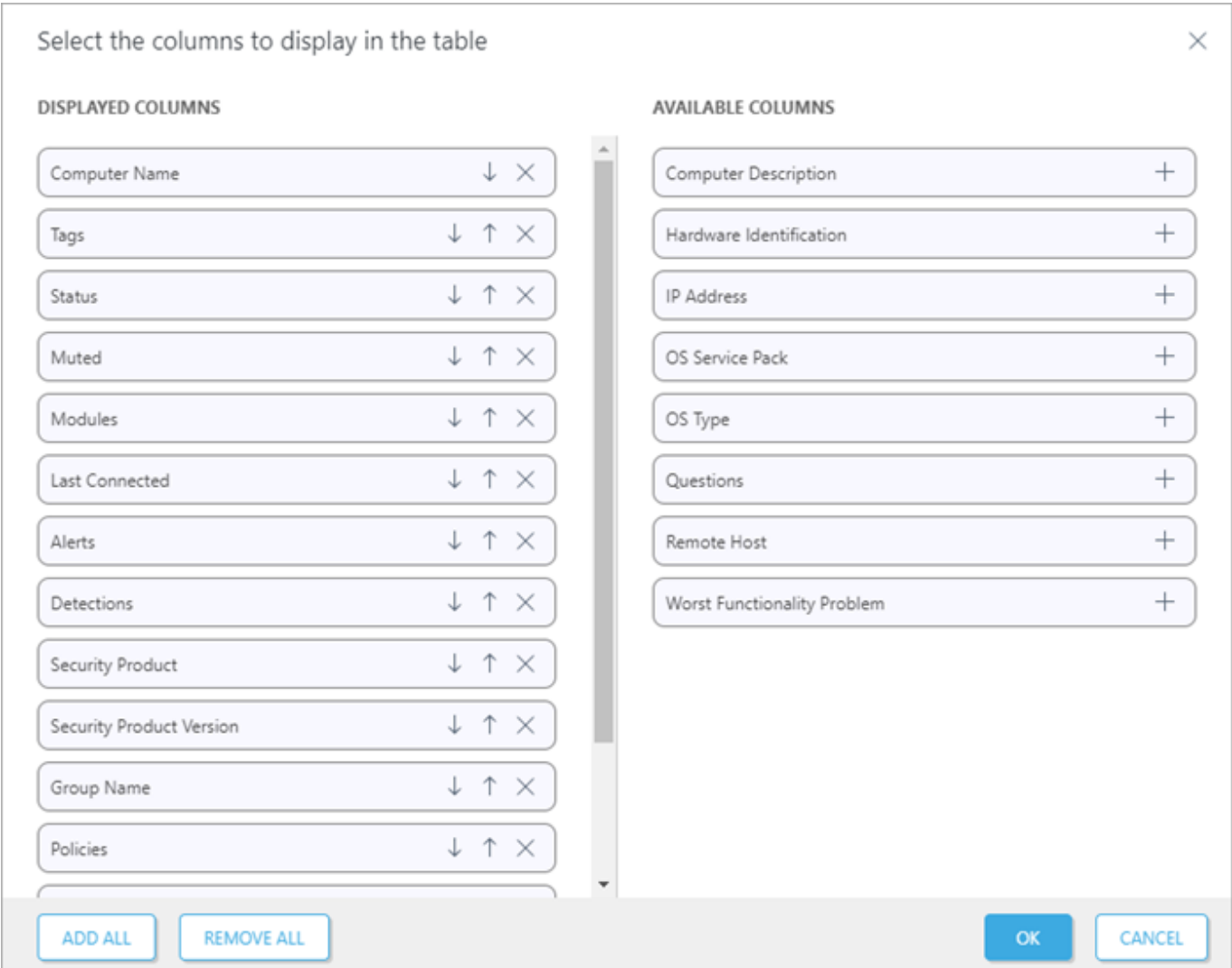
- 昇順(A-Z, 0-9)または降順(Z-A, 9-0)で並べ替えるには、1回または2回クリックします。

- 並べ替えを適用した後、列ヘッダーの前に小さな矢印が表示され、並び順が示されます。
- 以下の「[複数の並べ替え](#)」も参照してください。

メインテーブルの管理の  歯車アイコンをクリックします。

アクション

-  **列の編集** – ウィザードを使用して、(+ 追加、X 削除、↓ ↑ 並べ替え) 表示される項目を調整します。ドラッグアンドドロップを使用して、列を調整することもできます。



The dialog box titled "Select the columns to display in the table" is divided into two main sections: "DISPLAYED COLUMNS" on the left and "AVAILABLE COLUMNS" on the right. The "DISPLAYED COLUMNS" section contains a list of columns currently shown in the table, each with a small icon (down arrow, up arrow, or X) for sorting or removal. The "AVAILABLE COLUMNS" section contains a list of columns that can be added to the table, each with a plus icon. At the bottom of the dialog, there are buttons for "ADD ALL", "REMOVE ALL", "OK", and "CANCEL".

DISPLAYED COLUMNS	AVAILABLE COLUMNS
Computer Name	Computer Description
Tags	Hardware Identification
Status	IP Address
Muted	OS Service Pack
Modules	OS Type
Last Connected	Questions
Alerts	Remote Host
Detections	Worst Functionality Problem
Security Product	
Security Product Version	
Group Name	
Policies	

-  **列の自動調整** – 列幅を自動的に調整します。

テーブルソート

- **並べ替えのリセット** – 列の並べ替えをリセットします。
- **複数の並べ替え** – 複数の列(最大4列)を選択して、表データを並べ替えることができます。各列について、次の項目を調整できます。
 - **並べ替えの優先順位** – **上へ移動**または**下へ移動**ボタン(最初の列: プライマリソート、2 番目の列 – セカンダリソートなど)をクリックして列の順序を変更します。複数の並べ替えを適用すると、インデックス番号が列ヘッダーの前に表示され、並べ替えの優先順位を示します。

o並べ替え動作 - ドロップダウンメニューから昇順または降順を選択します。

Sort by Multiple Columns

☒ Computer Name Ascending

☒ Status Descending

☐ Muted n/a

☐ Modules n/a

☐ Last Connected n/a

☐ Alerts n/a

☐ Detections n/a

☐ Security Product n/a

☐ Security Product Version n/a

☐ Group Name n/a

☐ Policies n/a

☐ OS Name n/a

☐ OS Version n/a

☐ OS Platform n/a

MOVE UP MOVE DOWN SORT CANCEL

<input type="checkbox"/>	COMPUTER NAME	TAGS	STATUS
--------------------------	---------------	------	--------

1プライマリソート - コンピュータ名列: 昇順の並べ替えが適用されます。

2セカンダリソート - ステータス列: セカンダリソートとして降順の並べ替えが適用されます。

レポート

- 形式を指定してテーブルをエクスポート - 次の任意の形式でレポートとしてテーブルをエクスポートします。 .pdfまたは.csvを選択できます。CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します
- レポートテンプレートの保存 - 新しいレポートテンプレートをテーブルから作成します。

タグ

ESET PROTECTでは、すべての関連するオブジェクト(コンピューター、検出、タスク、インストーラー、ポリシー、通知、ライセンスなど)に、ユーザーが定義したタグを設定できます。これは、フィルタリ

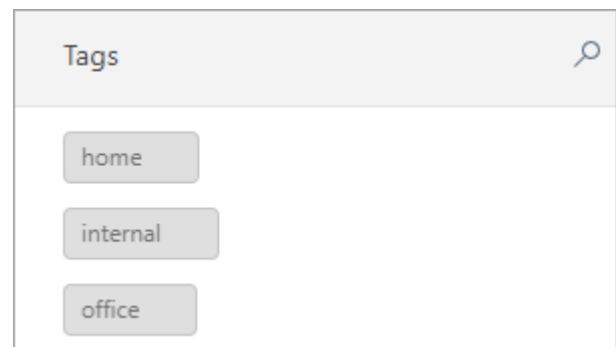
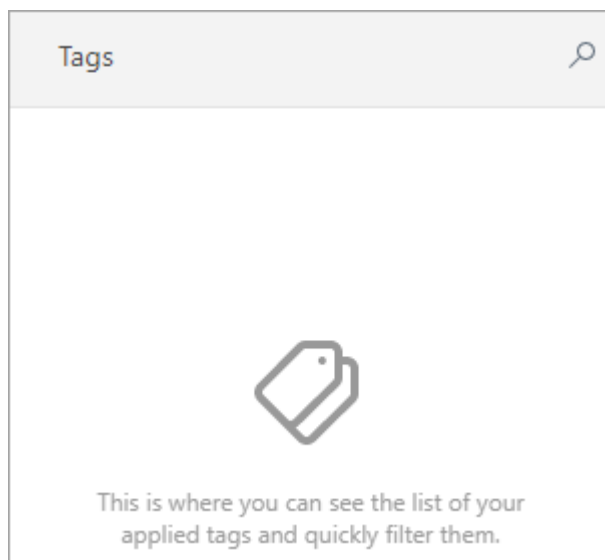
ングや検索を強化するために使用できます。タグは、ESET PROTECT Webコンソールのすべての主要な画面でネイティブに統合されています。

タグはユーザーが定義したキーワード(ラベル)であり、別のオブジェクトに追加して、グループ化、フィルタリング、検索を容易にすることができます。たとえば、関連する資産に「VIP」タグを割り当てると、関連付けられているすべてのオブジェクトをすばやく識別することができます。

タグを手動で[作成](#)して[割り当てる](#)ことができます。 [MSPオブジェクトは、顧客名で自動的にタグ付けされます](#)

タグウィンドウ

ESET PROTECT Webコンソールメニュー画面の左下に表示される**タグ**セクションには、既存のタグが表示されます。



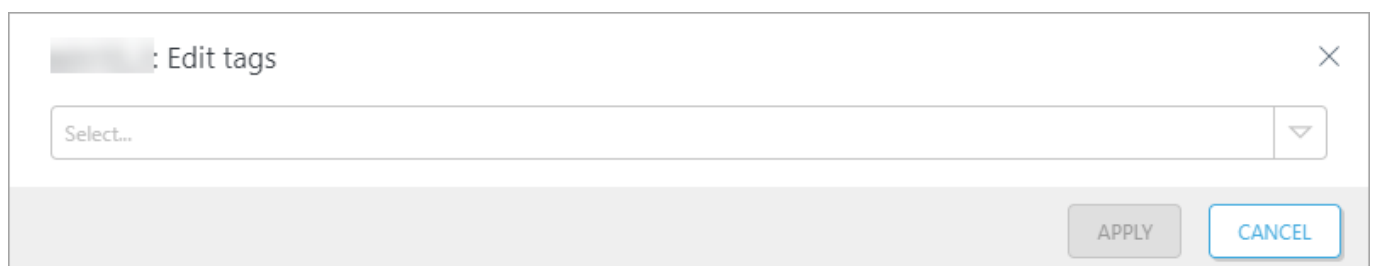
タグ管理の権限

オブジェクトのタグを管理するには、[ユーザー](#)は、オブジェクトへの十分なアクセス権([権限セット](#)が割り当てられていること)が必要です。追加のユーザーもタグを管理できます。たとえば、自分が作成したタグを別のユーザーが削除することができます。

タグの割り当て

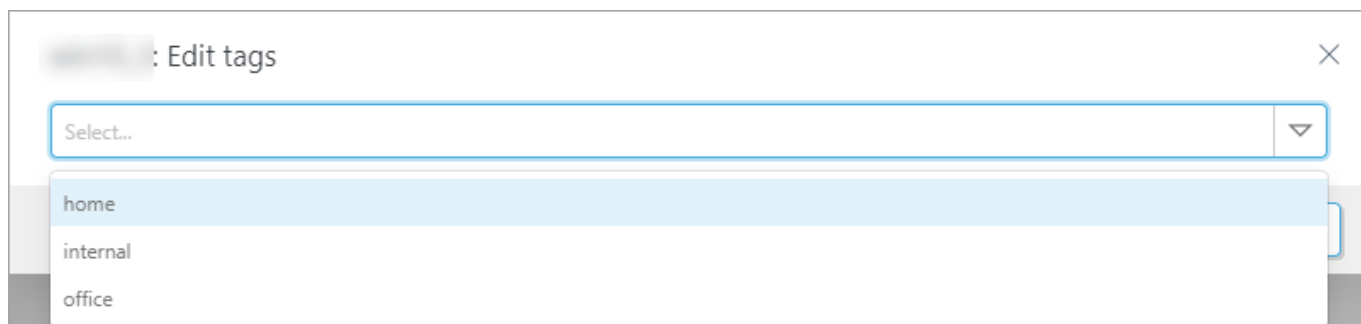
タグは、1つ以上のオブジェクトに割り当てることができます。

タグを割り当てるには、オブジェクトの横のチェックボックスをオンにして、**アクション** > **タグ**をクリックします。



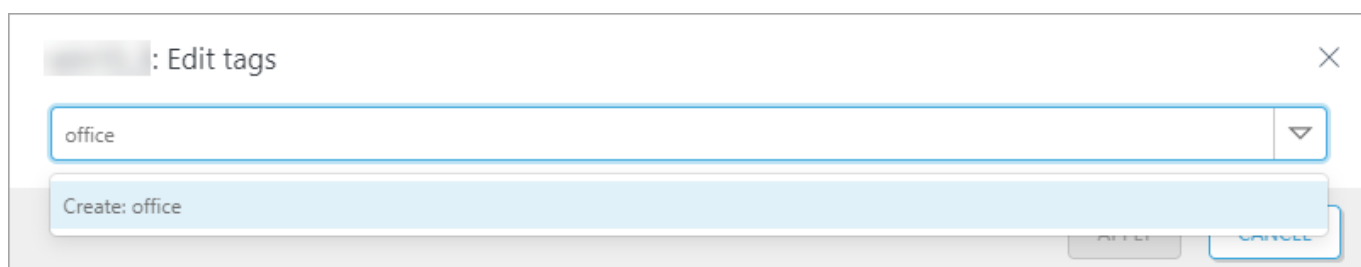
既存のタグを割り当てるには、入力フィールドでリストからタグをクリックして、**適用**をクリックしま

す。



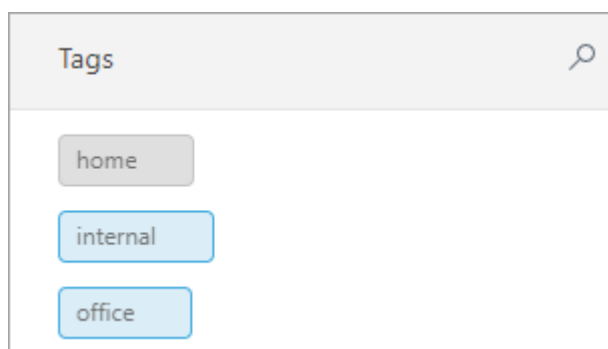
新しいタグの作成

新しいタグを作成するには、タグ名を入力し、「タグ名」を作成をクリックしてから、適用をクリックします。




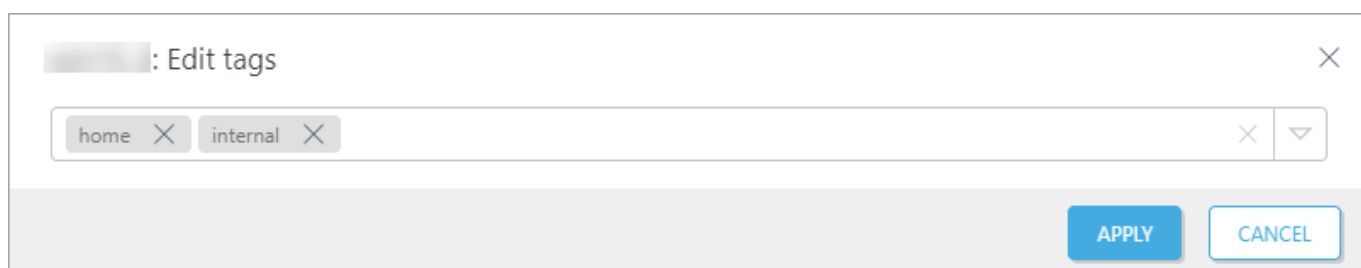
オブジェクトをタグでフィルタリング

タグをクリックして、フィルターをリストのオブジェクトに適用します。選択したタグは青色です。




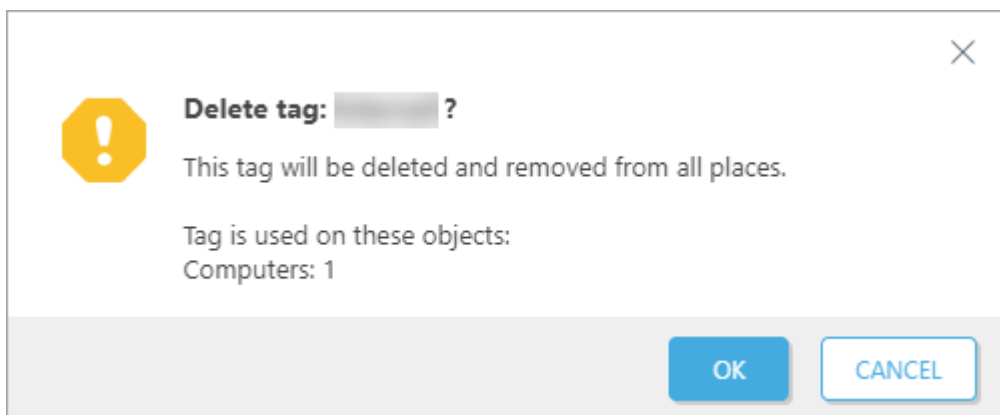
タグの割り当て解除

タグを割り当てるには、オブジェクトの横のチェックボックスをオンにして、アクション>  タグをクリックします。Xをクリックしてタグを削除し、適用をクリックします。



タグの削除

タグを削除するには、**タグ**ウィンドウでタグにマウスカースルを置き、 アイコンをクリックして、**OK** をクリックし、ESET PROTECT Web コンソールのすべてのオブジェクトからタグを削除することを確認します。



CSVのインポート

リストをインポートするには、正しい構造のカスタム **.csv**ファイルを使用して実行できます。この機能は、ESET PROTECT ユーザーインターフェースのさまざまなメニューで使用されます。インポート対象によって列が異なります。

1. **CSVのインポート**をクリックします。
2. **アップロード - ファイルの選択**をクリックして、アップロードする**.csv**ファイルを選択し、**アップロード**をクリックします。
3. **区切り文字** - 個別のテキスト文字を区切るための文字。該当する区切り文字(**セミコロン**、**カンマ**、**スペース**、**タブ**、**ドット**、**縦線**)を選択し、**.csv**ファイルで使用する文字に合わせます。**.csv**ファイルで別の文字を区切り文字として使用する場合は、**その他**チェックボックスをオンにし、文字を入力します。**データプレビュー**には、文字列を区切るために使用する区切り文字を特定できるように**.csv**ファイルの内容が表示されます。
4. **列マッピング** - **.csv**ファイルがアップロードおよび解析されると、インポートされた**.csv**ファイルの任意の各列をテーブルに表示されたESET PROTECT列とマッピングできます。**ドロップダウン**リストを使用して、特定のESET PROTECT列に関連付ける**CSV**列を選択します。**.csv**ファイルにヘッダー行がない場合は、**CSVの最初の行に見出しを含める**チェックボックスをオフにします。
5. **テーブルプレビュー**を表示し、列マッピングが正しく設定され、インポート処理が想定どおりに動作することを確認します。
6. 各列が正常にマッピングされ、**テーブルプレビュー**に問題がない場合は、インポートをクリックして処理を開始します。

Import CSV

Upload

Delimiter

Column mapping

CSV headings ⓘ

☒ First line of CSV contains headings

CSV column

TABLE COLUMN	CSV COLUMN
NAME	All\Lost & found\ (All\Lost & found\)
DESCRIPTION	<< Select >>

Table preview

NAME	DESCRIPTION
All\Lost & found\	
All\Lost & found\	

BACK





CONTINUE





IMPORT

CANCEL

トラブルシューティング - Webコンソール

以下の表は、最も一般的なWebコンソールログインエラーメッセージと状況、その意味、一部の追加トラブルシューティング手順について示します。

エラーメッセージ	考えられる原因
 ログインできませんでした:ユーザー名またはパスワードが無効です	ユーザー名とパスワードを正しく入力したことを確認してください。ESET PROTECT Webコンソール パスワード をリセットできます。
 ログインできませんでした:「未接続」状態で接続が失敗しました	ESET PROTECT Serverサービスとデータベースサービスが実行中であるかどうかを確認します。段階的な手順については、 ナレッジベース記事 を参照してください。
 ログインできませんでした:ユーザーはブロックされました。後でもう一度試してください。	同じIPアドレスからログインの試みが10回失敗すると(たとえば、正しくない資格情報)、このIPアドレスからのさらなるログインの試みは一時的にブロックされます。10分後に、正しい資格情報を使用してログインしてください。
 ログインできませんでした:通信エラー	ESET PROTECT Serverサービスが 実行中 であり、 Apache Tomcat が 実行中で正しく動作している ことを確認します。Apache Tomcatの ログファイル を参照してください。この問題の詳細については、 ナレッジベース記事 を参照してください。

エラーメッセージ	考えられる原因
 ログインできませんでした:接続タイムアウト	ネットワーク接続とファイアウォール設定を確認し、ESET PROTECT Web コンソールがESET PROTECT サーバーに到達できることを確認します。またESET PROTECT サーバーが過負荷状態である可能性があります。再起動してくださいESET PROTECT Web コンソールとESET PROTECTサーバーの別のバージョンを使用している場合、この問題が発生することがあります。
 ログインできませんでした:ユーザーにはアクセス権が割り当てられていません	ユーザーにはアクセス権が割り当てられていません。管理者でログインし、ユーザーのアカウントを編集して、1つ以上の 権限設定 をこのユーザーに割り当てます。
 ログインできませんでした:応答解析エラー	Web コンソールとESET PROTECTサーバーのバージョンが互換性がありません。これはコンポーネントアップグレード中またはその後に発生することがあります。問題が解決しない場合は、正しいバージョンのWeb コンソールを手動で展開してください。
 暗号化されていない接続を使用していますESET PROTECT Web コンソールを使用してWebサーバーを構成してください	セキュリティの理由から、 HTTPSを使用するようにESET PROTECT Web コンソールを設定 することをお勧めします。
JavaScriptが無効です。ブラウザのJavaScriptを有効にしてください。	JavaScriptを有効にするか、 Webブラウザ をアップデートします。
SEC_ERROR_INADEQUATE_KEY_USAGE (Mozilla Firefoxのみ)。	Mozilla Firefoxの 証明書ストアは破損しています 。

エラー	考えられる原因
ログイン画面が表示されないか、ログイン画面が表示されるときに読み込み状態が続きます。	<ul style="list-style-type: none"> ESET PROTECT Serverサービスを再起動しますESET PROTECT Serverサービスが起動し、再度実行されたら、Apache Tomcatサービスを再起動します。この手順を実行するとESET PROTECT Web コンソールログイン画面が正しく読み込まれます。ナレッジベース記事もお読みください。 Apache Tomcatが<code>era.war</code>ファイルから内容を展開できずESET PROTECT Web コンソールにアクセスできない場合は、ナレッジベース記事の手順に従ってください。
テキストは、コンテンツメニューおよびESET PROTECT Web コンソールの クイックリンク メニューにありません。	この問題は、広告ブロックブラウザ拡張が原因の場合があります。この問題を解決するにはESET PROTECT Web コンソールページの広告ブロックブラウザ拡張を無効にします。
ログイン後、Web Consoleが正しく表示されません(要素が不足しているなど)。	サポートされているWebブラウザ を使用していることを確認してください。
ログイン後、一部のWeb コンソール画面が読み込まれません。	<p>ESET PROTECT Web コンソール画面(コンピューターなど)の一部が読み込まれない場合は、C:\Program Files\Apache Software Foundation\[Tomcatフォルダー]にある<code>Tomcat9w.exe</code>ファイルを開きます</p> <ul style="list-style-type: none"> 全般タブで停止をクリックして、Apache Tomcatサービスを停止します。 Javaタブを選択し、Java Optionsの下に次のコードを追加します。 <code>-Duser.country=US</code> <code>-Duser.language=en</code> 全般タブで開始をクリックして、Apache Tomcatサービスを開始します。
Web コンソールの読み込みに時間がかかります。多数のオブジェクトを読み込むと、コンソールがクラッシュします。	Web コンソールでは、大きいオブジェクトセットを処理するときには、必要なメモリ量が多くなります。 エンタープライズ向けの設定 についてはESET PROTECT Web コンソールを参照してください。

エラー	考えられる原因
Web コンソールの一部の画面が正しく読み込まれず、エラーが表示される。たとえば、ポリシーを編集するときに、次のエラーが表示されず。[ERROR WHILE INITIALIZING CONFIGURATION EDITOR.: (TYPEERROR) : ((INTERMEDIATE VALUE)(INTERMEDIATE VALUE), K).INITCONFIGEDITOR IS NOT A FUNCTION]	この問題は、一部のWebコンソールモジュールの読み込みを防止するリバースプロキシを使用している場合に発生します。(Apache Tomcatに読み込まれた)個別のWebコンソールモジュールのURL文字列は動的に変更される場合があります(たとえば、era/webconsole/configEngine/02645EFC6ABCDE2B449042FB8563FD3/v0.0/css/001_ce.ltr.css)のera/webconsole/configEngine/の後の文字列)。この問題を解決するには、リバースプロキシが正しく構成されていることを確認してください。
大規模な(10 MBを上回る)ファイル(ポリシーなど)をインポートするときには、プロセスが失敗します。	Webコンソールのファイルサイズ制限は10 MBです。[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\configフォルダーにあるEraWebServerConfig.propertiesファイルを編集すると、変更できます。file_size_limit=10をより大きい値に変更します。最大値は250です。

- ESET PROTECTをアップグレードした後、アップグレードされたWebコンソールにログインする前に、WebブラウザキャッシュとCookieを削除することをお勧めします。
- Webコンソールは安全なプロトコル(HTTPS)を使用するため、セキュリティ証明書または信頼できない接続に関するメッセージがWebブラウザで表示される場合があります(正確なメッセージの内容は使用中のブラウザによって異なります)。これは、ブラウザで、アクセスしようとしているサイトの身元を確認しようとしているためです。[このサイトの閲覧を続行する] (Internet Explorer)か、[I Understand the Risks]をクリックし、[Add Exception...]をクリックしてから、[Confirm Security Exception] (Firefox)をクリックしてESET PROTECT Webコンソールにアクセスします。これはESET PROTECT WebコンソールURLにアクセスしようとしている場合にのみ適用されます。HTTPS/SSL接続の設定方法の詳細については、「[ナレッジベース記事](#)」を参照してください。

ESET PROTECTからエンドポイント製品を管理する方法

ESETビジネスソリューションの管理を開始する前に、初期設定を実行する必要があります。特に、[スタートアップウィザード](#)を省略した場合、[ステータス概要](#)を使用することをお勧めします。管理者はESET PROTECT Webコンソールからさまざまなタスクを実行し、製品をインストールして、クライアントコンピュータを制御できます。

ESET Managementエージェントとエンドポイントセキュリティ製品のインストール

ESET PROTECTでは、各管理対象のクライアントコンピュータにESET Managementエージェントをインストールする必要があります。ESET Managementエージェントは、エンドポイントセキュリティ製品と一緒にインストールできます。インストール前に、ESET PROTECTに[ライセンスをインポート](#)し、その後のインストールで使用できるようにすることをお勧めします。エンドポイント製品をインストールするには複数の方法があります。

- [エージェントとESETセキュリティ製品のインストーラー](#)、または[ESET Remote Deployment Tool](#)を使用して、エンドポイント製品とESET Managementエージェントを同時にインストールします。
- クライアントタスクを使用して、既にESET Managementエージェントがインストールされたクライアントに[ESETエンドポイント製品をインストール](#)します。

エンドポイントセキュリティ製品の管理 ESET PROTECT


すべてのエンドポイントセキュリティ製品はESET PROTECT Webコンソールから管理できます。ポリシーは、単一のコンピューターまたはグループに設定を適用するために使用されます。たとえば、[ポリシーを作成](#)し、特定のWebローカルティへのアクセスをブロックしたり、[スキャナー設定検出感度](#)(Endpoint 7.2以降で提供)を変更したり、すべての他の設定を変更したりできます。[例](#)に示すように、ポリシーは[マージ](#)できます。ESET PROTECTを使用して設定されるポリシーはクライアントコンピューターのユーザーによって上書きできません。ただし、管理者は[上書き](#)機能を使用して、ユーザーがクライアントで一時的に変更することを許可できます。変更が完了したら、クライアントから[最終設定を要求](#)し、新しいポリシーとして保存できます。

[タスク](#)を使用して、クライアントを管理することもできます。タスクはWebコンソールから展開されESET Managementエージェントによってクライアントで実行されます。Windowsエンドポイントの最も一般的なクライアントタスク:

- [モジュールのアップデート](#) (ウイルスデータベースのアップデート)
- [オンデマンド検査](#)の実行
- カスタム[コマンド](#)の実行
- コンピューターと製品[設定](#)の要求

コンピューターステータスの報告とクライアントから ESET PROTECT に情報を取得する

各クライアントコンピューターはエージェント経由でESET ManagementESET PROTECTに接続されます。エージェントは、クライアントコンピューターとソフトウェアに関するすべての必要な情報をESET PROTECTサーバーに報告します。 エージェントとサーバー間の通信は既定では1分に設定されますがESET Managementエージェントポリシーで[変更](#)できます。 エンドポイントまたはESETセキュリティ製品からのすべてのログはESET PROTECTサーバーに送信されます。

インストールされたESET製品の情報と、クライアントのOSとステータスに関する他の基本情報は、[コンピューター](#)にあります。クライアントを選択し、[詳細を表示](#)をクリックします。ウィンドウの  [設定](#) セクションで、ユーザーは古い設定を検索したり、現在の設定を要求したりできます。[SysInspector](#) セクションでは、ユーザーがログを要求できます(Windowsコンピューターからのみ)。

Webコンソールでは、クライアントデバイスからすべての[検出](#) のリストにアクセスできます。1つのデバイスからの検出は、[コンピューター](#)に表示されます。クライアントを選択し、[詳細を表示](#) > [検出と隔離](#) をクリックします。 クライアントコンピューターが[ESET Enterprise Inspector](#)を実行する場合Enter Enterprise Inspector検出を表示して管理できます。

オンデマンドでカスタム[レポート](#)を生成するか、スケジュールされたタスクを使用して、ネットワークのクライアントデータを表示できます。定義済みレポートテンプレートは重要なデータをすばやく収集できます。また、独自の[新しいテンプレート](#)を作成できます。レポートの例には、コンピューター、検出、隔離、必要なアップデートに関する集約情報があります。



ユーザーは十分な[権限](#)があるレポートテンプレートのみを使用できます。既定では、すべてのテンプレートが[すべてグループ](#)に保存されます。レポートには、ユーザーの権限範囲内のコンピューターとイベントの情報のみが含まれます。レポートテンプレートがその他のユーザー間で共有される場合でも、各ユーザーのレポートにはそのユーザーに権限があるデバイスの情報しか含まれません。アクセス権の詳細については、[権限の一覧](#)を参照してください。

ESETプッシュ通知サービス

ESET Push Notification Service(EPNS)は、サーバーにクライアント宛での通知がある場合に、ESET PROTECTサーバーからメッセージを受信します。ESET PROTECTが即時にクライアントに通知を送信(プッシュ)できるように、接続は常時実行されています。接続が切断されると、クライアントは再接続を試みます。常時接続の主な目的は、クライアントでメッセージを受信できるようにすることです。

Webコンソールユーザーは、ESET PROTECTサーバーとESET Managementエージェントの間で、EPNS経由でウェイクアップ コールを送信できます。ESET PROTECTサーバーは、**Wake on LAN** コールを送信します。[サーバー設定](#)で**Wake on LAN**のマルチキャストアドレスを設定できます。

接続詳細

ローカルネットワークを設定し、EPNSとの通信を許可するにはESET ManagementエージェントとESET PROTECTサーバーの両方がEPNSサーバーに接続する必要があります。 エージェントでEPNSとの接続を確立できない場合は、ウェイクアップコールのみが影響を受けます。

転送セキュリティ	SSL
プロトコル	MQTT (コンピューター間接続プロトコル)
ポート	<ul style="list-style-type: none">プライマリ:8883フォールバック:ESET Managementエージェントポリシーで設定された443およびプロキシポート MQTTポートであるポート8883が推奨されます。443はフォールバックポートであり、他のサービスと共有されます。またHTTP Proxyサーバーの動作がないか、開いている接続数の上限に達した場合は、ファイアウォールがポート443での接続を中断できます。
ホストアドレス	<i>epns.eset.com</i>
プロキシ互換性	通信を転送するためにHTTPプロキシを使用している場合は、ウェイクアップコールもHTTPプロキシ経由で送信されます。認証はサポートされていません。ウェイクアップコールを送信するコンピューターで、エージェントポリシーでHTTPプロキシを設定していることを確認します。HTTPプロキシが動作していない場合、ウェイクアップコールは直接送信されます。

トラブルシューティング

- ファイアウォールがEPNSへの接続を許可するように設定されていることを確認します。上記または[ナレッジベース記事](#)の詳細を参照してください。
- エージェントとサーバーの両方が443および8883ポートでEPNSサーバーに直接接続できます(接続を検証するには、telnetコマンドを使用します)。

VDI複製、ハードウェア検出

ESET PROTECTはVDI環境、コンピューターの複製および非永続ストレージシステムをサポートします。この機能は、マスターコンピューターのフラグを設定し、複製またはハードウェア変更後に表示される[質問](#)を解決するために必要です。

- 質問が解決されるまでは、クライアントコンピューターは、ESET PROTECTにレプリケーション(接

続)できません。 サーバー、クライアントは、質問が解決されたかどうかのみを確認します。

- ハードウェア検出の無効化は元に戻せません。最大限の注意を払い、物理コンピューターでのみ使用してください。
- 複数の[質問](#)を解決するときに、[ステータス概要](#) - 質問タイルを使用します。

どのOSとハイパーバイザーがサポートされますか。



ESET PROTECTでVDIの使用を開始する前に、[ナレッジベース記事](#)で各種VDI環境のサポートされている機能とサポートされていない機能についてお読みください。

- [Windows](#)オペレーティングシステムだけがサポートされます。
- ESET仮想エージェントホストはサポートされません。
- ESET Full Disk Encryptionはサポートされていません。
- MDMで管理された サポートされていません。
- Virtual Box内のリンククローンは、相互に識別できません。
- ごくまれに、検出がESET PROTECTによって自動的にオフになる可能性があります。これはESET PROTECTが信頼できる方法で[ハードウェア](#)を分析できないときに発生します。
- サポート対象の設定の一覧を参照してください。

oCitrix PVS 7.0以降を搭載した物理コンピューター

oCitrix XenServer 7以降を搭載したCitrix PVS 7.0以降の仮想マシン

oCitrix XenServer 7以降を搭載したCitrix PVS 7.0+およびCitrix XenDesktop

oCitrix Machine Creation Services

o(PVSなし) Citrix XenServer7以降を搭載したCitrixXenDesktop

oVMware Horizon 7.xおよび8.0とVMware ESXi

oMicrosoft SCCM (再イメージング用)



ESET PROTECT 9.0 は[VMware Horizon 8.x インスタントクローン](#)と [Citrix XenCenter/XenServer 8以上のマシンカタログ](#)をサポートします。

VDI環境

VDIプールにはESET Managementエージェントでマスターコンピューターを使用できます。VDIコネクターは不要です。すべての通信は、ESET Managementエージェント経由で処理されます。VDIプール(コンピューターカタログ)を設定する前に、ESET Managementエージェントをマスターコンピューターにインストールする必要があります。

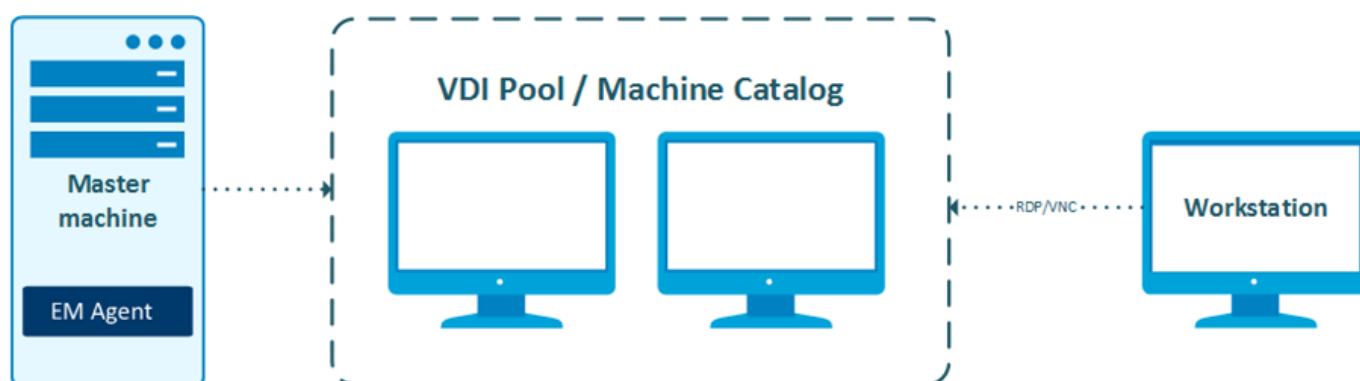
- VDIプールを作成する場合は、プールを作成する前に、[コンピューター詳細](#) > 仮想化でマスターコンピューターにフラグを設定します。複製のマスターとして設定する(既存のコンピューターと一

致する)を選択します。

- マスターコンピューターがESET PROTECTから削除される場合ID(複製)の回復は禁止されます。プールからの新しいコンピューターは、毎回新しいIDを取得します(新しいコンピューターエントリがWebコンソールで作成されます)。
- 初めてVDIプールのコンピューターが接続するときには、必須の1分の接続間隔になります。最初の数回のレプリケーションの後、接続間隔はマスターから継承されます。
- VDIプールを使用するときには、ハードウェア検出を無効にしないでください。
- 複製されたコンピューターとともにマスターコンピューターを実行できるため、マスターコンピューターを最新の状態に保つことができます。

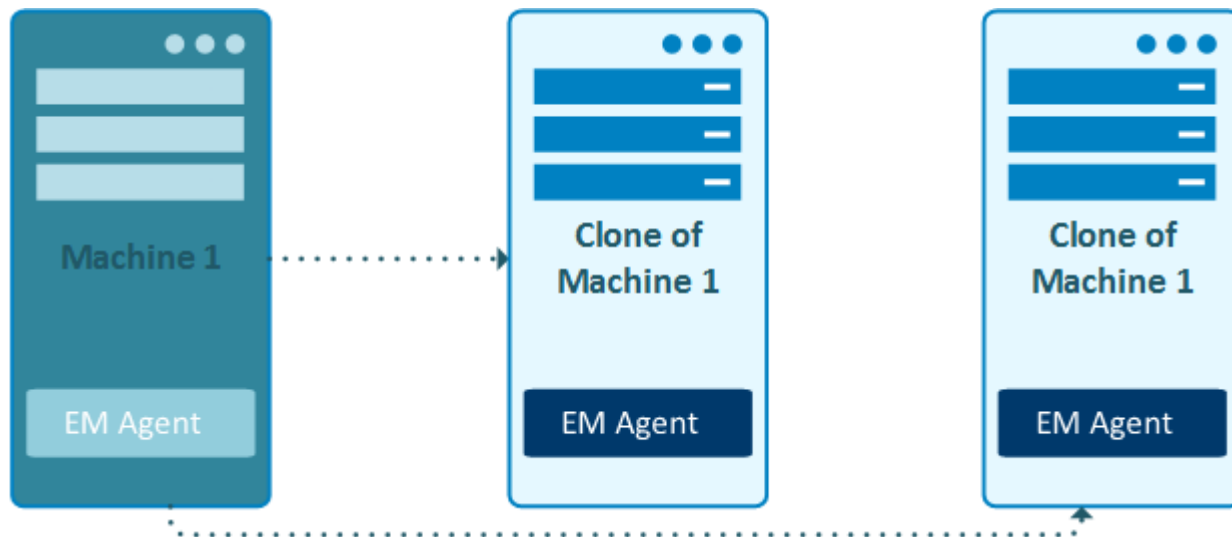
VDIコンピューターの既定のグループ

- ! マスターから複製された新しいコンピューターは、**Lost and found**静的グループに移動します。これは変更できません。



ハイパーバイザーでのコンピューターの複製

標準コンピューターの複製を作成できます。[質問](#)が表示されるまで待ち、今回のみ新しいコンピューターを作成するを選択して解決します。



物理コンピューターへのシステムのイメージ化

ESET Managementエージェントがインストールされたマスターイメージを使用し、物理コンピューターに展開できます。2つの方法でこれを実現できます。

1. システムは、各イメージ展開後に、ESET PROTECTで新しいコンピューターを作成します。

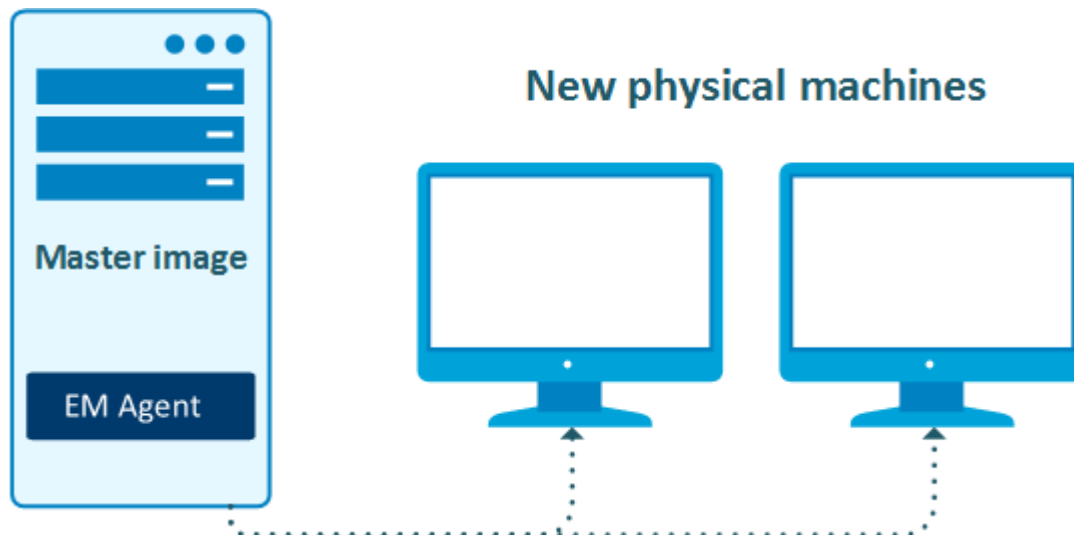
- [質問](#)で各新しいコンピューターを手動で解決し、**毎回新しいコンピューターを作成する**を選択します。
- 複製前にマスターコンピューターにフラグを設定します。**複製のマスターに設定する(新しいコンピューターを作成)**を選択します。

2. イメージが新しいコンピューターに展開された後に、システムはESET PROTECTに新しいコンピューターを作成します。ESET PROTECTで以前の履歴があるコンピューターでイメージが再展開された場合(ESET Managementエージェントが既に展開されている)、このコンピューターはESET PROTECTで前のIDに接続されます。

- [質問](#)で各新しいコンピューターを手動で解決し、**毎回既存のコンピューターと照合する**を選択します。
- 複製前にマスターコンピューターにフラグを設定します。**複製のマスターとして設定する(既存のコンピューターと一致する)**を選択します。



マスターコンピューターのイメージ(またはテンプレート)がある場合、必ず更新した状態を保ってください。マスターコンピューターでESETコンポーネントをアップグレードまたは再インストールした後は、必ずイメージを更新してください。



並列レプリケーション

ESET PROTECTサーバーは、複数のコンピューターの並列レプリケーションを認識し、ESET PROTECTで1つのIDに解決します。このようなイベントは、[コンピューター詳細](#) > [アラート](#)に報告されます(「[同じエージェントIDの複数の接続](#)」)。2つの方法でこの問題を解決できます。

- アラートの[ワンクリック](#)アクションを使用します。コンピューターは分割され、ハードウェア検出は、永久的にオフになります。
- ごくまれに、ハードウェア検出がオフのコンピューターでも競合する場合があります。このような場合、[クローンされたエージェントのリセットタスク](#)が唯一のオプションです。
- コンピューターで[クローンされたエージェントのリセットタスク](#)を実行します。これにより、ハードウェア検出を無効にする必要がありません。

トラブルシューティング

VDIクローンで問題がある場合は、[VDIトラブルシューティング手順](#)を実行します。

複製の質問の解決

コンピューターがESET PROTECTサーバーに接続するたびに、次の2つのフィンガープリントに基づいてエントリが作成されます。

- ESET ManagementエージェントUUID (汎用一意識別子) - ESET Managementエージェントがコンピューターに再インストールされた後に変更されます([二重エージェントの状況](#)を参照)。
- コンピューター[ハードウェアフィンガープリント](#) - コンピューターが複製または再展開された場合には変更されます。

ESET PROTECTサーバーが次のいずれかを検出した場合、質問が表示されます。

- 接続中の複製されたデバイス
- ESET Managementエージェントがインストールされた既存のデバイスのハードウェア変更

ハードウェアフィンガープリント検出は次のシステムではサポートされていません。



- Linux®macOS®Android®iOS
- 仮想エージェントホスト(ESET仮想化セキュリティ)で管理されたシステム
- ESET Managementエージェントがインストールされていないコンピューター

質問をクリックし、**質問の解決**を選択すると、次のオプションのメニューが表示されます。

新しいコンピューターが複製されているか、このコンピューターからイメージ化されます		
毎回既存のコンピューターと一致する	次のときにこのオプションを選択します。 <ul style="list-style-type: none">• コンピューターをマスターとして使用し、すべてのイメージはESET PROTECTで既存のコンピューターエントリに接続します。• コンピューターをマスターとして使用し、VDI環境を設定します。コンピューターはVDIプールにあり、ハードウェアフィンガープリントIDに基づいてIDを回復することが想定されます。	KB記事
毎回新しいコンピューターを作成する	コンピューターをマスターイメージとして使用し、ESET PROTECTがこのコンピューターのすべての複製を新しいコンピューターとして自動的に認識するようにするときには、このオプションを選択します。VDI環境では使用しないでください。	KB記事
今回のみ新しいコンピューターを作成する	コンピューターは1回のみ複製されます。選択すると、複製されたデバイスの新しいインスタンスを作成します。	KB記事
このコンピューターからコンピューターは複製されませんが、ハードウェアが変更されました		
毎回変更されたハードウェアを許可する	このデバイスのハードウェア検出を永久的に無効にします。存在しないハードウェア変更が報告された場合にのみ使用します。 <div>このアクションは元に戻せません。 ハードウェアの検出を無効にした場合は、エージェントとサーバーの両方がこの設定を保存します。エージェントの再展開では、無効なHW検出は復元されません。ハードウェア検出が無効なコンピューターは、ESET PROTECTのVDIシナリオには適していません。</div>	
今回変更されたハードウェアのみを許可する	選択すると、デバイスのハードウェアフィンガープリントを更新します。クライアントコンピューターのハードウェアが変更された後に、このオプションを使用します。今後のハードウェア修正は再度報告されます。	

解決をクリックすると、選択したオプションを送信します。

Resolve question

appears to have connected using different hardware

New computers are being cloned or imaged from this computer

☒ Match with the existing computer every time (mark this computer as master)

i

☐ Create a new computer every time (mark this computer as master)

i

☐ Create a new computer this time only

i

No computers are cloned from this computer, but its hardware has changed

☐ Accept changed hardware every time (disables hardware detection)

i

☐ Accept changed hardware only this time

i

The choice will be applied as soon as the computer is connected.
Data from related computers might not appear until a choice was made.

RESOLVE

GET HELP

CANCEL

二重エージェントの状況

クライアントコンピューターでESET Managementエージェントがアンインストールされ(コンピューターがWebコンソールから削除されない)、再インストールされた場合Webコンソールには2つの同じコンピューターがあります。1つはESET PROTECTに接続し、もう1つは接続していません。この状況は、質問ダイアログウィンドウで処理されません。このような状況は、エージェントの[削除手順](#)が正しくないことが原因です。手動で接続していないコンピューターをWebコンソールから削除する以外に解決策はありません。再インストール前に作成された履歴とログは、その後失われます。

接続していないコンピューターの削除タスクの使用

コンピューターのVDIプールがあり、質問(上記)を正しく解決できなかった場合Webコンソールは、プールからコンピューターを再読み込み後に、新しいコンピューターインスタンスを作成します。コンピューターインスタンスはWebコンソールに累積され、ライセンスが過剰に使用される可能性があります。[接続していないコンピューターを削除するタスク](#)を設定して、問題を解決することは推奨されません。このような手順では、削除されたコンピューターの履歴(ログ)が削除され、ライセンスも過剰に使用される可能性があります。

過剰使用のライセンス

ESET Management AgentがインストールされESETセキュリティ製品がアクティベーションされているクライアントコンピューターが複製されると、複製されたコンピューターはそれぞれ別のライセンスシートを使用できます。このプロセスはライセンスを使いすぎる可能性がありますVDI環境ではESET製品のアクティベーションでオフラインライセンスファイルを使用し、ESETにお問い合わせのうえライセンスを変更してください。

複製されたコンピューターの通知

3つの準備された通知があり、複製関連のアクション、ハードウェアの変更で使用するか、複製関連のイベントを使用して新しいカスタム通知を作成できます。[通知](#)を設定するにはWebコンソールで通知メニューに移動します。


45

- **新しいコンピュータの登録** - コンピューターが選択した静的グループに初めて接続された場合に通知します(グループすべてが既定で選択されます)。
- **コンピュータIDの回復** - コンピューターがハードウェアに基づいて特定された場合に通知します。コンピューターは、マスターコンピューターまたは他のソースから複製されました。
- **潜在的コンピューター複製の検出** - ソースコンピューターが以前にマスターとしてフラグが設定されていない場合は、ハードウェアの大幅な変更または複製について通知します。

トラブルシューティング

VDIクローンで問題がある場合は、[VDIトラブルシューティング手順](#)を実行します。

ハードウェアID

ESET PROTECTは、各管理対象デバイスのハードウェア詳細情報を収集し、特定を試みます。ESET PROTECTに接続されるすべてのデバイスは、 **コンピューターウィンドウのハードウェアID列**に表示される次のカテゴリのいずれかに属します。

- **ハードウェア検出有効** - 検出が有効で、正常に動作しています。
- **ハードウェア検出無効** - 検出はユーザーまたはESET PROTECTサーバーによって自動的に無効にされました。
- **ハードウェア情報なし** - ハードウェア情報がありません。クライアントデバイスがサポート対象外のOSまたは古いバージョンのESET Managementエージェントで実行されています。
- **ハードウェア検出を信頼できません** - 検出はユーザーによって信頼できないと報告され、無効にされます。このステータスは、検出が無効化される前に、1つのレプリケーション期間にのみ発生することがあります。

複製のためのマスター

[コンピューターの詳細](#)で、**仮想化 > 複製のマスターに設定**をクリックすると、次のポップアップウィンドウが表示されます。

Master for Cloning
×

When setting the master for cloning, there are two options available.
Use **Match with existing computers** if you require clones to recover their previous computer identities.
Use **Create new computers** if you require each new clone to be recognized as a new computer.
[More information about VDI, cloning and hardware detection](#)

Cloned computers identity handling

☒ Match with existing computers
☐ Create new computers

Recovering computer identities may lead to creating unwanted new identities if the cloned machine's provisioning has not yet been finished. To prevent this behavior, set the **clone naming pattern**. Please note that clones are recognized as such only if their **naming pattern set in the VDI environment matches their naming pattern set for the master for cloning**.
[More information about the VDI naming pattern](#)

☒ Identify clones by VDI naming pattern

VDI naming pattern for clones ⓘ

VM-instant-clone-{n}

SAVE

CANCEL

VDIプールを作成する前に、複製されたコンピュータのID処理オプションのいずれかを選択することをお勧めします。

- 既存のコンピューターと照合 - [毎回既存のコンピューター照合](#) オプションを参照してください。
- 新しいコンピューターを作成 - [毎回新しいコンピューターを作成](#) オプションを参照してください。

VMware インスタントクローンまたは Citrix XenCenter/XenServer マシンカタログを使用しない場合は、VDI 命名パターン設定をスキップし、**保存** をクリックします。後からコンピューター詳細で、複製のマスター設定を変更できます。

- 仮想化タイルの歯車アイコンをクリックして、設定を調整します。
- 仮想化 > 複製のマスターの設定解除をクリックして、設定を削除します。

ESET PROTECT 9.0は以下をサポートします：

- [VMware Horizon 8.x インスタントクローン](#)
- [Citrix XenCenter/XenServer 8以上のマシンカタログ](#)

VMware インスタントクローンまたは Citrix XenCenter/XenServer マシンカタログを設定する場合は、VDI 命名パターン設定を指定します。

1.VDI命名パターンで複製を特定チェックボックスをオンにします。

2.複製のVDI命名パターンを入力します。

VDI命名パターン

ESET PROTECTは、VDI環境で設定された命名パターンと一致する名前の複製のみを認識します。

- **VMware** – 命名パターンには、「VM-instant-clone-{n}」などの形式で、VDIインフラストラクチャによって生成された一意の番号{n}に指定されたプレースホルダーが必要です。命名パターンの詳細については、[VMwareマニュアル](#)を参照してください。
- **Citrix XenCenter/XenServer** – マシンカタログの命名体系でハッシュ#を使用します。例：VM-office-##命名方法の詳細については、[Citrixマニュアル](#)を参照してください。

3.[保存]をクリックします。 後からコンピューター詳細で、複製のマスター設定を変更できます。

- 仮想化タイルの歯車アイコンをクリックして、設定を調整します。
- 仮想化>複製のマスターの設定解除をクリックして、設定を削除します。

トラブルシューティング

VDIクローンで問題がある場合は、[VDIトラブルシューティング手順](#)を実行します。

ESET Management エージェント展開

このセクションでは、ネットワーク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するために使用できるすべての方法を説明します。エージェントは非常に重要です。クライアントコンピューターで実行中のESETセキュリティソリューションは、エージェント経由でのみESET PROTECTサーバーと通信するためです。

ESET PROTECT構造へのクライアントコンピューターの追加

ネットワークでクライアントコンピューターの管理を開始する前に、ESET PROTECTに追加する必要があります。次の方法のいずれかを使用して追加します。

- [Active Directory同期](#)
- [RD Sensor](#)
- [新しいデバイスを手動で追加する](#)

ESET Management エージェント展開

ESET Managementエージェント展開には複数の方法があります。エージェントをローカルまたはリモートで展開できます。

- [ローカル展開](#) - ESET Management (エージェントとESETセキュリティ製品)を、クライアントコンピューターにローカルインストールします。

i 小規模なネットワーク(最大50コンピューター)の場合にのみ、ローカル展開を使用することをお勧めします。より大きいネットワークの場合は、[GPOおよびSCCMを使用してESET Managementエージェントを展開](#)できます。

- [リモート展開](#) – クライアントコンピューターの数が多い場合のESET Managementエージェントの展開では、この方法を使用することをお勧めします。

Deploy Agent

Agent connects computers to ESET PROTECT and allows you to manage them remotely. Select the deployment method appropriate for your network.

LOCAL DEPLOYMENT

- ☒ Create **All-in-one Installer** (Windows only)
- ☐ Create **Agent Live Installer**
- ☐ **Download Agent** from ESET website

REMOTE DEPLOYMENT

- ☐ Use **GPO or SCCM** for deployment
- ☐ Server Task **Agent installation**
- ☐ Use the standalone **Deployment Tool**

Create All-in-one Installer (Windows only)

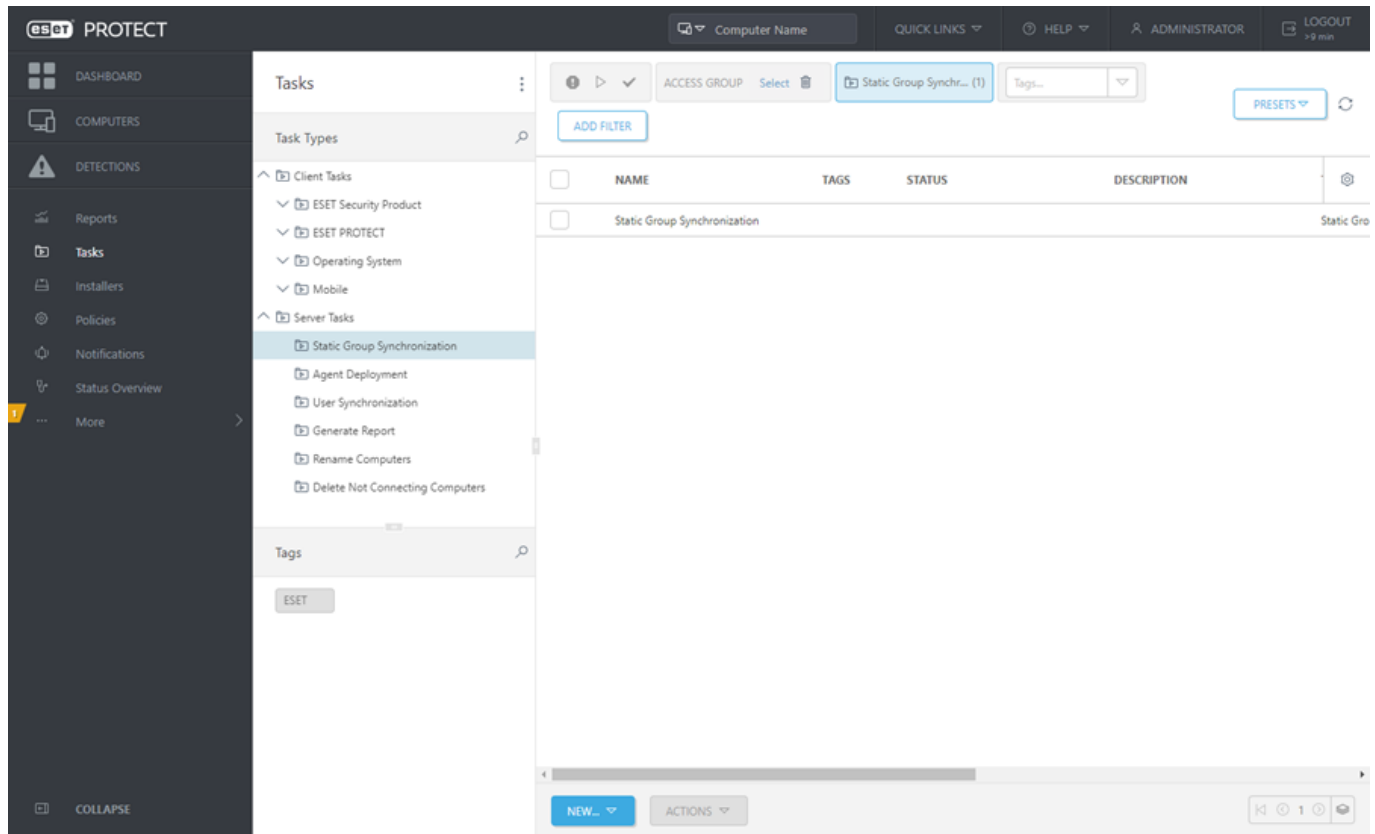
Live Installer will automatically download and install a product and connect your device to ESET PROTECT.

CREATE INSTALLER **SELECT EXISTING**

CANCEL

Active Directory同期を使用してコンピューターを追加する

AD同期は、**静的グループ同期**サーバータスクを実行して行われます。ESET PROTECTインストール中に自動的に実行するように選択できる定義済みの既定のタスクです。コンピューターがドメインにある場合、同期が実行され、ADからのコンピューターが既定のグループの **すべて**に一覧表示されます。



同期処理を開始するには、タスクをクリックして、**[今すぐ実行]**を選択します。[新しいAD同期タスクを作成する](#)必要がある場合は、ADから新しいコンピューターを追加するグループを選択します。また、同期元のADのオブジェクトと、重複の場合の処理を選択します。ADサーバー接続設定を入力し、[\[同期モード\]](#)を**Active Directory/Open Directory/LDAP**に設定します。この[ESETナレッジベース記事](#)の段階的な手順に従います。


新しいデバイスを手動で追加する

この機能では、自動的に検出または追加されないコンピューターまたはモバイルデバイスを手動で追加できます。コンピューターまたはグループタブから、新しいコンピューターまたはモバイルデバイスを追加できます。

1. 新しいコンピューターを追加するには、**[コンピューター]**> **[新規追加]**をクリックしてから、**[コンピューター]**を選択(あるいは既存の**[静的グループ]**の横の⚙️をクリックしてから**[新規追加]**をクリック)します。

2. **コンピューターの追加** – いくつかの方法で追加できます。

o 追加するコンピューターの**IPアドレス**または**ホスト名**を入力するとESET PROTECTがネットワーク上で検索します。必要に応じて、コンピューターの**[説明]**を入力できます。

o **[デバイスの追加]**をクリックして、その他のデバイスを追加します。デバイスのリストからコンピューターを削除する場合は、**ごみ箱アイコン**  をクリックするか、**[すべて削除]**をクリックします。

o **[CSVのインポート]**をクリックして、追加するコンピューターのリストを含む.csvファイルをアップロードします。詳細については、[CSVのインポート](#)を参照してください。

o **[コピーと貼り付け]**をクリックして、カスタム区切り文字で区切られたコンピューターのカス

タムリストを貼り付けます。この機能は.csvインポートと同様に機能します。

3. **タグを選択**をクリックして、[タグを割り当て](#)ます。

4. **親グループ** – 既存の親グループを選択してから、**OK**をクリックします。

5. **FQDN解決を使用する**:

☐ チェックボックスをオンにするとESET PROTECTサーバーは、指定されたIPアドレスまたはコンピューターホスト名を完全修飾ドメイン名に変換します。

☐ チェックボックスをオフにして、指定されたコンピューター名をインポートします。このオプションではFQDN形式の名前でのコンピューターの一括インポート(たとえば、.csvからのインポート)が高速になります。

6. 追加しているコンピューターが既に ESET PROTECTにある場合は、**[競合解決]**ドロップダウンメニューを使用して、実行するアクションを選択します。

- **検出されたときに確認**: 競合が検出された場合、プログラムのアクション(以下のオプションを参照)を選択するように求められます。
- **重複するデバイスをスキップする**: 重複するコンピューターは追加されません。
- **重複するデバイスを作成する**: 新しいコンピューターが追加されますが、異なる名前になります。
- **重複するデバイスをグループに移動...**: 競合するコンピューターは**親グループ**に移動されます。

7. 変更が完了したら、**[追加]**をクリックします。

The screenshot displays the 'Add Computers' page in the ESET PROTECT web interface. The left sidebar contains navigation links: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies, Notifications, Status Overview, and More. The main content area has a breadcrumb trail: < BACK Computers > Add Computers. The 'Add Computers' section includes a sub-header 'List of devices' and a table with two columns: NAME and DESCRIPTION. A single row is present with 'Device_1' and 'Description_1'. To the right of the table is a 'Remove All' link. Below the table are three buttons: '+ ADD DEVICE', 'IMPORT CSV...', and 'COPY & PASTE'. Further down, the 'Tags' section has a 'Select tags' link. The 'Settings' section includes a 'Parent Group' dropdown set to '/All/Lost & found', a 'Use FQDN resolution' checkbox that is checked, and a 'Conflict Resolution' dropdown set to 'Ask when detected'. At the bottom of the form are 'ADD' and 'CANCEL' buttons.

i 複数のコンピューターを追加すると時間が長くなる場合があります(逆DNS検索を実行する場合があります。上記の**FQDN解決の使用**を参照してください)。

8. 追加するデバイスのリストが表示されたポップアップウィンドウが開きます。**OK**または[エージェントの展開](#)をクリックできます。

9. エージェントの**展開**をクリックした場合は、実行する展開タイプを選択します。

Deploy Agent

Agent connects computers to ESET PROTECT and allows you to manage them remotely. Select the deployment method appropriate for your network.

LOCAL DEPLOYMENT

- ☒ Create **All-in-one Installer** (Windows only)
- ☐ Create **Agent Live Installer**
- ☐ **Download Agent** from ESET website

REMOTE DEPLOYMENT

- ☐ Use **GPO** or **SCCM** for deployment
- ☐ Server Task **Agent installation**
- ☐ Use the standalone **Deployment Tool**

Create All-in-one Installer (Windows only)

Live Installer will automatically download and install a product and connect your device to ESET PROTECT.

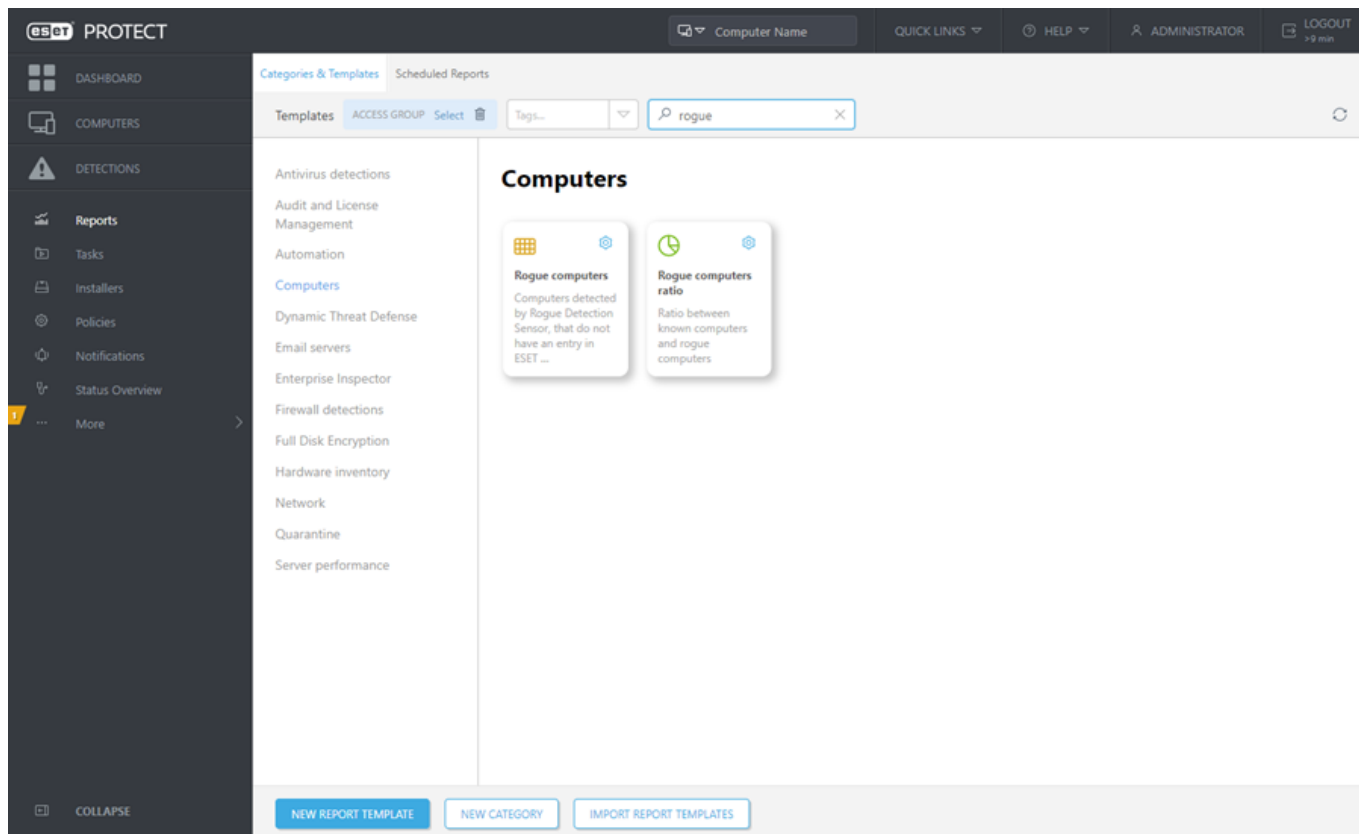
CREATE INSTALLER **SELECT EXISTING**

CANCEL

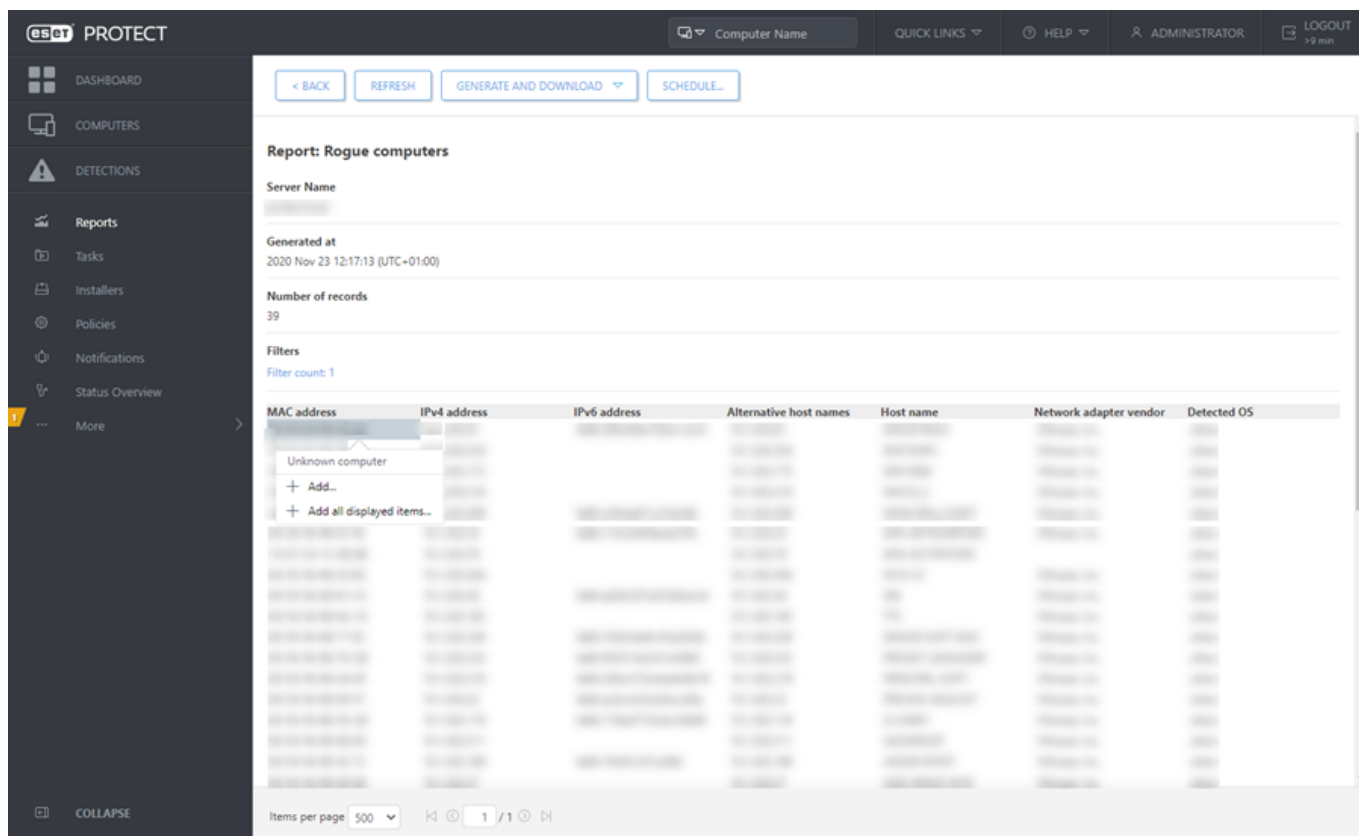
RD Sensorを使用してコンピューターを追加する

[AD同期](#)を使用していない場合、ネットワーク構造の管理されていないコンピューターを検索する最も簡単な方法は、RD Sensorを使用することです。RD Sensorは、展開されたネットワークを監視し、エージェントがない新しいデバイスがネットワークに接続するときに、この情報をESET PROTECTに報告します。

レポートの中で、コンピューターセクションに移動し、**管理対象外のコンピューターレポート**をクリックします。




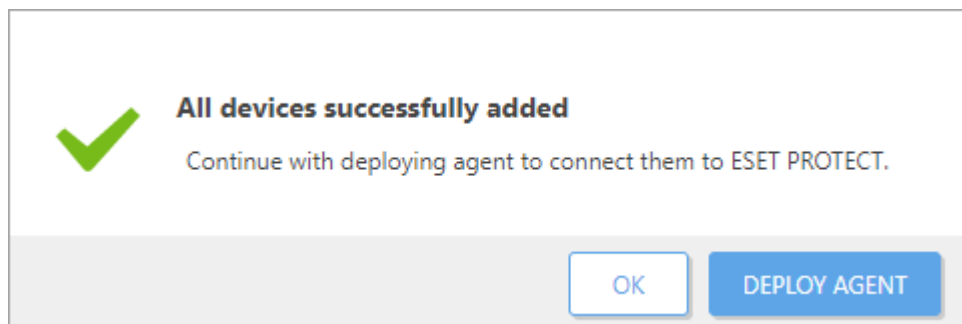
管理対象外のコンピューターレポートにはRDSensorで検出されたコンピューターが一覧表示されます。[RDSensorポリシー](#)を使用するとRDSensorによって報告された情報を調整できます。コンピューターを追加するには、追加するコンピューターをクリックするか、表示されているすべての項目を追加できます。



1つのコンピューターを追加している場合は、定義済みの名前を使用するか、独自の名前を指定できます（これは、実際のホスト名ではなくESET PROTECT Webコンソールで使用される表示名です）。必要に応じ

て、説明も追加できます。コンピューターが既にESET PROTECTディレクトリに存在する場合、通知が表示され、重複したコンピューターの処理方法を決定できます。使用可能なオプションは次のとおりです。**エージェントの展開** **スキップ** **再試行** **移動** **複製** **キャンセル**。コンピューターが追加されると、**エージェントの展開** オプションでポップアップウィンドウが開きます。

[すべての表示されている項目を追加]をクリックすると、追加するコンピューターのリストが表示されます。この時点でESET PROTECTディレクトリに含めない場合は、特定のコンピューターの横にある  をクリックします。リストからコンピューターを削除したら、[追加]をクリックします。[追加]をクリックしたら、重複が検出された場合の処理を選択します(リストのコンピューター数によっては少し遅延する場合があります)。オプションは次のとおりです。**スキップ**、**再試行**、**移動** **複製** **キャンセル**。オプションを選択したら、ポップアップウィンドウが開きます。これらのコンピューターで**エージェントの展開**を実行するオプションが選択されています。



RDSensor検査の結果は、`detectedMachines.log`ログファイルに書き込まれます。これには、ネットワーク上で検出されたコンピュータのリストが含まれます。`detectedMachines.log`ファイルは次の場所にあります。

- Windows

`C:\ProgramData\ESET\Rogue Detection Sensor\Logs\detectedMachines.log`

- Linux

`/var/log/eset/RogueDetectionSensor/detectedMachines.log`

ESET Rogue Detection Sensorポリシー設定

ポリシーを使用してESET RD Sensorの動作を変更できます。これは一般的にアドレスのフィルタリングを変更するために使用されます。たとえば、検出されないように、特定のアドレスをブラックリストに含めることができます。

[ポリシー]をクリックし、[カスタムポリシー]を展開して、既存のポリシーを編集するか、新しいポリシーを作成します。

フィルタ

IPv4フィルター

IPv4アドレスフィルタリングを有効にする – フィルタリングを有効にするとIPv4フィルタリストのホワイトリストに含まれるか、ブラックリストに含まれないIPアドレスだけが検出されます。

フィルター – リストがホワイトリストかブラックリストかを指定します。

IPv4アドレスリスト – [IPv4リストの編集]をクリックして、リストからアドレスを追加または削除します。

MAC アドレスプレフィックスフィルター

MAC アドレスプレフィックスフィルタリングを有効にする – フィルタリングを有効にすると、MAC アドレスプレフィックス (xx:xx:xx) アドレスが MAC アドレスリストに含まれるコンピューターのみが検出されるか、ブラックリストに含まれないコンピューターを検出します。

フィルタリングモード – リストがホワイトリストかブラックリストかを指定します。

MAC アドレスプレフィックスリスト - [MAC プレフィックスリストの編集] をクリックして、リストからプレフィックスを追加または削除します。

検出

アクティブな検出 – このオプションを有効にすると、RD Sensor はローカルネットワークのコンピューターをアクティブに検索できます。これにより検索結果が改善されますが、一部のコンピューターでファイアウォール警告が発生することがあります。

OS 検出ポート - RD Sensor は定義済みのポートのリストを使用して、ローカルネットワークのコンピューターを検索します。ポートリストを編集できます。

詳細設定

製品改善プログラムに参加 – 顧客経験の向上のため、匿名のクラッシュレポート統計を ESET に送信することを有効または無効にします。

割り当て

このポリシーを受信するクライアントを指定します。**[割り当て]** をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。ポリシーを適用するコンピューターを選択し、**OK** をクリックします。

概要

このポリシーの設定を確認し、**[完了]** をクリックします。

ローカル展開

この展開方法は、オンプレミスインストール向けです。インストールパッケージを作成またはダウンロードし、共有フォルダー、フラッシュドライブ、電子メール経由でのアクセスを許可します。



インストーラーパッケージは、管理者または管理者権限があるユーザーによってインストールされる必要があります。



小規模なネットワーク (最大 50 コンピューター) の場合にのみ、ローカル展開を使用することをお勧めします。より大きいネットワークの場合は、[GPO および SCCM を使用して ESET Management エージェントを展開](#) できます。

ローカル展開は次の3つの方法で実行できます。

- [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する](#) (Windows のみ)
- [エージェント ライブ インストーラーの作成](#) (Windows、Linux、macOS)

- [Webサイトからエージェントをダウンロード](#) (Windows/Linux/macOS)

ローカル展開と権限

ESET Managementエージェントをローカルで展開できるようにする方法については、この[例](#)の手順に従ってください。

i ユーザーがインストーラーを作成するときには、[証明書](#)を操作できます。証明書が含まれる静的グループアクセスの[証明書の使用](#)アクセス権をユーザーに割り当てる必要があります。ユーザーがESET Managementエージェントを展開する場合、実際のサーバー証明書が署名される認証機関の使用権限を割り当てる必要があります。証明書と認証局へのアクセスを分割する方法については、この[例](#)をお読みください。アクセス権の詳細については、[権限の一覧](#)を参照してください。

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する

オールインワンインストーラー(ESET ManagementエージェントとESETセキュリティ製品を含む)パッケージを作成する手順は、[スタートアップウィザード](#)に似ています。

! 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。

メニューバーのクイックリンクセクションで、[他の展開オプション]をクリックします。[エージェントの展開]ウィンドウで、[オールインワンインストーラーの作成(Windowsのみ)]の下に[インストーラーの作成]をクリックします。オールインワンインストーラーを作成ウィンドウが開きます。

基本

クラッシュレポートと匿名のテレメトリデータ(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に送信することに同意しない場合は、[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フにします。チェックボックスがオンの場合、テレメトリデータとクラッシュレポートがESETに送信されます。

パッケージの内容 - 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。
- **完全ディスク暗号化** - 暗号化オプションは、有効な[ESET Full Disk Encryption](#)ライセンスでのみ表示されます。
- **Enterprise Inspectorエージェント** - ESET Enterprise Inspectorエージェントをインストーラーに含めます。

セキュリティ製品

1. **ライセンス** (任意) - [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。既に[ライセンス管理](#)に既存のライセンスがある場合は、使用するライセンスを選択し、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。ライセンスがない場合は、ライセンスなしでインストーラーを作成し、[製品を後からアクティベーション](#)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、そのグループのライセンスに対する**書き込み**権限がある管理者にのみ許可されています。

2. **製品** - ESET Managementエージェントと一緒にインストールするESETセキュリティ製品を選択します。

i 製品インストールファイルが表示されない場合は、リポジトリが**AUTOSELECT**に設定されていることを確認します。詳細については、[サーバー設定](#)の**詳細設定**セクションを参照してください。

3. **言語** - ESETセキュリティ製品インストーラーの言語バージョンを選択します。

4. 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。

5. **保護設定** - 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。

インストーラーでこれらの保護設定を定義せず、後からポリシーで設定する場合は、**今すぐ保護設定を定義しない**チェックボックスをオンにします。

6. [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。詳細については、[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](#)を参照してください。

Enterprise Inspectorエージェント

ESET Enterprise Inspectorエージェント要件:

- ESET Enterprise InspectorエージェントをアクティベーションするにはESET Enterprise Inspector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。

1. **ライセンス** (任意) - インストール中にESET Enterprise InspectorエージェントをアクティベーションするESET Enterprise Inspectorライセンスを選択することをお勧めします。ライセンスなしでインストーラーを作成する場合は、後からESET Enterprise Inspectorエージェントをアクティベーションできます。

2. **製品/バージョン** - ESET Enterprise Inspectorエージェントのバージョンを選択します。最新の使用可能なバージョンがあらかじめ選択されています。

3. **設定ポリシー** (任意) - 既存のESET Enterprise Inspectorエージェントポリシーを選択し、ESET Enterprise Inspectorエージェントインストール中にポリシー設定を適用します。

4. [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。詳細については、[ESET製品のエンドユーザーライセンス契約\(EULA\)と利用規約、およびプライバシーポリシー](#)を参照してください。


5. ESET Enterprise Inspectorサーバーホスト名と、ESET Enterprise Inspector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)。


6. ESET Enterprise Inspectorサーバーに接続するための認証局を選択します。

証明書

ピア証明書およびESET PROTECT認証局が使用可能な証明書に基づいて自動的に選択されます。自動的に選択されたものとは別の証明書を使用する場合は、**ESET PROTECT証明書**をクリックし、使用可能な証明書のリストを表示して、使用する証明書を選択します。[カスタム証明書](#)を使用する場合は、ラジオボタンをクリックして、.pfx証明書ファイルをアップロードします。

必要に応じて、**証明書パスフレーズ**を入力します。たとえばのESETPROTECTインストール中にパスフレーズを指定した場合、またはパスフレーズ付きのカスタム証明書を使用する場合は、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.exe ファイルに埋め込まれているため、抽出できます。

詳細

このセクションで、オールインワンインストーラーパッケージをカスタマイズできます:

- 任意で、パッケージインストーラーの**名前**を変更し、**説明**を入力できます。
- タグを選択**をクリックして、[タグを割り当て](#)ます。
- 親グループ(任意)** - インストール後にコンピューターが配置され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。
- ESET AV Remover** - 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。
- 初期インストーラー設定(任意)** - [設定ポリシー](#)をESET Managementエージェントに適用する場合に、このオプションを使用します。**エージェント設定(任意)**の下で**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。
- 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**を指定できます(既定は2222)。
- HTTPプロキシを使用する場合は、**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。HTTPプロキシは既定でポート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。

! 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す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]**をクリックします。

9. 生成されたオールインワンインストーラー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。

o32ビットバージョンをダウンロード (例: *PROTECT_Installer_x86_en_US.exe*)

o64ビットバージョンをダウンロード (例: *PROTECT_Installer_x64_en_US.exe*)

oARM64バージョン (例: *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。ESET PROTECTサーバーはローカルでオールインワ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。

10. 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。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。

エージェントライブインストーラーの作成 - Windows/Linux/macOS

このタイプのエージェント展開は、リモートおよびローカル展開オプションが環境で動作しない場合に使用できます。このような場合、電子メールでエージェントライブインストーラを配布し、ユーザーに展開させることができます。また、エージェントライブインストーラは、リムーバブルメディア(USBフラッシュドライブなど)から実行することもできます。

! エージェントインストールパッケージをダウンロードし、ESET PROTECTサーバーに接続するには、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必要があります。

メニューバーのクイックリンクセクションで、**他の展開オプション**をクリックします。**[エージェントの展開]**ウィンドウで、**[エージェントライブインストーラーの作成]**を選択し**[インストーラーの作成]**ボタンをクリックします。エージェントライブインストーラーウィンドウが開きます。

パッケージの作成

クラッシュレポートと匿名のテレメトリデータ(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に送信することに同意しない場合は、**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フにします。チェックボックスがオンの場合、テレメトリデータとクラッシュレポートがESETに送信されます。

証明書

ピア証明書およびESET PROTECT認証局が使用可能な証明書に基づいて自動的に選択されます。自動的に選択されたものとは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リストを表示して、使用する証明書を選択します。**カスタム証明書**を使用する場合は、ラジオボタンをクリックして、**.pfx**証明書ファイルをアップロードします。詳細については、[のカスタム証明書ESET PROTECT](#)を参照してください。

必要に応じて、**証明書パスフレーズ**を入力します。たとえばのESETPROTECTインストール中にパスフレーズを指定した場合、またはパスフレーズ付きのカスタム証明書を使用する場合です。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。

設定

このセクションで、エージェントライブラインストーラーパッケージの次の設定をカスタマイズできます。

1. 任意で、パッケージインストーラーの**名前**を変更し、**説明**を入力できます。
2. **タグを選択**をクリックして、[タグを割り当て](#)ます。
3. **エージェント設定(任意)** - [設定ポリシー](#)をESET Managementエージェントに適用する場合に、このオプションを使用します。**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。
4. **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**を指定できます(既定は2222)。
5. **親グループ(任意)** - インストール後にコンピューターが配置され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。
6. HTTPプロキシを使用する場合は、**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。プロキシの詳細については、[こちら](#)をお読みください。



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す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。

7. [完了]をクリックして「Windows」「Linux」およびmacOSエージェントインストーラファイルのリンクを生成します。

Packages to download

Agent installer for Windows
[Download](#)

Agent installer for Linux
[Download](#)

Agent installer for Mac
[Download](#)

8. ダウンロードするインストーラファイルの下の**ダウンロード**をクリックし、*zip*ファイルを保存します。

9. ESET Managementエージェントを展開するクライアントコンピューターでファイルを展開し、*PROTECTAgentInstaller.bat* (Windows)または*PROTECTAgentInstaller.sh*スクリプト (LinuxおよびMacOS)を実行して、インストーラを実行します。

- i

 - 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します。エージェントの問題がある場合「ESET PROTECTサーバーに接続していない場合など」は、[トラブルシューティング](#)を参照してください。
 - ESET PROTECT9.0は、管理されたコンピューターでの[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。

カスタムリモートロケーションからの展開

ESETリポジトリ以外の場所からエージェントを展開するには、インストールスクリプトを修正し、エージェントパッケージがある新しいURLを指定します。新しいパッケージのIPアドレスを使用できます。

次の行を見つけて修正します。

Windows:

```
set
url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x64.msi
set
url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_x86.msi
set
url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent_arm64.msi
```

Linux:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9.../agent-linux-i386.sh
```

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9  
.../agent-linux-x86_64.sh
```

macOS:

```
eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v9  
.../agent_macosx_x86_64.dmg
```

ローカル共有フォルダーからの展開

ESETリポジトリダウンロードサーバーを使用せずに、ローカル共有フォルダーからエージェントライブインストーラーを使用してESET Managementエージェントを展開する場合は。

- ESET Managementエージェントインストーラーとエージェントライブインストーラーが同じフォルダーにある場合

a) Windows/Linux/macOS版のエージェントライブインストーラースクリプトを作成します。

b) テキストエディターでエージェントライブインストーラーを開き、ESET ManagementエージェントインストーラーのESETリポジトリURLダウンロードリンクを検索します(上記の[カスタムリモート場所からの展開](#)を参照)。

c) ESETリポジトリからESET Managementエージェントインストーラーをダウンロードします。

d) エージェントライブインストーラーとESET Managementエージェントインストーラーを同じフォルダーに配置します。

e) エージェントライブインストーラーは、同じフォルダーにあるESET Managementエージェントインストーラーを自動的に検出します。



エージェントライブインストーラーで参照されるのと同じESET Managementエージェントインストーラーバージョンとファイル名(.msi、.dmg、.sh)を使用します。

- ESET Managementエージェントインストーラーとエージェントライブインストーラーが別のフォルダーにある場合は、次の手順に従います。

Windows:

1. .msiエージェントインストーラーをローカルディレクトリにコピーします。
2. PROTECTAgentInstaller.batファイルを編集し、ローカルエージェントインストーラーを使用します。

- agent_x64.msi

a) 行set url=%installDirectory%\agent_x64.msiを変更し、ローカルダウンロードファイルを参照します。

b) 行set url=%installDirectory%\agent_x64.msiの前にcopy /y
\\server\share\agent_x64.msi %installDirectory%コマンドを追加します。

- agent_x86.msi

a)行set url=%installDirectory%\agent_x86.msiを変更し、ローカルダウンロードファイルを参照します。

b)行set url=%installDirectory%\agent_x86.msiの前にcopy /y \\server\share\agent_x86.msi %installDirectory%コマンドを追加します。

• agent_arm64.msi

a)行set url=%installDirectory%\agent_arm64.msiを変更し、ローカルダウンロードファイルを参照します。

b)行set url=%installDirectory%\agent_arm64.msiの前にcopy /y \\server\share\agent_arm64.msi %installDirectory%コマンドを追加します。

元のファイルは次のようになります。

```
37
38 set url=http://repository.eset.com/vl/com/eset/apps/business/era/agent/v8/8.1.1188.0/agent_x64.msi
39 set checksum=e72d5da32819367e7fe81688df302291c19019e5
40 if defined IsArch_x86 (
41   set url=http://repository.eset.com/vl/com/eset/apps/business/era/agent/v8/8.1.1188.0/agent_x86.msi
42   set checksum=5e3441ca2eadb0e99930deb9f9315eda7d7cf8de
43 )
44 if defined IsArch_arm64 (
45   set url=http://repository.eset.com/vl/com/eset/apps/business/era/agent/v8/8.1.1188.0/agent_arm64.msi
46   set checksum=0d2103cbf7a00cf62c06ffcaecacf3aa25fal337
47 )
```

以下の更新されたファイルを参照してください。独自のURL(ローカル共有フォルダ)を使用しますが、%installDirectory%を変更しないでください。

```
37
38 copy /y \\server\share\agent_x64.msi %installDirectory%
39 set url=%installDirectory%\agent_x64.msi
40 set checksum=e72d5da32819367e7fe81688df302291c19019e5
41 if defined IsArch_x86 (
42   copy /y \\server\share\agent_x86.msi %installDirectory%
43   set url=%installDirectory%\agent_x64.msi
44   set checksum=5e3441ca2eadb0e99930deb9f9315eda7d7cf8de
45 )
46 if defined IsArch_arm64 (
47   copy /y \\server\share\agent_arm64.msi %installDirectory%
48   set url=%installDirectory%\agent_arm64.msi
49   set checksum=0d2103cbf7a00cf62c06ffcaecacf3aa25fal337
50 )
```



エージェントライブインストーラーは、checksumに基づいてインストールファイルの整合性を確認します。これは各ファイルで生成された固有の文字列です。ファイル変更の場合checksumも変更されます。



インストールパッケージが実行されるユーザーアカウントにローカル共有フォルダーへの書き込み権限があることを確認してください。パスにはスペースを使用できます。たとえば、\\server\share\Agent_x64.msi (引用符""は使用しない)です。

3. 次の行を置換します。

```
" echo.packageLocation = DownloadUsingHTTPProxy^("!url!", "!http_proxy_hostname!",
"!http_proxy_port!", "!http_proxy_username!", "!http_proxy_password!"^)
```

```

100 echo On Error Resume Next
101 echo.packageLocation = DownloadUsingHTTPProxy^("url!", "http_proxy_hostname!", "http_proxy_port!", "http_proxy_username!", "http_proxy_password!")
102 echo.If packageLocation = "" Then

```

変更後: echo.packageLocation = "!url!"

```

100 echo.On Error Resume Next
101 echo.packageLocation = "!url!"
102 echo.If packageLocation = "" Then

```

4. ファイルを保存します。

macOS:

1. テキストエディターで *PROTECTAgentInstaller.sh* スクリプトを開きます。
2. 次の行を削除します。62-69および73-86。

```

62 arch=$(uname -m)
63 eraa_installer_url="http://repository.eset.com/v1/com/ese/ap/business/era/agent/v8/8.0.3209.0/agent_macosx_x86_64.dmg"
64 eraa_installer_checksum="1ef3bb053159574e691397d0149d7492659dce12"
65 if $(echo "$arch" | grep -E "(x86_64|amd64)$" 2>&1 > /dev/null)
66 then
67     eraa_installer_url="http://repository.eset.com/v1/com/ese/ap/business/era/agent/v8/8.0.3209.0/agent_macosx_x86_64.dmg"
68     eraa_installer_checksum="1ef3bb053159574e691397d0149d7492659dce12"
69 fi
70
71 echo "ESET Management Agent live installer script. Copyright © 1992-2020 ESET, spol. s r.o. - All rights reserved."
72
73 if test ! -z $eraa_server_company_name
74 then
75     echo " * CompanyName: $eraa_server_company_name"
76 fi
77 echo " * Hostname: $eraa_server_hostname"
78 echo " * Port: $eraa_server_port"
79 echo " * Installer: $eraa_installer_url"
80 echo
81
82 if test -z $eraa_installer_url
83 then
84     echo "No installer available for '$arch' architecture."
85     exit 1
86 fi

```

3. 以下でハイライトされた行をローカルインストーラーへのパスで置換します(独自のローカル共有フォルダーパスを使用)。

```
local_dmg= "/path_to_local_agent/agent_macos_x86_64.dmg"
```

```

146 done < "$local_migration_list"
147
148 local_dmg="$(mktemp -q -u /tmp/EraAgentOnlineInstaller.XXXXXXXX) "
149 echo "Downloading installer image '$seraa_installer_url':"
150
151 eraa_http_proxy_value=""
152 if test -n "$seraa_http_proxy_value"
153 then
154     export use_proxy=yes
155     export http_proxy="$seraa_http_proxy_value"
156     (curl --fail --connect-timeout 300 --insecure -o "$local_dmg" "$seraa_installer_url" || curl --fail --
157     connect-timeout 300 --noproxy "*" --insecure -o "$local_dmg" "$seraa_installer_url") && echo "$local_dmg"
158     >> "$files2del"
159 else
160     curl --fail --connect-timeout 300 --insecure -o "$local_dmg" "$seraa_installer_url" && echo "$local_dmg"
161     >> "$files2del"
162 fi
163
164 if test ! -s "$local_dmg"
165 then
166     echo "Failed to download installer file"
167     exit 2
168 fi
169
170 /bin/echo -n "Checking integrity of of downloaded package " && echo "$seraa_installer_checksum $local_dmg"
171 | shasum -c

```

```

146 done < "$local_migration_list"
147
148 local_dmg= "/path_to_local_agent/agent_macos_x86_64.dmg"
149
150 local_mount="$(mktemp -q -d /tmp/EraAgentOnlineInstaller.XXXXXXXX) " && echo "$local_mount" | tee
151 "$dirs2del" >> "$dirs2umount"

```

4. ファイルを保存します。

Linux:

1. テキストエディターで *PROTECTAgentInstaller.sh* スクリプトを開きます。
2. 次の行を削除します。32および33:

```

31 arch=$(uname -m)
32 eraa_installer_url=
33 "http://repository.eset.com/v1/com/eset/apps/business/era/agent/v8/8.0.2216.0/agent_linux_i386.sh"
34 eraa_installer_checksum="7994d7c3199ed817ea7ff84f22a05a2d2585a233"
35
36 if $(echo "$arch" | grep -E "(x86_64|amd64)$" 2>&1 > /dev/null)

```

3. 次の行とローカルインストーラーへのパスを入力します。

```

31 arch=$(uname -m)
32 local_installer="/path_to_local_agent/agent_linux_i386.sh"
33
34 if $(echo "$arch" | grep -E "(x86_64|amd64)$" 2>&1 > /dev/null)

```

4. 行36 - 54をローカルx86_64インストーラーへのパスで置換します。画像でハイライトされた領域を参照してください。固有のURL(ローカル共有フォルダー)を使用します(以下の例は使用しない)。

```

35 then
36     eraa_installer_url=
37     "http://repository.eset.com/v1/com/eset/apps/business/era/agent/v8/8.0.2216.0/agent_linux_x86_64.sh"
38     eraa_installer_checksum="756004e83b290c45ef4a482207d0d2759e68b6a7"
39 fi
40 echo "ESET Management Agent live installer script. Copyright © 1992-2020 ESET, spol. s r.o. - All rights
reserved."
41
42 if test ! -z $eraa_server_company_name
43 then
44     echo " * CompanyName: $eraa_server_company_name"
45 fi
46 echo " * Hostname: $eraa_server_hostname"
47 echo " * Port: $eraa_server_port"
48 echo " * Installer: $eraa_installer_url"
49 echo
50
51 if test -z $eraa_installer_url
52 then
53     echo "No installer available for '$arch' architecture."
54     exit 1
55 fi

```

```

34 if $(echo "$arch" | grep -E "(x86_64|amd64)$" 2>&1 > /dev/null)
35 then
36     local_installer="/path_to_local_agent/agent_linux_x86_64.sh"
37 fi

```

5. 行54-75を削除します。

```

45 echo $eraa_ca_cert_b64 | base64 -d > "$local_ca_path" && echo "$local_ca_path" >> "$cleanup_file"
46 fi
47
48
49 local_installer="$(mktemp -q -u)"
50
51 eraa_http_proxy_value=""
52
53 echo "Downloading ESET Management Agent installer..."
54
55 if test -n "$eraa_http_proxy_value"
56 then
57     export use_proxy=yes
58     export http_proxy="$eraa_http_proxy_value"
59     (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$eraa_installer_url" || wget
--connect-timeout 300 --no-proxy --no-check-certificate -O "$local_installer" "$eraa_installer_url" ||
curl --fail --connect-timeout 300 -k "$eraa_installer_url" > "$local_installer") && echo
"$local_installer" >> "$cleanup_file"
60 else
61     (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$eraa_installer_url" || curl
--fail --connect-timeout 300 -k "$eraa_installer_url" > "$local_installer") && echo "$local_installer"
>> "$cleanup_file"
62 fi
63
64 if test ! -s "$local_installer"
65 then
66     echo "Failed to download installer file"
67     exit 2
68 fi
69
70 echo -n "Checking integrity of installer script " && echo "$eraa_installer_checksum $local_installer" |
shasum -c
71
72 chmod +x "$local_installer"

```

6. ファイルを保存します。

Webサイトからエージェントをダウンロード

[Webサイト](#)からESET Managementエージェントインストールパッケージをダウンロードします。クライアントコンピューターのOSに応じて、該当するパッケージを選択します。

- [Linux](#)サーバー支援およびオフラインインストール
- [macOS](#)
- [Windows](#)

○ [サーバー支援インストール](#) – エージェントインストールパッケージを使用してESET PROTECTサーバーから証明書を自動的にダウンロードします(ローカル展開方式の場合に推奨される方法)。

- 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。
 - 別のユーザーによるサーバー支援インストールを許可する場合は、次の[権限](#)が設定されていることを確認します。
- ❗ ○ユーザーにはサーバーのピア証明書を署名した認証局の使用権限と1つ以上のピア証明書の使用権限が必要です。このような証明書が存在しない場合、ユーザーは新しい証明書を作成する書き込み権限が必要です。
- ユーザーがコンピューターを追加する静的グループの書き込み権限。

○ [オフラインインストール](#) – エージェントインストールパッケージを使用します。手動で証明書をエクスポートし、この展開方法で適用する必要があります。

クライアントコンピューター

(`C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html`)で[ステータスログ](#)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認します。

i エージェントの問題がある場合(ESET PROTECTサーバーに接続していない場合など)は、[トラブルシューティング – エージェント展開](#)セクションを参照してください。

リモート展開

❗ 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。

リモート展開は次の方法で実行できます。

- [ESET Remote Deployment Tool](#) – このツールではESET Management Webコンソールで作成された[ESET PROTECTエージェント\(およびESETセキュリティ製品\)インストーラー](#)パッケージを展開できます。
- [グループポリシーオブジェクト\(GPO\)とSystem Center Configuration Manager \(SCCM\)](#) – クライアントコンピューターでのESET Managementエージェントの一括展開でこの方法を使用することをお勧め

めします。

- [エージェント展開](#) サーバータスク - GPO または SCCM の代替。

ESET Management エージェントのリモート展開中に問題が発生した場合 (サーバータスクのエージェント展開が失敗する場合) は、次の項目を参照してください。

- [トラブルシューティング - エージェント展開](#)
- [トラブルシューティング - エージェント接続](#)
- [ESET Management エージェント展開のシナリオ例](#)

リモート展開と権限

ユーザーが GPO インストーラーまたは SCCM スクリプトを作成できるようにする場合は、[例](#)に合わせて権限を設定します。

次の[権限](#)は、サーバータスクエージェント展開で必要です。

- 展開が実行されるグループとコンピューターの書き込み権限
- 証明書が含まれる静的グループへのアクセスがある**証明書**の使用権限
- サーバータスクとトリガーセクションのエージェント展開の使用権限

GPO と SCCM を使用したエージェント展開

[ローカル展開](#)の他に、グループポリシーオブジェクト (GPO) [System Center Configuration Manager \(SCCM\)](#) [Symantec Altiris](#) [Puppet](#) などの管理ツールを使用して、エージェントをリモート展開することもできます。



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。

以下の手順に従い、GPO または SCCM を使用して ESET Management エージェントをクライアントに展開します。

[ESET ダウンロードページ - スタンドアロンインストーラーセクション](#) からエージェントのインストーラー (.msi) ファイルをダウンロードします。

メニューバーの **クイックリンクのその他の展開オプション** をクリックし、「**展開のために GPO または SCCM を使用**」を選択し、**[スクリプトの作成]** ボタンをクリックするとポップアップウィンドウが開きます。

証明書

クラッシュレポートと匿名のテレメトリデータ (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 に送信することに同意しない場合は、**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フにします。チェックボックスがオンの場合、テレメトリデータとクラッシュレポートが ESET に送信されます。

ピア証明書およびESET PROTECT認証局が使用可能な証明書に基づいて自動的に選択されます。自動的に選択されたものとは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リストを表示して、使用する証明書を選択します。**カスタム証明書**を使用する場合は、ラジオボタンをクリックして、**.pfx**証明書ファイルをアップロードします。詳細については、[のカスタム証明書ESET PROTECT](#)を参照してください。

必要に応じて、**証明書パスフレーズ**を入力します。たとえばESET PROTECTのインストール中にパスフレーズを指定した場合、またはパスフレーズ付きのカスタム証明書を使用する場合です。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。

詳細

ESET Managementエージェントインストールパッケージをカスタマイズできます。

- 1.インストールパッケージの**名前**および**説明**(任意)フィールドを入力します。
- 2.**タグを選択**をクリックして、[タグを割り当て](#)ます。
- 3.**親グループ(任意)** - インストール後にコンピューターが配置され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。
- 4.**初期インストーラー設定(任意)** - [設定ポリシー](#)をESET Managementエージェントに適用する場合に、このオプションを使用します。**エージェント設定(任意)**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。
- 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**を指定できます(既定は2222)。
- 6.HTTPプロキシを使用する場合は、**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。プロキシの詳細については、[こちら](#)をお読みください。



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す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。

- 7.**完了**を選択すると、**install_config.ini**ファイルの新しいポップアップウィンドウが開きます。**ファイルの保存**を選択します。

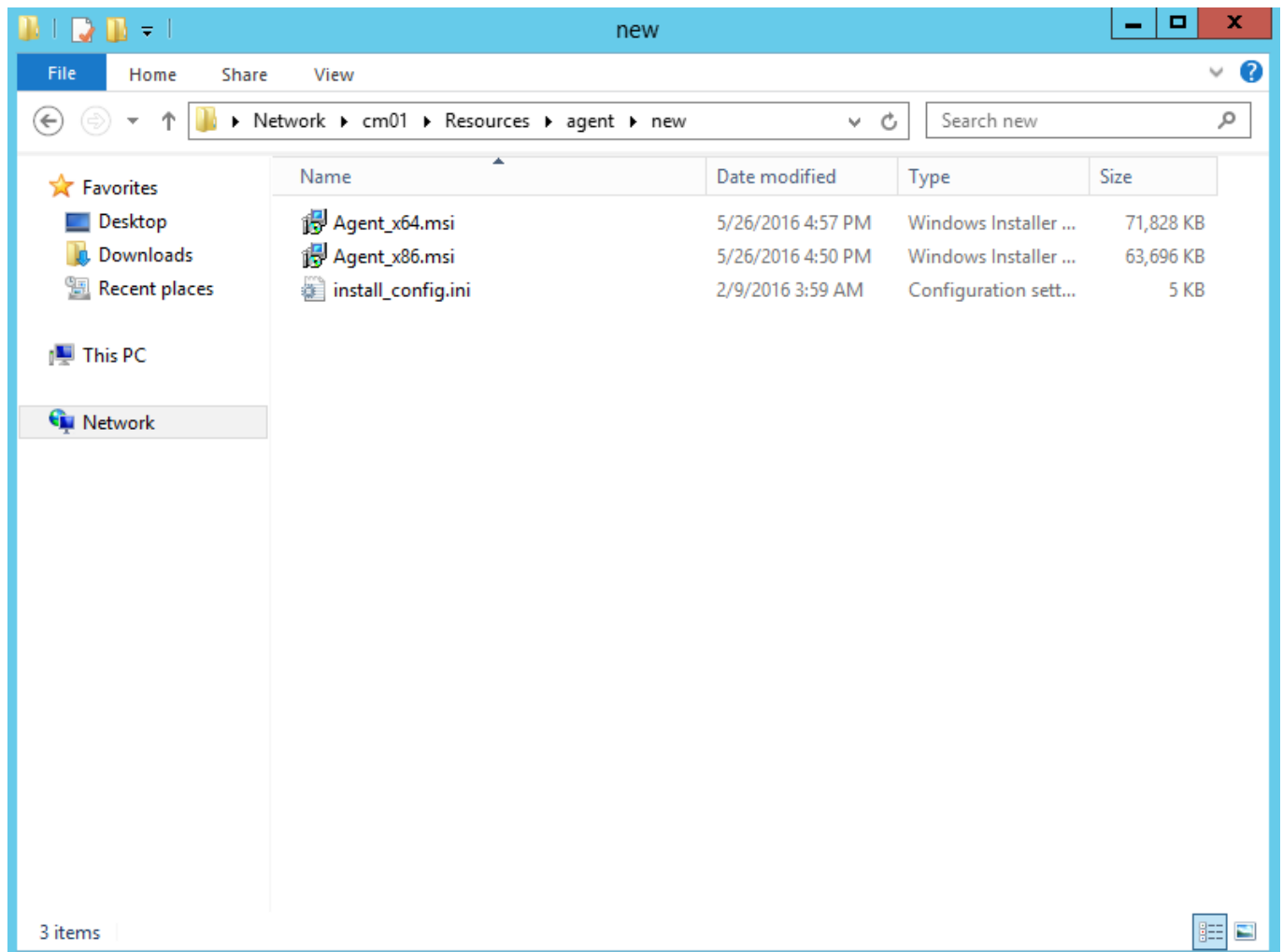
次の該当するリンクをクリックし、2つの一般的なESET Managementエージェント展開方法に関する段階的な手順を確認します。

- 1.[グループポリシーオブジェクト\(GPO\)を使用したESET Managementエージェントの展開](#) - 言語によっては、ナレッジベース記事が提供されていない場合があります。

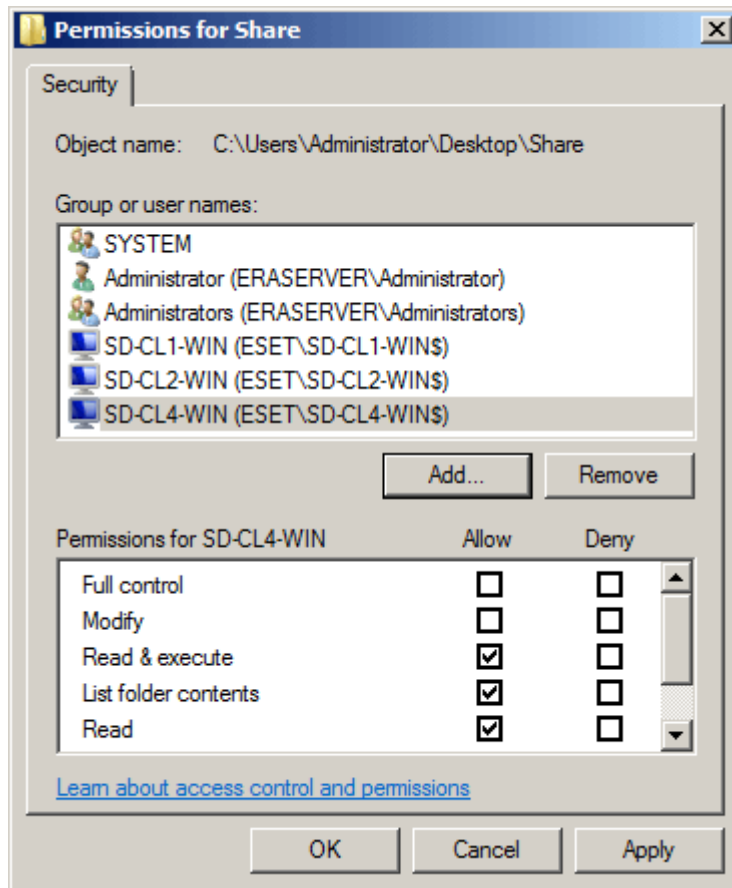
展開手順 - SCCM

[SCCM](#)を使用してESET Managementエージェントを展開するには、次のステップを続けます。

1. ESET Managementエージェントのインストーラーの`.msi`ファイルと`install_config.ini`ファイルを共有フォルダに配置します。



! クライアントコンピューターには、この共有フォルダへの読み取り/実行アクセス権が必要です。



2. SCCMコンソールを開き、[ソフトウェアライブラリ]をクリックします。[アプリケーション管理]で[アプリケーション]を右クリックし、[アプリケーションの作成]を選択します。**Windows**インストーラ図(*.msiファイル)を選択します。

The screenshot shows the 'Create Application Wizard' window with the 'General' tab selected. The left sidebar contains a tree view with 'General' (selected), 'Import Information', 'Summary', 'Progress', and 'Completion'. The main area is titled 'Specify settings for this application' and contains explanatory text: 'Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.'

There are two radio button options:

- ☒ **A**utomatically detect information about this application from installation files:
- ☐ **M**anually specify the application information

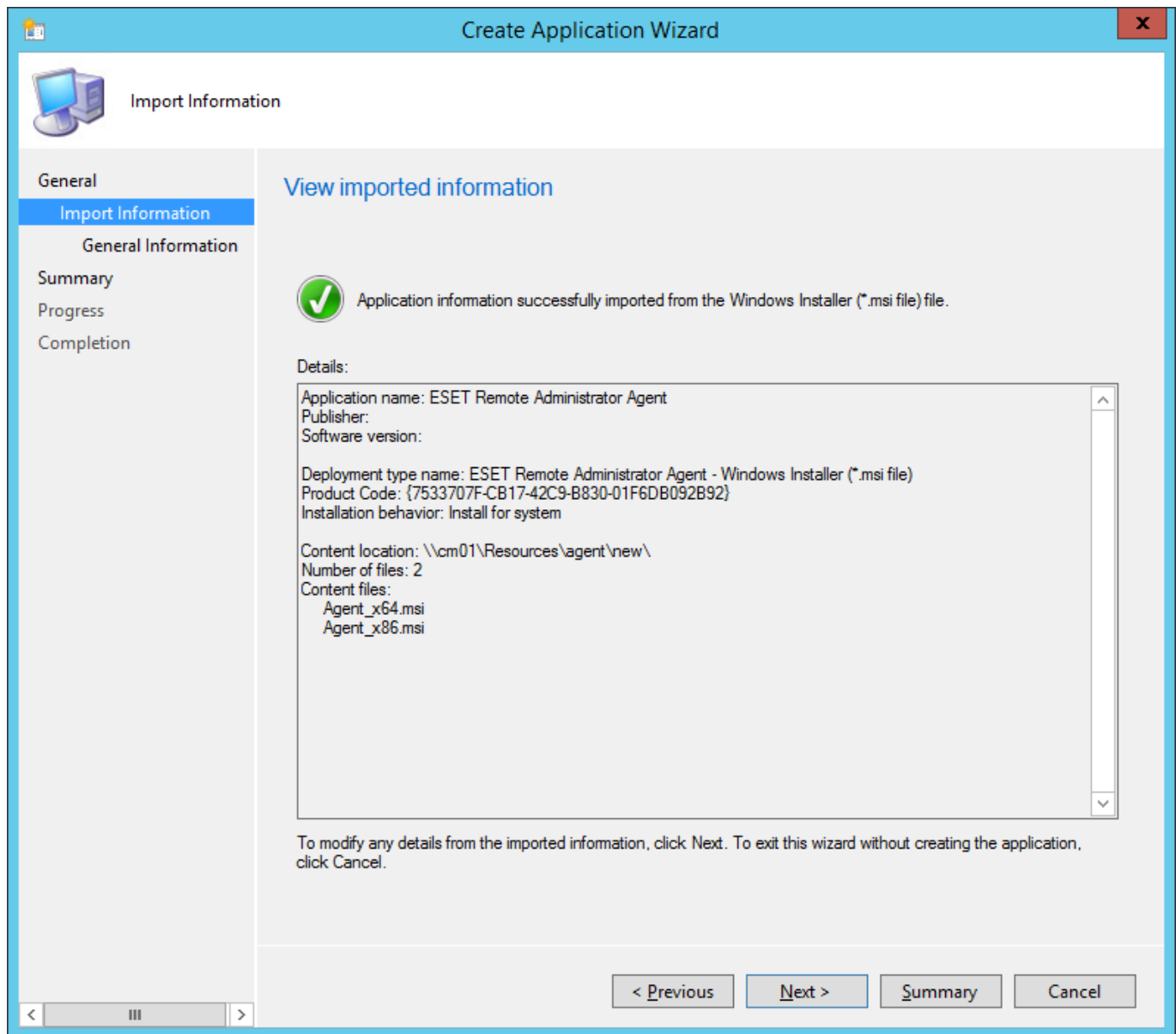
Under the first option, there are two input fields:

- Type:** A dropdown menu showing 'Windows Installer (*.msi file)'.
- Location:** A text box containing '\\cm01\Resources\agent\new\Agent_x64.msi'. Below this is an example: 'Example: \\Server\Share\File'.

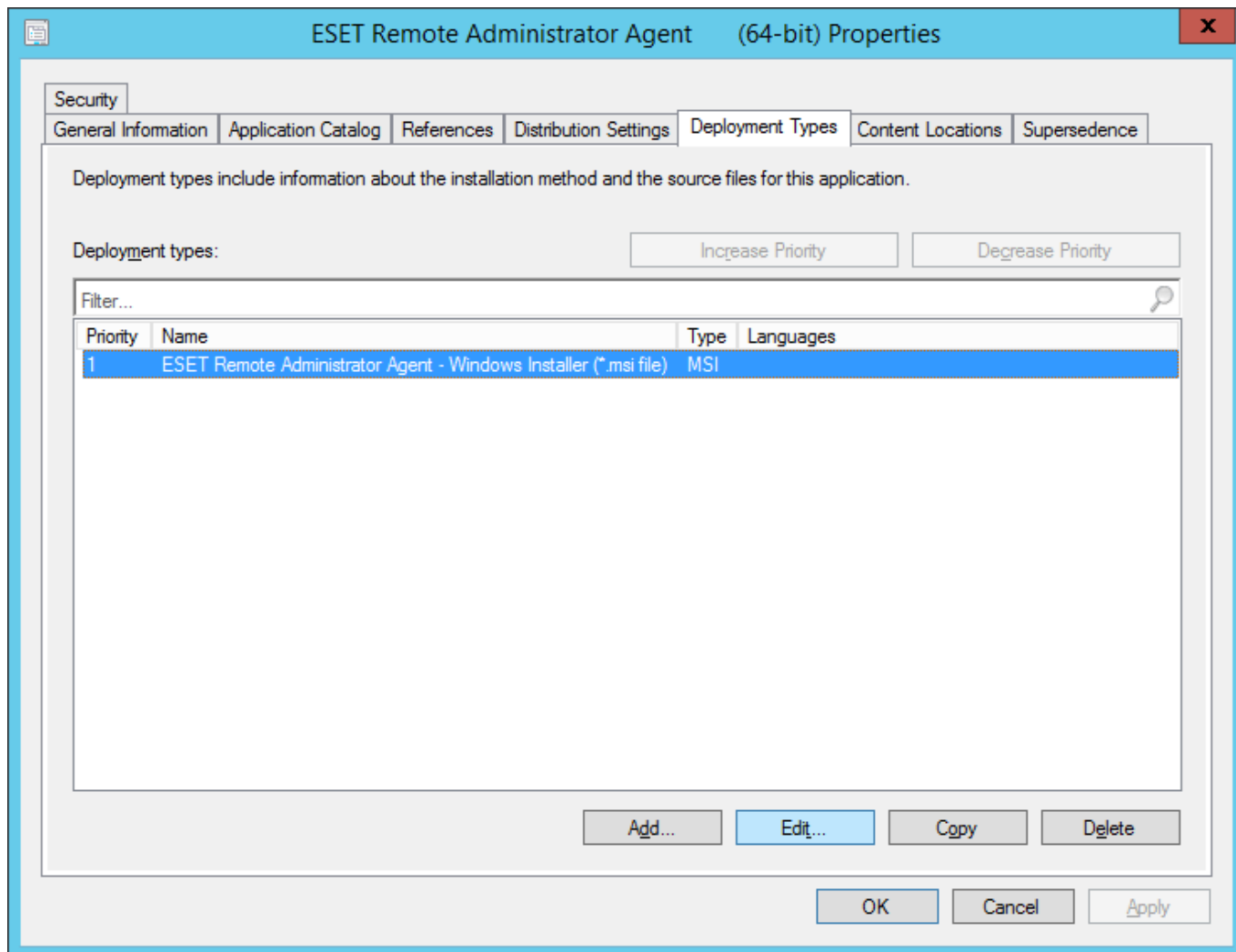
A 'Browse...' button is located to the right of the Location field.

At the bottom right, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

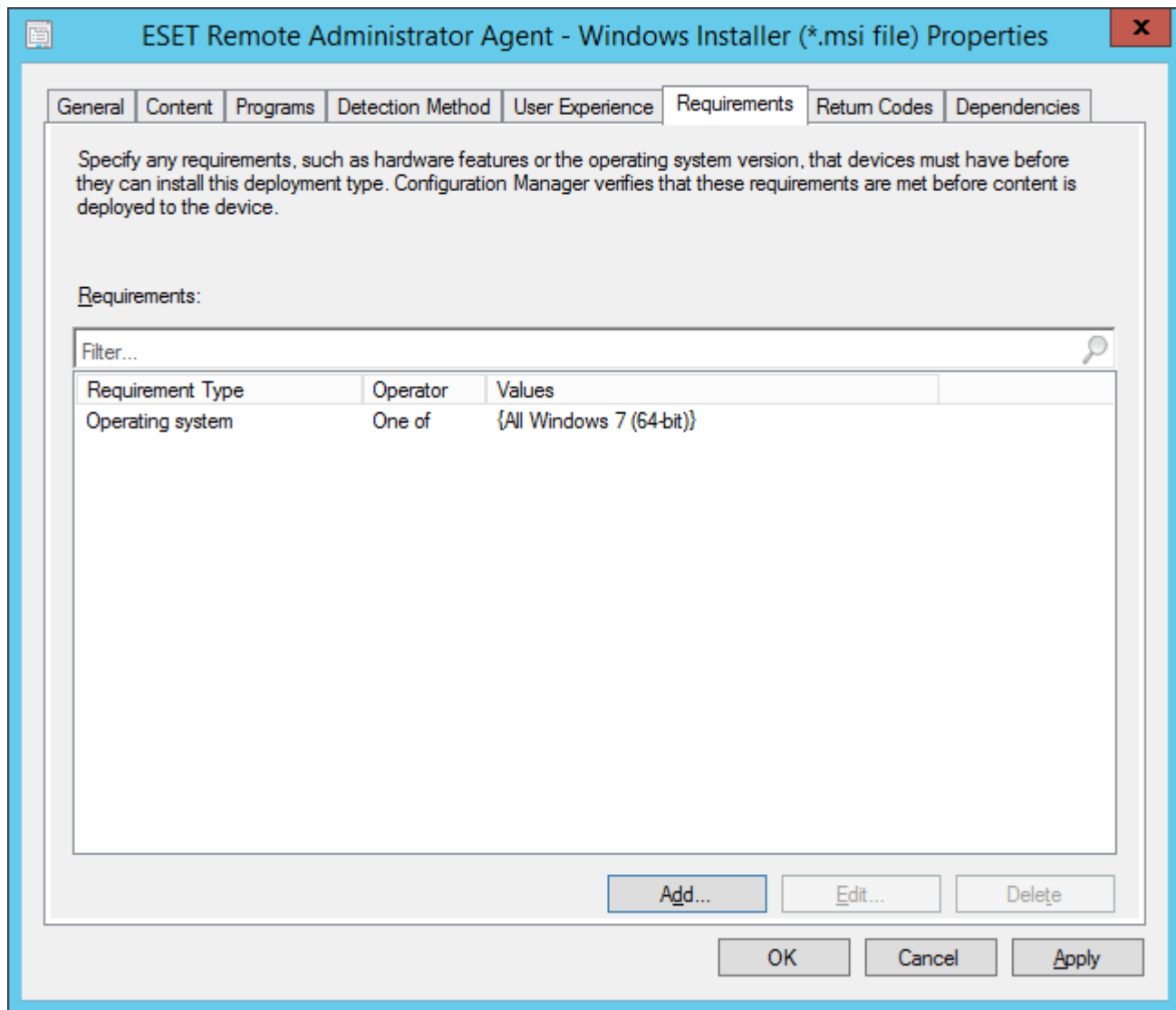
3. アプリケーションに関するすべての必要な情報を指定し、[次へ]をクリックします。



4. ESET Management エージェントアプリケーションを右クリックし、**[展開タイプ]**タブをクリックし、**[唯一の展開]**をクリックして、**[編集]**をクリックします。



5. [要件]タブをクリックし、[追加]をクリックします。[条件]ドロップダウンメニューからオペレーティングシステムを選択し、[演算子]ドロップダウンメニューから[いずれか]を選択して、該当するチェックボックスをオンにしてインストールするオペレーティングシステムを指定します。完了したら[OK]をクリックし、[OK]をクリックして、残りのウィンドウを閉じ、変更を保存します。



Create Requirement

Category:
Device

Condition:
Operating system Create...

Rule type:
Value

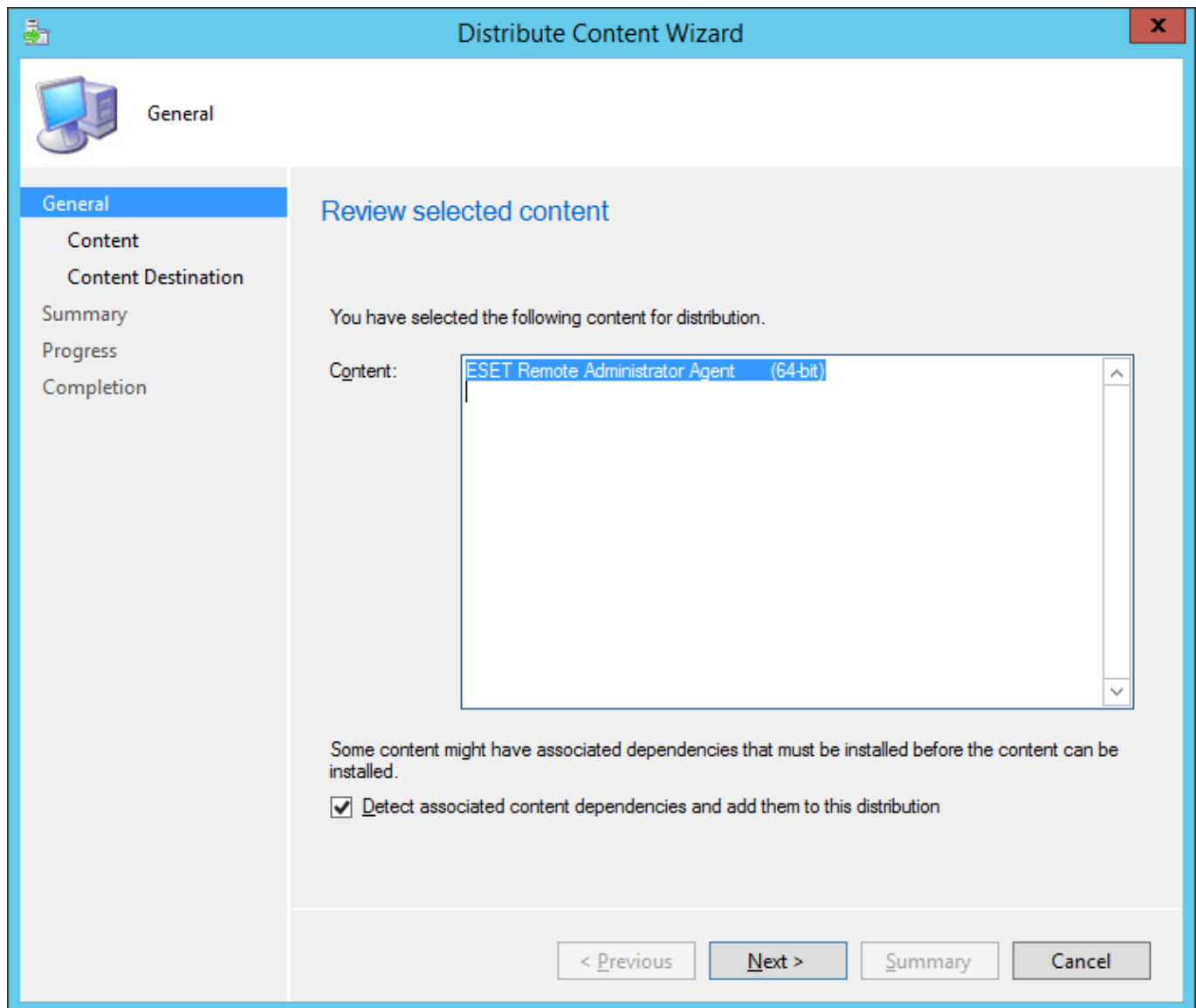
Operator:
One of

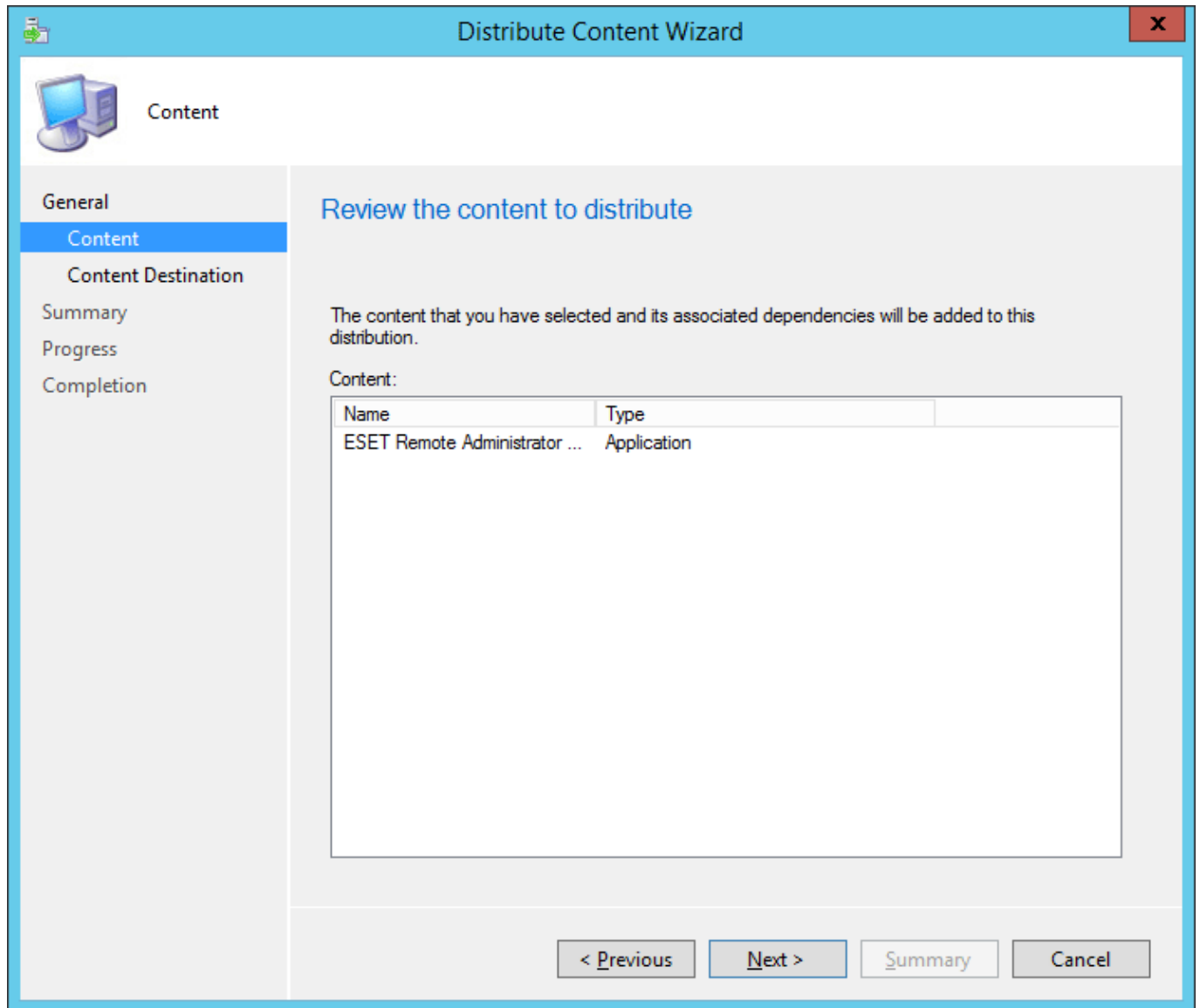
☒ Select all

- ☐ Windows XP
- ☐ Windows Vista
- ☒ Windows 7
 - ☒ All Windows 7 (64-bit)
 - ☐ All Windows 7 (32-bit)
 - ☐ Windows 7 (64-bit)
 - ☐ Windows 7 SP1 (64-bit)
 - ☐ Windows 7 (32-bit)
 - ☐ Windows 7 SP1 (32-bit)

OK Cancel

6. [システムセンターソフトウェアライブラリ]で、新しいアプリケーションを右クリックし、コンテキストメニューから[コンテンツの配布]を選択します。ソフトウェアの展開ウィザードのプロンプトに従い、アプリケーションの展開を完了します。





7.アプリケーションを右クリックして、**[展開]**を選択します。ウィザードに従い、コレクションとエージェントを展開する場所を選択します。

Add Distribution Points

Select distribution points that will host this content.

Software Update Packages are never distributed to Cloud Distribution Points.

Available distribution points:

Filter...

Name	Type	Description
<input checked="" type="checkbox"/> [Icon]	On-premises	
<input type="checkbox"/> [Icon]	On-premises	

OK

Cancel

Content Destination

General
Content
Content Destination
Summary
Progress
Completion

Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

Content destination:

Filter...

Name	Description	Associations
[Icon]	Distribution point	

Add

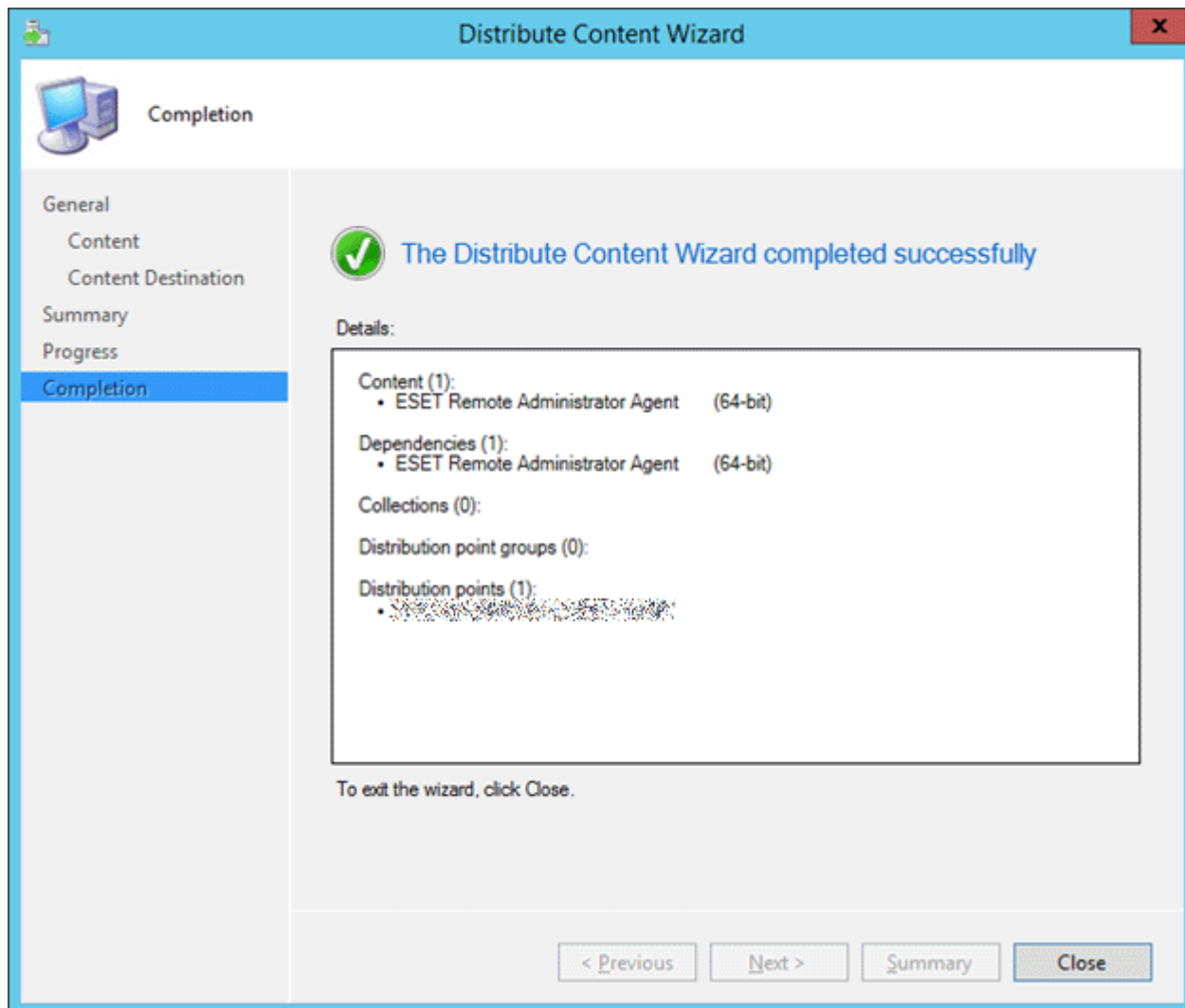
Remove

< Previous


Next >

Summary

Cancel



Deploy Software Wizard



General

General

Content

Deployment Settings

Scheduling

User Experience

Alerts

Summary

Progress

Completion

Specify general information for this deployment

Software:

ESET Remote Administrator Agent (64-bit)

Browse...

Collection:

Applications - Workstations BTS - ESET Remote Administrat

Browse...

☐ Use default distribution point groups associated to this collection

☒ Automatically distribute content for dependencies

Comments (optional):

< Previous


Next >

Summary

Cancel

Deploy Software Wizard

X



Deployment Settings

General

Content

Deployment Settings

Scheduling

User Experience

Alerts

Summary

Progress

Completion

Specify settings to control how this software is deployed

Action:

Install

Purpose:

Required

☐

Pre-deploy software to the user's primary device

☐

Send wake-up packets

☐

Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

< Previous


Next >

Summary

Cancel

Deploy Software Wizard

X

Scheduling

General

Content

Deployment Settings

Scheduling

User Experience

Alerts

Summary

Progress

Completion

Specify the schedule for this deployment

This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.

Time based on:

UTC

☐ Schedule the application to be available at:

9. 2.2015

12:32

Installation deadline:

☒ As soon as possible after the available time

☐ Schedule at:

9. 2.2015

12:32

< Previous

Next >


Summary

Cancel

84

Deploy Software Wizard

X



User Experience

General

Content

Deployment Settings

Scheduling

User Experience

Alerts

Summary

Progress

Completion

Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications:

Display in Software Center and show all notifications

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

☐ Software Installation

☐ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

☒ Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

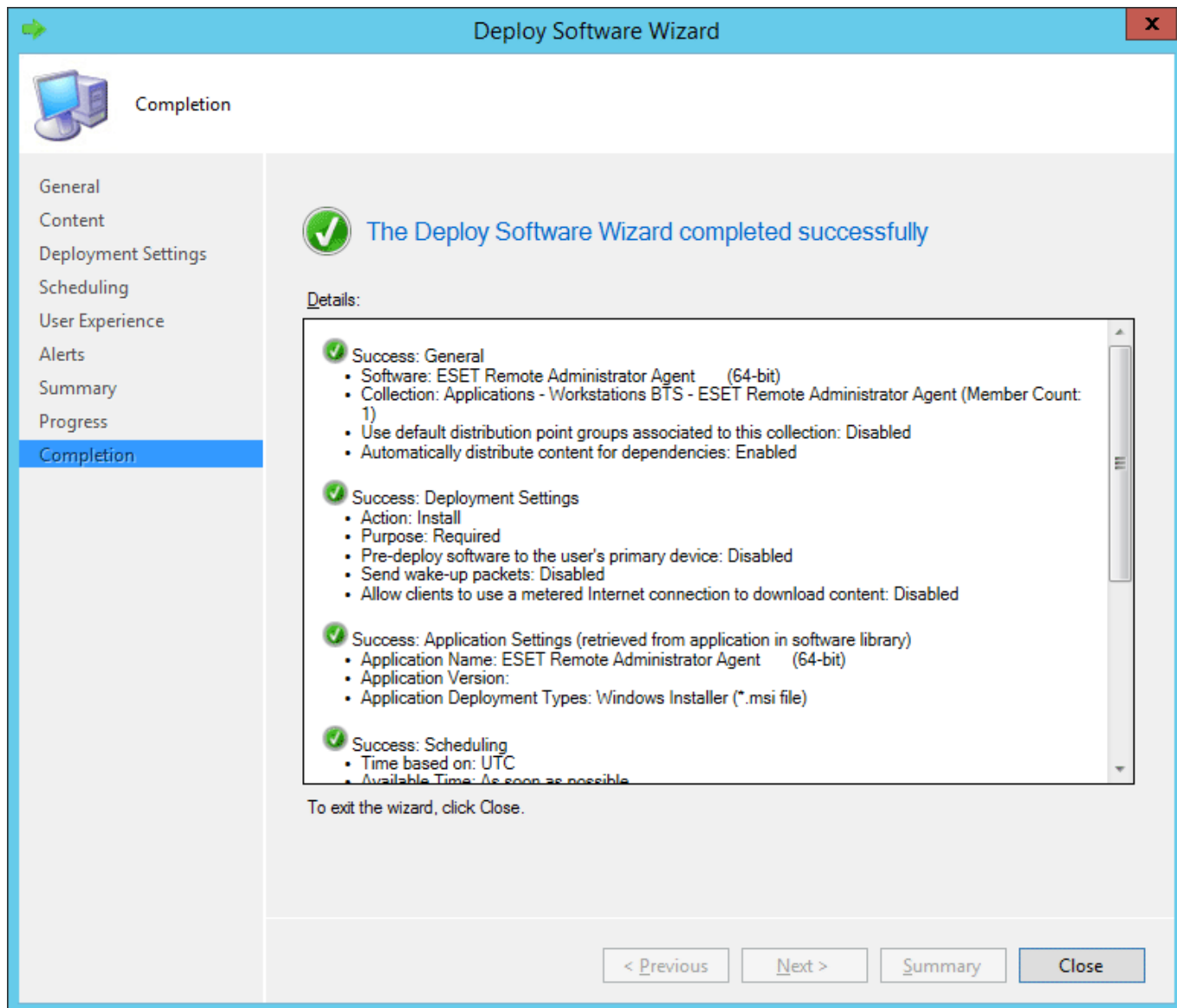
< Previous

Next >

Summary

Cancel

85



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。

i 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。

この方法を使用してESET ManagementエージェントとESETセキュリティ製品を展開するには、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でESET Remote Deployment toolを実行します。

4. 次の展開オプションのいずれかを選択します。

- [Active Directory](#) - Active Directory資格情報を入力する必要があります。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を検査する必要があります。
- [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する必要があります。
- [コンピューターを手動で追加する](#) - 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。

i 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 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。

i 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。

Active Directoryからコンピューターを選択

[前の章](#)からESET ManagementエージェントおよびESETセキュリティ製品の展開を続行するには：

1. エンドユーザーライセンス契約を読んで同意し、[次へ](#)をクリックします。

2. **Active Directory**サーバーとIPアドレスまたはホスト名、および接続先のポートを入力します。

3. ユーザー名とパッケージを入力して**Active Directory**サーバーにログインします。[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。

4. 任意で、後から**ESET PROTECT**にインポートするために**Active Directory**構造をエクスポートする場合は、[**ESET PROTECT** のコンピューターリストをエクスポートする]チェックボックスをオンにします。

i コンピューターが**Active Directory**にある場合は、[次へ]をクリックします。既定のドメインコントローラーに自動ログインします。

5. 追加するコンピューターの横のチェックボックスをオンにし、[次へ]をクリックします。選択したグループ内のすべてのコンピューターを一覧表示するには、サブグループを含めるチェックボックスをオンにします。

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。

! 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)。

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、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。

Progress	
COMPUTER	STATUS
✓ [redacted]	Success

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。

i 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。

ローカルネットワークのコンピューターを検査

[前の章](#)からESET ManagementエージェントおよびESETセキュリティ製品の展開を続行するには:

1. エンドユーザーライセンス契約を読んで同意し、**次へ**をクリックします。
2. 10.100.100.10-10.100.100.250形式でネットワークの**IP範囲**を入力します。
3. 次の**検査方法**のいずれかを選択します。

- **Ping検査** - コマンドpingでローカルコンピューターを検索します。

i このネットワークの一部のクライアントコンピューターは、ファイアウォールの接続ブロックのため、pingコマンドへの応答を送信する必要はありません。

- **ポート検査** - ポート番号を使用して、ネットワークを検査します。ESET Managementエージェントのリモート展開については、使用される[サポートされたポート](#)を参照してください。既定のポート番号は445です。
4. ネットワークのコンピューターを検索するには、**[検査の開始]**をクリックします。
 5. 追加するコンピューターの横のチェックボックスをオンにし、**[次へ]**をクリックします。
 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。

! 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)。

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、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。

Progress	
COMPUTER	STATUS
✓ [redacted]	Success

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。

i 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。

コンピューターのリストのインポート

[前の章](#)からESET ManagementエージェントおよびESETセキュリティ製品の展開を続行するには:

1. エンドユーザーライセンス契約を読んで同意し、**次へ**をクリックします。
2. 次のオプションのいずれかを選択します。
 - **テキストファイル(各行に1コンピューター)**: ホスト名またはIPアドレスがあるファイル。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。
 - **管理コンソールからエクスポート**: [ESET PROTECT Web コンソールからエクスポートされた](#) ホスト名またはIPアドレスがあるファイル。
3. **[参照]**をクリックして、アップロードするファイルを選択し、**[次へ]**をクリックします。
4. 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。

 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)

5. **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。
6. 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。
7. **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。

ESET Remote Deployment Tool

Deployment configuration

Select an installer package generated by management console. Package platform (x64 or Win32) must correspond with targeted computers.

Deployment package [Browse...](#)

☒ Use ESET AV Remover

☐ Use ESET offline install package

Enter local administrator credentials or domain administrator credentials. When using local administrator credentials make sure to disable remote User Account Control (951016) in advance otherwise remote deployment will not work properly. When using domain administrator credentials to deploy computers make sure all the computers are members of the same domain.

User name

Password

☐ Use current user credentials

Deployment method ☒ Built-in ☐ PsExec

[Back](#) [Next](#) [Cancel](#)

! **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。

8. 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、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。

Progress	
COMPUTER	STATUS
✓	Success

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。

i 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。

コンピューターを手動で追加

[前の章](#)からESET ManagementエージェントおよびESETセキュリティ製品の展開を続行するには:

1. エンドユーザーライセンス契約を読んで同意し、**次へ**をクリックします。
2. ホスト名またはIPアドレスを手動で入力し、**[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)

3. 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。
4. **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。
5. 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。
6. **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。

7. 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、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。

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

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。

i 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 Remote Deployment Tool - ト ラ ブ ル シ ュ ー テ ィ ン グ

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。

i 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。

複数のエラーメッセージと、以下の表の一覧にあるさまざまな理由により、展開が失敗する場合があります。

エラーメッセージ	考えられる原因
ネットワークパスが見つからない (エラーコード0x35)	<ul style="list-style-type: none">クライアントがネットワークで到達できません。ファイアウォールが通信をブロックしています受信ポート135、137、138、139、445がクライアントのファイアウォールまたはWindows Firewallで開いていません受信ファイルとプリンター共有例外の許可が使用されていません。クライアントのホスト名を解決できませんでした。有効なFQDNコンピューター名を使用してください
アクセスが拒否されました (エラーコード0x5) ユーザー名またはパスワードが正しくありません(エラーコード0x52e)	<ul style="list-style-type: none">ドメインに参加しているサーバーからドメインに参加しているクライアントに展開するときには、ドメイン\ドメイン管理者の形式でドメイン管理者グループのメンバーであるユーザーの資格情報を使用します。サーバーから同じドメインにないクライアントに展開するときには、ターゲットコンピューターのUACフィルタリングを無効にしますサーバーから同じドメインにないクライアントに展開するときには、管理者の形式で管理者グループのメンバーであるローカルユーザーの資格情報を使用します。ターゲットコンピューター名が自動的にログインの最初に追加されます。管理者アカウントのパスワードが設定されていません不十分なアクセス権ですADMIN\$管理共有が使用できませんIPC\$管理共有が使用できません簡易ファイル共有の使用が有効です
このインストールパッケージは、この種類のプロセッサではサポートされていません。(エラーコード1633)	インストールパッケージは、このプラットフォームではサポートされていませんESET PROTECT Webコンソールで、正しいプラットフォーム (64ビットまたは32ビットオペレーティングシステム) のインストールパッケージを作成し、ダウンロードします。
セマフォタイムアウト期間が終了しました	クライアントは、展開パッケージがあるネットワーク共有にアクセスできません。これは、SMB 1.0が共有で無効になっているためです。

考えられる原因に応じて、適切なトラブルシューティング手順を実施します。

考えられる原因	トラブルシューティングの手順
クライアントがネットワークで到達できません	ESET PROTECTサーバーからクライアントの接続を確認します。応答がある場合は、リモートでクライアントコンピューターにログインします(リモートデスクトップ経由など)。

考えられる原因	トラブルシューティングの手順
ファイアウォールが通信をブロックしています	クライアントとサーバーの両方で、ファイアウォール設定と、これらの2台のコンピュータ間に存在する他のファイアウォール(該当する場合)を確認します。展開が成功した後、ポート2222と2223がファイアウォールで開きません。これらのポートが2つのコンピュータ(クライアントとサーバー)間のすべてのファイアウォールで開いていることを確認します。
クライアントのホスト名を解決できませんでした	DNSの問題に対する考えられる解決策には次の点があります(ただしこれに限定されません)。 • エージェント展開の問題があるサーバーまたはクライアントのIPアドレスおよびホスト名のnslookupコマンドを使用します。結果はコンピュータからの情報と一致するはずです。たとえば、ホスト名のnslookupは、ipconfigコマンドが問題のホストに表示するIPアドレスを解決します。nslookupコマンドはクライアントとサーバーで実行される必要があります。 • 重複するDNSレコードがあるかどうか手動で調査します。
管理者アカウントのパスワードが設定されていません	管理者アカウントの適切なパスワードを設定します(空のパスワードは使用しないでください)。
不十分なアクセス権です	エージェント展開タスクの作成時にドメイン管理者の認証情報を使用してください。ワークグループにクライアントコンピュータがある場合、その特定のコンピュータでローカル管理者アカウントを使用します。 Windows7以降では、エージェント展開タスクを実行するためにAdministratorユーザーアカウントを有効にする必要があります。管理者グループのメンバーであるローカルユーザーを作成するか、ビルトインローカル管理者アカウントを有効にできます。 Administratorユーザーアカウントを有効にする 1.管理コマンドプロンプトを開きます 2.次のコマンドを入力します。 <code>net user administrator /active:yes</code>
ADMIN\$管理共有が使用できません	クライアントコンピュータは共有リソースADMIN\$を有効にする必要があります。他の共有([スタート]>[コントロールパネル]>[管理ツール]>[コンピューター管理]>[共有フォルダ]>[共有])間でこれがあることを確認してください。
IPC\$管理共有が使用できません	サーバーがIPC\$にアクセスできることを確認します。サーバーのコマンドプロンプトから次のコマンドを発行します。 <code>net use \\clientname\IPC\$</code> clientnameはターゲットコンピュータの名前です。
簡易ファイル共有の使用が有効です	アクセスが拒否されましたというエラーメッセージが表示され、ドメインとワークグループの両方を含む混合環境を使用している場合は、エージェント展開の問題が発生しているすべてのコンピュータで、[簡易ファイル共有を使用する]または[共有ウィザードを使用する]を無効にします。例えばWindows 7の場合は次のようにします。 • スタートをクリックし、検索ボックスにfolderと入力してから、フォルダーオプションをクリックします。表示タブをクリックして、詳細設定ボックスでリストを下方方向にスクロールし、共有ウィザードを使用の横のチェックボックスをオフにします。

エージェント保護

ESET Managementエージェントはビルトインの自己防衛メカニズムで保護されています。この機能は次のことを実現します。

- ESET Management エージェントレジストリエントリの修正に対する保護(HIPS)
- ESET Management エージェントに属するファイルを修正、置換、削除、または改ざんできません(HIPS)

- ESET Management エージェントプロセスを終了できません
- ESET Management エージェントサービスを停止、一時停止、無効化、アンインストール、または危険にさらすことができません

一部の保護は、ESET 製品に含まれる HIPS 機能で対応します。

i ESET Management エージェントの完全な保護を保証するために、クライアントコンピューターで HIPS を有効にする必要があります。

パスワード保護の設定

自己防衛の他に ESET Management エージェントへのアクセスをパスワードで保護できます (Windows のみ)。パスワード保護が使用される場合は、正しいパスワードを入力しないと ESET Management エージェントをアンインストールまたは修復できません。ESET Management エージェントパスワードを設定するには、適切な [ESET Management エージェントのポリシー](#) を作成する必要があります。

ESET Management エージェント設定

ESET Management エージェントポリシーを使用して ESET Management エージェントの特定の設定を構成できます。ESET Management エージェントには定義済みのポリシーがあります。たとえば、**接続 - 次の間隔で接続** (エージェント接続間隔) または **アプリケーションレポート - すべてのインストール済みアプリケーションを報告** (ESET アプリケーション以外を含む) などです。ロケーションに基づくポリシーを適用する方法については、[例](#)をお読みください。

[ポリシー] をクリックし、[ビルトインポリシー] > [ESET Management エージェント] を展開して、既存のポリシーを編集するか、新しいポリシーを作成します。

■ 接続

- **接続するサーバー** - サーバーリストの **編集** をクリックして ESET PROTECT サーバー接続詳細 (ホスト名/IP およびポート番号) を追加します。複数の ESET PROTECT サーバーを指定できます。たとえば、[ESET PROTECT サーバーの IP アドレスを変更した場合](#) または移行を実行している場合です。
- **データ制限** - データを送信する最大バイト数を指定します。
- **接続間隔** - 定期間隔を選択し、接続間隔を指定するか、[CRON 式](#) を使用します。
- **証明書** - ESET Management エージェントのピア証明書を管理できます。**証明書の変更** をクリックし ESET Management エージェントで使用される ESET Management エージェント証明書を選択します。詳細については、「[ピア証明書](#)」を参照してください。

■ 更新

- **アップデート間隔** - アップデートを受信する間隔。定期的な間隔を選択して、設定を構成するか、または [CRON 式を使用します](#)。
- **アップデートサーバー** - ESET Management エージェントがモジュールのアップデートを受信するアップデートサーバー。
- **アップデートの種類** - 受信するアップデートの種類を選択します。定期またはリリース前アップ

デートを選択します。リスクがあるので、プロダクションシステムのリリース前アップデートを選択することは推奨しません。

- **自動アップグレードを有効にする** - このオプションは、ESET Management エージェント 8.1 以降に適用されます。既定では、[ESET Management エージェントは自動的に最新の互換性があるバージョンにアップグレード](#)されます。このオプションをオフにすると ESET Management エージェントの自動アップグレードを無効にできます。

■ 詳細設定

- **HTTP プロキシ**: プロキシサーバーを使用し、ネットワーク上のクライアントのインターネットトラフィックと ESET PROTECT サーバーへのエージェントレプリケーションを容易にできます。

o プロキシ設定タイプ

■ **グローバルプロキシ** - エージェントレプリケーションと ESET サービスのキャッシュ (アップデートなど) で別のプロキシサーバーを使用します。

■ **サーバーごとに別のプロキシ** - エージェントレプリケーションで 1 つのプロキシを使用し、ESET サービスのキャッシュには別のプロキシを使用します (アップデートなど)。

o **グローバルプロキシ** - このオプションは、**プロキシ設定タイプ** で選択した場合にのみ使用できます。**編集** をクリックし、プロキシ設定を設定します。

サービスごとに別のプロキシを選択する場合にのみ、以下の 2 つのオプションを使用できます。プロキシ設定のいずれかのみを使用できます。たとえば、**ESET サービスのみ**を設定し、**レプリケーション**をオフにします。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。

o **(ESET 管理サーバーへの) レプリケーション** - エージェントをサーバーに接続する [プロキシ](#) の接続設定を構成します。

o **ESET サービス** - ESET サービスをキャッシュに保存するプロキシの接続設定を構成します。

- **ウェイクアップコール** - ESET PROTECT サーバーは、[EPNS](#) 経由でクライアントコンピューターで ESET Management エージェントとの即時複製を実行します。これは ESET Management エージェントが ESET PROTECT サーバーに接続するときに、定期間隔を待機しない場合に便利です。例えば、クライアントでただちに [タスク](#) を実行する場合や、[ポリシー](#) をただちに適用する場合に便利です。
- **互換性** - ESET Management エージェントによる ESET 製品バージョン 5 以前の管理ができるようにするには、特定のリスニングポートを設定する必要があります。また ESET 製品を設定し、このポートに報告させる必要があります。また ESET PROTECT サーバーアドレスが **localhost** に設定される必要があります。
- **オペレーティングシステム** - スイッチを使用して、クライアントコンピューターの特定の情報または問題を報告します。
- **リポジトリ** - すべてのインストールファイルが格納されているリポジトリの場所です。

i 既定のリポジトリは **AUTOSELECT** です。

- **製品改善プログラム** - クラッシュレポートおよび匿名のテレメトリデータのESETへの送信を有効または無効にできます。
- **ロギング**-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。最新のESET Managementエージェント[ログファイル](#)はクライアントコンピューターにあります。
- **設定** - [パスワード保護設定](#)はESET Managementエージェントの保護機能です(Windowsのみ)。 [パスワードを設定](#)しESET Managementエージェントパスワード保護を有効にします。ポリシーが適用されると、パスワードを指定しないかぎりESET Managementエージェントをアンインストールまたは修復できません。



このパスワードを忘れた場合は、ターゲッ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できません。

割り当て

このポリシーを受信するクライアントを指定します。[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。ポリシーを適用するコンピューターを選択し、**OK**をクリックします。

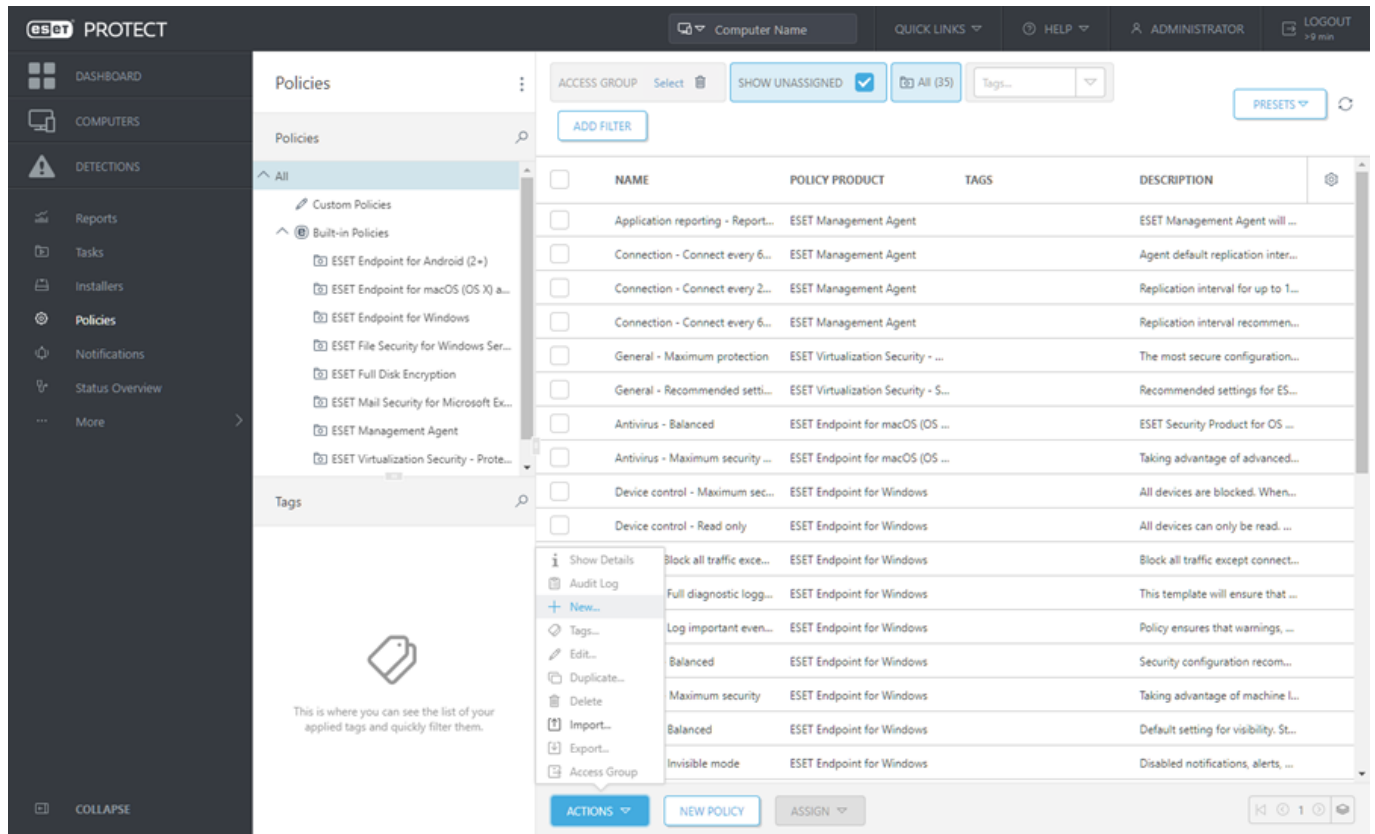
概要

このポリシーの設定を確認し、[完了]をクリックします。

ESET Managementエージェント接続間隔のポリシーの作成

この例ではESET Managementエージェント接続間隔に関する新しいポリシーを作成します。この値は、[インフラストラクチャのサイズ](#)に基づいて調整してください。ESET PROTECTをインストールしESET ManagementエージェントとESETエンドポイント製品をクライアントコンピューターに展開した後にポリシーを使用します。

[新しい静的グループを作成](#)します。[ポリシー]をクリックして、新しいポリシーを追加します。下部にある[アクション](#)をクリックし、**新規**を選択します。

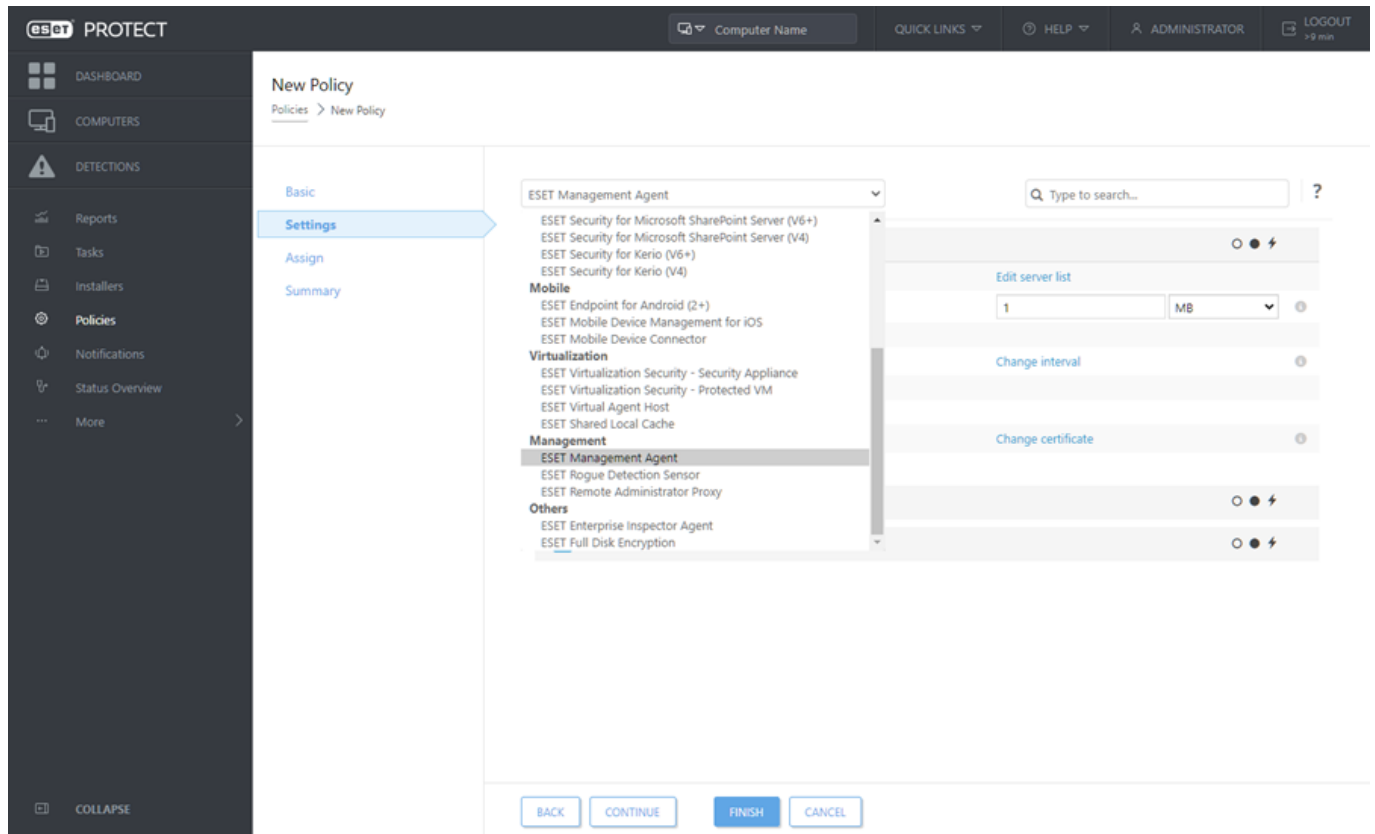


基本

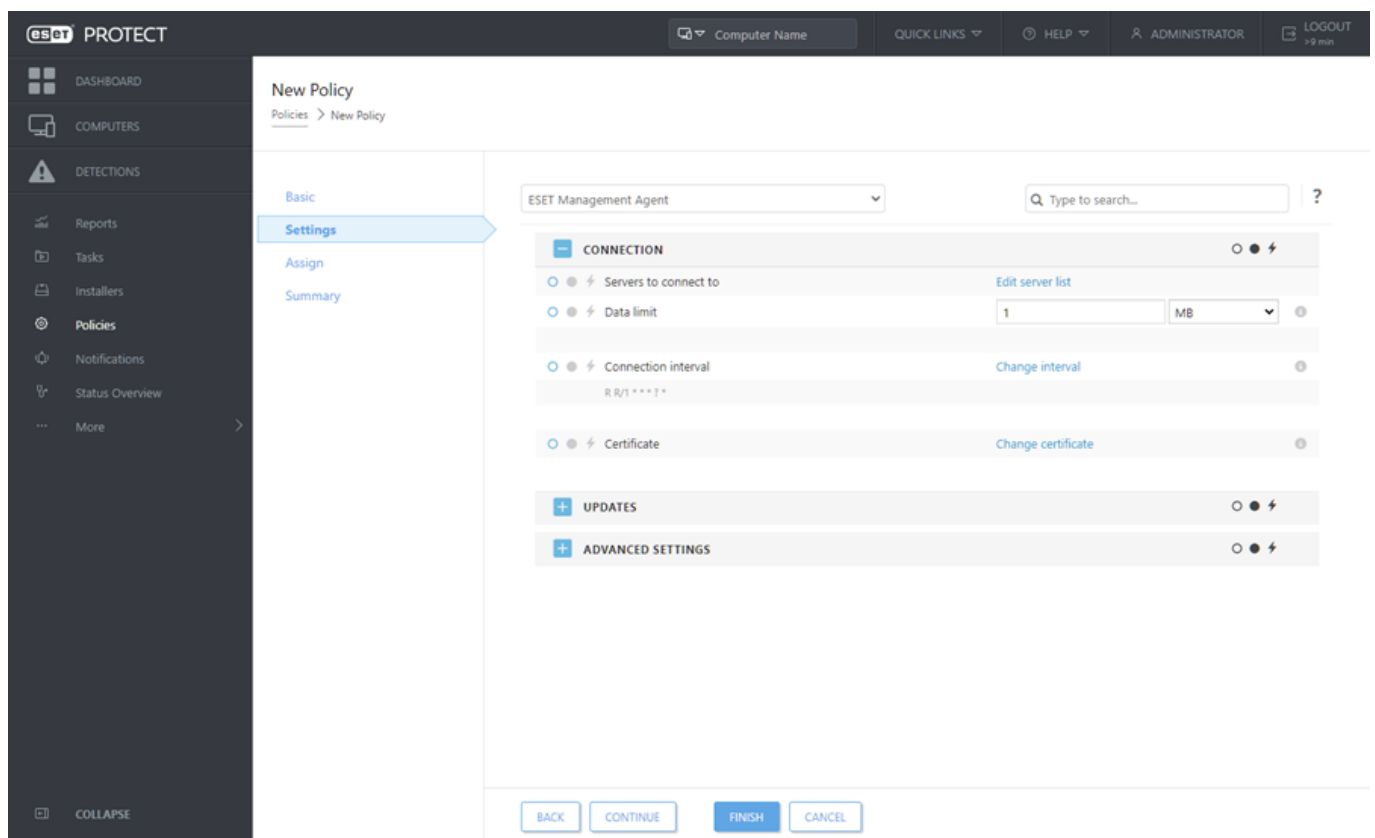
新しいポリシーの**名前**を入力します(Agent Connection Intervalなど)。**[説明]**フィールドは任意です。

設定

[製品]ドロップダウンメニューから、**[ESET Management エージェント]**を選択します。



接続間隔 > 間隔の変更をクリックします。



[定期間隔]フィールドで、任意の間隔(ESET Managementエージェントの既定のレプリケーション間隔は60秒)に値を変更し、[保存]をクリックします。

Interval

Interval between connections

☒ Regular interval
 ☐ CRON expression

Regular interval

CRON expression

Save

Cancel

割り当て

このポリシーを受信するクライアント(個別のコンピューター/モバイルデバイスまたはグループ全体)を指定できます。

ESOT PROTECT

Computer Name

QUICK LINKS

HELP

ADMINISTRATOR

LOGOUT 9 min

DASHBOARD

COMPUTERS

DETECTIONS

Reports

Tasks

Installers

Policies

Notifications

Status Overview

More

New Policy

Policies > New Policy

Basic

Settings

Assign

Summary

ASSIGN...

UNASSIGN

TARGET NAME	TARGET DESCRIPTION	TARGET TYPE
NO DATA AVAILABLE		

BACK

CONTINUE

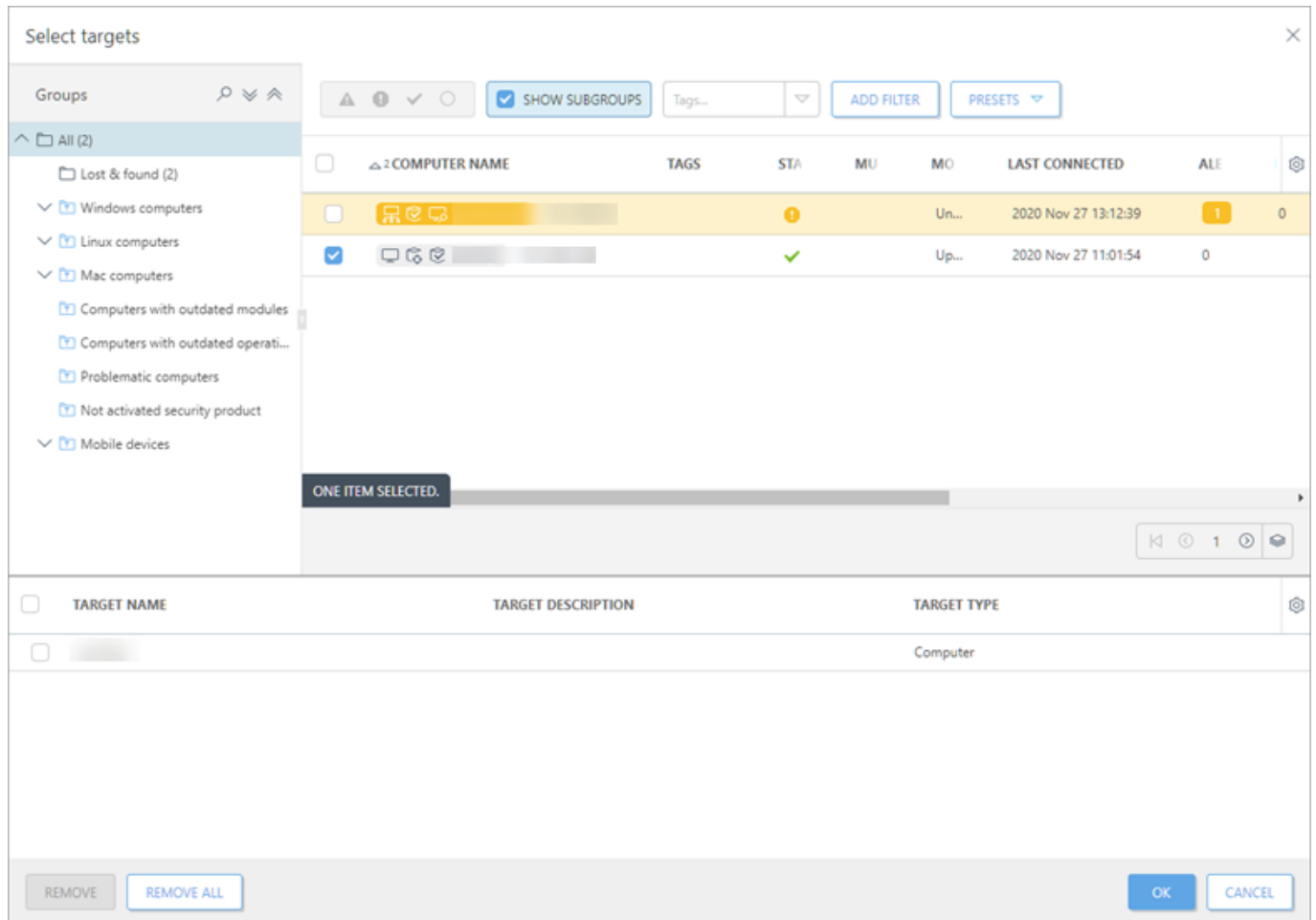
FINISH

CANCEL

[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。任意のコンピューターまたはグループを選択し、**OK**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、Webコンソールの速度低下を防止します。
多数のコンピューターを選択するとWebコンソールに警告が表示されます。



概要

このポリシーの設定を確認し、[完了]をクリックします。ポリシーは、次回ESET PROTECTサーバーに接続した後にターゲットに適用されます(エージェント接続間隔によって異なります)。

i ポリシーをただちに適用するには、コンピューターのターゲットでウェイクアップコールの送信アクションを実行できます。

新しいESET Managementサーバーに接続するためのESET PROTECTエージェントのポリシーを作成する

このポリシーでは、設定を修正してESET Managementエージェントの動作を変更できます。特に、クライアントコンピューターを新しいESET PROTECTサーバーに移行するときには、次の手順が有効です。

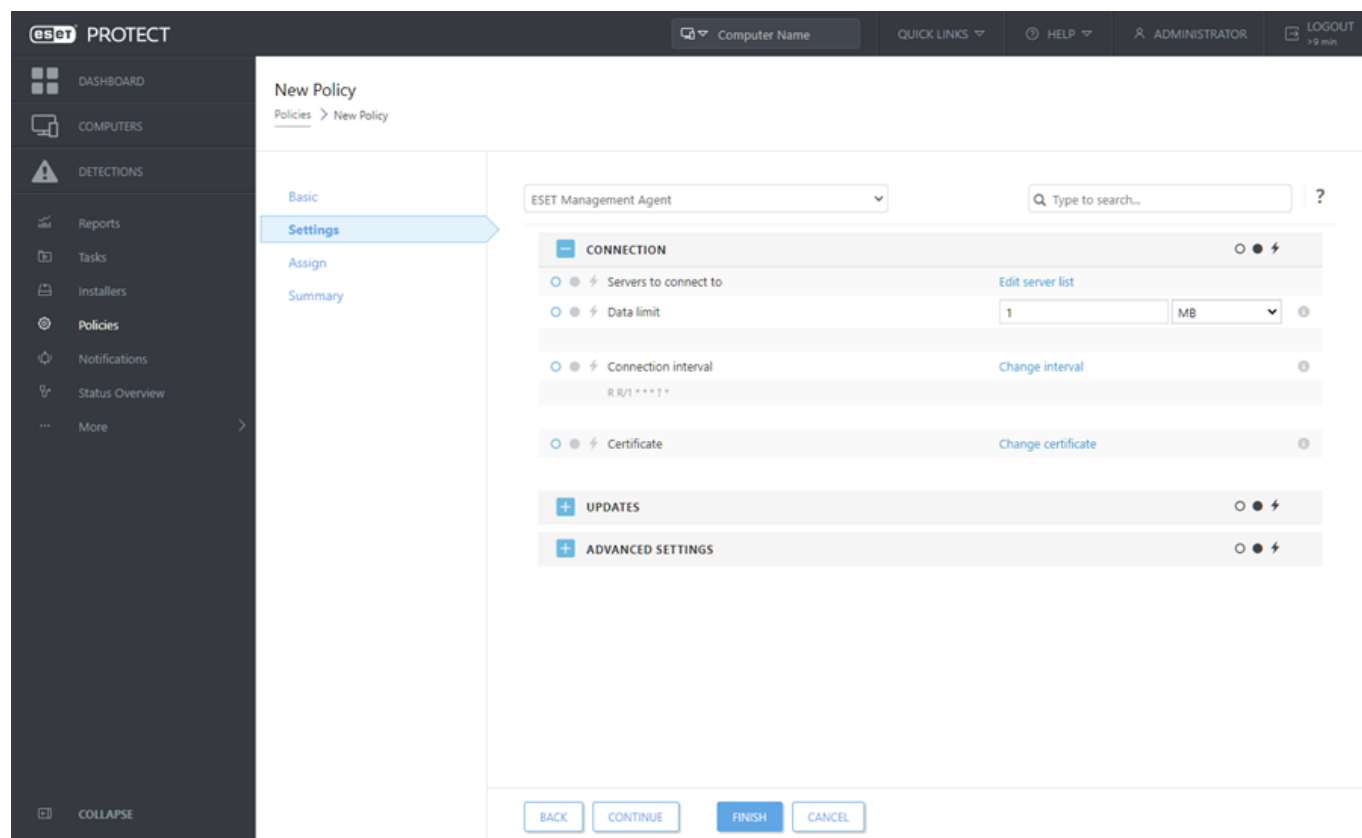
新しいポリシーを作成して、新しいESET PROTECTサーバーのIPアドレスを設定し、ポリシーをすべてのクライアントコンピューターに割り当てます。[ポリシー] > [新規作成]を選択します。

基本

ポリシーの**名前**を入力します。[説明]フィールドは任意です。

設定

ドロップダウンメニューから**ESET Management エージェント** を選択し、**[接続]**を展開し、**接続するサーバー**の横の**[サーバーリストの編集]**をクリックします。



ウィンドウが開き、ESET PROTECT エージェントが接続できる ESET Management サーバーアドレスの一覧が表示されます。**[追加]**をクリックし、新しい ESET PROTECT サーバーの IP アドレスを**[ホスト]**フィールドに入力します。既定の ESET PROTECT サーバーポートの 2222 番以外を使用する場合は、カスタムポート番号を指定します。

Servers?□×

Server	Port	
127.0.0.1	2222	

Add

Edit

Remove

↑

▲

▼

↓

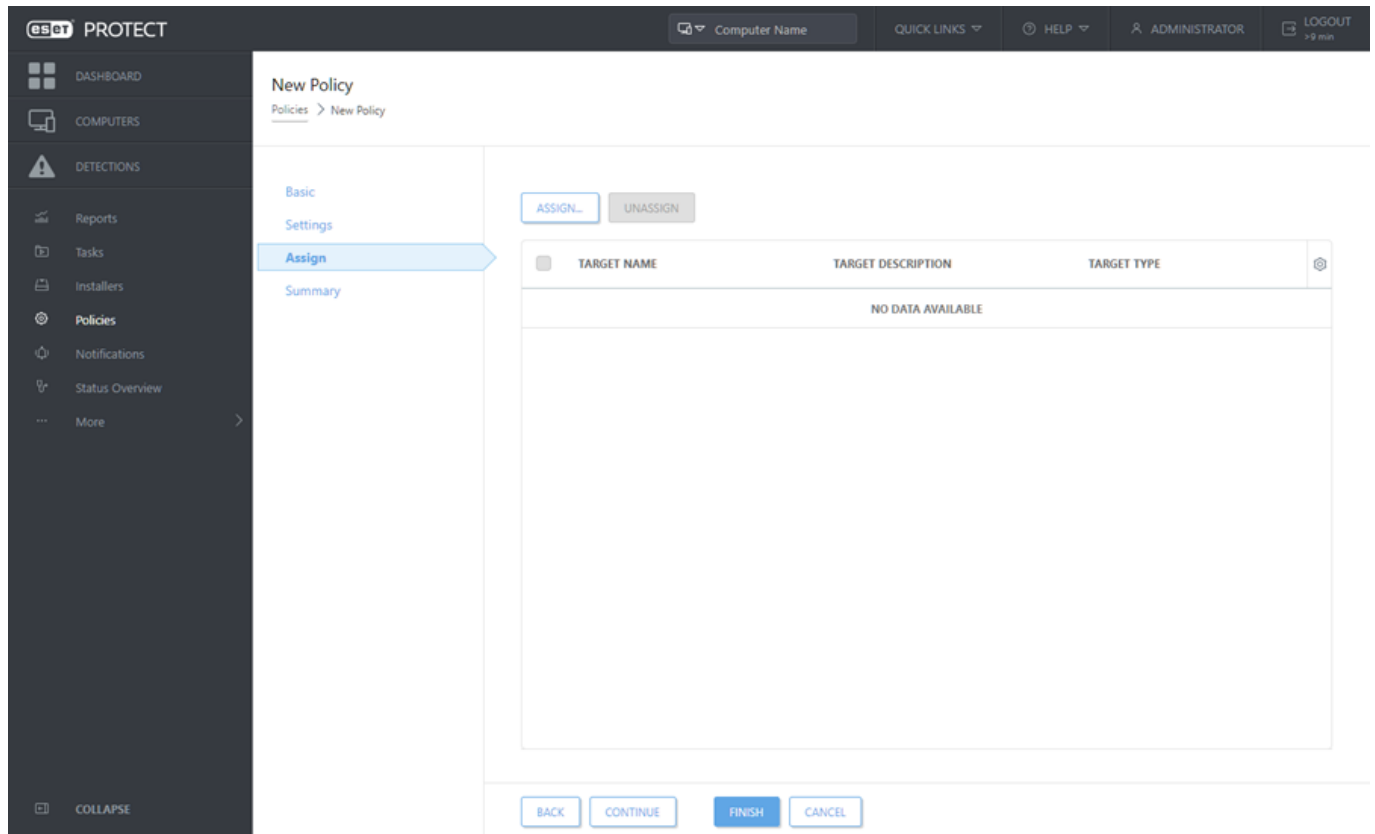
Save

Cancel

一覧に複数のエントリがある場合は、矢印ボタンを使用してESET PROTECTサーバーの優先度を変更します。二重の上矢印ボタンをクリックして、新しいESET PROTECTサーバーが最上位にあることを確認してから、[保存]をクリックします。

割り当て

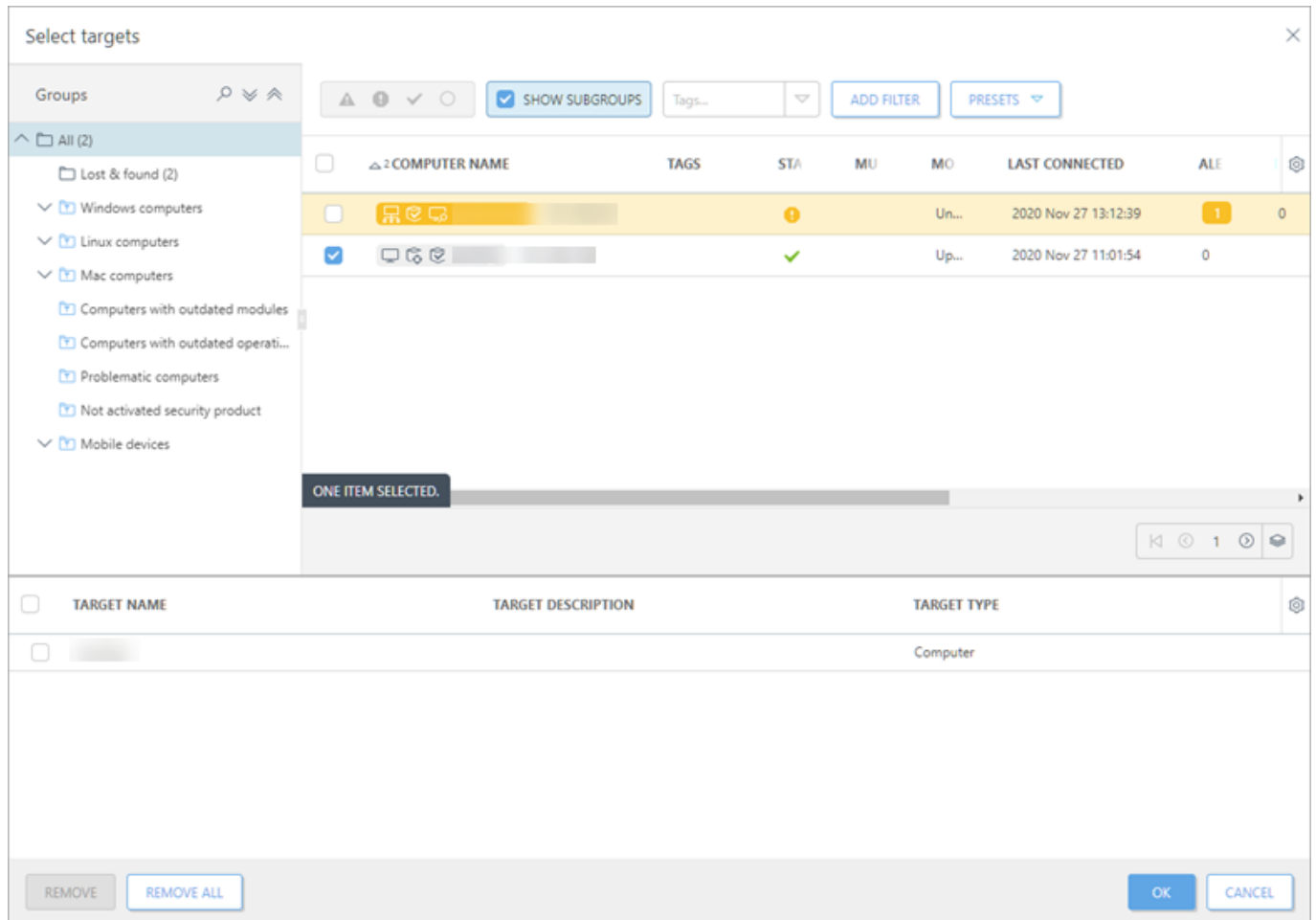
このポリシーを受信するクライアント(個別のコンピューター/モバイルデバイスまたはグループ全体)を指定できます。



[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。任意のコンピューターまたはグループを選択し、**OK**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、**Web**コンソールの速度低下を防止します。
多数のコンピューターを選択すると**Web**コンソールに警告が表示されます。



概要

このポリシーの設定を確認し、[完了]をクリックします。ポリシーは、次回ESET PROTECTサーバーに接続した後にターゲットに適用されます(エージェント接続間隔によって異なります)。

i ポリシーをただちに適用するには、コンピューターのターゲットでウェイクアップコールの送信アクションを実行できます。

ポリシーを作成してESET Managementエージェントパスワード保護を有効にする

次の手順に従い、パスワードを適用してESET Managementエージェントを保護する新しいポリシーを作成します。パスワード保護設定を使用される場合は、パスワードを入力しないかぎりESET Managementエージェントをアンインストールまたは修復できません。詳細については、「[エージェント保護](#)」を参照してください。

基本

このポリシーの**名前**を入力します。[説明]フィールドは任意です。

設定

ドロップダウンリストから**ESET Managementエージェント**を選択し、[詳細設定]を展開して[設定]に移

動し、[パスワード保護設定]フィールドにESET Managementエージェント保護で使用するパスワードを入力します。誰かがクライアントコンピューターのESET Managementエージェントをアンインストールまたは修復しようとする場合に、このパスワードが必要です。



このパスワードは安全な場所に記録してください。クライアントコンピューターからESET Managementエージェントアンインストールを許可するにはパスワードを入力する必要があります。パスワード保護設定ポリシーが設定されると、正しいパスワードを入力しないとESET Managementエージェントをアンインストールできません。

割り当て

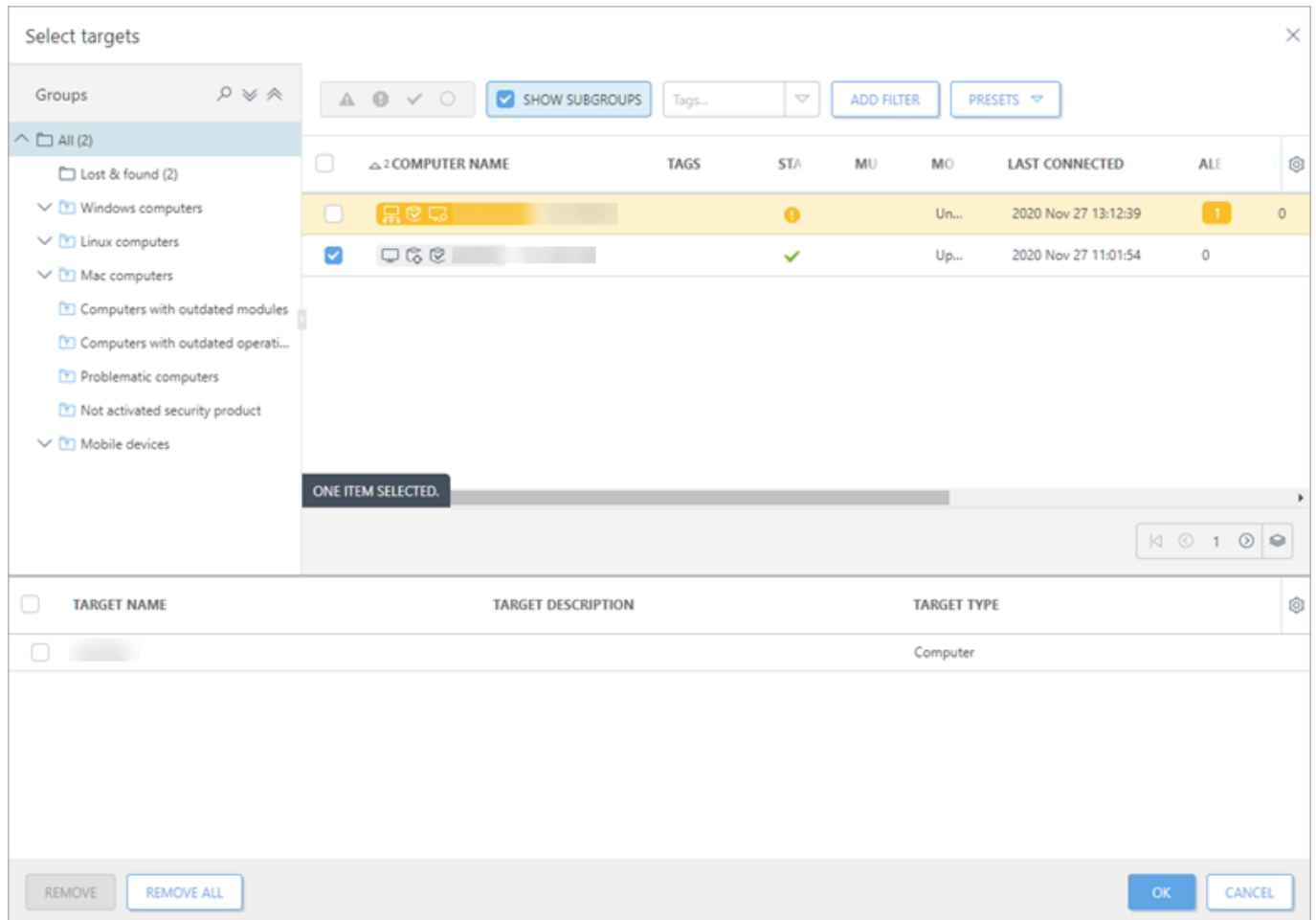
このポリシーを受信するクライアント(個別のコンピューター/モバイルデバイスまたはグループ全体)を指定できます。

The screenshot shows the ESET Protect web interface. On the left is a dark sidebar with navigation options: DASHBOARD, COMPUTERS, DETECTIONS, Reports, Tasks, Installers, Policies (highlighted), Notifications, Status Overview, and More. The main content area is titled 'New Policy' and has a breadcrumb 'Policies > New Policy'. Below the title are tabs for 'Basic', 'Settings', 'Assign' (active), and 'Summary'. In the 'Assign' tab, there are 'ASSIGN...' and 'UNASSIGN' buttons. Below these is a table with headers 'TARGET NAME', 'TARGET DESCRIPTION', and 'TARGET TYPE'. The table body is empty, displaying 'NO DATA AVAILABLE'. At the bottom of the main area are buttons for 'BACK', 'CONTINUE', 'FINISH', and 'CANCEL'.

[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。任意のコンピューターまたはグループを選択し、**OK**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、Webコンソールの速度低下を防止します。
多数のコンピューターを選択するとWebコンソールに警告が表示されます。



概要

このポリシーの設定を確認し、[完了]をクリックします。ポリシーは、次回ESET PROTECTサーバーに接続した後にターゲットに適用されます(エージェント接続間隔によって異なります)。

i ポリシーをただちに適用するには、コンピューターのターゲットでウェイクアップコールの送信アクションを実行できます。

ESET Managementエージェント自動アップグレード

ESET PROTECTでは、管理されたコンピューターでのESET Managementエージェントの自動アップグレードが可能です。

ESET Managementエージェント自動アップグレード要件

- ESET Managementエージェント8.1以降。
- エージェント自動アップグレードは、8.1より後のESETPROTECTサーバーバージョンをインストール(または8.1より後のESET PROTECTサーバーバージョンにアップグレード)した後に開始します。

ESET Managementエージェント自動アップグレードの仕組み

- エージェントは、インストールされているESET PROTECTサーバーと互換性がある最新バージョンにアップグレードされます。通常、このバージョンはインストールされているESETPROTECTサーバーのバージョンです(例: 9.0)。

- 既定ではエージェント自動アップグレードが有効です。[ESET Management エージェントポリシー](#) > アップデートで無効にし、**自動アップグレードを有効にする**スライダーバーを無効にできます。
- 管理者がすぐにアップグレードを開始しない場合は、新しいバージョンのESET Management エージェントがリポジトリにリリースされた後、ESET Management エージェント自動アップグレードトリガーは2週間後にトリガーされます。
- 自動アップグレードは、ネットワークおよび管理されたコンピューターに対する影響の増大を防止するために、長期間、アップグレードプロセスが段階的に配布されることを保証するために設計されています。

トラブルシューティング - エージェント接続

クライアントコンピューターがESET PROTECTサーバーに接続していない可能性がある場合は、クライアントコンピューターでローカルにESET Management エージェントのトラブルシューティングを実行することをお勧めします。

既定ではESET Management エージェントは20分ごとにESET PROTECTサーバーと同期します。この設定を変更するには、[ESET Management エージェント接続間隔](#)の新しいポリシーを作成します。

最新のESET Management エージェントログファイルを確認します。ファイルは次の場所にあります。

Windows	<code>C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs</code>
Linux	<code>/var/log/eset/RemoteAdministrator/Agent/ /var/log/eset/RemoteAdministrator/EraAgentInstaller.log</code>
macOS	<code>/Library/Application Support/com.eset.remoteadministrator.agent/Logs/ /Users/%user%/Library/Logs/EraAgentInstaller.log</code>

- **last-error.html** - ESET Management エージェントが実行中に記録された最後のエラーを示すプロトコル (表)。
- **software-install.log** - ESET Management エージェントによって実行された最後のリモートインストールタスクのテキストプロトコル。
- **trace.log** - 記録されたエラーを含むすべてのESET Management エージェントアクティビティの詳細なレポート。

i **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)。

- **status.html** ESET Management エージェントとESET PROTECTサーバーとの通信の現在の状態を示す表。ログにはHTTPプロキシ設定、適用されたポリシー(適用された除外を含む)のリスト、デバイスが属する動的グループのリストも含まれます。

i エージェント接続のトラブルシューティングでの**status.html**ファイルの使用については、[ナレッジベース記事](#)を読むことをお勧めします。

ESET Management エージェントがESET PROTECTサーバーに接続できなくなる最も一般的な問題:

- インターネットネットワークが正しく構成されていません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が、ESET Management エージェントがインストールされているクライアントコンピューターと通信できることを確認してください。

- ESET PROTECT サーバーがポート 2222 番でリスニングするように構成されていません。
- DNS が正しく動作していないか、ポートがファイアウォールによってブロックされています。ESET PROTECT で使用される [ポートの一覧](#)を確認するか、ナレッジベース記事の「[ESET 製品の完全な機能を許可するためには、他社製のファイアウォールでどのアドレスとポートを開く必要がありますか。](#)」を参照してください。
- [ESET PROTECT サーバー認証機関の公開鍵と一致しない虚偽または制限された特徴を含む誤って生成された証明書が使用されています。問題を解決するには、新しい ESET Management エージェント証明書を作成してください。](#)

トラブルシューティング – エージェント展開

ESET Management エージェント展開中には問題が発生する場合があります。展開が失敗した場合、さまざまな原因が考えられます。このセクションでは次のことができます。

o ESET Management エージェント展開が失敗した原因を探す

o 以下の表に従って考えられる原因を確認する

o 問題を解決して、展開を正常に実行する

Windows

1. エージェント展開が失敗した理由を見つけるには、**レポート > 自動**に移動し、**過去30日間のエージェント展開タスク情報**をクリックします。展開情報のテーブルが表示されます。**進行状況**列には、エージェント展開が失敗した理由を説明するエラーメッセージが表示されます。

詳細が必要な場合は、ESET PROTECT サーバートレースログの詳細レベルを変更できます。**[詳細] > [サーバー設定] > [詳細設定] > [ロギング]**に移動し、ドロップダウンメニューから**[エラー]**を選択します。エージェント展開をもう一度実行します。失敗したら ESET PROTECT サーバートレースログファイルの下にある最新のログエントリを確認します。レポートには、問題の解決方法が提案されます。

最新のファイルは次の場所にあります。

ESET PROTECT サーバーログ	<i>C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log</i>
ESET Management エージェントログ	<i>C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs</i>

i *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* と同じフォルダー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)。
ESET Management エージェントの接続の問題がある場合には、詳細について、「[トラブルシューティング – エージェント接続](#)」を参照してください。

2. 以下の表は、エージェント展開が失敗したさまざまな理由が記載されています。

エラー メッセー ジ	考えられる原因
接続で きませ んでし た	<ul style="list-style-type: none"> クライアントがネットワークで到達できません。ファイアウォールが通信をブロックしています 受信ポート135、137、138、139、445がクライアントのファイアウォールまたはWindows Firewallで開いていません受信ファイルとプリンター共有例外の許可が使用されていません。 クライアントのホスト名を解決できませんでした。有効なFQDNコンピューター名を使用してください
アクセ スは拒 否され ました	<ul style="list-style-type: none"> ドメインに参加しているサーバーからドメインに参加しているクライアントに展開するときには、以下の形式のDomainAdminグループのメンバーであるユーザーの資格情報を使用します。Domain\DomainAdmin ドメインに参加しているサーバーからドメインに参加しているクライアントに展開するときには、ネットワークサービスからESET PROTECTサーバーサービスを一時的に昇格し、ドメインアカウント管理者の下で実行できます。 サーバーから同じドメインにないクライアントに展開するときには、ターゲットコンピューターのUACフィルタリングを無効にします サーバーから別のドメインのクライアントにデプロイする場合は、Administratorsグループのメンバーであるローカルユーザーの資格情報を次の形式で使しますAdminターゲットコンピュータ名は、ログインの前に自動的に追加されます。 管理者アカウントのパスワードが設定されていません 不十分なアクセス権です ADMIN\$管理共有が使用できません IPC\$管理共有が使用できません 簡易ファイル共有が有効です
パッケー ジがリ ポジト リに見 つかり ません	<ul style="list-style-type: none"> リポジトリへのリンクが正しくありません リポジトリが使用できません リポジトリには特定の必要なパッケージがありません
エ ラー1603	<ul style="list-style-type: none"> •<i>ra-agent-install.log</i> ファイルを確認してください。次の場所にあります。次の場所にあります。ターゲットコンピューターの <i>C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log</i> • エラーが解決しない場合は、ナレッジベース記事の手順に従ってください。

3. 考えられる原因に応じて、適切なトラブルシューティング手順を実施します。

- **クライアントがネットワークで到達できません** - ESET PROTECTサーバーからクライアントの接続を確認します。応答がある場合は、リモートでクライアントコンピューターにログインします(リモートデスクトップ経由など)。
- **ファイアウォールが通信をブロックしています** - クライアントとサーバーの両方で、ファイアウォール設定と、これらの2台のコンピュータ間に存在する他のファイアウォール(該当する場合)を確認します。
- **クライアントのホスト名を解決できませんでした** - DNSの問題に対する考えられる解決策には次の点があります(ただしこれに限定されません)。

o エージェント展開の問題があるサーバーまたはクライアントのIPアドレスおよびホスト名のnslookupコマンドを使用します。結果はコンピューターからの情報と一致するはずですが。たとえば、ホスト名のnslookupは、ipconfigコマンドが問題のホストに表示するIPアドレスを解決します。nslookupコマンドはクライアントとサーバーで実行される必要があります。

o重複するDNSレコードがあるかどうか手動で調査します。

- **ポート2222と2223がファイアウォールで開いていません** - 上記と同じ。2台のコンピューター(クライアントとサーバー)間のすべてのファイアウォールでこれらのポートが開いていることを確認してください。
- **管理者アカウントのパスワードが設定されていません** - 管理者アカウントの適切なパスワードを設定します(空のパスワードは使用しないでください)。
- **不十分なアクセス権** - [エージェント展開タスク](#)の作成時にドメイン管理者の認証情報を使用してください。ワークグループにクライアントコンピューターがある場合、その特定のコンピューターでローカル管理者アカウントを使用します。



展開が成功した後、ポート2222と2223がファイアウォールで開きません。これらのポートが2つのコンピューター(クライアントとサーバー)間のすべてのファイアウォールで開いていることを確認します。

- Administratorユーザーアカウントを**有効にする**

1.管理コマンドプロンプトを開きます

2.次のコマンドを入力します。

```
net user administrator /active:yes
```

- **ADMIN\$管理共有が使用できません** - クライアントコンピューターで共有リソースADMIN\$を有効にする必要があります。他の共有([スタート]>[コントロールパネル]>[管理ツール]>[コンピューター管理]>[共有フォルダ]>[共有])間でこれが存在することを確認してください。
- **管理共有が使用できません** - サーバーがIPC\$にアクセスできることを確認します。サーバーのコマンドプロンプトから次のコマンドを発行します。

```
net use \\clientname\IPC$[]clientnameはターゲットコンピューターの名前です。
```

- **簡易ファイル共有の使用が有効です - アクセスが拒否されました**というエラーメッセージが表示され、ドメインとワークグループの両方を含む混合環境を使用している場合は、エージェント展開の問題が発生しているすべてのコンピューターで、**[簡易ファイル共有を使用する]**または**[共有ウィザードを使用する]**を無効にします。例えばWindows 7の場合は次のようにします。

oスタートをクリックし、**検索**ボックスにfolderと入力してから、**フォルダーオプション**をクリックします。**表示**タブをクリックして、**詳細設定**ボックスでリストを下方向にスクロールし、**共有ウィザードを使用**の横のチェックボックスをオフにします。

- **リポジトリへのリンクが正しくありません** - ESET PROTECT Webコンソールで**[管理]>[\[サーバー設定\]](#)**に移動し、**[詳細設定]>[リポジトリ]**をクリックして、リポジトリのURLが正しいことを確認します。
- **パッケージがリポジトリに見つかりません** - 通常、このエラーメッセージは、ESET PROTECTリポジトリに接続していないときに表示されます。インターネット接続を確認してください。

LinuxとMac OS

LinuxまたはMac OSでエージェント展開が動作しない場合、一般的に、SSHの問題が原因です。クライアントコンピューターを確認し、SSHデーモンが実行中であることを確かめてください。修正したら、エー

ジェント展開をもう一度実行します。

ESET Management エージェント展開のシナリオ例

このセクションではESET PROTECT展開の4つの検証済みシナリオを示します。

- 1.ESET PROTECTサーバーアプライアンスまたはLinux ESET PROTECTサーバーから [ドメインに参加していない](#) Windowsターゲットへの展開。
- 2.Windows ESET PROTECTサーバー、ドメインに参加していないWindowsソースから、[ドメインに参加していない](#) Windowsターゲットへの展開。
- 3.ESET PROTECTサーバーアプライアンスまたはLinux ESET PROTECTサーバーから [ドメインに参加している](#) Windowsターゲットへの展開。
- 4.Windows ESET PROTECTサーバー、ドメインに参加しているWindowsソースから、[ドメインに参加している](#) Windowsターゲットへの展開。

ドメインに参加していない対象へのESET Management エージェントの展開シナリオ例

この手順では、次のシナリオについて説明します。

- ESET PROTECTサーバーアプライアンスまたはLinux ESET PROTECTサーバーからドメインに参加していない **Windowsターゲット**への展開。
- Windows ESET PROTECTサーバー、ドメインに参加していないWindowsソースから、**ドメインに参加していない** Windowsターゲットへの展開。

前提条件

- 同じローカルネットワーク。
- 機能するFQDN名。例: desktop-win7.test.localは192. 168. 1. 20に対応します(逆も同様)。
- 既定値でMSDNからインストールされたクリーンなオペレーティングシステム。

対象:

Windows 10 Enterprise

Windows 8.1 Enterprise

Windows 7 Enterprise

1. Administratorsグループのメンバーであるユーザーとパスワードを作成します。例: **管理者**
 - a.**Microsoft Management Console**を開きます。開くには、**実行**コンソールを開き、フィールド

に“mmc”と入力し、**OK**をクリックします。

b. ローカルユーザーとグループナックインをファイル → スナックインの追加と削除から追加します。新しいユーザーをユーザーフォルダーに追加し、フィールドに必須情報を入力します(必ずパスワードを入力します)。**[グループ]**セクションで、**Administrators**グループの**[プロパティ]**を開き、**[追加]**ボタンをクリックして新しく作成されたユーザーをグループに追加します。新しく作成されたユーザーのログイン名を**[選択するオブジェクト名を入力]**に入力し、**[名前の確認]**ボタンをクリックして検証します。

2. ネットワークと共有センターでネットワーク設定をパブリックネットワークからプライベートネットワークに変更します。これには、**アクティブなネットワークセクションを表示**の左側でパブリックネットワークをクリックします。

3. ホームまたはオフィスネットワークの場所設定で**Windows**ファイアウォールをオンまたはオフにするをクリックし、**Windows**ファイアウォールをオフにするを選択して、プライベートネットワークの**Windows**ファイアウォールを無効にします。

4. ネットワークと共有センターで**詳細共有設定の変更**をクリックし、プライベートネットワークの**ファイルとプリンター共有が有効であることを確認**します。

5. User Account Control (UAC) リモート制限を無効にする:

a. レジストリエディターを開きます。開くには、**regedit** を**実行**コンソールに入力し、**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**を検索します

b. システムファイルで新しい**DWORD**値の名前を **LocalAccountTokenFilterPolicy** にして作成します。

c. 作成されたファイルを開き、**値データ**を**1**に設定します。

ESET PROTECT Web コンソール:

ESET PROTECT Web コンソールで、新しい [エージェント展開](#) サーバータスクを作成します。

1. **ターゲット** - ターゲット Windows コンピューターを選択します。

2. **サーバーホスト名(任意)** - ESET PROTECT サーバーの FQDN 名または IP アドレスを入力します。(コンピューターの FQDN 名を確認するには、**コンピューター**を右クリックし、**プロパティ**を選択します。FQDN 名は完全なコンピューター名の横に表示されます)。

3. **ユーザー名** - **管理者**(ドメイン名またはコンピューター名プレフィックスなし)を入力し、このユーザーのパスワードを入力します。

4. **ESET PROTECT 証明書** - **証明書が選択されていません**をクリックして、**エージェント証明書**を選択します。

5. **完了**をクリックして、タスクを実行します。

ドメインに参加している対象へのESET Management エージェントの展開シナリオ例

この手順では、次のシナリオについて説明します。

- ESET PROTECTサーバーアプライアンスまたはLinux ESET PROTECTサーバーからドメインに参加しているWindowsターゲットへの展開。
- Windows ESET PROTECTサーバー、ドメインに参加しているWindowsソースから、ドメインに参加しているWindowsターゲットへの展開。

前提条件

- 同じローカルネットワーク。
- 機能するFQDN名。例: desktop-win10.protect.localは10.0.0.2に対応します(逆も同様)。
- 既定値でMSDNからインストールされたクリーンなオペレーティングシステム。
- netbios名PROTECTを使用して作成されたドメインprotect.local
- ドメインコントローラーのDomain AdminsセキュリティグループのメンバーであるユーザーDomainAdmin
- 各コンピューターがユーザーDomainAdminでドメインprotect.localに参加していて、このユーザーがAdministratorであること。
- DomainAdminは各コンピューターにログインし、ローカル管理タスクを実行できること。
- Windows ESET PROTECT Serverサービスは「PROTECT\DomainAdmin」資格情報で一時的に実行されていること。展開後、ネットワークサービスアカウントは十分です(仮想アプライアンスまたはLinuxでの変更は不要です)。

対象:

Windows 10 Enterprise

Windows 8.1 Enterprise

Windows 7 Enterprise

1. ネットワークと共有センターを開きます。
2. ネットワークが[アクティブなネットワークの表示]セクションで[ドメインネットワーク]であることを確認します。
3. ドメインネットワークの場所設定でWindowsファイアウォールをオンまたはオフにするをクリックし、Windowsファイアウォールをオフにするを選択して、ドメインネットワークのWindowsファイアウォールを無効にします。

4. ネットワークと共有センターで詳細共有設定の変更をクリックし、ドメインネットワークのファイルとプリンター共有が有効であることを確認します。

ESET PROTECT Webコンソール:

ESET PROTECT Webコンソールで、新しい[エージェント展開](#)サーバータスクを作成します。

1. **ターゲット** - ターゲットWindowsコンピューターを選択します。
2. **サーバーホスト名(任意)** - ESET PROTECTサーバーのFQDN名またはIPアドレスを入力します。(コンピューターのFQDN名を確認するには、**コンピューター**を右クリックし、**プロパティ**を選択します[FQDN名は完全なコンピューター名の横に表示されます])。
3. **ユーザー名** - **PROTECT\DomainAdmin** (ドメイン全体を含める必要があります)と、このユーザーのパスワードを入力します。
4. **ESET PROTECT証明書** - 証明書が選択されていませんをクリックして、**エージェント証明書**を選択します。
5. **完了**をクリックして、タスクを実行します。

ESET PROTECT メインメニュー

すべてのクライアントは[ESET PROTECT Webコンソール](#)で管理されます。互換性がある[ブラウザ](#)を使用して、任意のデバイスからESET PROTECT Webコンソールにアクセスできます。ウィザードを使用している場合を除き、左側には常に**メインメニュー**があります。☰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。

左側のメインメニューにはESET PROTECTのメインセクションと次の項目があります。

☐	ダッシュボード
💻	コンピューター
⚠️	検出
📊	レポート
📁	タスク
📖	インストーラー
⚙️	ポリシー
🔔	通知
🔗	ステータス概要
⋮	詳細

ダッシュボード

ダッシュボードは、既定ページとなっており、ユーザーがESET PROTECT Webコンソールにログインした後、はじめに表示されます。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。

ダッシュボード操作

- **追加** - **+** 記号(ダッシュボードヘッダーの上)をクリックし、新しいダッシュボードを追加します。新しいダッシュボードの名前を入力し、**ダッシュボードの追加**をクリックして確認します。新しい空のダッシュボードが作成されます。
- **移動** - **⇄** 記号(ダッシュボード名をクリックしてドラッグし、他のダッシュボードに相対的な場所を変更します。
- 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。
- ダッシュボードを選択し、**ダッシュボード**の横 **⚙** 歯車アイコンをクリックして、**既定に設定**を選択し、ダッシュボードにアクセスできるすべての新しいWebコンソールユーザーの既定のダッシュボードとしてダッシュボードを使用します。

選択したダッシュボードタイトルの横の歯車アイコン **⚙** をクリックし、ドロップダウンメニューで次のオプションを取得します。

🔄 ページの更新	このダッシュボードでレポートテンプレートを更新します。
✕ 削除	ダッシュボードを削除します。
📄 名前の変更	ダッシュボード名を変更します。
📋 複製	ユーザーのホームグループで同じパラメーターのダッシュボードのコピーを作成します。
レイアウトの変更	このダッシュボードの新しいレイアウトを選択します。変更により、現在のテンプレートがダッシュボードから削除されます。

i これらの既定のダッシュボードをカスタマイズできません。ステータス概要、セキュリティ概要、DynamicThreat Defense

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。

ステータス概要

ステータス概要ダッシュボードは、ESET PROTECTにログインするたびに表示される既定の画面です(別のダッシュボードを既定のダッシュボードに設定していない場合)。ネットワークに関する一般情報が表

示されます。

- **デバイスフィルター** – 最後に報告されたステータスに基づき、管理されたデバイス数を表示します。4つのタイルをそれぞれクリックし、デバイスのフィルタリングされたリストを表示できます。
- **デバイスステータス** – 該当するタブでインストールされたセキュリティ製品のタイプに基づき、管理されたデバイス数を表示します。グループのセキュリティ製品が展開されていない場合、タブには該当するインストーラーパッケージを展開するオプションが表示されます。
- **接続ステータス** – 最後に接続された管理されたデバイスの一覧を表示します。
- **製品バージョンステータス** – プラットフォームに基づき、最新および古いセキュリティ製品バージョンの比率を表示します。

○ **不明** (灰色) – インストールされているESET製品のバージョンは認識されません(ESET製品の新規インストールの直後など)。

○ **最新** (緑) – 最新バージョンのESET製品がインストールされています。

○ **最新の状態ではない** – 古いアプリケーション表示黄/赤色のグラフをクリックすると、インストールされたESET製品のアップデートを選択して、アップデートを開始できます。

■ **黄色** - ESET製品のインストールされているバージョンは最新ではありませんが、サポートされています(通常、最近検出されたセキュリティ脆弱性が含まれている場合を除き、最新バージョンよりも古い2つのバージョンは黄色です)。

■ **赤** - ESET製品のレガシーバージョンまたはセキュリティ脆弱性が検出された古いバージョン(サポート対象外で、ESET PROTECTリポジトリから削除)。

- **管理ステータス - 管理および保護** (ESETエージェントとセキュリティ製品がインストールされたクライアントデバイス)、**管理** (エージェントのみのクライアントデバイス)、**管理対象外** (ESET PROTECTに認識されているネットワークにあり、エージェントがないクライアントデバイス)、**Rogue** (ESET PROTECTに認識されずRogue Detection Sensorで検出されたクライアントデバイス)。
- **RSSフィード** - [WeLiveSecurity](#) および [Esetナレッジベースポータル](#) からRSSフィードを表示します。**RSSフィード**で歯車アイコンをクリックすると、**フィード自動再生をオフにするか**、**個別のフィードソースをオフにするか**、**RSSフィードをオフにすることができます**。

インシデント概要

重要度、検出方法、解決ステータス、検出がある上位10のコンピューター/ユーザーなど、過去7日間に見つかった未解決の検出の概要を示します。

Dynamic Threat Defense

[ESET Dynamic Threat Defense](#)を使用している場合は、便利なESET Dynamic Threat Defense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ステータス

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のCPUの負荷、データベース接続などESET PROTECTの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

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 Dynamic Threat Defense](#) (適切なライセンスがある場合))が表示されます。

ダッシュボードレポートのアクション

 サイズの変更	クリックすると、レポートを全画面モードで表示することができます。
 更新	レポートテンプレートを更新します。
 ダウンロード	ダウンロード をクリックし、レポートを生成してダウンロードします。 .pdf または .csv を選択できます。CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します
 変更	テンプレートのリストから別のレポートテンプレートを選択します。
 レポートテンプレートの編集	既存のレポートテンプレートを編集します。 新しいレポートテンプレートを作成する 場合と同じ設定とオプションが適用されます。
 更新間隔の設定	テンプレートのカスタム更新間隔を設定します。
 スケジュール	レポートのスケジュール - トリガー調整 、およびレポート配信のスケジュールを修正できます。 スケジュールされたレポートタブ に、すべてのスケジュールされたレポートが表示されます。
 削除	ダッシュボードからレポートテンプレートを削除します。
 名前の変更	レポートテンプレート名を変更します。
このセル	このダッシュボードの新しいレイアウトを選択します。変更により、現在のテンプレートがダッシュボードから削除されます。

ダッシュボードの権限

ユーザーはダッシュボードを操作する適切な権限が必要です。ユーザーが[アクセス権](#)があるグループに含まれるレポートテンプレートのみをダッシュボードで使用できます。[レポートとダッシュボードの権限](#)がユーザーに割り当てられていない場合は、ダッシュボードセクションにデータが表示されません。管理者は既定ですべてのデータを表示できます。

- **読み取り** – レポートテンプレートとカテゴリを一覧表示します。レポートテンプレートに基づいてレポートを生成できます。ユーザーは自分のダッシュボードを読み取れます。
 - **使用** – 使用可能なレポートテンプレートでダッシュボードを修正できます。
 - **書き込み** – レポートテンプレートとカテゴリを作成、修正、削除できます。
- すべての既定のテンプレートは[すべて]グループにあります。

ドリルダウン

ドリルダウンダッシュボード機能を使用して、詳細にデータを検査できます。サマリーが特定の項目を対話的に選択し、詳細データを表示できます。サマリー情報からドリルダウンして関心項目に焦点を当て、この特定の項目に関する詳細を表示します。通常は、ドリルダウンできる複数のレベルがあります。

複数のドリルダウンオプションがあります。

- **詳細情報の表示** – コンピューター名と説明、静的グループ名など。クリックした行の元のデータ(未集計)を表示します。
- **値のみを表示** – 選択した重要度レベルのデータのみを表示します。情報、緊急、セキュリティリスク、セキュリティ通知など。
- **列の展開** 値 – 集計情報が表示されます(通常はカウントまたは合計)。例えば、列に数値だけがあり、[列「コンピューター」を展開]をクリックすると、コンピューターに関するすべての詳細が一覧表示されます。
- **コンピューターの一覧で表示** – コンピューターページに移動します(100項目の結果のみを表示)。

ワンクリックアクション

検出された問題に関する情報が記載されたレポートでは、表/グラフの項目をクリックすると、追加のドリルダウンオプションを使用できます。

- **選択したアラートを解決するタスク** – 即時実行される提案されたタスクを選択すると、アラートを解決できます。

タスク経由でアラートを解決できず、ポリシー設定では解決できる場合は、次のオプションが表示されます。

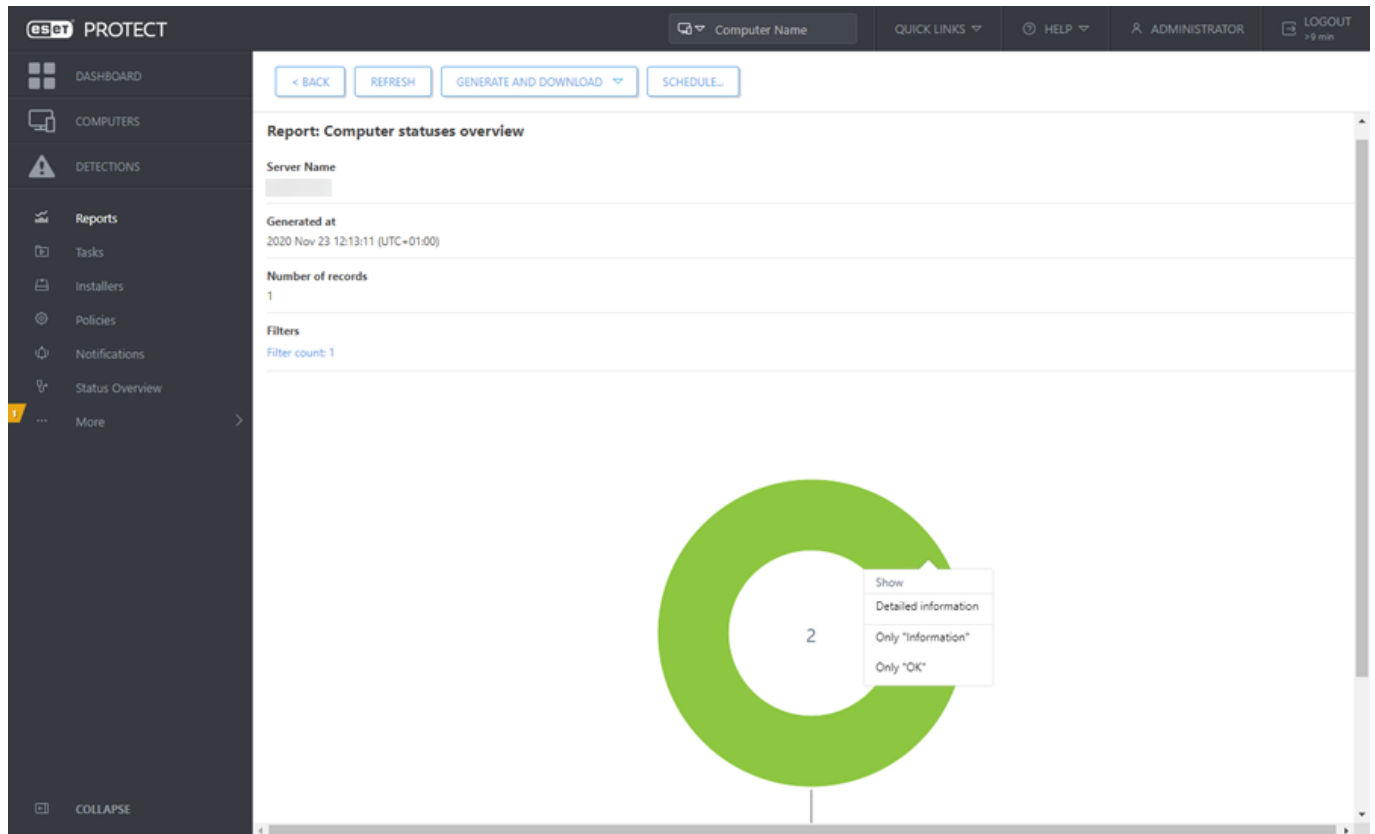
o [ポリシーの管理](#)

o 新しいポリシー

- **Webの検索** – 選択したアラートをGoogle検索します。選択したアラートを解決する提案された応答(タスクまたはポリシー設定)がない場合は、このオプションを使用できます。

i 他のレポートのドリルダウンで取得した結果には、最初の1,000項目のみが表示されます。

レポートを生成およびダウンロードする場合は、[生成とダウンロード]をクリックします。 .pdfまたは.csvを選択できます CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します



Report: Drill Down - Detailed information

Server Name: [REDACTED]

Generated at: October 28, 2021 16:48:40 (UTC+02:00)

Number of records: 2

Filters: Filter count: 3




Severity	Time of occurrence	Status	Computer name	Static group name	Adapter IPv4 address	IPv4 subnetwork	Adapter IPv6 address	IPv6 subnetwork
Warning	October 25, 2021 17:21:31	Security notification	[REDACTED]	Lost & found	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Warning	October 22, 2021 09:55:17	Security notification	[REDACTED]	Lost & found	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

コンピューター

ESETPROTECTに追加したすべてのクライアントデバイスは、[グループ](#)に分かれてこちらに表示されます。各デバイスは1つの[静的グループ](#)に割り当てられます。(左側の)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。

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、**Lost + found** グループに表示されます。ESET PROTECT Web コンソールに表示されるクライアントのステータスは、クライアントの ESET セキュリティ製品の設定とは異なります。このため、特定のステータスがクライアントに表示されない場合でも ESET PROTECT Web コンソールには表示されます。クライアントをドラッグアンドドロップし、グループ間を移動します。

ボタン **新規追加** をクリックし、次を選択します。

-  **コンピューター** - [コンピューターを選択した静的グループに追加できます](#)
-  **モバイルデバイス** - [モバイルデバイスを選択した静的グループに追加できます](#)。
-  **ディレクトリサーバー経由で同期** - [静的グループ同期](#) タスクを実行できます。

デバイスをクリックすると、そのデバイスで使え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、下のバーのアクションボタンをクリックします。アクションメニューには、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。様々なアイコンタイプとステータスの詳細については、[アイコン凡例](#)を参照してください。**アラート**列でアラート数をクリックし、[コンピューター詳細](#)セクションでアラートのリストを表示します。








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。

○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。

○赤(警告) - コンピューターは14日以上接続されていません。



ビューのフィルタリング

ビューをフィルタリングするには複数の方法があります。

- **標準フィルター**: フィルタリング条件を追加するには、**フィルターの追加**をクリックし、リストから項目を選択します。検索文字列を入力するか、フィルターフィールドでドロップダウンメニューから項目を選択して、**Enter**を押します。アクティブなフィルターは青でハイライト表示されます。
- **ステータスアイコン**を使用して、重要度別にフィルタリングできます。 **赤 - エラー**  **黄 - 警告**  **緑 - OK**  **灰色 - 管理されていないコンピューター**。重要度アイコンは、特定のクライアントコンピューター上の ESET 製品に関する現在のステータスを表します。それぞれのアイコンをオンまたはオフにして、アイコンを組み合わせる使用することができます。たとえば、警告のあるコンピューターだけを確認するには、 黄色のアイコンをオンの状態のままにします(残りのアイコンをオフにする必要があります)。 警告および  エラーの両方を確認するには、この2つのアイコンをオンのままにします。
- **フィルターの追加** > **製品カテゴリ**をクリックし、ドロップダウンメニューを使用して、表示するデバイスのタイプを選択することができます。

○**すべてのデバイス** - クライアントの表示制限(フィルタ)なしに、すべてのクライアントコンピューターを再度表示するには、ドロップダウンメニューからこのオプションを選択します。表示を絞り込む場合は、フィルタオプションの組み合わせを使用します。

○**ESET 保護** - ESET 製品で保護

○**ESET PROTECT** - エージェント  RD Sensor  サーバーなどの個別の ESET PROTECT コンポーネント。

oその他 - 共有ローカルキャッシュ、仮想アプライアンス Enterprise Inspector エージェント Enterprise Inspector サーバー

- **サブグループの表示** チェックボックス - 現在選択されているグループに対するサブグループを表示します。
- 高度なフィルタリングでは、[動的グループ](#) または [レポート](#) を使用します。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#) します。
- [フィルター](#) とフィルタープリセットを追加します。 [タグ](#) を使用して、表示される項目をフィルタリングできます。

i リスト内で特定のコンピューターを見つけることができず 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。

コンピューター詳細


コンピューターの詳細を確認するには、静的または動的グループでクライアントコンピューターを選択し、**詳細を表示** をクリックするか、コンピューター名をクリックして、右側に [コンピューターのプレビュー](#) サイドパネルを表示します。

情報ウィンドウは、次の部分で構成されています。

i 概要:

コンピューターの状況の概要を示す次のタイルがあります。

コンピューター

- **編集アイコン**  をクリックして、コンピューターの名前または説明を変更します。既に同じ名前の別の管理対象コンピューターがある場合は、**重複する名前を許可する** を選択できます。
- **タグを選択** をクリックして、[タグを割り当て](#) ます。
- **FQDN** - コンピューターの完全修飾ドメイン名

i Active Directory の下で実行されるクライアントコンピューターと ESET PROTECT サーバーがある場合は、[静的グループ同期](#) タスクを使用して、**名前** および **説明** フィールドの入力を自動化できます。

- **親グループ** - コンピューターの親静的グループを変更します。
- **IP** - コンピューターの IP アドレス。
- **適用されたポリシー数** - 数字をクリックし、適用されたポリシーの一覧を表示します。

- **動的グループのメンバー** – クライアントコンピューターが最新のレプリケーション中に存在していた動的グループのリスト。

ハードウェア

このタイルには、主要なハードウェアパラメーター、オペレーティングシステムの情報、および固有の識別子の一覧が表示されます。タイルをクリックすると、**詳細 – ハードウェア**タブが表示されます。

アラート

- **アラート** – 現在のコンピューターの問題のリストへのリンク。
- **未解決の検出数** – 未解決の検出数。カウントをクリックし、未解決の検出の一覧を表示します。
- **前回の接続時間: 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。
 - 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。
 - 赤(警告) – コンピューターは14日以上接続されていません。
- **前回検査時刻** – 前回検査の時間情報。
- **検出エンジン** – ターゲットデバイスの検出エンジンのバージョン。
- **更新** – アップデートステータス

製品とライセンス

コンピューターにインストールされているESETコンポーネントの一覧。タイルをクリックすると、**詳細 – 製品とライセンス**タブが表示されます。

暗号化

暗号化タイルは、[ESET Full Disk Encryption](#)によってサポートされるワークステーションでのみ表示されます。

ESET Dynamic Threat Defense

タイルには、サービスに関する基本情報が表示されます。次の2つのタイルステータスがあります。

- 白 – 既定の状態ESET Dynamic Threat Defenseがアクティベーションされ、動作した後、タイルは白状態です。
- 黄 - ESET Dynamic Threat Defenseサービスの問題がある場合は、タイルが黄色に変わり、問題に関

する情報が表示されます。

使用可能なアクション:

- **有効にする** – このオプションは、[製品ライセンスをインポート](#)した後に使用できます。クリックすると、現在のコンピューターでESET Dynamic Threat Defense製品のアクティベーションタスクとポリシーを設定します。

i ESET Dynamic Threat Defenseがインストールされた各デバイスではESET LiveGrid®レピュテーションシステムおよびESET LiveGrid®フィードバックシステムを有効にする必要があります。デバイスポリシーを確認してください。


- **送信** されたファイル - [送信された ファイル](#)メニューへのショートカット。
- **詳細** – 製品ページへのショートカット。

ユーザー

- **ログインユーザー**(コンピューターのみ) – デバイスにログインしたユーザーのドメインとユーザー名。
- **割り当てられたユーザー**

o **ユーザーの割り当て**をクリックし、[コンピューターユーザー](#)からこのデバイスにユーザーを割り当てます。

! コンピューターは1つの処理で最大200人のユーザーにのみ割り当てることができます。

o **ごみ箱アイコン**  をクリックし、現在のユーザーの割り当てを解除します。



o **割り当てられたユーザーのユーザー名**をクリックし、アカウント詳細を表示します。

位置情報 (モバイルデバイスのみ)。 **iOS Apple Business Manager (ABM)**のデバイスは、[紛失モード]が有効なときにのみローカライズできます 

仮想化

コンピューターを[複製のマスター](#)に設定し、VDI設定を表示した後に、タイルが表示されます。歯車アイコンをクリックしてVDI設定を変更します。

ネットワーク隔離 ボタンをクリックして、コンピューターでネットワーク隔離クライアントタスクを実行します。

-  [ネットワークから隔離する](#)
-  [ネットワーク隔離を終了](#)

仮想化ボタンは、複製用にコンピューターを設定するために使用されます。コンピューターが複製されるか、コンピューターのハードウェアが変更されるときに必要です。

- [複製のマスターとして設定する](#)

- **ハードウェア検出を無効にする** – ハードウェア変更の検出を永久的に無効にします。このアクションは元に戻せません。

- **複製のマスターから解除する** – マスターフラグを削除します。これが適用された後、コンピューターの新しいクローンを作成するたびに [質問](#)が発生します。

[ハードウェアフィンガープリント](#) 検出は次のシステムではサポートされていません。



- Linux、macOS、Android、iOS
- 仮想エージェントホスト(ESET仮想化セキュリティ)で管理されたシステム
- ESET Managementエージェントがインストールされていないコンピューター

設定

設定タブ – インストールされているESET製品(ESET Managementエージェント、ESETエンドポイントなど)の設定の一覧を含みます。使用可能なアクションは次のとおりです。

- **設定の要求**をクリックするとESET Managementエージェントのタスクを作成し、すべての管理対象の製品設定を収集できます。タスクがESET Managementエージェントに配信された後、ただちに実行され、結果は次の接続時にESET PROTECTサーバーに配信されます。これにより、すべての管理対象製品設定のリストを表示できます。

- コンテキストメニューから設定を開き、ポリシーに変換します。設定をクリックし、ビューアーで表示します。


- 設定を開くと、ポリシーに変換できます。**ポリシーに変換**をクリックします。現在の設定がポリシーウィザードに転送され、新しいポリシーとして設定を修正および保存できます。


- 診断およびサポート目的で設定をダウンロードします。選択した設定をクリックし、ドロップダウンメニューで**診断用にダウンロード**をクリックします。

適用されたポリシータブ – デバイスに適用されたポリシーのリスト。コンピューターにインストールされていないESET製品またはESET製品機能のポリシーを適用した場合は、一覧のポリシーが灰色で表示されます。

選択したデバイスに割り当てられたポリシーと、デバイスを含むグループに適用されたポリシーが表示されます。



ロックされた  (編集できない) ポリシー(特定のビルトインポリシー([自動アップデート](#)ポリシーやESET Dynamic Threat Defenseポリシーなど)、またはユーザーに**読み取り**権限がありますが、**書き込み**権限ではないポリシーの横にはロックアイコンがあります。

 **[ポリシーの管理]**をクリックし、ポリシーを管理、編集、割り当て、または削除できます。ポリシーは**順序(ポリシー順序列)**に基づいて適用されます。ポリシー適用の優先度を変更するには、ポリシーの横のチェックボックスをオンにして、**すぐに適用**または**後で適用**ボタンをクリックします。

適用された除外タブ – デバイスに適用された[除外](#)のリスト。

🕒 ログ (コンピューターのみ)

- **SysInspector - [ログの要求]** (Windowsのみ) をクリックし、[SysInspector ログ要求](#) タスクを選択したクライアントで実行します。タスクが完了した後、新しいエントリがESET SysInspectorログのリストに追加されます。リストのログをクリックすると、[展開します。](#)
- **Log Collector - Log Collectorの実行** をクリックして、[Log collector タスク](#) を実行します。タスクが完了した後、新しいエントリがログのリストに追加されます。リストのログをクリックすると、ダウンロードします。
- **診断ログ - 診断 > オン** をクリックすると、現在のコンピューターで診断モードを開始します。診断モードは、クライアントにすべてのログをESET PROTECTサーバーに送信させます。すべてのログは24時間以内に参照できます。ログは5つのカテゴリに分けられます。**迷惑メールログ、ファイアウォールログ、HIPSログ、デバイス コントロールログおよびWeb コントロールログ** **診断 > すべてのログを再送信** をクリックし、次のレプリケーションでエージェントからすべてのログを再送信します。 **診断 > オフ** をクリックすると、診断モードが停止します。

デバイスごとのログ配信のファイルサイズ上限は200MBです。Webコンソールの **詳細を表示 > ログ** セクションからログにアクセスできます。タスクによって収集されたログが200 MBより大きい場合は、タスクが失敗します。タスクが失敗した場合は次の処理を実行できます。

- デバイスでローカルにログを収集します。

i • ログの詳細レベルを変更し、タスクを再実行します。

OWindowsターゲットの場合、/Targets:EraAgLogsパラメーターを使用してESETManagementエージェントログのみを収集します。

OLinux/macOSターゲットの場合、--no-productlogsパラメーターを使用して、インストールされたESETセキュリティ製品からログを除外します。

▷ タスクの実行時刻

実行されたタスクのリスト。ビューをフィルタリングし、結果を絞り込めます。また、[タスクの詳細](#)を表示したり、タスクを編集、複製、削除、実行/再実行したりすることもできます。

📦 インストール済みアプリケーション

バージョン、サイズ、セキュリティステータスなどの詳細と、クライアントにインストールされたプログラムを一覧表示します。[ポリシー設定](#) 経由で非ESETアプリケーションの報告をオンにできます。プログラムを選択し、**アンインストール** をクリックして削除します。**アンインストールパラメーター** を入力するように要求されます。これらはインストーラー(インストールパッケージ)の任意のコマンドラインパラメーターです。アンインストールパラメーターは各ソフトウェアインストーラーで固有です。特定の製品のマニュアルで詳細を確認してください。

ESET製品のアップデートが利用可能な場合は、**ESET製品のアップデート** ボタンをクリックしてESET製品をアップデートできます。



- ESET PROTECT9.0は、管理されたコンピューターでの[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。
- iOSデバイスは、1日に1回、インストールされているソフトウェアのリストをESET PROTECTに報告します。ユーザーはリストを強制的に更新できません。

⚠ アラート

アラートとその詳細の一覧を示します。問題、ステータス、製品、発生日時、重要度など。コンピューターセクションから直接このカテゴリにアクセスするには、[アラート]列でアラートカウントをクリックします。[ワンクリックアクション](#)でアラートを管理できます。

? 質問(コンピューターのみ)

複製関連の質問の一覧は、**質問**タブに表示されます。変更または複製されたコンピューターの質問の解決について[お読みください](#)。

🔍 検出と隔離

- **検出** - すべての[検出](#)タイプが表示されますが、フィルタリングできます。 **検出カテゴリ** - ウイルス対策 [ブロックされたファイル](#) [Enterprise Inspector](#) ファイアウォール [HIPS](#) [Web保護](#)
- **隔離** - [隔離](#)された検出と、検出名、検出タイプ、オブジェクト名、サイズ、最初の発生日時、数、ユーザー理由などの詳細の一覧を表示します。

... 詳細

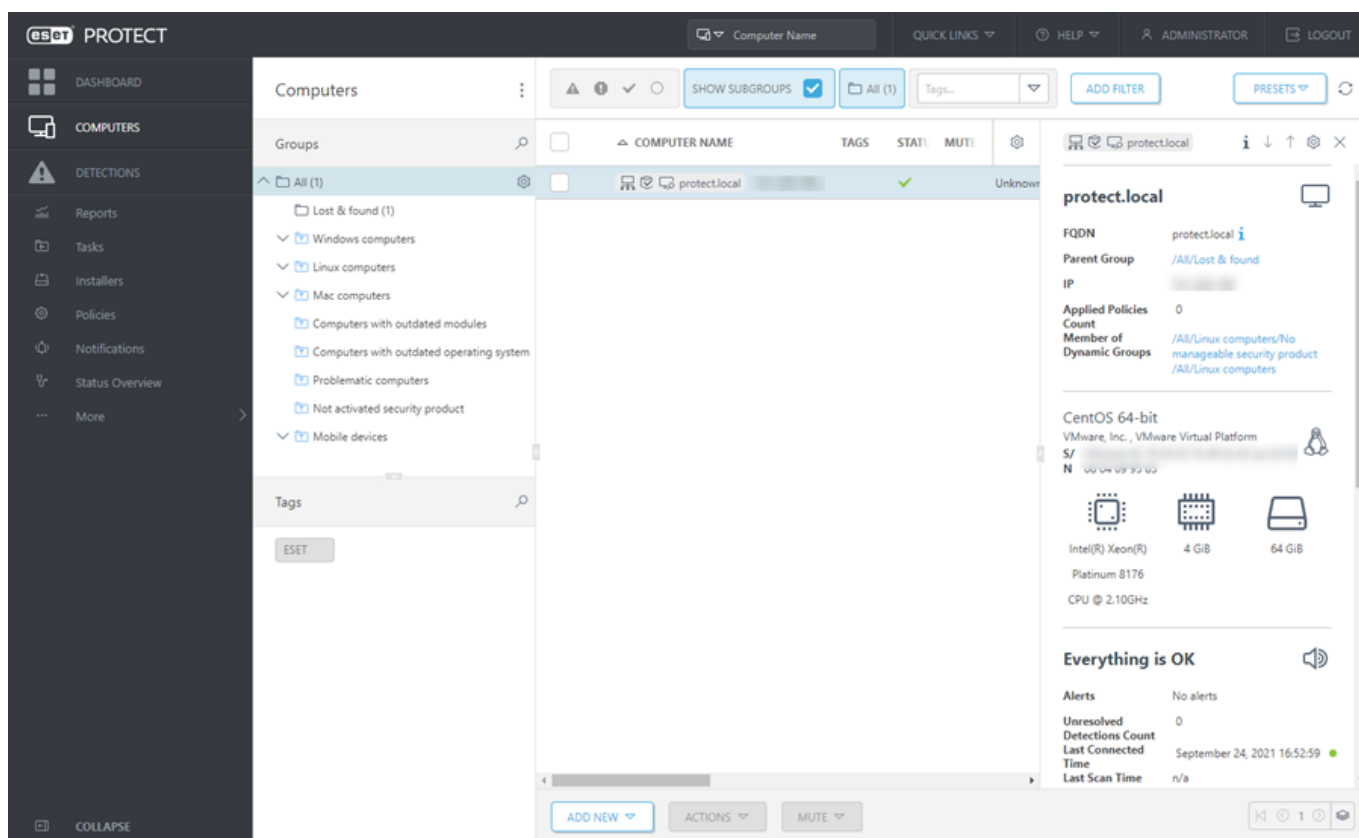
- **基本** - デバイスの情報 OS名、タイプ、バージョン、シリアル番号 FQDN名など。デバイスがミュートかどうか、管理されているかどうか、前回更新時刻、適用されたポリシー数に関する情報。
- **ハードウェア** - コンピューターのハードウェアの情報、メーカー、モデル、ネットワーク情報(IP IPv4 IPv6 サブネット、ネットワークアダプターなど)
- **製品とライセンス** - 現在の検出エンジンのバージョン、インストール済みESETセキュリティ製品のバージョン、使用済みライセンス。
- **暗号化** - [ESET Full Disk Encryption](#)を使用する場合は、ディスク暗号化ステータス概要を参照してください。

コンピュータープレビュー

コンピューターでコンピューター名をクリックして、右側にコンピューターのプレビューサイドパネルを表示します。コンピューターのプレビューサイドパネルには、選択したコンピューターに関する最も重要な情報が表示されます。

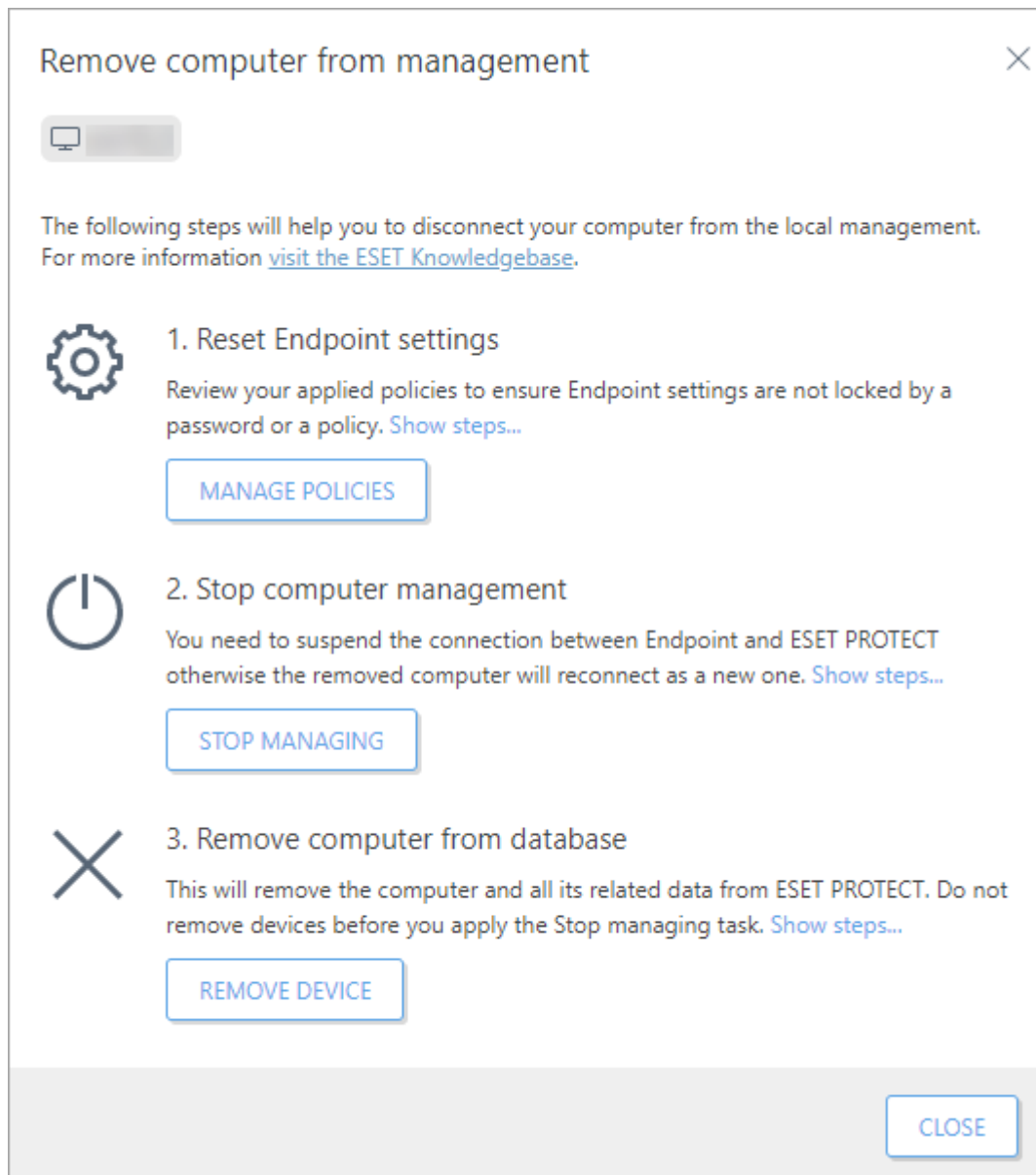
コンピュータープレビュー操作:

- **i 詳細を表示** - [コンピューター詳細](#)メニューを開きます
- **↓ 次へ** - コンピューターのプレビューサイドパネルに次のデバイスを表示します。
- **↑ 前へ** - コンピューターのプレビューサイドパネルに以前のデバイスを表示します。
- **⚙️ コンピューター詳細の内容を管理** - コンピューターのプレビューサイドパネルのセクションと表示順を管理できます。
- **✕ 閉じる** - コンピューターのプレビューサイドパネルを閉じます。



コンピューターを管理から削除する

デバイスを管理から削除するには、コンピューターをクリックし、デバイスを選択して、**🗑️ 削除**をクリックします。ダイアログボックスには、選択したコンピューターを管理から削除するために必要な手順が表示されます。



次のステップに進むときには、前の手順を正常に完了したことを確認します。これは正しいデバイス削除に必要です。

1. **エンドポイント設定のリセット - ポリシーの管理**をクリックし、適用されているすべてのポリシーを削除して、ローカルデバイス管理を許可します。[ポリシー](#)セクションのポリシー削除ルールを参照してください。エンドポイント製品設定にアクセスパスワードが設定されている場合は、パスワードを削除するための新しいポリシーを作成します(パスワードを設定する場合は選択しますが、パスワードは入力しないでください)ESET Full Disk Encryptionで暗号化されたコンピュータの場合は、[復号手順](#)に従います。

2. **コンピューター管理の停止 - 管理の停止**タスクを実行するかESET ManagementエージェントまたはESETセキュリティ製品をコンピューターでローカルからアンインストールします。これにより、コンピューターとESET PROTECT間の接続が一時停止します。

3. **コンピューターをデータベースから削除** - コンピューターがESET PROTECTに接続していないことを確認した後、管理されたデバイスのリストから削除できます。

- インストールされている**ESETセキュリティ製品をアクティベーション解除**するチェックボックスをオンにし、選択したコンピューターにインストールされているすべてのESET製品からライセンスを削除します。[ESETビジネス製品のアクティベーション解除](#)も参照してください。

グループ

グループは、コンピューターと他のオブジェクトが分類されるフォルダーと考えることができます。

コンピューターとデバイスには、定義済みのグループおよびグループテンプレートを使用して、新しいグループを作成することもできます。クライアントコンピューターはグループに追加できます。これにより、ニーズに合わせて構成および編成されたコンピューターを保持できます。静的グループにコンピューターを追加できます。


静的グループは手動で管理されます。動的グループはテンプレートの特定の条件に基づいて自動で配置されます。コンピューターがグループにある場合、ポリシー、タスク、設定をこれらのグループに割り当てることができます。ポリシー、タスク、設定はグループのすべてのメンバーに割り当てられます。クライアントグループには2種類あります。

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。グループメンバーは、静的で手動で追加/削除のみで、動的条件に基づいておりません。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。オブジェクトが含まれていない場合にのみ、静的グループを削除できます。


動的グループ



動的グループは、特定の条件を満たしてグループのメンバーになるデバイスのグループです(タスクやポリシーなどの他のオブジェクトではありません)。クライアントデバイスが条件を完全に満たしていない場合、グループから削除されます。条件を満たすコンピューターは、グループに自動的に追加されます。このため、動的という名称になっています。

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。

グループアクション


コンピューターに移動し、管理するグループを選択します。グループボタンまたはグループの横の歯車アイコンをクリックします。次のオプションのメニューが表示されます。

グループアクション	グループアクション説明	適用先	
		静的グループ	動的グループ
 詳細を表示	選択したグループの <u>概要</u> を表示します。	✓	✓
 監査ログ	選択した項目の <u>監査ログ</u> を表示します。	✓	✓
 新しい静的グループ	選択したグループは、既定で親グループとなっていますが、 <u>新しい静的グループを作成</u> するときに親グループを後で変更することができます。	✓	X


グループアクション	グループアクション説明	適用先	
		静的グループ	動的グループ
十 新しい動的グループ	選択したグループは、既定で親グループとなっていますが、 新しい動的グループを作成 するときに親グループを後で変更することができます。	✓	✓
十 新しい通知	新しい通知 を作成します。	X	✓
十 新規追加	新しいデバイス を追加できます。	✓	X
▷ タスク	<p>このグループのデバイスで実行されるクライアントタスクを選択できます。</p> <p>🔍 検査 - 選択したグループのすべてのクライアントで、オンデマンド検査タスクを実行します。</p> <p>🔄 アップデート:</p> <ul style="list-style-type: none"> 🔄 モジュールのアップデート - モジュールアップデートタスク(アップデートを手動でトリガー)が実行されます。 🔄 ESET製品のアップデート - 古いESETセキュリティ製品がインストールされているコンピューターで、ソフトウェアのインストールタスクを実行します。 🔄 OSのアップデート - 選択したグループのコンピューターで、OSのアップデートタスクを実行します。 <p>📱 モバイル - 詳細については、Anti-Theftアクションを参照してください。</p> <ul style="list-style-type: none"> 🔑 再登録 - 新しいクライアントタスクを作成します。 📍 検索 - モバイルデバイスのGPS座標を要求します。 🔒 ロック - 不審なアクティビティが検出されるか、デバイスが紛失に設定されると、デバイスがロックされます。 🔓 ロック解除 - デバイスのロックが解除されます。 🔑 パスコードをクリア - iOS/iPadOSデバイスからパスコードを削除します。 📢 警報/紛失モード - リモートで大音量の警報音をトリガーします。デバイスがミュートに設定されていても、警報音が作動します。 ✕ 初期設定リセット - デバイスに保存されているすべてのデータが完全に消去されます。 <p>▷ タスクの実行 - 1つ以上のクライアントタスクを選択し、選択したデバイスで実行します。</p> <p>十 新しいタスク - 新しいクライアントタスクを作成します。タスクを選択し、このタスクの調整 (任意)を設定します。このタスクは、タスク設定に従って、キューに追加されます。このオプションは、使用可能なタスクのリストから選択した既存のタスクをただちにトリガーします。このタスクはただちに実行されるため、トリガーは使用できません。</p> <p>🕒 最後に使用されたタスク - すべてのグループとコンピューターで最近実行されたクライアントタスクの一覧。</p>	✓	✓
🕒 レポート	選択したグループから レポート を選択します。	✓	X
🔑 ポリシーの管理	選択したグループに割り当てられた ポリシーを管理 します。	✓	✓

グループアクション	グループアクション説明	適用先	
		静的グループ	動的グループ
 編集	選択したグループを編集します。新しいグループ(静的または動的)を作成する場合、同じ設定が適用されます。	✓	✓
 移動	グループを選択し、別グループのサブグループとして 移動 することができます。	✓	✓
 削除	選択したグループを削除します。	✓	✓
 すぐに適用  後で適用	動的グループの優先度を変更します。	X	✓
 インポート	コンピュータのリスト(通常はテキストファイル)を選択したグループのメンバーとして インポート することができます。コンピュータがこのグループのメンバーとして既に存在する場合は、選択したアクションに基づいて競合が解決されます。	✓	X
 エクスポート	グループ(選択した場合、およびサブグループ)のメンバーをリスト(.txt.txtファイル)に エクスポート します。このリストを使用して確認したり、後でインポートすることもできます。	✓	X

グループ詳細

選択したグループアクション  **詳細を表示**を選択すると、選択したグループの概要が表示されます。

概要:


概要では、 または **説明の追加** をクリックすると、グループ設定を編集できます。グループ配置、および親グループと子グループの情報が表示されます。選択したグループが[動的グループ](#)の場合、コンピューターが評価され、グループに割り当てられる条件となる[処理](#)と[ルール](#)が表示されます。

▷ タスク

グループに割り当てられた[クライアントタスク](#)を表示および編集できます。

ポリシー

既存のポリシーをグループに割り当てるか、新しいポリシーを作成できます。グループに割り当てられた[ポリシー](#)を表示および編集できます。

 選択したグループに割り当てられたポリシーのみを表示できます。ここでは、グループの個別のコンピューターに適用されたポリシーは表示されません。

ポリシーは順序(**ポリシー順序**列)に基づいて適用されます。ポリシー適用の優先度を変更するには、ポリシーの横のチェックボックスをオンにして、**すぐに適用**または**後で適用**ボタンをクリックします。

アラート

グループのコンピューターからの[アラート](#)のリスト。[ワンクリックアクション](#)でアラートを管理できます。

⊗ 除外

グループに適用された[除外](#)のリスト。

静的グループ


静的グループは次の目的で使用されます。

- デバイスを整理し、グループとサブグループの階層を作成します
- オブジェクトを整理します
- ユーザーのホームグループとして機能します

静的グループは手動でのみ[作成](#)できます。デバイスはこれらのグループに手動で移動できます。各コンピューターまたはモバイルデバイスは、1つの静的グループのみに属することができます。静的グループの管理は[グループアクション](#)から使用できます。


次の2つの既定の静的グループがあります。

- **すべて** - これはESET PROTECTサーバーネットワーク内のすべてのデバイスのメイングループになります。管理者が作成したすべてのオブジェクトは既定でこのグループに含まれます。常に表示され、名前を変更できません。このグループへのアクセスはすべてのサブグループへのアクセスをユーザーに付与します。このため、注意して配布してください。
- **Lost + Found-** **すべて**グループの子グループ。新しいコンピューターが初めてESET PROTECTサーバーに接続すると、自動的にこのグループに表示されます。グループ名を変更し、コピーできますが、削除または移動はできません。

コンピューターを別の静的グループに移動するには、コンピューターをクリックし、 **グループに移動**を選択し、ターゲット静的グループを選択して、**OK**をクリックします。

静的グループは次の場合にのみ削除できます。

- ユーザーはこのグループに対する書き込み権限がある
- グループが空



静的グループにオブジェクトがある場合、削除処理が失敗します。各メニューには、オブジェクトがある[\[アクセスグループ\]](#)フィルターボタンがあります(たとえば、[インストーラー](#))

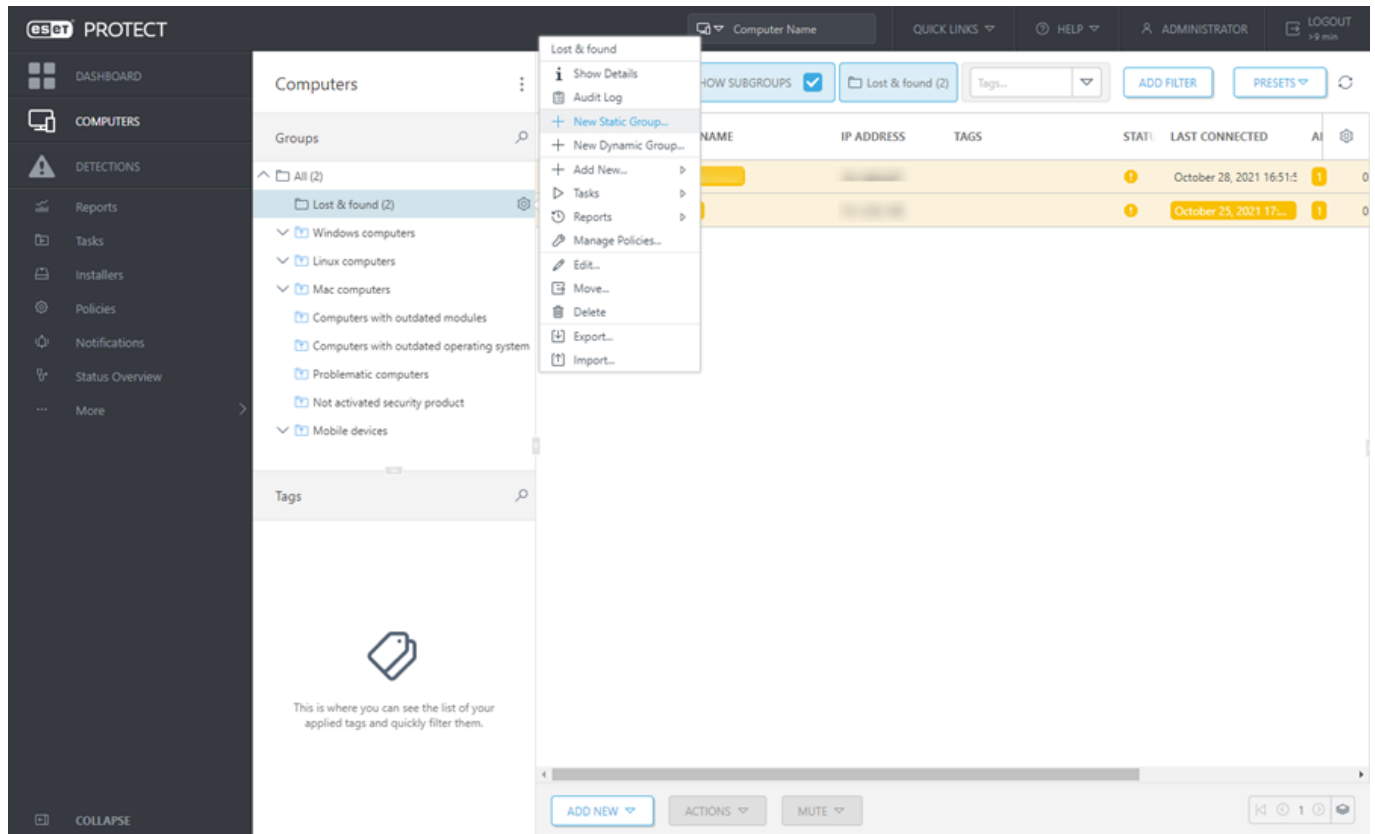


ACCESS GROUP Select 

[選択]をクリックして静的グループを選択します。このグループに含まれるオブジェクトのみがビューに一覧表示されます。このフィルタリングされたビューでは、ユーザーは簡単に1つのグループからオブジェクトを操作できます。

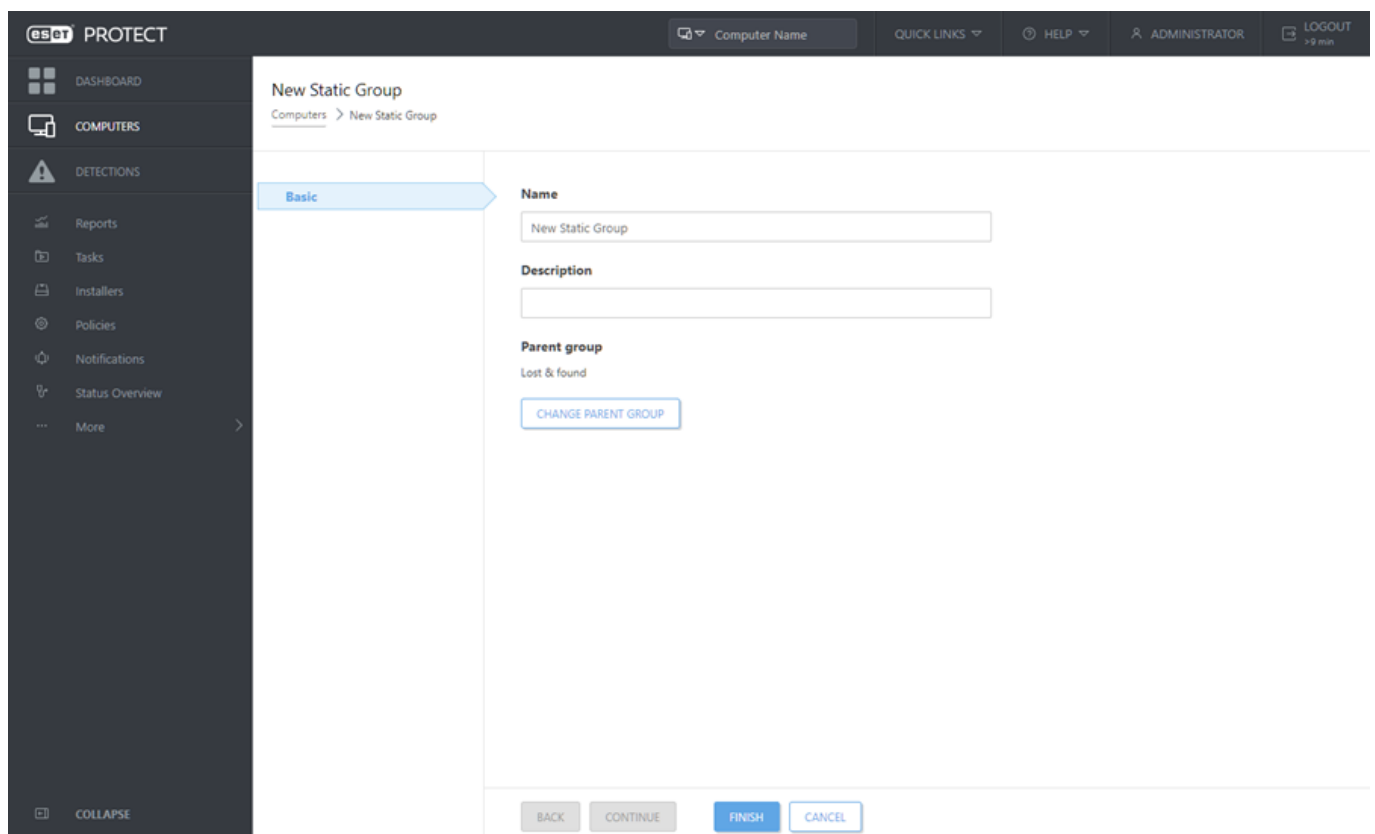
新しい静的グループを作成します

新しい静的グループを作成するには、**コンピューター**をクリックし、静的グループの横の歯車アイコンを選択して、**新しい静的グループ**を選択します



基本

新しいグループの**名前**と**説明**を入力します。任意で、**親グループ**を変更できます。既定では、親グループは、新しい静的グループの作成時に選択したグループです。親グループを変更する場合は、**親グループの変更**をクリックし、ツリーから親グループを選択します。新しい静的グループの親は静的グループである必要があります。動的グループには静的グループを含めることができません。**完了**をクリックして、新しい静的グループを作成します。



Active Directoryからのクライアントのインポート


ADからクライアントをインポートするには、新しいサーバタスクを作成します。[静的グループの同期](#)

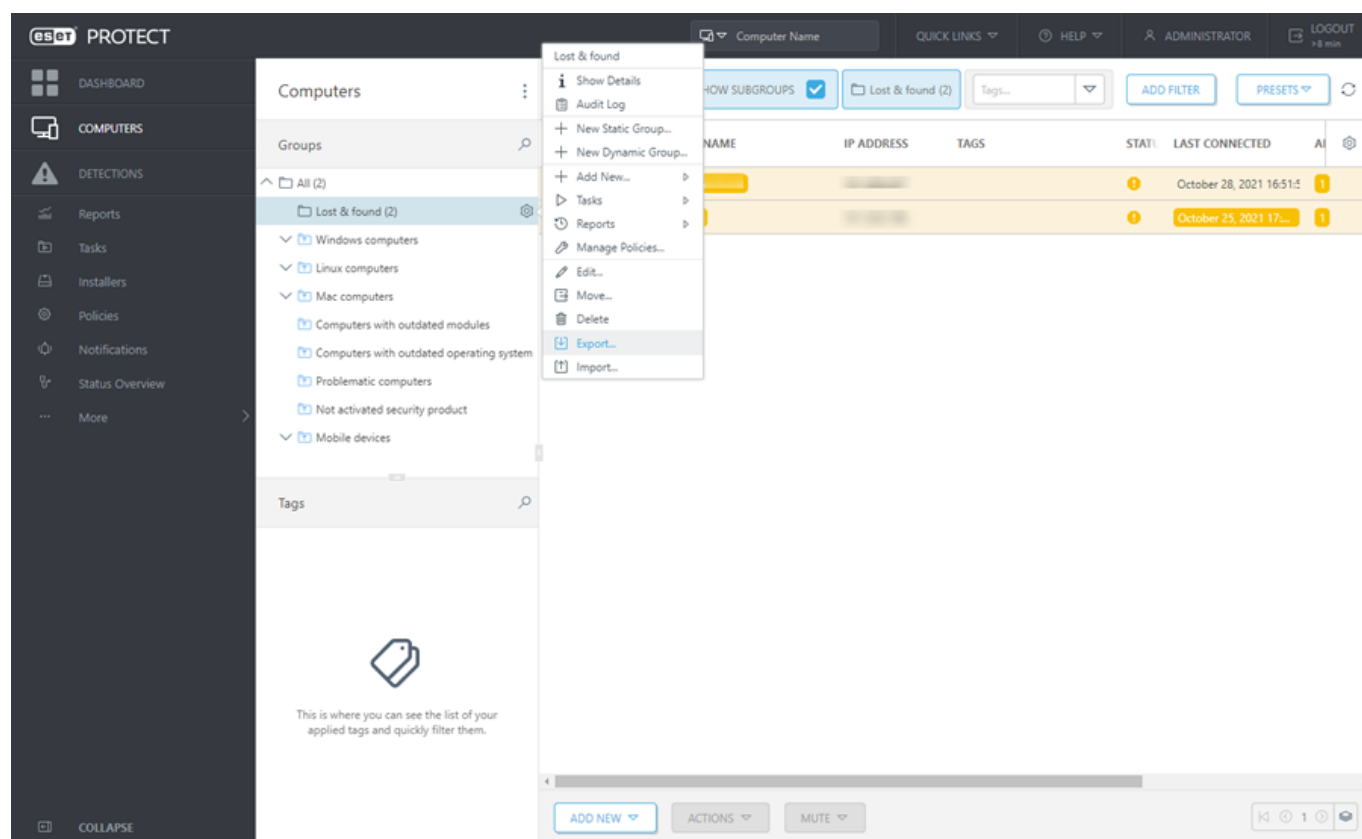
新しいコンピューターを追加するグループをADから選択します。また、同期元のADのオブジェクトと、重複の場合の処理を選択します。ADサーバー接続設定を入力し、[同期モード](#)をActive Directory/Open Directory/LDAPに設定します。

静的グループのエクスポート

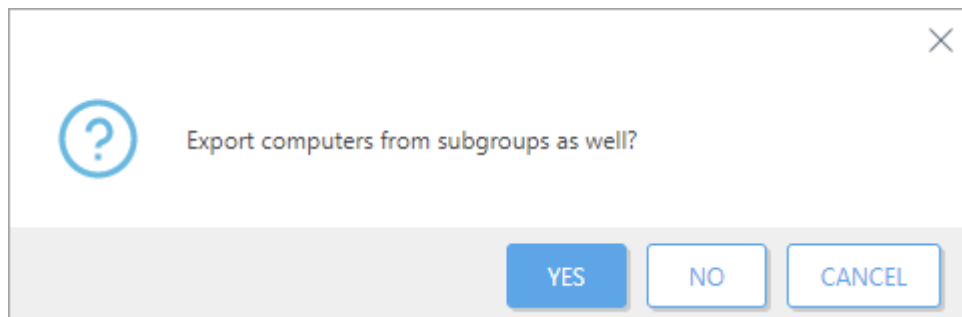
ESET PROTECT構造にあるコンピューターのリストは簡単にエクスポートできます。リストをエクスポートし、バックアップとして保存すると、グループ構造を復元する場合などに、後からリストをインポートできます。

i 静的グループには1つ以上のコンピューターを含む必要があります。空のグループをエクスポートすることはできません。

1. コンピューターに移動し、エクスポートする静的グループを選択します。
2. 歯車アイコンをクリックし、 **エクスポート**を選択します。



3. 選択した静的グループにコンピューターを含むサブグループが含まれている場合は、サブグループからコンピューターをエクスポートすることもできます。

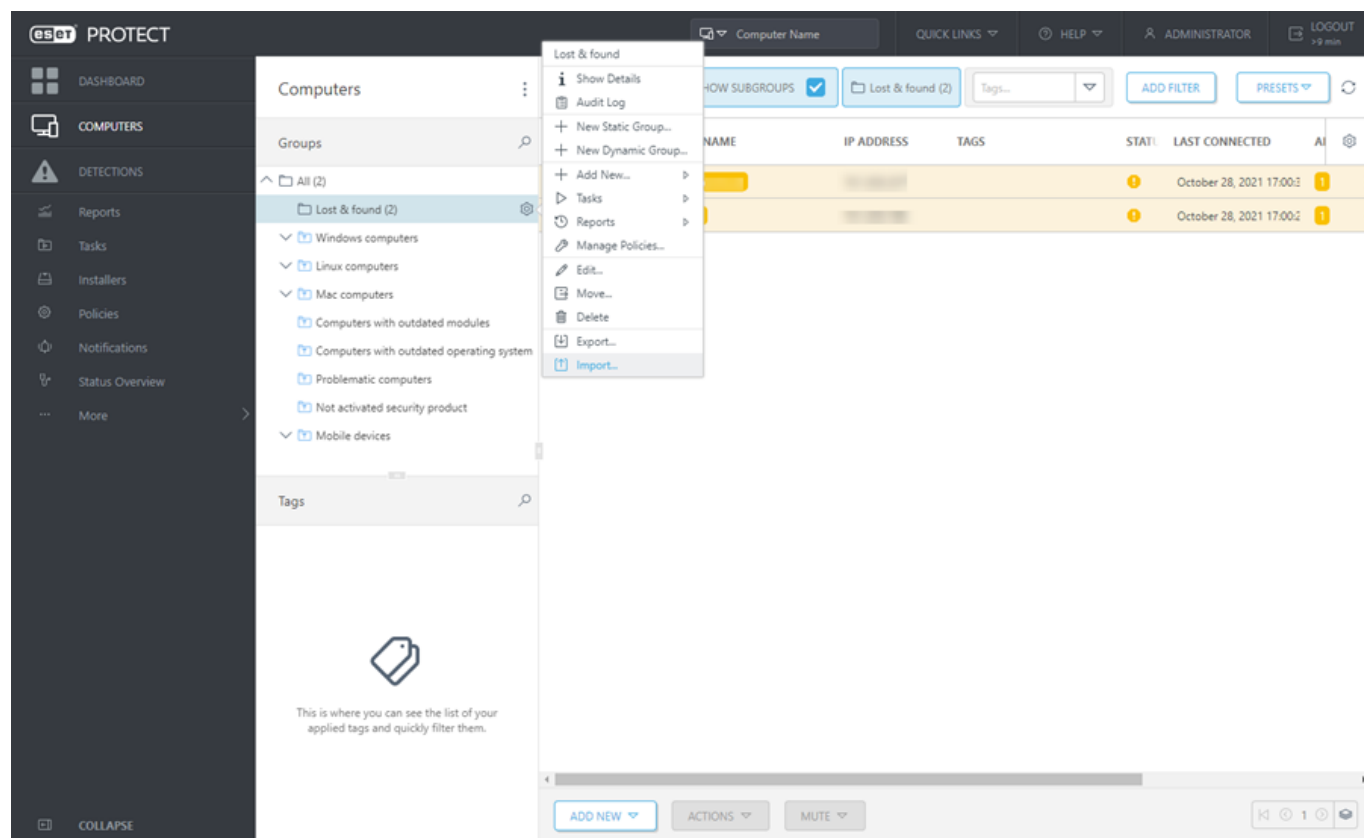



4. ファイルは.txt形式で保存されます。

i 動的グループは、動的グループテンプレートで定義された条件に従ったコンピューターへのリンクにすぎないため、エクスポートできません。

静的グループのインポート

静的グループから[エクスポート](#)したファイルはESET PROTECT Webコンソールに再度インポートでき、既存のグループ構造に含めることができます。



1. コンピューターをクリックし、静的グループを選択します。
2. 歯車アイコンをクリックし、 インポートを選択します。
3. 参照をクリックし、.txtファイルに移動します。
4. グループファイルを選択して、開くをクリックします。ファイル名がテキストボックスに表示されます。
5. 次のオプションのいずれかを選択して競合を解決します。

• 同じエントリが他の場所で見つかった場合は、デバイスを作成または移動しないでください②
静的グループが存在し、.txtファイルからコンピューターがグループにすでに存在する場合、そのコンピューターはスキップされ、インポートされません。これに関する情報が表示されます。

• インポートされたパスにデバイスが存在しない場合は、既存のデバイスを移動します。可能な場合は、管理対象デバイスのみを同じパスに保持します②

静的グループが存在し、.txtファイルからのコンピューターがこのグループにすでに存在する場合、インポート前にコンピューターを他の静的グループに移動する必要があるため、インポート後、そのコンピューターは移動後の場所から元の場所に戻ります。

• インポートされたパスにデバイスが存在しない場合は、既存のデバイスを複製します②
静的グループが存在し、.txtファイルからのコンピューターがこのグループにすでに存在する場合、そのコンピューターの複製が同じ静的グループ内に作成されます。元のコンピューターは、完全な情報と一緒に表示され、複製はコンピューター名のみ表示されます。

6.インポートをクリックすると、静的グループとコンピューターがインポートされます。

動的グループ

動的グループは、コンピューターステータスに基づきフィルタリングと見なすことができます。1つのコンピューターに複数のフィルタが適用される場合があります。このため、複数の動的グループを割り当てられます。これにより、動的グループが静的グループと異なります。1つのクライアントは複数の静的グループに属することができないためです。

動的グループは特定の条件に基づいて選択されたクライアントのグループです。コンピューターが特定の動的グループのメンバーになるには、[動的グループテンプレート](#)で定義された特定の[条件](#)を満たす必要があります。各テンプレートは1つまたは複数の[ルール](#)から構成されています。新しい[テンプレート](#)を作成するときに、これらのルールを指定できます。クライアントコンピューターが条件を完全に満たしていない場合、グループから削除されます。定義済みの条件を満たす場合、グループに追加されます。

デバイスはESET PROTECTにチェックインするたびに、動的グループに含まれるかどうかを評価されます。デバイスが動的グループテンプレートで指定された値を満たす場合、自動的にこのグループに割り当てられます。コンピューターはエージェント側でフィルタリングされるため、追加情報をサーバーに転送する必要はありません。エージェントは、クライアントが属する動的グループを独自に判断し、この判断だけをサーバーに通知します。

i クライアントデバイスが接続されていない場合(オフの場合など)、動的グループのメンバーシップは更新されません。デバイスが再接続された後、動的グループのメンバーシップが更新されます。

一部の定義済み動的グループは、ESET PROTECTをインストールした後に使用できます。 カスタム動的グループを作成できます。このためには2つの方法があります。

- まずテンプレートを作成し、次に[動的グループを作成](#)します。
- 新しい動的グループを作成するときには、[新しいテンプレート](#)を作成します。


他のESET PROTECTの部分で動的グループを使用できます。[ポリシーをそれらに割り当てる](#)(ポリシーは[これ](#)に従って適用)か、グループのすべてのコンピューターに対する[タスク](#)を準備できます。

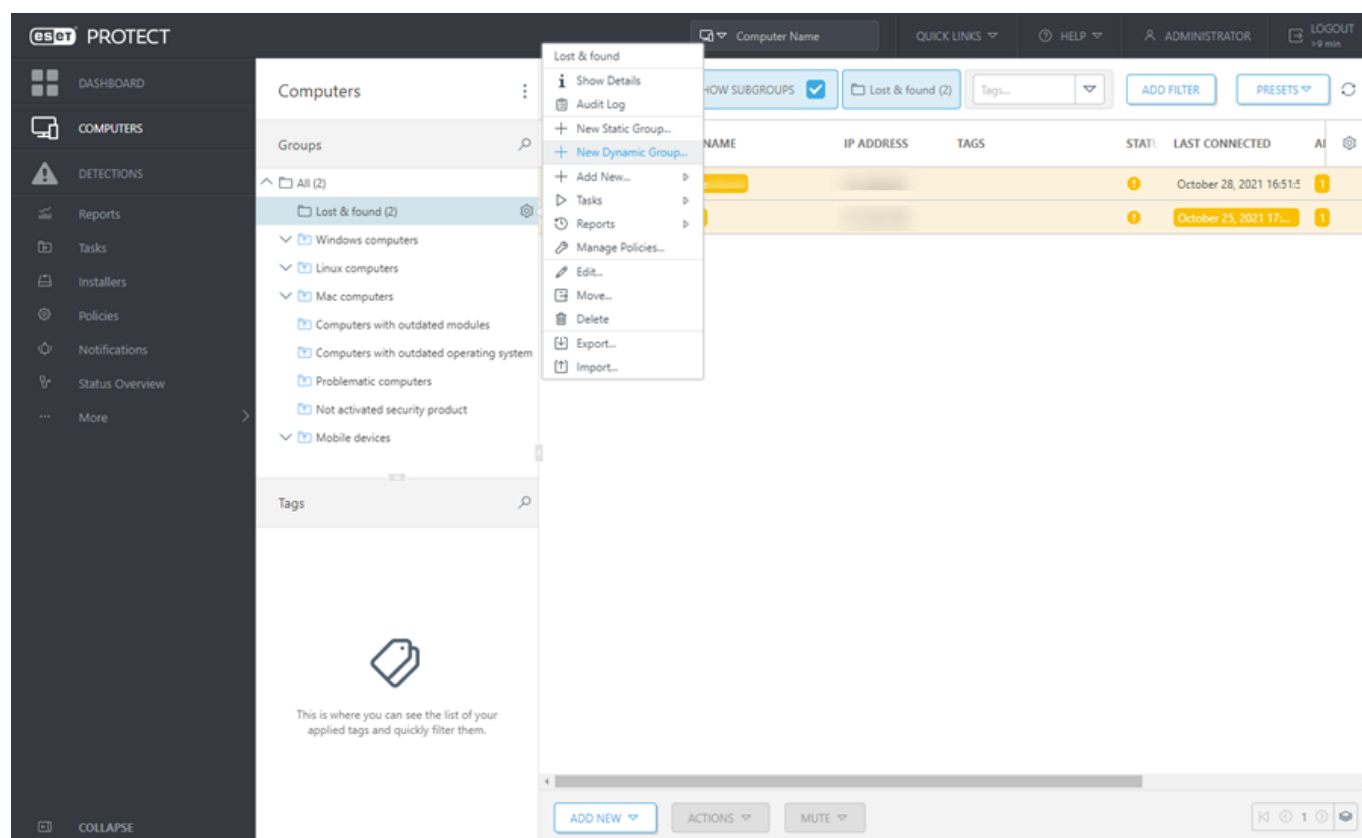
動的グループは静的グループまたは動的グループ内(の下)にすることができます。ただし、静的グループは動的グループ内にすることはできません。特定の静的グループの下に動的グループは、静的グループのデバイスだけをフィルタリングします。動的グループが別の動的グループ内にある場合、上位の動的グループの結果をフィルタリングします。グループが作成されると、[ツリー全体を自由に移動できます](#)②

動的グループの管理は [グループアクション](#) から使用できます。

新しい動的グループの作成

次の手順に従い、新しい動的グループを作成します。

1. **コンピューター**をクリックして、グループの横の歯車アイコンを選択して、**新しい動的グループ**を選択します。新しい動的グループウィザードが表示されます。



2. 新しいテンプレートの名前と説明を入力します。

3. **[親グループの変更]**をクリックすると、親グループも変更できます。

4. テンプレートをクリックします。すべての動的グループは、グループがクライアントコンピューターをフィルタリングする方法を定義するテンプレートから作成されます。無制限の数の動的グループを1つのテンプレートから作成できます。

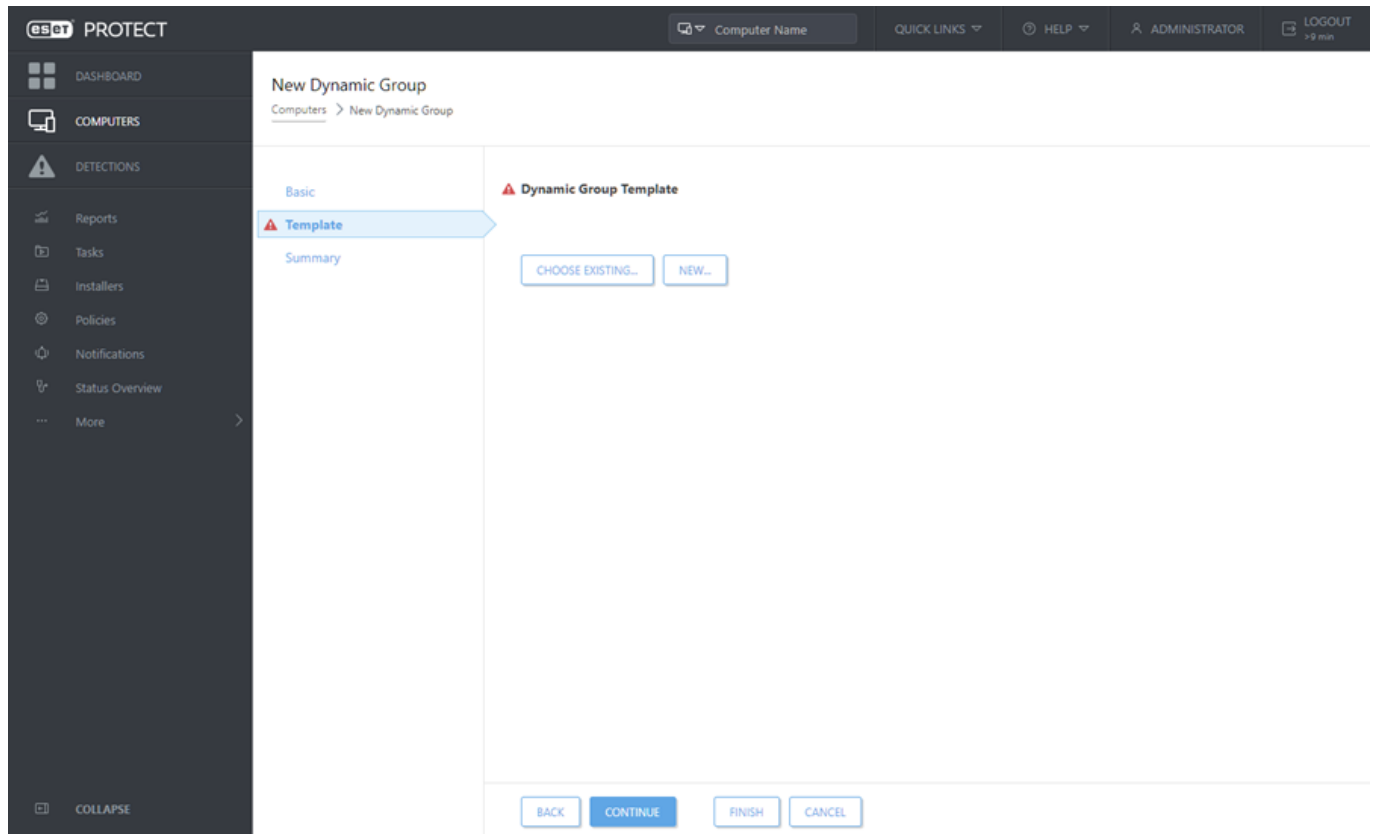
i

テンプレートは静的グループに保存される静的オブジェクトです。ユーザーはテンプレートにアクセスするために適切な権限が必要です。ユーザーが動的グループテンプレート进行操作するにはアクセス権が必要です。すべての定義済みテンプレートは静的グループすべてにあり、既定では管理者のみが使用できます。他のユーザーには追加の権限を割り当てる必要があります。結果として、ユーザーは既定のテンプレートを表示または使用できない可能性があります。テンプレートはユーザーが権限を持つグループに移動できます。

テンプレートを複製するには、ソーステンプレートがあるグループ(動的グループテンプレート)に対する使用権限とユーザーのホームグループ(複製が保存される場所)に対する書き込み権限がユーザーに割り当てられている必要があります。オブジェクトの複製の例を参照してください。

- 定義済みのテンプレートまたは既に作成したテンプレートからグループを作成する場合は、[既存から選択]をクリックし、リストから該当するテンプレートを選択します。
- テンプレートを作成しておらず、リストの定義済みテンプレートのいずれも適していない場合は、[新規]をクリックして、新しいテンプレートに従います。


動的グループテンプレートのルールを使用して、新しい動的グループを作成する方法については、例を参照してください。



5.概要をクリックします。新しいグループは親グループの下に表示されます。

静的または動的グループの移動

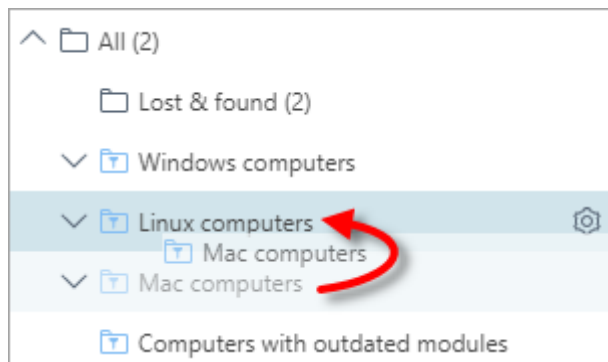
動的グループは、静的グループを含む他のグループのメンバーになれます。静的グループは動的グループに移動できません。また、定義済み静的グループ(**Lost + found**静的グループなど)を他のグループに移動できません。他のグループは自由に移動できます。


グループの横の歯車アイコンをクリックし、[移動]を選択します。ポップアップウィンドウが表示され、グループツリー構造を示します。選択したグループの移動先のグループ(動的または静的)を選択します。移動先のグループが親グループになります。また、グループをドラッグして、選択した移動先グループにドロップし、グループを移動することもできます。

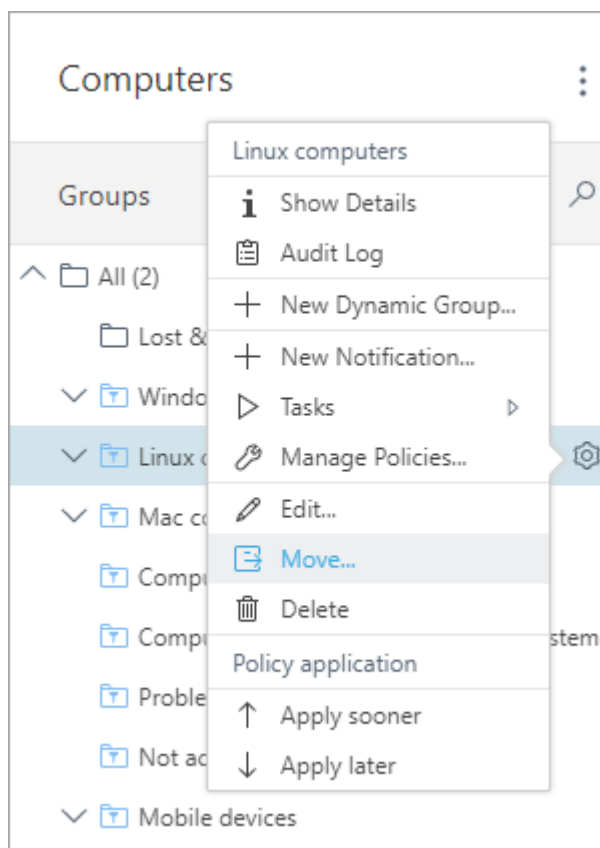
i 新しい場所の動的グループは、前の場所に関係せずに、コンピューター(テンプレートに基づく)をフィルタリングし始めます。


3つの方法でグループを移動できます。

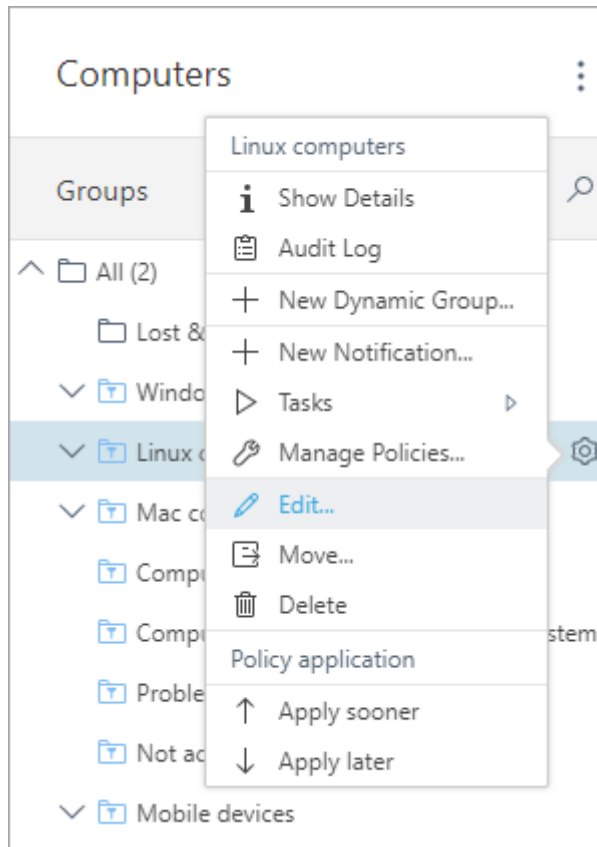
- **ドラッグアンドドロップ**– 移動するグループをクリックし続け、新しい親グループの上で放します。



- 歯車アイコン  > **移動** > リストから新しい親グループを選択して、**OK**をクリックします。

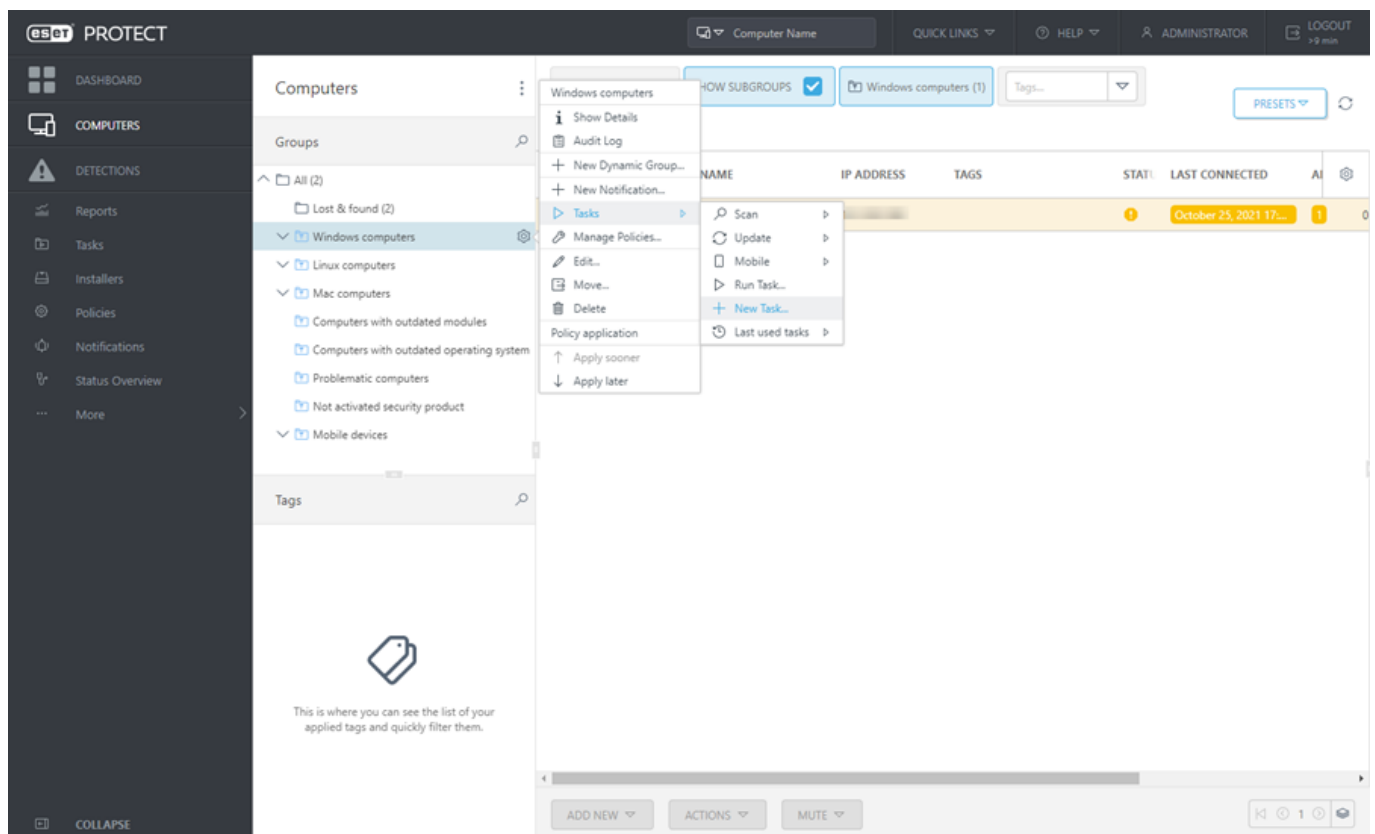


- 歯車アイコン  > **編集** > **親グループの変更**を選択します。リストから新しい親グループを選択して、**OK**をクリックします。



グループへのクライアントタスクの割り当て

コンピューターから、静的または動的グループを選択し、歯車アイコン ⚙️ > タスク > + 新しいタスクをクリックします。[新しいクライアントタスクウィザード](#)が開きます。

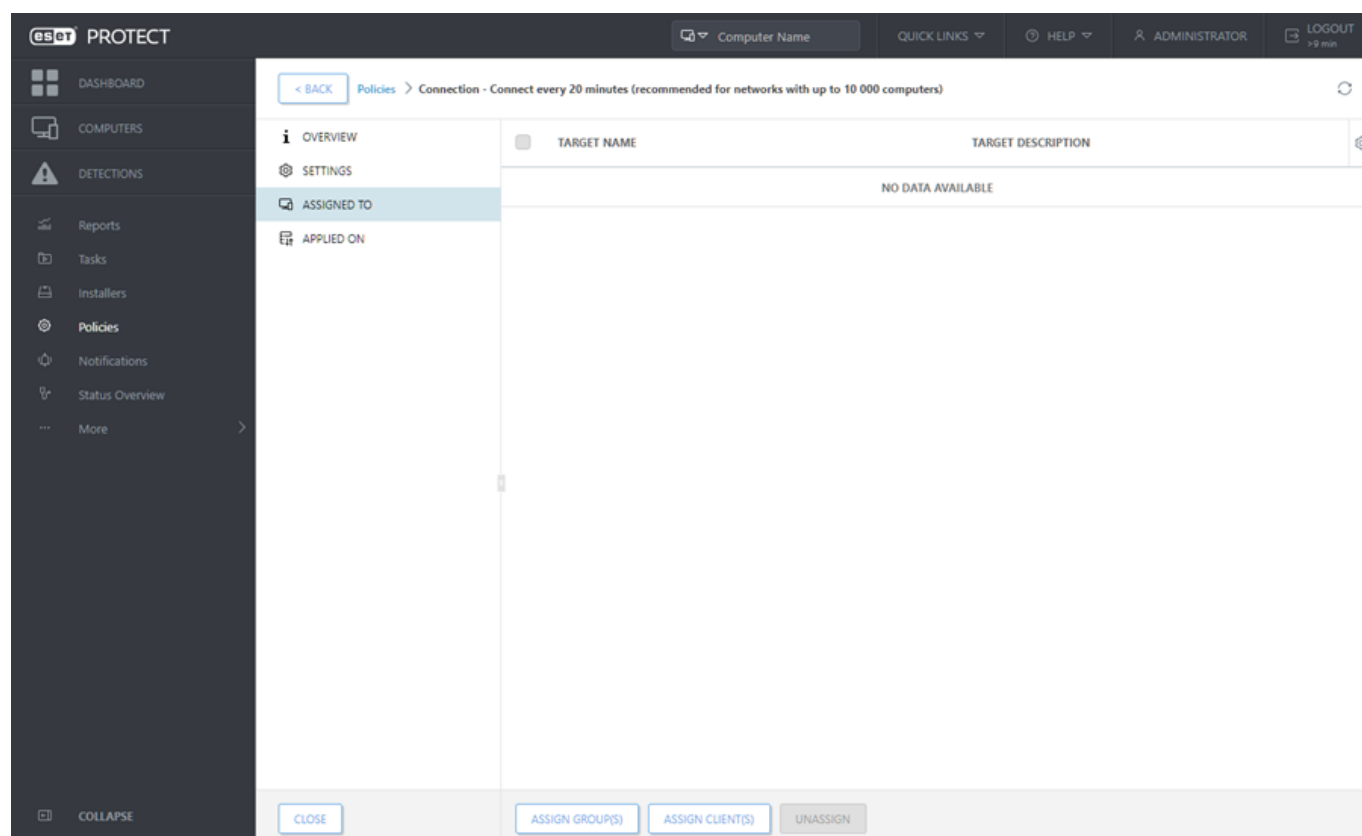


グループへのポリシーの割り当て

ポリシーが作成された後、**静的**または**動的**グループに割り当てることができます。ポリシーは2つの方法で割り当てることができます。

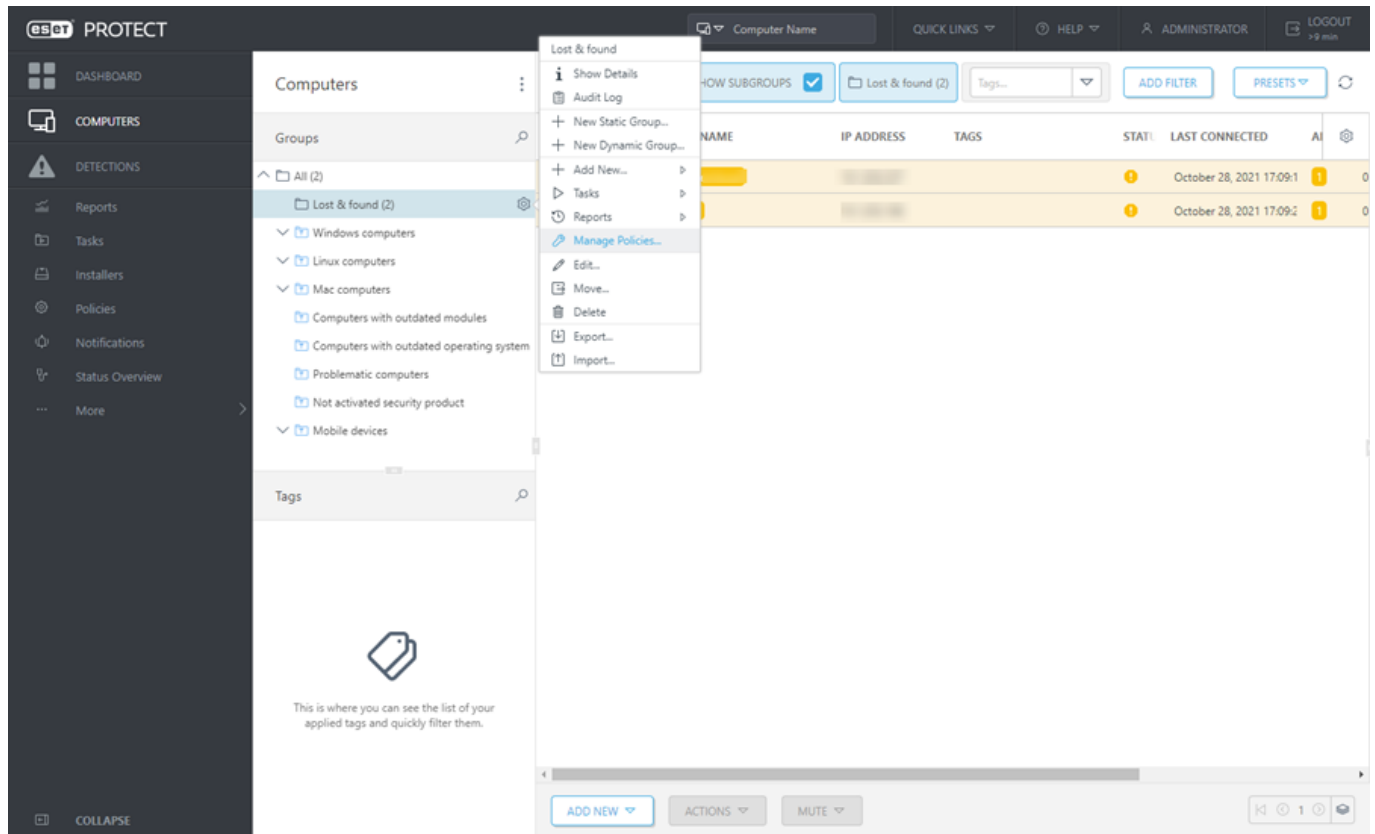
方法I.

ポリシーの下、**アクション>詳細を表示>割り当て先>グループの割り当て**をクリックします。リスト(その他のグループを選択できます)静的または動的グループを選択し、**[OK]**をクリックします。



方法II.

1. コンピューターをクリックし、グループ名の横の歯車[⚙]アイコンをクリックして、ポリシーの管理を選択します。



2. ポリシーアプリケーション順序ウィンドウで、ポリシーの追加をクリックします。

3. このグループに割り当てるポリシーの横にあるチェックボックスをオンにし、OKをクリックします。

4. [閉じる]をクリックします

特定のグループに割り当てられたポリシーを確認するには、グループを選択し、ポリシータブをクリックして、グループに割り当てられたポリシーのリストを表示します。

特定のポリシーに割り当てられたグループを表示するには、ポリシーを選択し、詳細を表示>割り当て先を表示します。

i ポリシーの詳細については、[ポリシー](#)の章を参照してください。

検出

検出セクションには、管理されたデバイスで見つかったすべての検出の概要が表示されます。

左側には、グループ構造が表示されます。グループを参照し、特定のグループのメンバーの見つかった検出を確認できます。アカウントのグループに割り当てられたクライアントで見つかったすべての検出を表示するには、すべてのグループを選択し、適用されたフィルターを削除します。

検出ステータス

脅威ステータスに基づいて、2種類の検出があります。

- **未解決の検出** - 未解決の検出はまだ駆除されていない検出です。検出を駆除するには、検出を含むフォルダーで駆除を有効にして、**詳細検査**を実行します。検出を駆除し、検出を排除するには、

検査タスクを正常に完了する必要があります。検出から24時間以内にアクティブな検出を解決しない場合は、**アクティブ**状態から、未解決になります。

- **解決済みの検出** - これらは、ユーザーによって[解決済み](#)に設定された検出ですが、**詳細検査**によって検査されていません。解決済みに設定された検出があるデバイスは、検査が実行されるまで、フィルタリングされて表示されます。

処理された検出ステータスは、ESETセキュリティ製品が検出に対してアクションを実行したかどうかを示します(検出タイプと[駆除レベル設定](#)によって異なります)。

- **はい** - ESETセキュリティ製品は検出に対してアクション(削除、駆除、または隔離)を実行しました。
- **いいえ** - ESETセキュリティ製品は検出に対してアクションを実行しませんでした。

レポート、通知、動的グループテンプレートでは、フィルターとして**処理された検出**を使用できます。



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](#)²



[データベースクリーンアップ](#)中に、駆除されたインシデントログに対応する[検出](#)の項目も(検出ステータスには関係なく)削除されます。既定では、インシデントログ(および検出)のクリーンアップ期間は6か月に設定されています。この期間は、[サーバー設定](#)で変更できます。

検出の集約

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。同じ検出が繰り返し発生する場合² Webコンソールは1行に表示され、解決が容易になります。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。

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。

フィルタリング検出

既定では、正常に駆除された検出を含む、過去7日間のすべての検出タイプが表示されます。複数の条件で検出をフィルタリングできます。ミュートされたコンピューターおよび発生が既定で有効にされます。

i 一部のフィルターは既定で有効です。メインメニューに**検出**が表示され、検出リストに表示されない場合は、チェックをすると、有効なフィルターが表示されます。

より詳細に表示するには、次の例のような他のフィルターを追加できます。

• 検出カテゴリ -  ウイルス対策  [ブロックされたファイル](#)  [Enterprise Inspector](#)  ファイアウォール  HIPS  Web保護

• 検出タイプ

• 検出を報告したクライアントのIPアドレス

• スキャナー - 検出を報告したスキャナーの種類を選択します。たとえば、ランサムウェア対策スキャナーは、[ランサムウェア保護](#)によって報告された検出を示しています。

• アクション - 検出に対して実行されたアクションを選択します。ESETセキュリティ製品は次のアクションをESET PROTECTに報告します。


o 駆除 - 検出が駆除されました。


o 削除 / 削除により駆除 - 検出は削除されました。

o 削除されたオブジェクトの一部 - 検出を含むアーカイブが削除されました。

o ブロック / 切断 - 検出されたオブジェクトへのアクセスがブロックされました。

o 保持 - さまざまな理由により、アクションは実行されませんでした。例：

 [対話アラート](#)で、アクションを実行しないようにユーザーが手動で選択しました。

 ESET セキュリティ製品 [検出エンジン設定](#)では、検出カテゴリの**保護**レベルがレポートレベルより低く設定されます。

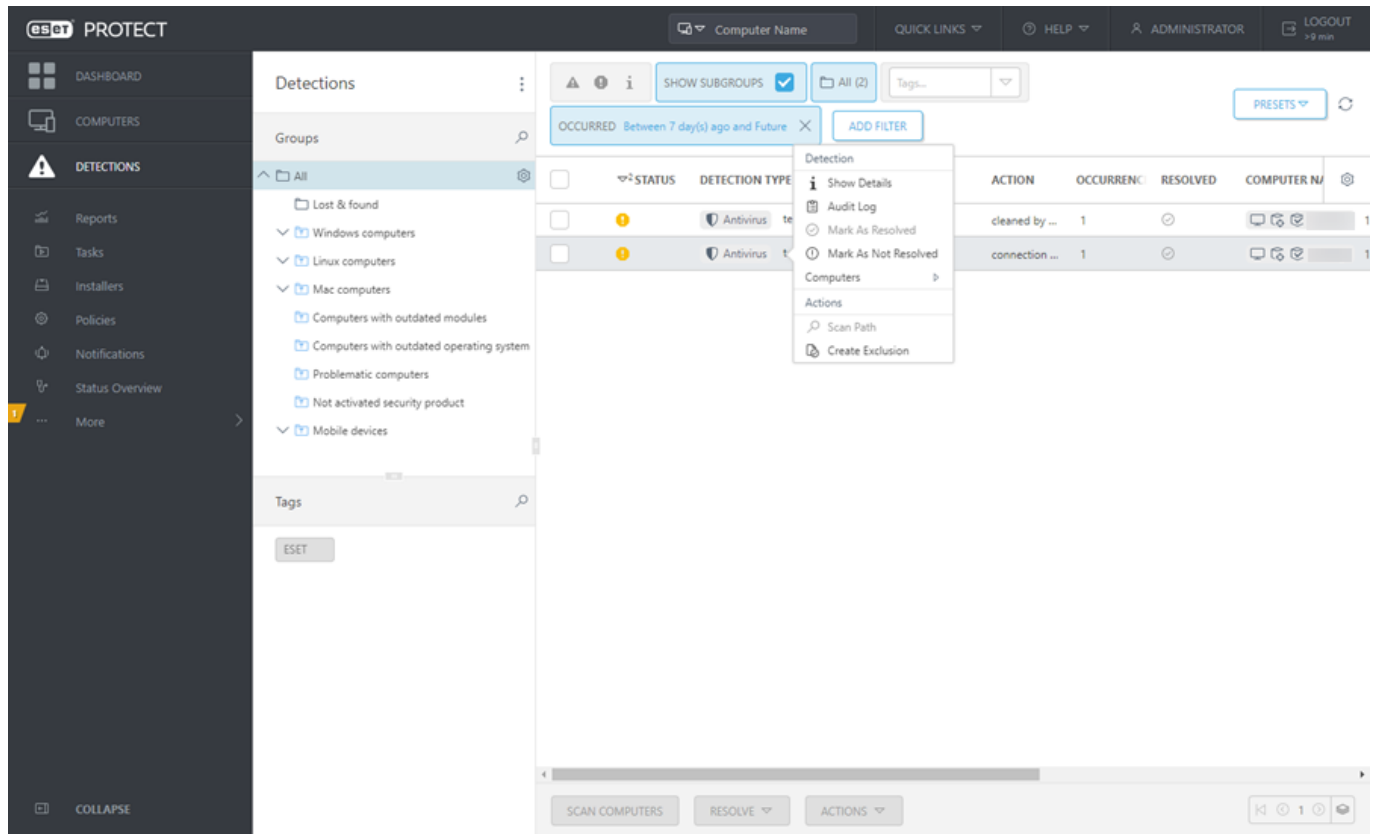
フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

• [サイドパネルとメインテーブルを管理](#)します。

• [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

検出の管理



検出名をクリックすると、右側の[検出プレビュー](#)サイドパネルが表示されます。








検出を管理するには、アイテムをクリックして、使用可能なアクションのいずれかを選択するか、1つ以上のアイテムの横のチェックボックスをオンにして、[検出](#)画面の下の部分にあるボタンを使用します。

- **コンピューターの検査** – 選択した検出を報告したデバイスで、[オンデマンド検査タスク](#)を実行します。
- **i 詳細を表示** – 検出詳細を参照してください。

o 概要 - 概要 セクションには、検出の基本情報が表示されます。このセクションでは、さまざまなアクションで検出を管理(使用可能なアクションは検出カテゴリによって異なります)したり、[コンピューター詳細](#)に移動して、検出が発生したコンピューターの詳細を確認したりすることができます。

o 発生 - 発生 セクションは、検出が[集約](#)されているときにのみ有効であり、個別の検出が一覧表示されます。同じ検出に関するすべての発生を解決済み/未解決に設定できます。






- **コンピューター** – 検出が見つかったときにコンピューターで実行できるアクションの一覧が表示されます。この一覧は、[コンピューター](#)セクションの一覧と同じです。
- **📋 監査ログ** – 選択した項目の[監査ログ](#)を表示します。
- **✅ 解決済みに設定 / ⚠️ 未解決に設定** – ここまたは[コンピューター詳細](#)で、検出を解決済み/未解決に設定できます。
- **▶ タスクの実行** – 既存のタスクを実行し、トリガーを作成してタスクを完了します。
- **🔍 パスを検査(🛡️ ウイルス対策検出 – ファイルと既知のパスでのみ使用可能) – 定義済みのパスと対象で[オンデマンド検査タスク](#)を作成します。**

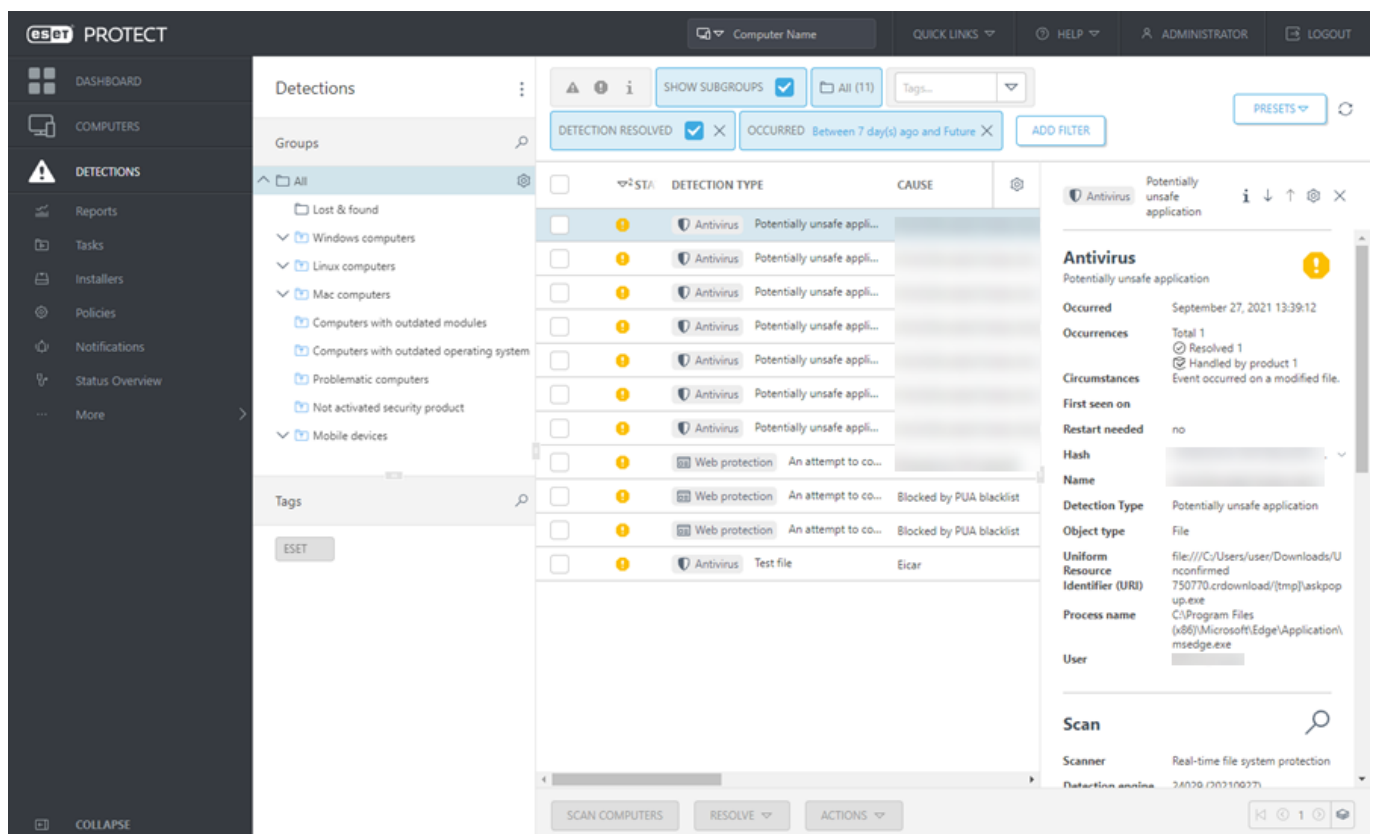
-  除外の作成( ウイルス対策検出と  ファイアウォールIDSルールでのみ使用可能) - [検出除外](#)を作成します。
-  EIに表示は  Enterprise Inspector項目でのみ使用でき、[ESET Enterprise Inspector](#) Webコンソールで直接項目詳細を開くことができます。
-  EDTDにファイルを送信は、 [ブロックされたファイル](#)でのみ使用できますESET Dynamic Threat Defense Webコンソールからマルウェア分析のファイル([ESET PROTECT](#))を送信できます。[提出されたファイル](#)では、ファイル分析の詳細を確認できますESET Dynamic Threat Defenseで分析のために手動で他の実行ファイルを送信する場合は、ESETエンドポイント製品から実行できます(ESET Dynamic Threat Defenseライセンスが必要です)。

検出プレビュー




検出で、検出名をクリックすると、右側に検出プレビューサイドパネルが表示されます。検出プレビューサイドパネルには、選択した検出に関する最も重要な情報が表示されます。


検出プレビューの操作:


-  詳細を表示 - [検出詳細](#) ウィンドウを開きます。
-  次へ - 検出プレビューサイドパネルに次のデバイスを表示します。
-  前へ - 検出プレビューサイドパネルに前のデバイスを表示します。
-  検出詳細のコンテンツを管理 - 検出プレビューサイドパネルのセクションと表示順を管理できます。
-  閉じる - 検出プレビューサイドパネルを閉じます。



除外の作成

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/グループに適用できます。[詳細 > 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。

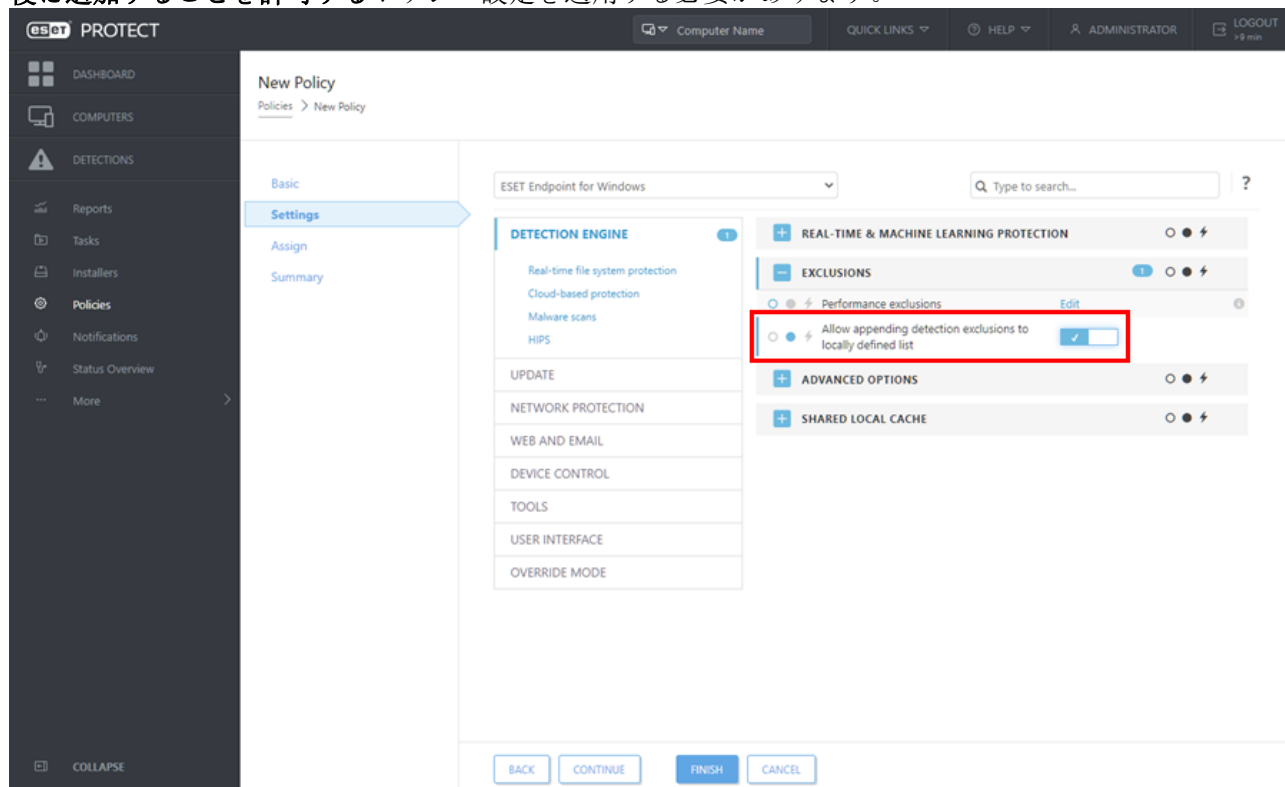
 除外は注意して使用してください。コンピューターが感染するおそれがあります。

ESET PROTECTには、次の2つの **ウイルス対策除外**カテゴリがあります。

- **パフォーマンスの除外** - パスで定義されたファイルとフォルダーの除外。ポリシーを使用して作成できます。「[パフォーマンスの除外形式と例](#)」も参照してください。
- **検出除外** - 検出名、検出名とそのパス、またはオブジェクトハッシュ(SHA-1)によって定義されたファイルの除外。「[検出名による検出除外の例](#)」も参照してください。

検出除外の制限

- ESET PROTECTでは、ポリシーを使用して、検出除外を作成することはできません。
- 以前にポリシーに検出除外が含まれていた場合、[ポリシーから除外リストに除外を移行](#)できます。
- 既定では、検出除外は、管理されたコンピューターの既存のローカル除外を置き換えます。既存のローカル除外リストを保持するには、検出除外を適用する前に、**検出除外をローカル定義されたリストの最後に追加することを許可する**ポリシー設定を適用する必要があります。



設定


選択した**除外条件**に基づいて、1つ以上の検出を除外できます。

ウイルス対策検出

- **パスと検出** – ファイル名 (file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe など) を含む、検出名とパスで各ファイルを除外します。
- **正確なファイルSHA-1ハッシュ**で各ファイルを除外します。
- **検出検出名**で各ファイルを除外します。

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。

ファイアウォール検出 - IDSルール




- **検出とコンテキスト (推奨)** – 検出、アプリケーションID、IPアドレスによって、次の条件の組み合わせでファイアウォール検出を除外します。
- **IPアドレス** – リモートIPアドレスでファイアウォール検出を除外します。このオプションは、特定のコンピューターとのネットワーク通信で誤検出が発生する場合に使用します。
- **検出** – 検出を除外し、複数のリモートコンピューターからトリガーされた誤検出を無視します。
- **アプリケーション** – ネットワーク検出からアプリケーションを除外します。IDS誤検出の原因となるアプリケーションのネットワーク通信を許可します。

検出タイプに基づいて、推奨オプションがあらかじめ選択されています。

一致するアラートを解決 チェックボックスをオンにすると、除外の対象となるアラートを自動的に解決します。

任意で、コメントを追加できます。

対象

 検出除外 ( **ウイルス対策検出** および  **ファイアウォールIDSルール**) は、互換性があるESETセキュリティ製品 がインストールされているコンピューターにのみ割り当てることができます。除外は互換性のないESETセキュリティ製品には適用されず、無視されます。

既定では、除外はユーザーのホームグループに適用されます。

割り当てを変更するには、**コンピューターの追加** または **グループの追加** を選択し、除外が適用される対象を選択するか、既存の割り当てを選択して、**対象の削除** をクリックします。



プレビュー

作成された除外の概要を表示できます。すべての除外設定が、設定に基づいて、正しいことを確認します。



除外を作成した後に編集することはできません。割り当てのみを [変更するか、除外を削除](#) できます。

完了をクリックして、除外を作成します。


作成したすべての除外は、[詳細 > 除外](#) で確認できます。コンピューターまたはグループに除外が適用されているかどうかを確認するには、コンピューターの詳細 > [設定 > 適用された除外](#) またはグループ詳細 > [除外](#) に移動します。

除外と互換性のあるESETセキュリティ製品




除外は互換性のないESETセキュリティ製品には適用されず、無視されます。

ウイルス対策検出除外

すべての[管理可能なESETセキュリティ製品](#)は、次を除き、 **ウイルス対策検出除外**に対応します。

- ESET Endpoint Security for Android
- ESET Dynamic Threat Defense
- ESET Enterprise Inspector
- ESET仮想セキュリティ
- ESET Endpoint for macOSバージョン6.8.1以降。

ファイアウォールIDSの除外

次のESETセキュリティ製品は  **ファイアウォールIDS**の除外に対応しています。

- ESET Endpoint Antivirus for Windows (バージョン8.0以降)
- ESET Endpoint Security for Windows (バージョン8.0以降)

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**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**

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。

ESET Enterprise Inspector

ESET Enterprise Inspectorは、包括的なエンドポイント検出および応答システムであり、インシデント検出、インシデント管理と応答、データ収集、危険検出の指標、特異性の検出、動作検出、ポリシー違反などの機能があります。ESET Enterprise Inspectorをインストール、機能の詳細については、[ESET Enterprise Inspectorヘルプ](#)を参照してください。

ESET Enterprise Inspector 設定

ESET Enterprise Inspectorには、次の目的で、ESET PROTECTが必要です。

- 適切な権限を持つ[ESET Enterprise Inspectorユーザー](#)を作成します。ESET PROTECT 9.0にはESET Enterprise Inspectorユーザー向けの定義済み[権限セット](#)が含まれます。
- [ESET Enterprise Inspector](#)サーバーインストール中に使用される[証明書](#)を作成します。
- ESET Enterprise Inspectorに接続されたデバイスでESET PROTECTを[アクティベーション](#)します。



ESET Enterprise InspectorをアクティベーションするにはESET Enterprise Inspectorライセンスが必要です。

ESET Enterprise InspectorでのESET PROTECT検出の報告

ESET Enterprise InspectorにESET Enterprise Inspectorエージェント(正しく設定されESET PROTECTサーバーに接続済み)を実行する[デバイスを追加](#)する場合ESET Enterprise InspectorはESET PROTECT[検出](#)セクションで見つかった検出を報告します。これらの検出をフィルタリングするには、 **Enterprise Inspector**検出カテゴリを選択します。

ESET Enterprise Inspectorで報告される別の検出タイプは、 **ブロックされたファイル**です。これらはESET Enterprise Inspectorでブラックリストとして設定された実行ファイルの起動のブロックされた試みです([ブロックされたハッシュ](#))。EDTDにファイルを送信は、 **ブロックされたファイル**でのみ使用できます。ESET Dynamic Threat Defense Webコンソールからマルウェア分析のファイル([ESET PROTECT](#))を

送信できます。[提出されたファイル](#)では、ファイル分析の詳細を確認できます。ESET Dynamic Threat Defenseで分析のために手動で他の実行ファイルを送信する場合は、ESETエンドポイント製品から実行できます(ESET Dynamic Threat Defenseライセンスが必要です)。

ESET Enterprise InspectorでのESET PROTECT検出の管理

ESET Enterprise Inspector WebコンソールでのESET PROTECT検出の統合により、Enterprise Inspector検出を直接ESET PROTECT Webコンソールから管理できます。ESET Enterprise Inspector Webコンソールを開く必要はありません。たとえば、ESET PROTECT Webコンソールで検出を解決済みに設定する場合、ESET Enterprise Inspector Webコンソールでも解決済みに設定されます。逆も同様です。

検出をクリックし、**IEIに表示**を選択すると、ESET Enterprise Inspector Webコンソールに検出詳細が表示されます。

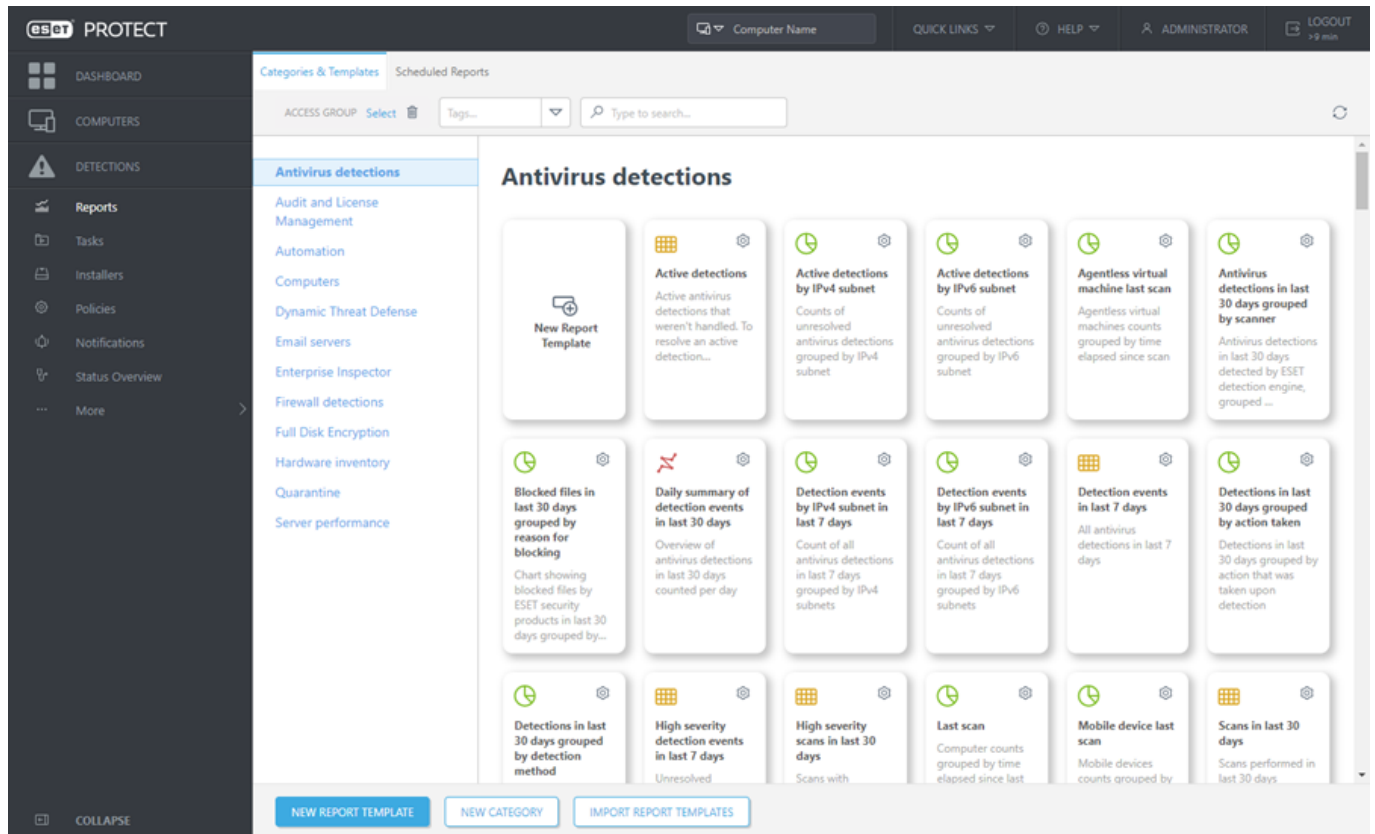
ESET PROTECT WebコンソールでEnterprise Inspector検出を管理するには、次のシステム要件を満たす必要があります。

- ESMC 7以降。
- ESETエンドポイントソフトウェア(ESET Endpoint Antivirus/ESET Endpoint Security)バージョン7以降が管理対象のコンピューターにインストールされていること。


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。レポートウィンドウには2つのタブがあります。

- **カテゴリとテンプレート** – これはレポートセクションの既定のタブです。レポートカテゴリとテンプレートの概要が含まれます。ここで新しいレポートとカテゴリを作成するか、他のレポート関連アクションを実行できます。
- **スケジュールされたレポート** – このタブにはスケジュールされたレポートの概要が表示されます。また、ここで[新しいレポートをスケジュール](#)できます。




レポートはレポートタイプ別に分類されたテンプレートから生成されます。レポートテンプレートはすぐに生成するか、[スケジュール](#)して後から生成できます。レポートをただちに[生成](#)して表示するには、任意のレポートテンプレートの横の**今すぐ生成**をクリックします。[カテゴリとテンプレート]リストから定義済みのレポートテンプレートを使用するか、カスタム設定の新しいレポートテンプレートを作成できます。[新しいレポートテンプレート](#)をクリックし、レポートテンプレートウィザードを開いて、新しいレポートのカスタム設定を指定します。新しいレポートカテゴリ([新しいカテゴリ](#))を作成するか、前にインポートされたレポートテンプレート([レポートテンプレートのインポート](#))をインポートします。



 ページの上には検索バーがあります。説明ではなく、カテゴリとテンプレート名を検索できます。







[タグ](#)を使用して、表示される項目をフィルタリングできます。

[Select](#)  [アクセスグループフィルターボタン](#)では、ユーザーが静的グループを選択し、属するグループに応じて、[表示されるオブジェクトをフィルタリング](#)できます。


レポートテンプレートの使用









レポートテンプレートを選択し、レポートテンプレートタイルの歯車アイコンをクリックします。使用可能なオプションは次のとおりです。



 今すぐ生成	レポートが生成され、出力データを確認できます。
 ダウンロード	ダウンロード をクリックし、レポートを生成してダウンロードします。 .pdf または .csv を選択できます。CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します

 スケジュール	レポートのスケジュール - トリガー調整 、およびレポート配信のスケジュールを修正できます。 スケジュールされたレポートタブ に、すべてのスケジュールされたレポートが表示されます。
 編集	既存のレポートテンプレートを編集します。 新しいレポートテンプレートを作成する 場合と同じ設定とオプションが適用されます。
 監査ログ	選択した項目の 監査ログ を表示します。
 複製	選択したレポートに基づいて、新しいレポートが追加されます。（複製には新しい名前が必要です。）
 削除	選択したレポートテンプレートを完全に削除します。
 エクスポート	レポートテンプレートは .dat ファイルにエクスポートされます。

レポートカテゴリの使用

レポートカテゴリを選択し、カテゴリの右端で歯車  アイコンをクリックします。使用可能なオプションは次のとおりです。

 新しい分類	名前を入力し、レポートテンプレートの新しいカテゴリを作成します。
 新しいレポートテンプレート	新しいカスタムレポートテンプレートの作成
 削除	選択したレポートテンプレートカテゴリを完全に削除します。
 編集	既存のレポートテンプレートカテゴリ名を変更します。
 監査ログ	選択した項目の 監査ログ を表示します。
 エクスポート	レポートテンプレートカテゴリとすべての含まれるテンプレートは .dat ファイルにエクスポートされます。後からすべてのテンプレートを含むカテゴリをインポートするには、 レポートテンプレートのインポート をクリックします。たとえば、カスタムレポートテンプレートを別の ESET PROTECT サーバーに移行する場合に便利です。
 アクセスグループ >  移動	レポートテンプレートカテゴリを別の静的グループに移動します。これで、ターゲットグループのローカル管理者がアクセスできます。ローカル管理者はグループ内でフルアクセス権限があります。

 レポートテンプレートのインポート/ エクスポート機能は、レポートテンプレートのみをインポートおよびエクスポートし、データが入った実際に生成されたレポートはエクスポートしません。

レポートの権限

レポートは ESET PROTECT データベース内のオブジェクトの構造に存在する静的オブジェクトです。新しいレポートテンプレートは作成したユーザーのホームグループに保存されます。レポートにアクセスするには、[権限](#)が必要です。レポートによって検査されるオブジェクトへのアクセス許可も必要です。たとえば、[コンピュータステータス概要](#)レポートを生成する場合は、[読み取り](#)権限を持つコンピュータからのみデータを収集できます。

- **読み取り** – レポートテンプレートとカテゴリを一覧表示します。レポートテンプレートに基づいてレポートを生成できます。ユーザーは自分のダッシュボードを読み取れます。
- **使用** – 使用可能なレポートテンプレートでダッシュボードを修正できます。
- **書き込み** – レポートテンプレートとカテゴリを作成、修正、削除できます。すべての既定のテンプレートは [すべて] グループにあります。

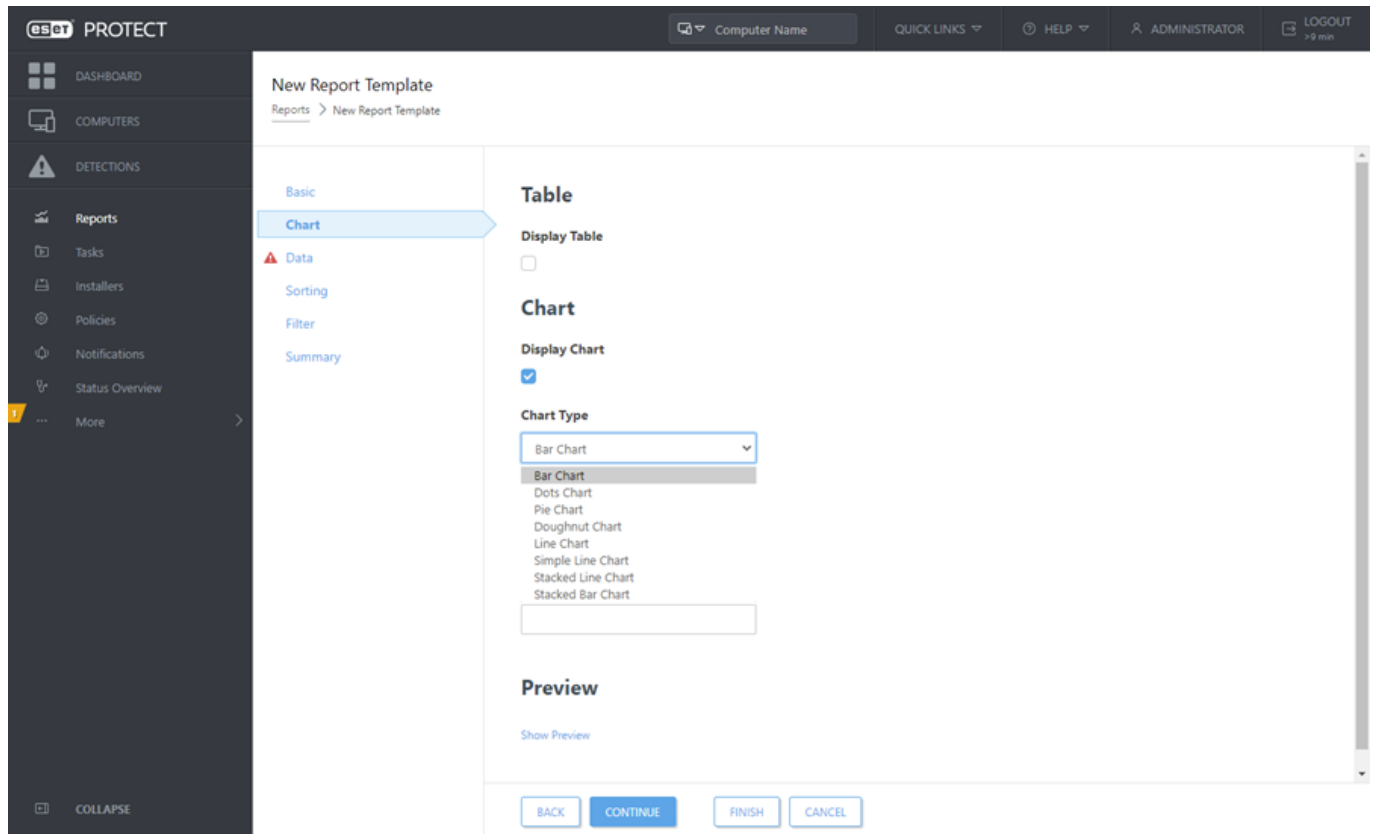
新しいレポートテンプレートの作成

[レポート](#)に移動し、新しいレポートテンプレートをクリックします。

The screenshot shows the 'New Report Template' form in the ESOT PROTECT interface. The form is divided into two main sections: 'Basic' and 'Chart'. The 'Basic' section is currently active and contains fields for 'Name' (pre-filled with 'New Report Template'), 'Description', 'Tags' (with a 'Select tags' link), and 'Category' (with a '<No category selected>' message). The 'Chart' section is collapsed. The left sidebar shows the navigation menu with 'Reports' highlighted. The top header includes the ESOT PROTECT logo, a search bar, and user information.

基本

テンプレートに関する基本情報を編集します。**名前**、**説明**および**カテゴリ**を入力します。定義済みカテゴリからのみ選択できます。新しいカテゴリを選択する場合([前の章](#)で説明した**新しいカテゴリ**オプション)を使用します。**タグを選択**をクリックして、[タグを割り当て](#)ます。



グラフ

グラフセクションで、レポートの種類を選択します。情報を行と列で並べ替えるテーブル、またはX軸とY軸を使用してデータを表示するグラフのいずれかの種類になります。

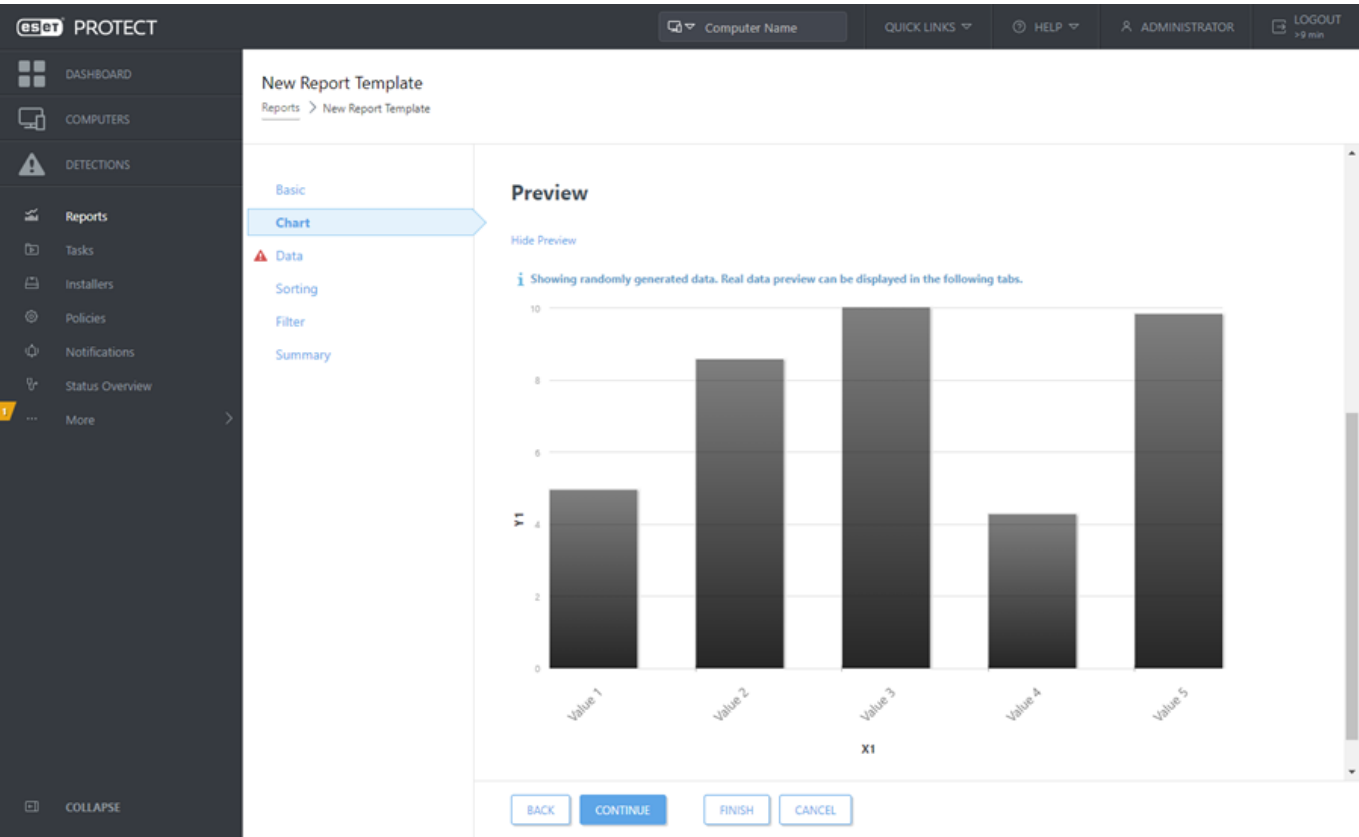
i 選択したグラフは、プレビューセクションに表示されます。この方法で、レポートがどのように表示されるかをリアルタイムで確認することができます。

グラフを選択すると、複数のオプションを使用することができます。

- **棒グラフ**—表示する値に比例した長方形棒のグラフ。
- **ドットグラフ** — このグラフでは、ドットを使用して、定量値(グラフに類似しています)を表示します。
- **円グラフ**—円グラフは、円形のグラフで、扇形に分割し、値を表示します。
- **ドーナツグラフ**—円グラフに類似していますが、ドーナツグラフは複数種類のデータを含めることができます。
- **折れ線グラフ**—直線の線分でない一連のデータ要素として情報を表示します。
- **単純折れ線グラフ**—データ要素を表示せず値に基づいた折れ線で情報を表示します。
- **積み上げ折れ線グラフ**—このグラフは、異なる単位のデータを分析する場合に使用します。
- **積み上げ棒グラフ**—単純棒グラフに類似していますが、複数のデータ型を異なる単位で棒に積み上げています。

必要に応じて、グラフのX軸およびY軸にタイトルを入力すると、グラフが読みやすくなり、傾向を簡単

に認識できます。








データ

データセクションでは、表示する情報を選択します。

- a. **テーブル列**: テーブル情報は、選択したレポートの種類に基づいて自動的に追加されます。名前ラベルおよびフォーマットをカスタマイズすることができます(下記参照)。
- b. **グラフ軸**: X軸およびY軸のデータを選択します。**軸の追加**をクリックすると、オプションのウィンドウが開きます。Y軸で利用できる選択肢は常に、X軸で選択した情報に依存、またはその逆となるのは、グラフがそれぞれの関係性を表示しており、データ互換性を持つ必要があるからです。必要な情報を選択して、**OK**をクリックします。


形式

データセクションで、 シンボルをクリックし、展開された書式オプションを表示します。フォーマットを変更して、データを表示する書式を変更できます。テーブル列とグラフ軸の書式を調整できます。一部のオプションは各データ型で使用できません。


列の形式	書式設定される現在の列に応じて、列を選択します。たとえば、 名前 列の書式を設定するときには、 重要度 列を選択し、名前の横の重大度アイコンを追加します。
最小値	表示された値の最小値を設定します。
最大値	表示された値の最大値を設定します。
色	列の配色を選択します。色は、 列の形式 で選択された列の値に従って、調整されます。
アイコン	    列の形式 の値に従い、書式設定された列にアイコンを追加します。

矢印のいずれか↓↑をクリックして、列の順序を変更します。

並べ替え

データセクションで選択されたデータに並べ替え可能な記号がある場合は、並べ替えを使用できます。**並べ替えの追加**をクリックし、選択したデータ間の関係性を定義することができます。開始情報(並べ替え値)および並べ替えの方法、**昇順**または**降順**のいずれかを選択します。ここで、グラフに表示する結果を定義します。**上**または**下**をクリックして、並べ替え要素の順序を変更します。ごみ箱アイコンをクリックし、選択から要素を削除します。

フィルター

フィルタ処理方法を定義します。**フィルターの追加**をクリックし、フィルタ要素リストにある値から選択します。ここでは、グラフに表示する情報を定義します。ごみ箱アイコンをクリックし、選択から要素を削除します。

概要

サマリーでは、選択したオプションおよび情報を確認します。**完了**をクリックして、新しいレポートテンプレートを作成します。

レポートの作成

レポートテンプレートからレポートを即座に生成するには、いくつかの方法があります。

- 上のバーの**クイックリンク**に移動し、**レポートの生成**をクリックします。既存のレポートテンプレートを選択し、**今すぐ生成**をクリックします。
- **レポート**をクリックし、**カテゴリ**と**テンプレートタブ**を選択します。レポートを生成するレポートテンプレートを選択します。テンプレートを変更する場合は、歯車アイコンをクリックし、**編集**をクリックします。

OESET PROTECT Webコンソールでは、レポートタイルをクリックして、レポートを生成して表示できます。レポートが生成されるときに、**生成してダウンロード**をクリックすると、任意の形式でレポートを保存します。**.pdf**または**.csv**を選択できます。CSVはテーブルデータにのみ適していて、**;** (セミコロン)を区切り文字として使用します

- **タスク > 新規 > +サーバータスク**に移動して、新しい**レポートの生成**タスクを作成します。

0タスクが作成され、**タスクタイプ**リストに表示されます。このタスクを選択し、ページの下の**今すぐ実行**をクリックします。タスクがすぐに実行されます。

0**レポートの生成**タスクで説明されている設定を構成し、**[完了]**をクリックします。



ESET PROTECT Webコンソールで表示されるレポートの項目をクリックすると、追加オプションを含む**ドリルダウン**メニューが表示されます。

レポートのスケジュール

レポートの生成をスケジュールする方法はいくつかあります。

- **タスク > 新規 > +**サーバータスクに移動して、新しい[レポートの生成](#)タスクを作成します。
- レポートに移動し、レポートを生成するレポートテンプレートを選択し、テンプレートタイトルの歯車アイコンをクリックして、**スケジュール**を選択します。定義済みのレポートテンプレートを使用して編集するか、[新しいレポートテンプレートを作成](#)します。
- [ダッシュボード](#)のレポートテンプレートのコンテキストメニューで**スケジュール**をクリックします。
- **レポート > スケジュールされたレポート**タブに移動し、 **スケジュール**。

レポートをスケジュールするときには、[レポートの生成](#)タスクに従い、複数のオプションがあります：

- i** • 1つのレポートで複数のレポートテンプレートを選択します。
- 電子メールでレポート配信を設定するか、ファイルに保存します。
- 任意で、トリガーと調整パラメーターを設定します。

レポートがスケジュールされた後、**完了**をクリックします。タスクが作成され、[トリガー](#)で定義した間隔で(1回または繰り返し)、[調整設定](#)(任意)に基づいて実行されます。

スケジュールされたレポートタブ

レポート > スケジュールされたレポートでスケジュールされたレポートを確認できます。このタブの他のアクションを以下に示します。

スケジュール	既存のレポートの新しいスケジュールを作成します。
i 詳細を表示	選択したスケジュールの詳細を表示します。
目 監査ログ	選択した項目の 監査ログ を表示します。
🏷 タグ	タグ を編集します(割り当て、割り当て解除、作成、削除)。
▶ タスクの実行	スケジュールされたレポートをすぐに実行します。
✎ 編集	レポートのスケジュールを編集します。レポートテンプレートを追加または選択解除、スケジュール設定の変更、またはレポートの調整および配信設定を編集できます。
📄 複製	ホームグループで重複するスケジュールを作成します。
🗑 削除	スケジュールを削除します。レポートテンプレートはそのままです。
📁 アクセスグループ > 移動	スケジュールを別のアクセスグループに移動します。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

古いアプリケーション

古いアプリケーションレポート(レポート>コンピューターカテゴリの下)を使用し、どのESET PROTECTコンポーネントが最新ではないのかを確認します。

このレポートを実行するには2つの方法があります。

- [新しいダッシュボード](#)を追加するか、既存のダッシュボードペインのいずれかを修正します。
- レポート>コンピューターカテゴリ > 古いアプリケーションタイルに移動し、**今すぐ生成**をクリックします。

古いアプリケーションがある場合は次の手順を実行できます。

- クライアントタスク[ESET PROTECTコンポーネントアップグレード](#)を使用してESET Managementエージェント、サーバMDMをアップグレードします。
- クライアントタスク[ソフトウェアインストール](#)を使用して、セキュリティ製品をアップグレードします。

SysInspectorログビューア

SysInspectorログビューアを使用すると、クライアントコンピューターで実行された後に、SysInspectorからログを表示できます。また、正常に実行された後に、[SysInspectorログ要求タスク](#)から直接SysInspectorログを開けます。ログファイルは、ローカルコンピューターのSysInspectorでダウンロードおよび表示できます。

i SysInspectorログは、Windowsクライアントからのみ要求できます。

SysInspectorログを表示する方法

ダッシュボードから

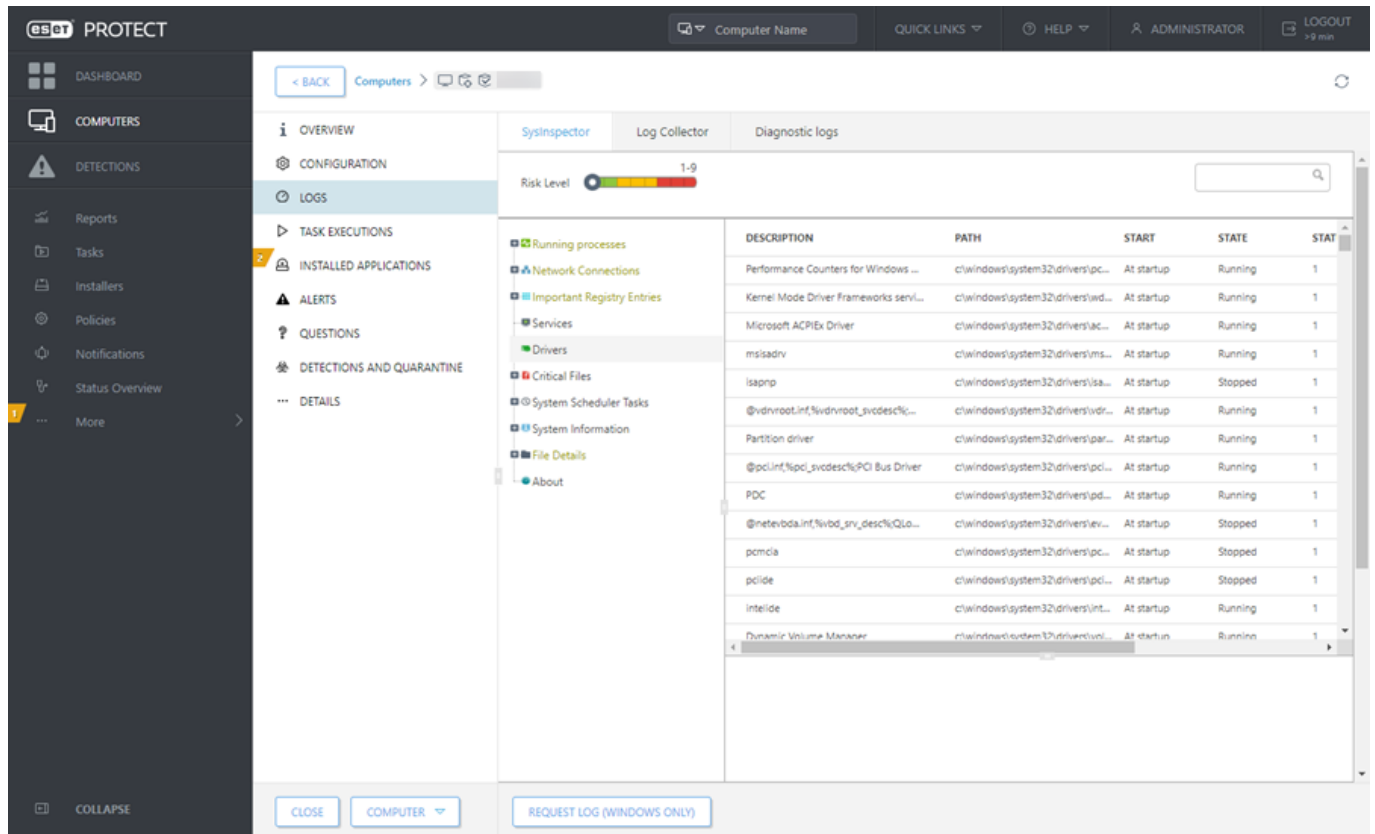
- 1.[新しいダッシュボード](#)を追加するか、既存のダッシュボードレポートのいずれかを編集します。
2. レポートテンプレート自動化>過去30日のSysInspectorスナップショット履歴を選択します。
3. レポートを開き、コンピューターを選択してから、ドロップダウンメニューから🕒 **SysInspectorログビューを開く**を選択します。

レポートから

- 1.[レポート](#)>自動カテゴリに移動します。
2. リストから過去30日のSysInspectorスナップショット履歴テンプレートを選択し、**今すぐ生成**をクリックします。
3. レポートを開き、コンピューターを選択してから、ドロップダウンメニューから🕒 **SysInspectorログビューを開く**を選択します。

コンピューターメニューから

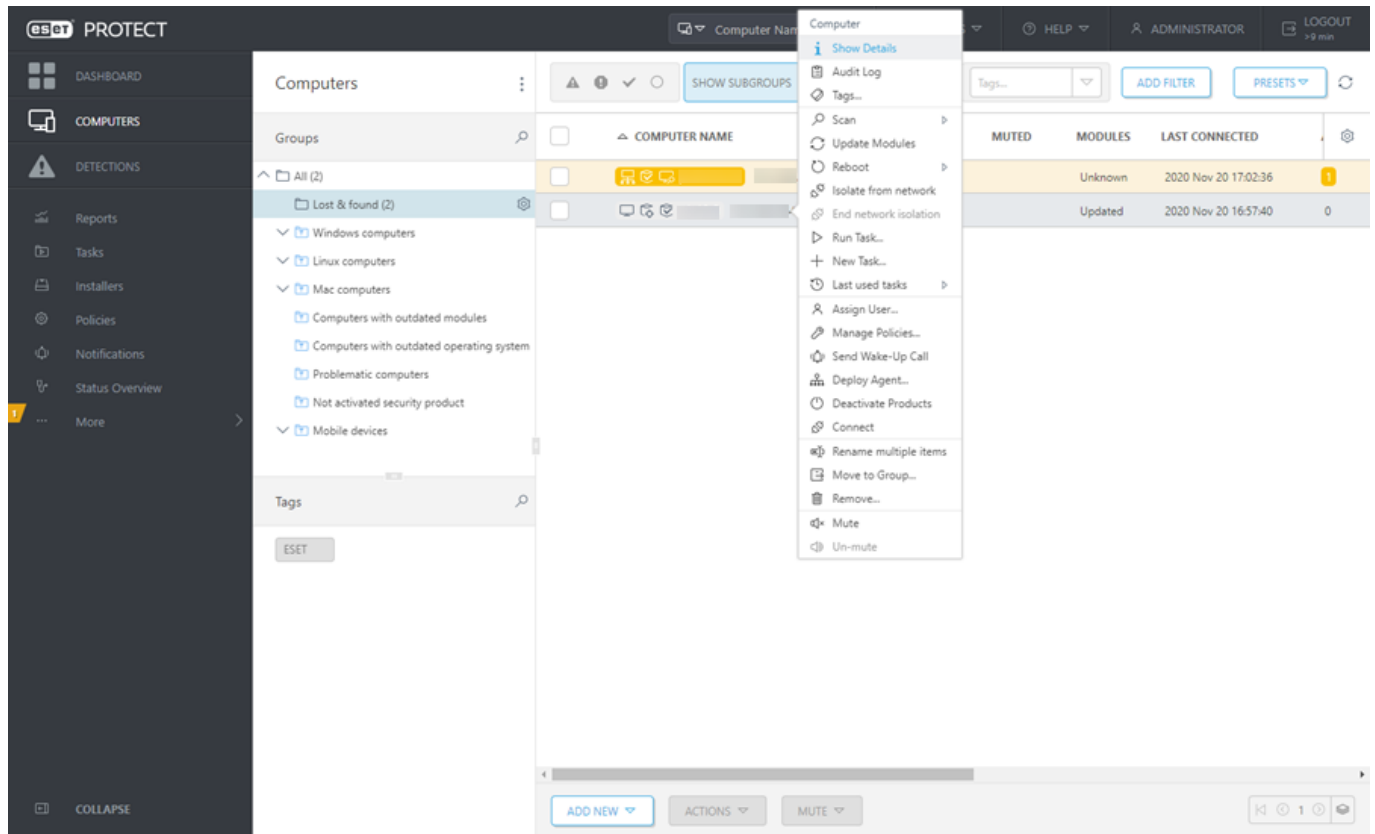
1. [\[コンピューター\]](#)に移動します。
2. 静的または動的グループでコンピューターを選択し、**i [詳細を表示]**をクリックします。
3. ログセクション > **SysInspector**タブに移動し、リストエントリをクリックして🕒 **SysInspector Log Viewerを開く**



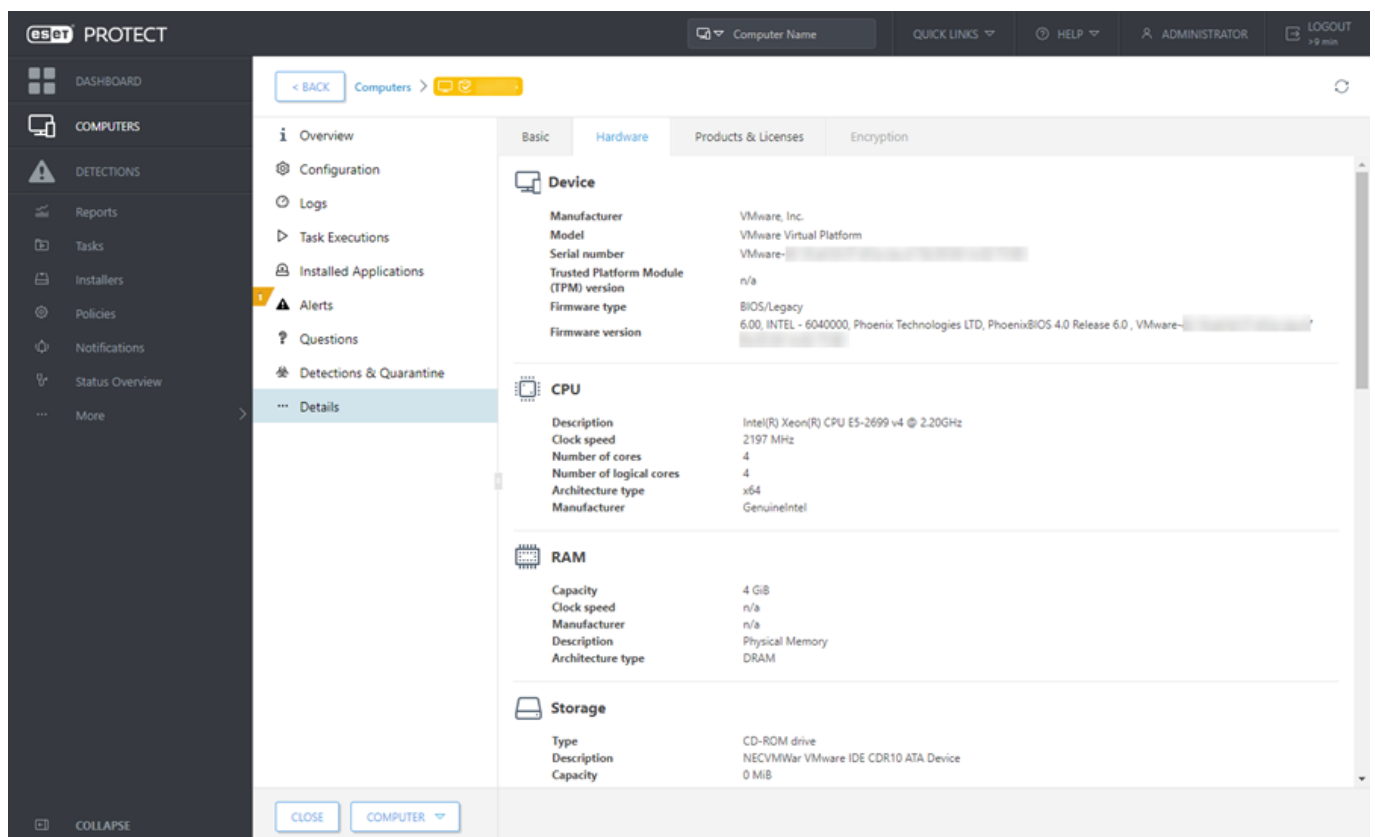
ハードウェアインベントリ

ESET PROTECTには、デバイスのRAMストレージ、プロセッサに関する詳細など、接続されたデバイスからハードウェアインベントリ詳細を取得する機能があります。

コンピューターをクリックし、接続されているデバイスをクリックして、**詳細を表示**を選択します。



詳細をクリックし、ハードウェアタブを選択します。



ハードウェアパラメーターに基づいて、接続されたデバイスをフィルタリングできます。次のハードウェアインベントリカテゴリから選択できます: シャーシ、デバイス情報、ディスプレイ、ディスプレイアダプター、入力装置、大容量記憶装置、ネットワークアダプター、プリンター、プロセッサ、RAM、サウンドデバイス。

ハードウェアインベントリレポート

レポート>ハードウェアインベントリには、定義済みのハードウェアインベントリレポートがあります。カスタムハードウェアインベントリレポートを作成できます。[新しいレポートテンプレート](#)を作成するときには、**データ**の下で、**HWインベントリフィルター**のいずれかからサブカテゴリを選択します。最初のテーブル列またはX軸を追加するときには、互換性があるデータのみを選択できます。

ハードウェアインベントリに基づく動的グループ

接続されたデバイスのハードウェアインベントリ詳細に基づいて、[カスタム動的グループを作成](#)できます。[新しい動的グループテンプレート](#)を作成するときには、[ルール](#)をハードウェアインベントリカテゴリから選択します。たとえばRAM容量でフィルタリングされたデバイスの動的グループを作成し、特定のRAM容量のデバイスの概要を取得できます。

ハードウェアインベントリと互換性のあるオペレーティングシステム

ハードウェアインベントリ機能は、[サポートされている](#)すべてのWindows®Linux*およびmacOSコンピューターで使用できます。

* 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するために、クライアント/サーバLinuxマシンに 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	<code>sudo apt-get install -y lshw</code>
Red Hat, CentOS, RHEL	<code>sudo yum install -y lshw</code>
OpenSUSE	<code>sudo zypper install lshw</code>

監査ログレポート

監査ログレポートにはESET PROTECTサーバーでユーザーが実行したすべてのアクションと変更が含まれます。

このレポートを実行するには、**レポート>監査とライセンス管理**カテゴリ > **監査ログ**をクリックします。

i Webコンソールの[詳細](#)>[監査ログ](#)の下で、監査ログを直接表示してフィルタリングできます。

! 監査ログを表示するにはWebコンソールユーザーに[監査ログ機能](#)を含む権限セットが必要です。ESMC 7.1以前からアップグレードした場合は、ユーザーに[監査ログ機能](#)を付与する必要があります(当初は[サーバー設定機能](#)が必要でした)。

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。最も一般的なシナリオに対応する定義済みのタスクがあります。あるいは、特定の設定を使用してカスタムクライアントタスクを作成できます。タスクを使用して、クライアントコンピューターからアクションを要求します。クライアントタスクを正常に実行するには、タスクとタスクが使用するオブジェクト(デバイス)に対する十分なアクセス権が必要です。

アクセス権の詳細については、[権限の一覧](#)を参照してください。

次の2つの主なタスクカテゴリがあります。[クライアントタスク](#)と[サーバータスク](#)。

- グループまたは個別のコンピューターに[クライアントタスクを割り当てる](#)ことができます。作成すると、[トリガー](#)を使用してタスクが実行されます。クライアントタスクには、別のトリガーを設定することもできます。クライアントタスクは、クライアントESET ManagementエージェントがESET PROTECTサーバーに接続するときにクライアントに配信されます。同じ理由から、タスク実行結果がESET PROTECTサーバーに通信されるまでに時間がかかることがあります。[ESET Managementエージェント接続間隔を管理](#)し、タスク実行時間を下げることができます。
- サーバータスクは、サーバーまたは他のデバイスでESET PROTECTサーバーによって実行されます。サーバータスクを、特定のクライアントまたはクライアントグループに割り当てることはできません。各サーバーは1つの[トリガー](#)のみを設定できます。さまざまなイベントでタスクを実行する必要がある場合は、各トリガーに個別のサーバータスクが必要です。

次の2つの方法で、新しいタスクを作成できます。

- **新規** > [+クライアントタスク](#) または [+サーバータスク](#) をクリックします。
- 左側で任意のタスクタイプを選択し、**新規** > [+クライアントタスク](#) または [+サーバータスク](#) をクリックします。

必要に応じて、次の定義済みタスクを使用できます(各タスクカテゴリにはタスクタイプが含まれます)。

[すべてのタスク](#)

[クライアントタスク](#)

[ESETセキュリティ製品](#)

[診断](#)

[ネットワークからのコンピューターの隔離を終了](#)

[ESETアプリケーション設定のエクスポート](#)

[コンピューターをネットワークから隔離する](#)

[モジュールアップデート](#)

[モジュールアップデートロールバック](#)

[オンデマンド検査](#)

[製品のアクティベーション](#)

[隔離管理](#)

[SysInspectorスクリプトの実行](#)

[EDTDにファイルを送信](#)

[サーバー検査](#)

[ソフトウェアインストール](#)

[SysInspector ログ要求\(Windowsのみ\)](#)

[隔離ファイルのアップロード](#)

[ESET PROTECT](#)

[診断](#)

[クローンされたエージェントのリセット](#)

[Rogue Detection Sensor データベースリセット](#)

[ESET PROTECT コンポーネントのアップグレード](#)

[管理の停止\(ESET Management エージェントのアンインストール\)](#)

[OS](#)

[メッセージの表示](#)

[オペレーティングシステムアップデート](#)

[コマンドの実行](#)

[コンピューターをシャットダウンする](#)

[ソフトウェアインストール](#)

[ソフトウェアアンインストール](#)

[管理の停止\(ESET Management エージェントのアンインストール\)](#)

[モバイル](#)

[アンチセフトアクション](#)

[メッセージの表示](#)

[ESET アプリケーション設定のエクスポート](#)

[モジュールアップデート](#)

[オンデマンド検査](#)

[製品のアクティベーション](#)

[サーバータスク](#)

[エージェント展開](#) - エージェントをクライアントコンピューターに配布します。

[未接続のコンピューターを削除](#) - ESET PROTECTに接続していないクライアントをWebコンソールから削除します。

[レポートの生成](#) - 必要に応じてレポートを生成するために使用されます。

[コンピューター名の変更](#) - このタスクはFQDN形式を使用してグループのコンピューターの名前を定期的に変更します。

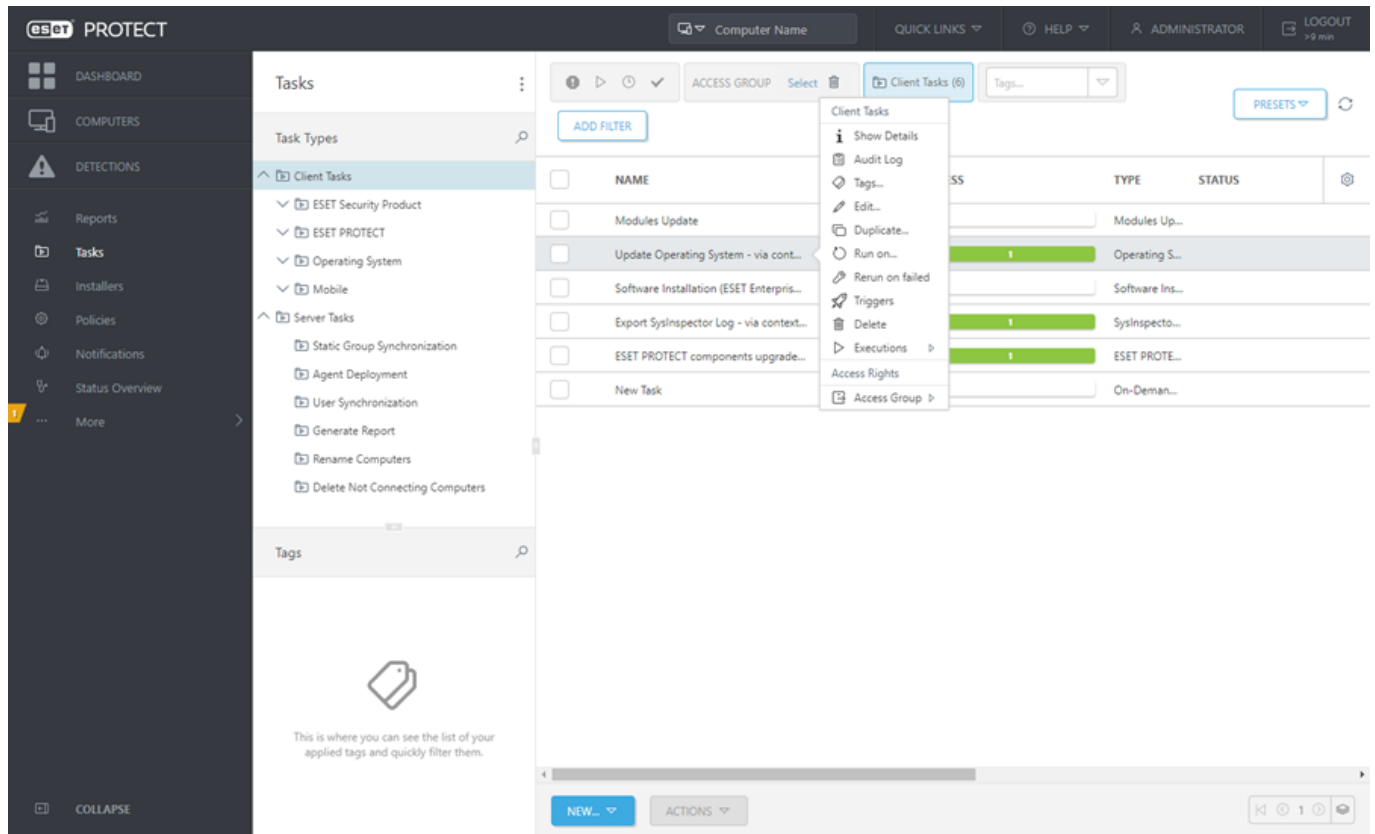
[静的グループ同期](#) - グループ情報を更新して、現在のデータを表示します。

[ユーザー同期](#) - ユーザーまたはユーザーグループを更新します。

クライアントタスク

グループまたは個別のコンピューターに[クライアントタスクを割り当てる](#)ことができます。作成すると、[トリガー](#)を使用してタスクが実行されます。クライアントタスクには、別のトリガーを設定することもできます。クライアントタスクは、クライアントESET ManagementエージェントがESET PROTECTサーバーに接続するときにクライアントに配信されます。同じ理由から、タスク実行結果がESET PROTECTサーバーに通信されるまでに時間がかかることがあります。[ESET Management エージェント接続間隔を管理](#)し、タスク実行時間を下げることができます。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。



新しいクライアントタスクを作成できます

- 1.新しいクライアントタスクを作成するには、**タスク>新規>+クライアントタスク**をクリックするか、任意のタスクタイプを選択して、**新規>+クライアントタスク**をクリックします。
2. **基本**セクションで、**名前や説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。
タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク(すべてのタスク)**の一覧を参照)は、タスクの設定と動作を定義します。
- 3.**[設定]**セクションでタスク設定を構成します。
- 4.**サマリー**セクションでこのタスクのすべての設定を確認し、**[トリガー]**をクリックします。
- 5.**トリガーの作成**をクリックして、クライアントタスクの**トリガー**を作成するか、**[閉じる]**をクリックして後からトリガーを作成します。

クライアントタスクトリガー

トリガーを実行するには、**クライアントタスク**に割り当てる必要があります。トリガーを作成するには、メインテーブルで**タスク**、クライアントタスクインスタンスの順にクリックし、ドロップダウンメニューから**実行日**を選択します。あるいは、**グループまたはコンピューターへのクライアントタスクの割り当て**ができます。

トリガーを定義するには、クライアントタスクが実行される**ターゲットコンピューター**または**グループ**を選択します。対象を選択し、**トリガー条件**を設定して、特定の時刻またはイベントにタスクを実行します。また、**詳細設定 - 調整**を使用して、必要に応じてトリガーを微調整できます。

基本

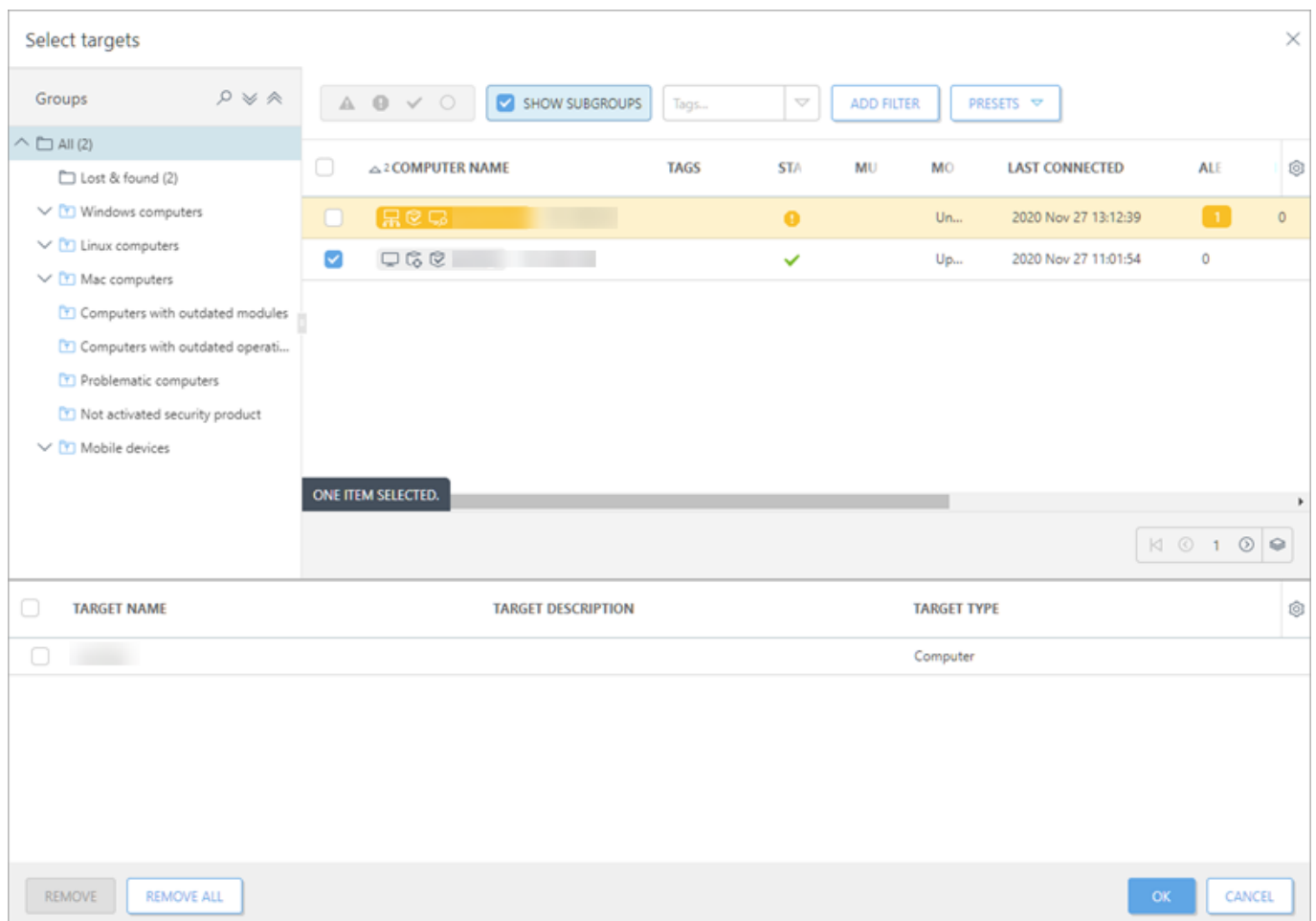
説明にトリガーの基本情報を入力し、[ターゲット]をクリックします。

対象

[対象]ウィンドウでは、このタスクの受信者であるクライアント(個別のコンピューターまたはグループ)を指定できます。

- [コンピューターの追加]をクリックすると、すべての静的および動的グループと、そのメンバーが表示され、デバイスを選択します。
- [グループの追加]をクリックすると、すべての静的および動的グループと、そのメンバーが表示され、グループを選択します。

! グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、Webコンソールの速度低下を防止します。
多数のコンピューターを選択するとWebコンソールに警告が表示されます。



TARGET NAME	TARGET DESCRIPTION	TARGET TYPE
COMPUTER NAME	TAGS	Computer

選択後、[OK]をクリックし、トリガーセクションに移動します。

トリガー

タスクをトリガーするイベントを決定します。

- **即時実行** - クライアントがESET PROTECTサーバーに接続し、タスクを受信したらすぐにタスクを

実行します。**有効期限**までにタスクを実行できない場合は、タスクはキューから削除されます。タスクは削除されませんが、実行もされません。

- **スケジュール** – 選択した時間にタスクを実行します。
- **イベントログトリガー** – ここで指定したイベントに基づいてタスクを実行します。このトリガーは、特定のイベントがログで発生したときに呼び出されます。タスクをトリガーする**ログタイプ**、**論理演算子**、および**フィルタリング条件**を定義します。
- **結合された動的グループトリガー** – このトリガーは、クライアントがターゲットオプションで選択された動的グループを結合するときに実行されます。静的グループまたは個別のクライアントが選択されると、このオプションは使用できません。
- **CRON式** – CRON式を使用して、トリガー間隔を設定できます。

i トリガーの詳細については、[タスクトリガーの種類](#)の章を参照してください。

詳細設定 – 調整

イベントログトリガーや**結合された動的グループトリガー**（上記を参照）など、頻繁に発生するイベントでタスクがトリガーされる場合に、タスクの実行を制限するために調整が使用されます。詳細については、[詳細設定 – 調整](#)の章を参照してください。

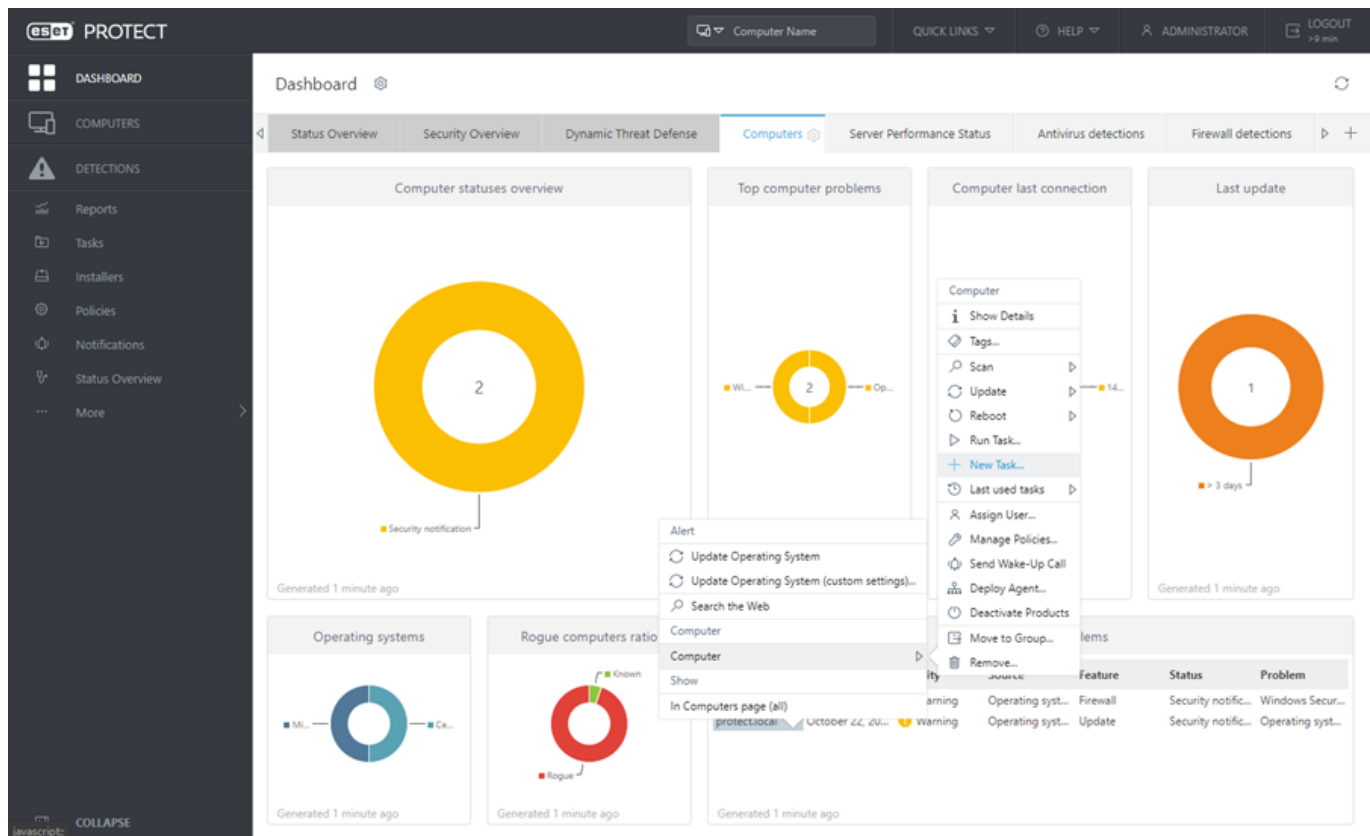
このタスクの受信者とタスクを実行するトリガーを定義したら、**[完了]**をクリックします。

グループまたはコンピューターへのクライアントタスクの割り当て

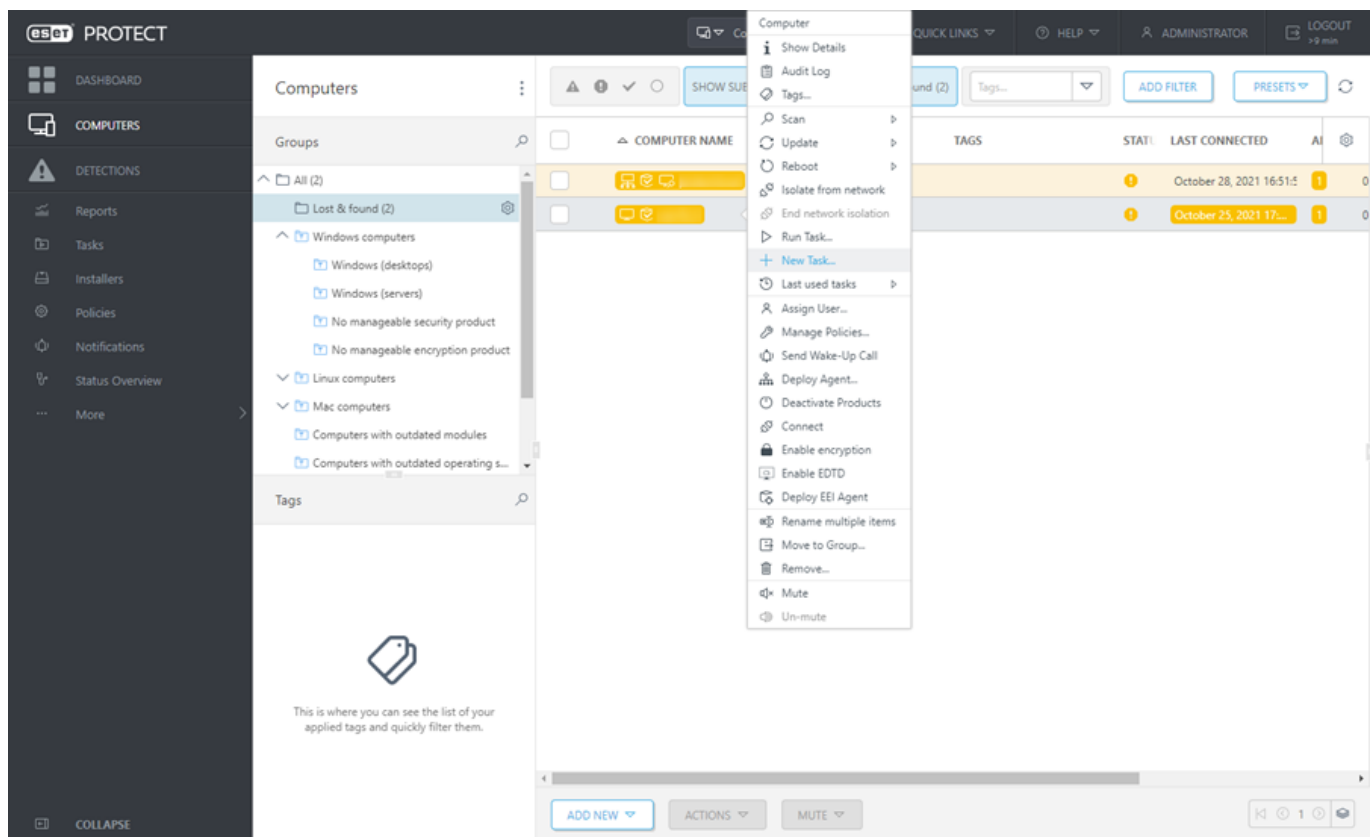
[クライアントタスクをグループに割り当てる](#)方法については、ここをお読みください。

タスクをコンピューターに割り当てる方法は2つあります。

1. **ダッシュボード > コンピューター > 問題があるコンピューター**をクリックして、**コンピューター**を選択し、**コンピューター**をクリックし、**＋新規タスク**を選択します。



2. [コンピューター] > チェックボックスを使用してコンピューターを選択 > + 新規タスク



新しいクライアントタスクウィザードが開きます。

アンチセフトアクション

アンチセフト機能は、モバイルデバイスを不正アクセスから保護します。

ユーザーのモバイルデバイス(ESET PROTECTで登録および管理)がなくなった場合や盗まれた場合には、一部のアクションを自動的に実行し、クライアントタスクを使用して他のアクションを実行できます。

不正ユーザーが信頼できるSIMカードを信頼できないカードと交換した場合ESET Endpoint Security for Androidによってデバイスが自動的にロックされ、アラートSMSがユーザー定義された電話番号に送信されます。このメッセージには、次の情報があります。

- 現在使用中のSIMカードのモバイルデバイス番号
- IMSI (International Mobile Subscriber Identity)番号
- モバイルデバイスのIMSI (International Mobile Subscriber Identity)番号

不正ユーザーは、このメッセージが送信されたことを知りません。このメッセージは、デバイスのメッセージングスレッドから自動的に削除されるためです。また、紛失したデバイスのGPS座標を要求し、クライアントタスクを使用して、デバイスに保存されたすべてのデータをリモートで消去できます。







タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。









基本

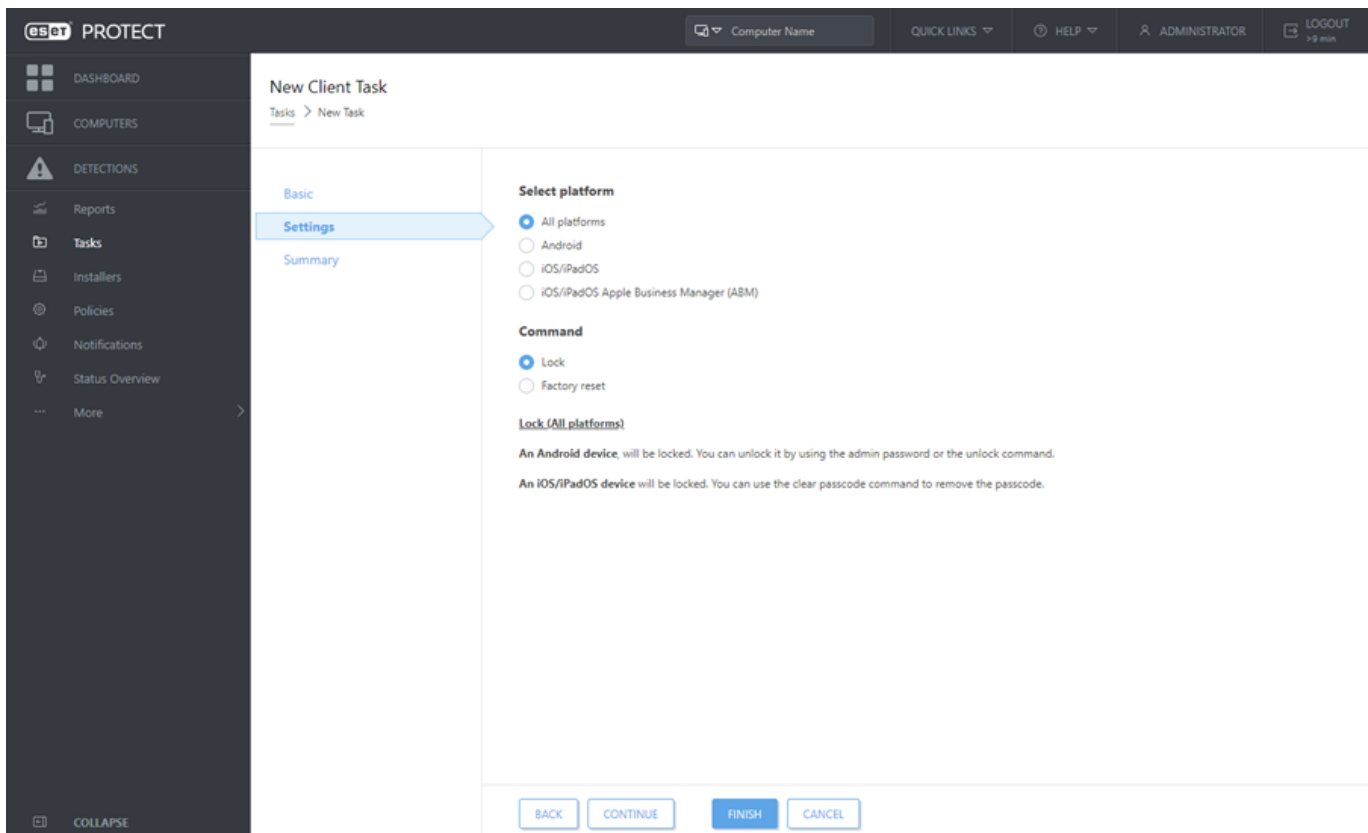
基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク(すべてのタスク)**の一覧を参照)は、タスクの設定と動作を定義します。

設定

操作	モバイルOSでの動作	説明
検索		デバイスは、GPS座標を含むテキストメッセージで返信します。より正確な位置情報が10分後に使用可能になった場合は、デバイスはもう一度メッセージを送信します。受信した情報は デバイス詳細 の下に表示されます。 <div>❗ 検索は、デバイスでGPSが有効な場合にのみ動作します。</div>
		❗ サポートされていません。
ロック		デバイスはロックされます。デバイスは、管理者パスワードまたはロック解除コマンドを使用して、 ロック解除 されます。
		デバイスはロックされます。パスコードは パスコードのクリア コマンドで削除できます。
ロック解除		デバイスはロック解除され、もう一度使用できます。デバイスの現在のSIMカードは信頼できるSIMとして保存されます。
		❗ サポートされていません。

操作	モバイルOSでの動作	説明
警報/紛失モードサウンド		デバイスはロックされ、5分間(またはロック解除されるまで)大音量を再生します。
		❗ サポートされていません。
パスコードをクリア		❗ サポートされていません。
		デバイスからパスコードを削除します。デバイスの電源がオンになったら、新しいパスコードを設定するように指示されます。
出荷時の状態にリセット		デバイスでアクセスできるすべてのデータを迅速に削除します(ファイルヘッダーは破棄されます)。デバイスは既定の初期設定にリセットされます。これには数分かかる場合があります。
		すべての設定と情報は削除され、デバイスは既定の出荷時の設定に戻されます。これには数分かかる場合があります。
紛失モードをオンにして検索		iOS ABMでのみサポートされます。デバイスは「紛失モード」に切り替わり、ロックダウンし、ESETPROTECTから 紛失モードをオフにする タスクを実行することによってのみロック解除できます。紛失したデバイス画面に表示される電話番号、メッセージ、追加情報をカスタマイズできます。デバイスの保護の状態が 紛失 に変更されます。
紛失モードをオフにする		iOS ABMでのみサポートされます。デバイスの保護の状態が変更され、デバイスは標準のサービス状態に戻ります。



ES ET PROTECT | Computer Name | QUICK LINKS | HELP | ADMINISTRATOR | LOGOUT > 9 min

NEW CLIENT TASK
Tasks > New Task

Basic | **Settings** | Summary

Select platform

- ☒ All platforms
- ☐ Android
- ☐ iOS/iPadOS
- ☐ iOS/iPadOS Apple Business Manager (ABM)

Command

- ☒ Lock
- ☐ Factory reset

Lock (All platforms)

An Android device, will be locked. You can unlock it by using the admin password or the unlock command.

An iOS/iPadOS device will be locked. You can use the clear passcode command to remove the passcode.

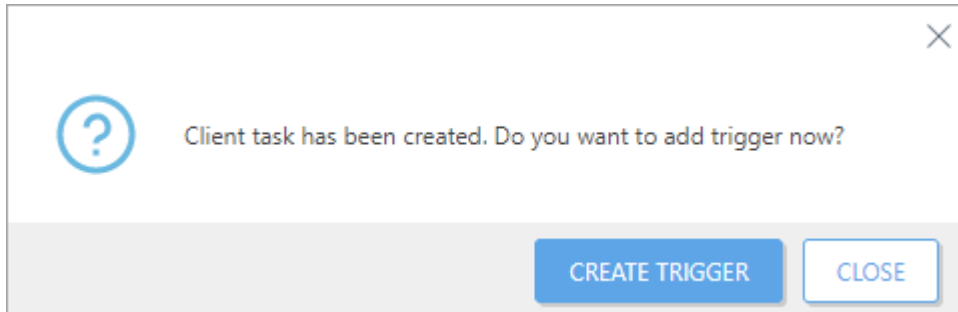
BACK CONTINUE FINISH CANCEL

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップ

プウィンドウが開きます:

- [\[トリガーの作成\]](#) (推奨)] をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から [トリガー](#) を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行** を選択します。



タスクには、作成した各タスクの [進行状況インジケータバー](#)、[ステータスアイコン](#)、および [詳細](#) が表示されます。

診断

診断 タスクを使用して、クライアントコンピューターで ESET セキュリティ製品から診断アクションを要求します。

タスクを作成するには、**タスク > 新規 > + クライアントタスク** をクリックするか、**コンピューター** で目的のクライアント デバイスをクリックし、**新しいタスク** を選択します。

基本

基本 セクションで、**名前** や **説明 (任意)** などのタスクに関する基本情報を入力します。 **タグを選択** をクリックして、[タグを割り当て](#) ます。

タスク ドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク** があらかじめ選択されます。**タスク** ([すべてのタスク](#) の一覧を参照) は、タスクの設定と動作を定義します。

設定

診断アクション

- **Log Collector の実行** - 特定のデータ (設定とログ) を選択したコンピューターから収集し、サポートケースの解決中に顧客のコンピューターからの情報の収集を容易にします。

Log Collector パラメーター - [Windows](#)、[MacOS](#)、[Linux](#) で Log Collector パラメーターを指定できます。すべての使用可能なデータを収集するには、**Log Collector パラメーター** フィールドを空欄にします。Log Collector パラメーターを指定する場合は、該当するオペレーティングシステムを搭載しているコンピューターのみをタスクのターゲットとして選択します。

デバイスごとのログ配信のファイルサイズ上限は200MBです。Webコンソールの詳細を表示 > ログセクションからログにアクセスできます。タスクによって収集されたログが200 MBより大きい場合は、タスクが失敗します。タスクが失敗した場合は次の処理を実行できます。

- デバイスでローカルにログを収集します。
- ログの詳細レベルを変更し、タスクを再試行します。

Windowsターゲットの場合、/Targets:EraAgLogsパラメーターを使用してESET Managementエージェントログのみを収集します。

Linux/macOSターゲットの場合、--no-productlogsパラメーターを使用して、インストールされたESETセキュリティ製品からログを除外します。

- **診断モードの設定** - 診断モードには次のカテゴリがあります。**迷惑メール ログ** **ファイアウォール ログ** **HIPS ログ** **デバイス コントロール ログ** および **Web コントロール ログ**。診断モードの主な目的は、トラブルシューティングが必要なときにすべてのレベルのログを収集することです。

オン - すべてのESETアプリケーションのログをオンにします。

オフ - 手動でログをオフにできます。あるいは、コンピューターの再起動後にログが自動的にオフになります。

診断ログを正常に作成するには、次の前提条件が必要です。

- 診断モードログは、WindowsおよびmacOSオペレーティングシステムを実行するクライアントコンピューターから収集できます。
- クライアントコンピューターにはESETセキュリティ製品をインストールして、アクティベーションする必要があります。

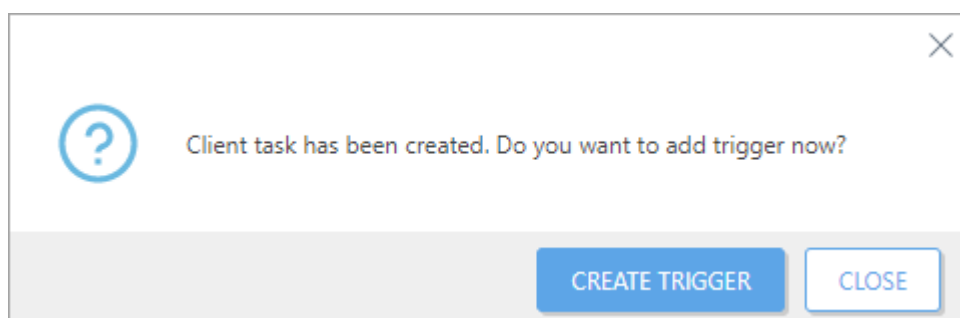
ESET Managementエージェントは、クライアントコンピューターにインストールされたESET製品によって収集されたログのみを送信します。ログカテゴリと詳細レベルは、製品タイプと設定によって異なります。各製品を(ポリシー経由)で設定し、特定のログを収集します。

24時間を経過した診断ログは夜間のクリーンアップ中に毎日削除されます。これによりESET PROTECTデータベースが過負荷から保護されます。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成 (推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から**トリガー**を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)[②](#)[ステータスアイコン](#)、および[詳細](#)が表示されます。

コンピューター詳細では、作成されたログを確認できます:[ログ](#) > [診断ログ](#)[②](#)

メッセージの表示

メッセージの表示タスクでは、メッセージを任意の管理対象デバイス(クライアントコンピューター、タブレット、モバイルなど)に送信できます。メッセージは画面表示としてユーザーに通知されます。

- Windows - メッセージは通知として表示されます。



Windowsでは、メッセージの表示クライアントタスクは、WindowsProfessional/Enterpriseエディションでのみ表示されるmsg.exeコマンドを使用します。結果として、このタスクを使用するとWindows Home版のクライアントコンピューターでは、メッセージを表示できません。

- macOSおよびLinux - メッセージは端末にのみ表示されます。



macOSまたはLinuxでメッセージを表示するには、まず、端末を開く必要があります。

タスクを作成するには、[タスク](#) > [新規](#) > [+ クライアントタスク](#)をクリックするか、[コンピューター](#)で目的のクライアント デバイスをクリックし、[新しいタスク](#)を選択します。

基本

基本セクションで、[名前](#)や[説明\(任意\)](#)などのタスクに関する基本情報を入力します。 [タグを選択](#)をクリックして、[タグを割り当て](#)ます。


[タスク](#)ドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、[タスク](#)があらかじめ選択されます。[タスク\(すべてのタスク\)](#)の一覧を参照)は、タスクの設定と動作を定義します。

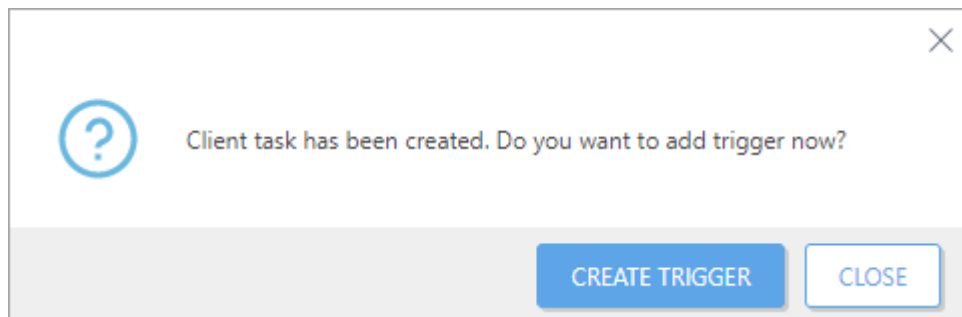
設定

タイトルとメッセージを入力できます。

概要

構成された設定の概要を確認し、[終了](#)をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- [\[トリガーの作成\(推奨\)\]](#)をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- [閉じる](#)をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから [実行](#)を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

ネットワークからのコンピューターの隔離を終了

ネットワークからのコンピューターの隔離を終了タスクは[ネットワークからのコンピューターの隔離](#)を終了し、隔離されたコンピューターの再接続を許可します。セキュリティの問題が解決されたときのみ、このタスクを使用してください。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本


基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

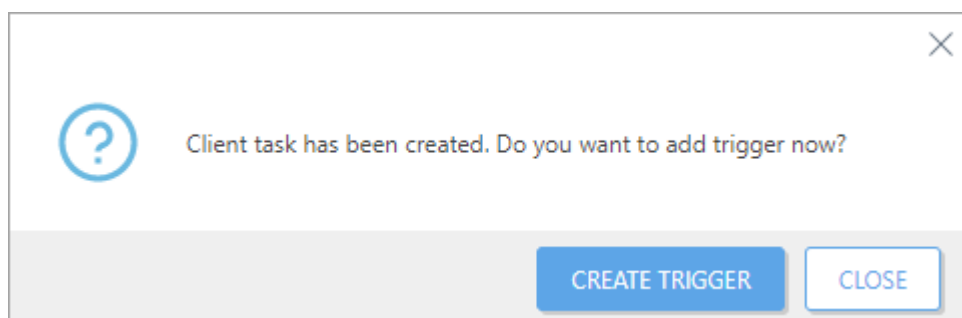
タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

i このタスクの設定はありません。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- [トリガーの作成](#) (推奨)]をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

ESETアプリケーション設定のエクスポート

ESETアプリケーション設定のエクスポートタスクは、クライアントにインストールされている個別のESET PROTECTコンポーネントまたはESETセキュリティ製品の設定をエクスポートするために使用されます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明 (任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

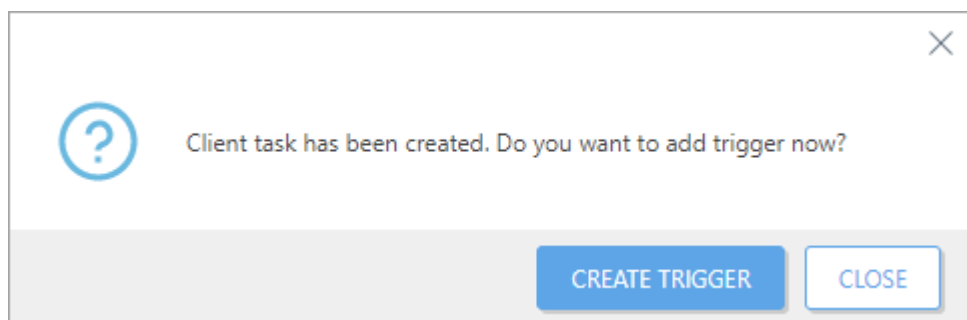
管理製品構成設定をエクスポート。

- **製品** – 設定をエクスポートするESET PROTECTコンポーネントまたはクライアントESETセキュリティ製品を選択します。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成 (推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から**トリガー**を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

タスクが完了したら、ターゲットコンピューターの[コンピューター詳細](#)の下**設定**タブで、エクスポートされた設定を確認できます。

コンピューターをネットワークから隔離する

ネットワークからコンピューターを隔離タスクでは、選択したコンピューターがネットワークから隔離されESET製品の正常な動作のために必要な接続を除くすべての接続がブロックされます。許可された接続は次のとおりです。

- コンピューターがIPアドレスを取得する
- *ekrn.exe*ESET ManagementエージェントESET Enterprise Inspectorエージェントの通信
- ドメインへのログイン

ネットワーク隔離は、ESETセキュリティ製品(EndpointAntivirus/Securityおよびサーバーセキュリティ製品)バージョン7.2以降とのみ互換性があります。

! ネットワーク隔離は、コンピューターの正常な動作を妨害する可能性が高いため、緊急時にのみ使用してください(例: 管理されたコンピューターで重大なセキュリティの問題が特定された場合)。[クライアントタスク](#)を使用すると、隔離を終了できます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

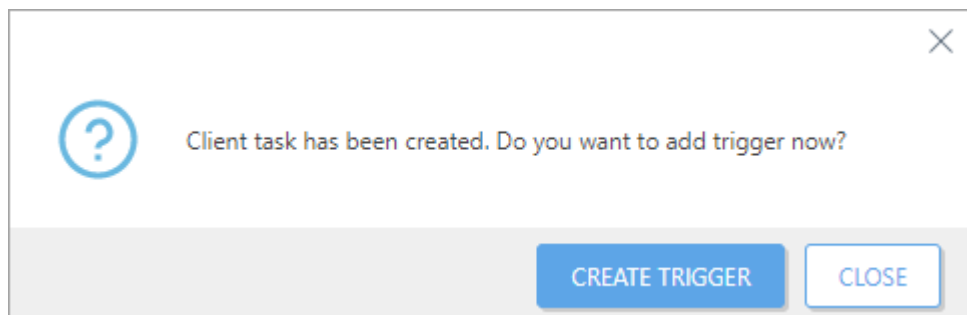
タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

i このタスクの**設定**はありません。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示

されます。

モジュールアップデート

モジュールアップデートタスクは、ターゲットデバイスにインストールされているセキュリティ製品のすべてのモジュールのアップデートを強制的に実行します。これは、すべてのシステムのすべてのセキュリティ製品を対象とした汎用タスクです。セキュリティ製品のバージョン情報セクションに、対象セキュリティ製品のすべてのモジュールが一覧表示されます。

タスクを作成するには、タスク > 新規 > **+** クライアントタスクをクリックするか、コンピューターで目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク(すべてのタスク)**の一覧を参照)は、タスクの設定と動作を定義します。

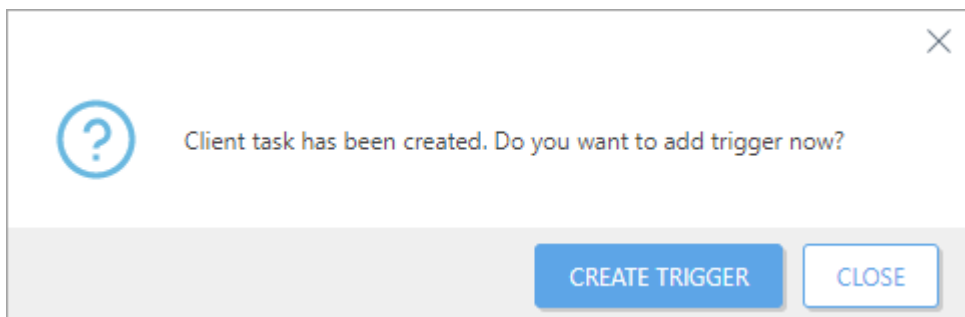
設定

- **アップデートキャッシュをクリアする** - このオプションを使用すると、クライアントのキャッシュにある一時更新ファイルを削除します。多くの場合、モジュールアップデートエラーを修復するために使用できます。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から**トリガー**を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの**進行状況インジケータバー**、**ステータスアイコン**、および**詳細**が表示されます。

モジュールアップデートのカスタムサーバーを設定

ジオブロックのためESETセキュリティ製品でモジュールアップデートが失敗した場合は、ポリシーを使用して、モジュールアップデートのカスタムサーバーを設定します。

1. ESETセキュリティ製品ポリシー設定で、**アップデート>プロファイル>アップデート**を選択します。
- i 2. モジュールアップデートで、**自動的に選択**をオフにし、**カスタムサーバーアドレス**を入力します。たとえばESET Endpoint Antivirus/Security 9 for Windowsで米国のアップデートサーバーを使用するには、http://us-update.eset.com/eset_upd/ep9/ (バージョン8: http://us-update.eset.com/eset_upd/ep8/) と入力します。
3. ユーザー名(EAV-XXXXXXX)とライセンスパスワードを入力します。[レガシーライセンス詳細](#)から取得できます。

モジュールアップデートロールバック

モジュールアップデートが問題を引き起こしたり、一部のクライアントには更新を適用しない場合(テストの場合やリリース前更新のテストなど)、**モジュールアップデートロールバック**タスクを使用できます。このタスクを適用すると、モジュールが前のバージョンにリセットされます。

タスクを作成するには、**タスク>新規>+ クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。


タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク(すべてのタスク)**の一覧を参照)は、タスクの設定と動作を定義します。

設定

このセクションを展開し、モジュールアップデートロールバック設定をカスタマイズします。

操作

- **アップデートを有効にする** – アップデートが有効で、クライアントは次のモジュールアップデートを受信します。
- **ロールバックして次の更新を無効にする** – 更新は、**[無効期間]**ドロップダウンメニューで指定した期間(24/36/48時間)または取り消されるまで無効です。

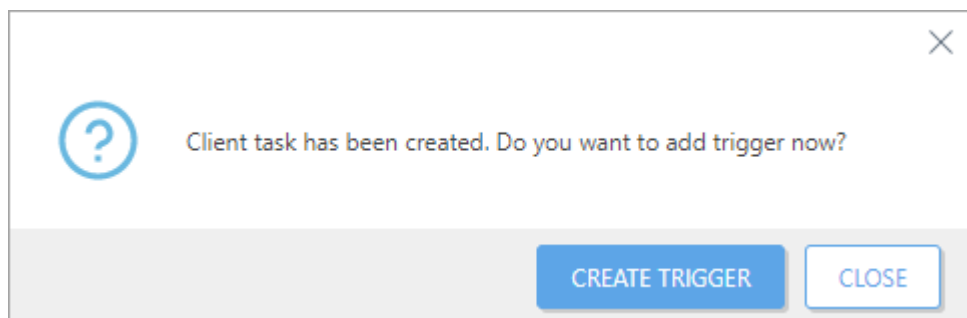
 **取り消されるまでオプションを使用すると、セキュリティリスクにつながるため注意してください。**

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。

- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

オンデマンド検査

オンデマンド検査タスクでは、定期的なスケジュール検査とは別に、クライアントコンピューターの検査を手動で実行できます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

検査後にコンピューターをシャットダウン - このチェックボックスをオンにすると、検査の完了後にコンピューターがシャットダウンします。

検査プロファイル

ドロップダウンメニューからプロファイルを選択できます。

- **詳細検査** - これはクライアントの定義済みプロファイルです。最も徹底的な検査プロファイルとして構成され、システム全体を確認します。ただし、最も時間とリソースが必要になります。
- **スマート検査** - スマート検査を使用すると、コンピューターの検査をすぐに開始して、ユーザーが操作しなくても感染しているファイルからウイルスを駆除できます。スマート検査の利点は、操作が簡単で、詳細な検査設定を必要としないことにあります。スマート検査では、ローカルドライブにあるすべてのファイルが検査されます。検出されたマルウェアがあれば、自動的に駆除または削除されます。駆除のレベルは自動的に既定値に設定されます。
- **コンテキストメニューから検査** - 定義済み検査プロファイルを使用してクライアントを検査します。検査対象をカスタマイズできます。

- **カスタム検査** – スキャン対象やスキャン方法などのスキャンパラメータを指定できます。カスタム検査の利点は、パラメータを詳細に設定できることです。設定はユーザー定義の検査プロファイルに保存できます。これは、簡単に同じパラメータで検査を繰り返し実行できます。カスタムプロファイルオプションでタスクを実行する前に、[プロファイルを作成する必要があります](#)。ドロップダウンメニューからカスタムプロファイルを選択すると、**カスタムプロファイル**フィールドに正確なプロファイル名を入力します。

駆除

既定では、**[検査して駆除]**が選択されます。この設定は、検出された感染オブジェクトの自動駆除を有効にします。これができない場合、オブジェクトは隔離されます。

検査対象

すべてのターゲットの**検査**オプションは、既定では選択されています。この設定を使用すると、検査プロファイルで指定されたすべての対象が検査されます。このオプションの選択を解除する場合は、**[対象の追加]**フィールドで検査対象を手動で指定する必要があります。検査対象をテキストフィールド入力し、**[追加]**をクリックします。対象は以下の**[検査対象]**フィールドに表示されます。検査対象はファイル、場所を指定できます。あるいは、次の文字列のいずれかを**検査対象**として使用して定義済みの検査を実行できます。

検査対象	検査した場所
\${DriveRemovable}	すべてのリムーバブルドライブとデバイス。
\${DriveRemovableBoot}	すべてのリムーバブルドライブのブートセクター。
\${DriveFixed}	ハードドライブ(HDDとSSD)。
\${DriveFixedBoot}	ハードドライブのブートセクター。
\${DriveRemote}	ネットワークドライブ。
\${DriveAll}	すべての使用可能なドライブ。
\${DriveAllBoot}	すべてのドライブのブートセクターとUEFI 用語集 のUEFIスキャナーの詳細をお読みください。
\${DriveSystem}	システムドライブ。
\${Share}	共有ドライブ(サーバー製品のみ)。
\${Boot}	メインブートセクター。
\${Memory}	システムメモリ。
\${Registry}	システムレジストリ(ESET Endpoint 8以降のみ)。
\${Wmi}	WMIデータベース(ESET Endpoint 8以降のみ)。

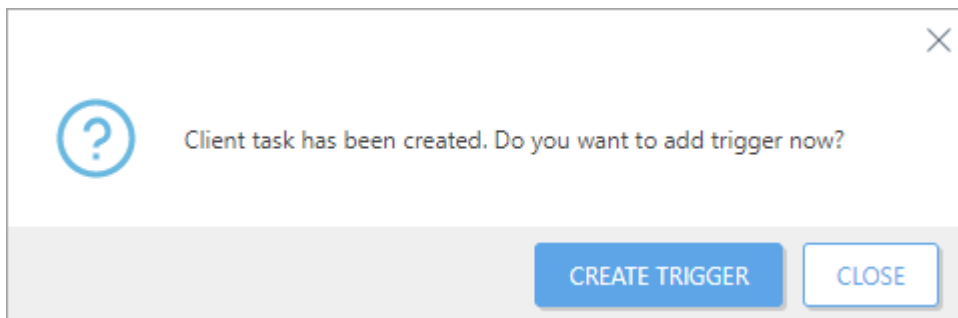
以下に、**オンデマンド検査**対象パラメーターを使用する方法の例を示します。

- ファイル: `C:\Users\Data.dat`
- フォルダー `C:\MyFolder`
- Unixパスまたはファイル `/usr/data`
- Windows UNCロケーション `\\server1\scan_folder`
- 事前定義文字列 `${Memory}`

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- [\[トリガーの作成\]](#) (推奨)] をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から [トリガー](#) を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行** を選択します。



タスクには、作成した各タスクの [進行状況インジケータバー](#)、[ステータスアイコン](#)、および [詳細](#) が表示されます。

オペレーティングシステムアップデート

オペレーティングシステムアップデートタスクを使用すると、クライアントコンピューターのオペレーティングシステムを更新できます。このタスクによって [Windows](#)、[macOS](#)、[Linux](#) オペレーティングシステムで更新が実行されます。

- **macOS** - タスクは次のコマンドを使用してすべてのアップデートをインストールします。

```
/usr/sbin/softwareupdate --install --all
```

- **Linux** - タスクはすべての更新をインストールします。さまざまなパッケージマネージャーを確認し、ほとんどの配布に対応します。
- **Windows** - OS アップデートをインストールします [Windows](#) を新しいバージョンにアップグレードする機能アップデートはインストールされません。

タスクを作成するには、**タスク > 新規 > + クライアントタスク** をクリックするか、**コンピューター** で目的のクライアント デバイスをクリックし、**新しいタスク** を選択します。

基本

基本 セクションで、**名前** や **説明 (任意)** などのタスクに関する基本情報を入力します。 **タグを選択** をクリックして、[タグを割り当て](#) ます。

タスク ドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク** があらかじめ選択されます。**タスク** ([すべてのタスク](#) の一覧を参照) は、タスクの設定と動作を定義します。

設定

- **EULA に自動的に同意 (Windows のみ)** - 自動的に EULA に同意する場合は、このチェックボックスを選択します。ユーザーにテキストは表示されません [EULA](#) の同意を有効にしない場合は、タスク

はEULAの同意が必要なタスクをスキップします。

- **任意のアップデートをインストール (Windowsのみ)** - 任意に設定されたアップデートもインストールされます。
- **再起動を許可する (WindowsおよびmacOS)** - 再起動が必要なアップデートがインストールされたら、クライアントコンピューターが強制的に再起動します。

oWindowsは、再起動の4時間前と、再起動の10分前に、計画されている強制再起動についてコンピューターユーザーに通知します。

omacOSは、アップデート後すぐに再起動します。



再起動を許可する チェックボックスを選択しない場合でも、再起動が必要なアップデートがインストールされます。

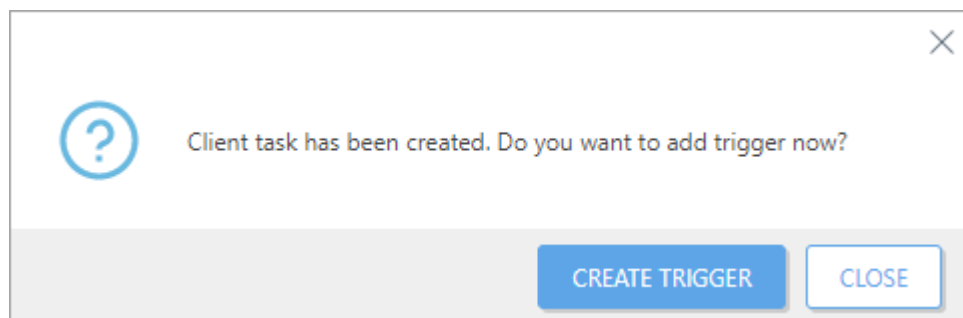


ターゲットデバイスがサポートされていないOSで動作している場合、**設定**はタスクに影響しません。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成 (推奨)]** をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から **トリガー** を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行** を選択します。



タスクには、作成した各タスクの **進行状況インジケータバー**、**ステータスアイコン**、および **詳細** が表示されます。

隔離管理

隔離管理 タスクを使用して、検査中に ESET PROTECT サーバー隔離内で検出された感染したオブジェクトまたは疑わしいオブジェクトを管理します。

タスクを作成するには、**タスク > 新規 > + クライアントタスク** をクリックするか、**コンピューター** で目的のクライアント デバイスをクリックし、**新しいタスク** を選択します。

基本

基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

隔離管理設定

アクション-隔離内のオブジェクトで実行するアクションを選択します。

- **オブジェクトを復元**(オブジェクトを元の場所に復元しますが、検査されます。隔離の理由が存在する場合は、オブジェクトはもう一度隔離されます)
- **オブジェクトを復元し、今後は除外する**(オブジェクトを元の場所に復元し、今後隔離されません)
- **オブジェクトの削除** - オブジェクトを完全に削除します。


フィルタの種類-以下に定義した条件に基づいて隔離内のオブジェクトをフィルタにかけます。

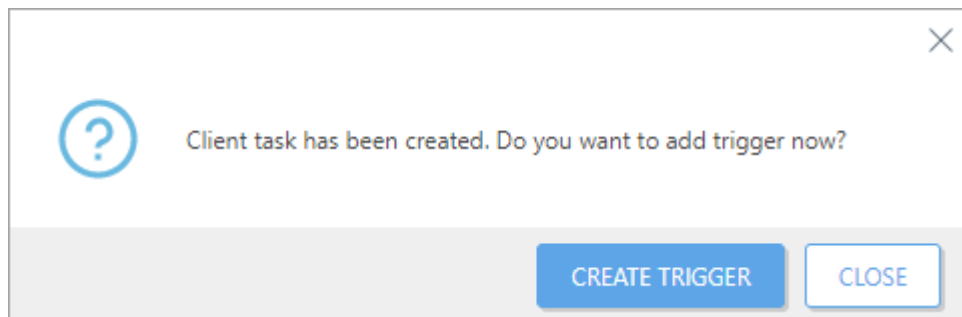
フィルタ設定:

- **ハッシュ項目** - フィールドにハッシュ値を追加します。例えば、すでに隔離されたオブジェクトなど、既知のオブジェクトのみを入力できます。
- **発生 > 発生元 & 発生先** - オブジェクトが隔離された場合、時間範囲を定義します。
- **サイズ > 最小/最大サイズ(バイト)**-隔離オブジェクトのサイズ範囲(バイトで)を定義します。
- **検出名**-隔離項目リストから検出を選択します。
- **オブジェクト名**-隔離項目リストからオブジェクトを選択します。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- **[[トリガーの作成](#) (推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

製品のアクティベーション

製品のアクティベーションタスクを使用して、クライアントコンピューターまたはモバイルデバイスでESETセキュリティ製品をアクティベーションします。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明 (任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

製品アクティベーション設定 - リストからクライアントのライセンスを選択します。このライセンスは、クライアントに既にインストールされた製品に適用されます。ライセンスが一覧表示されない場合は、**詳細 > ライセンス管理**に移動し、[ライセンスを追加](#)します。


製品のアクティベーションタスクは、[オフラインライセンス](#)を使用して、モバイル製品®ESET Endpoint For Androidをアクティベーションできます。

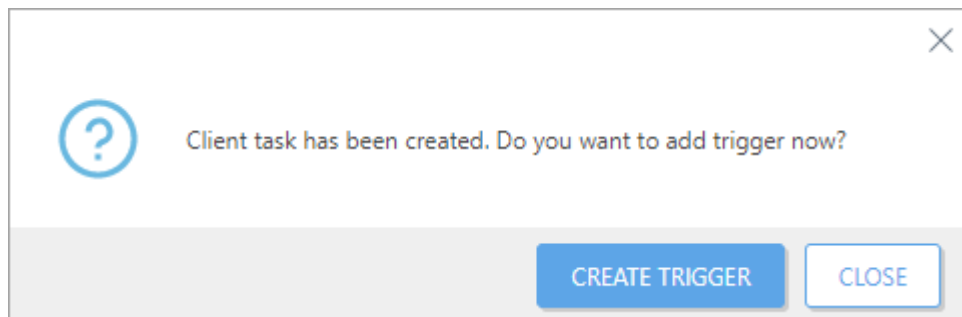


アクティベーションタスクでは、オフラインライセンスを使用して、バージョン4および5のESET製品をアクティベーションすることはできません。製品を手動でアクティベーションするか、サポートされている製品バージョンを使用する必要があります(最新バージョンを使用することをお勧めします)。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[[トリガーの作成](#) (推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

クローンされたエージェントのリセット

[ナレッジベース記事](#)に従い、定義済みイメージによってネットワークのESET Managementエージェントを配布できます。クローンされたエージェントには同じSIDがあり、問題の原因となることがあります(同じSIDを持つ複数のエージェント)。これを解決するためには、[クローンされたエージェントのリセット](#)タスクを使用してSIDをリセットし、一意に識別できるようにエージェントを割り当てます。

ESET Managementエージェントは、複製されたエージェントのリセットタスクを使用せずにWindowsで実行中の複製されたクライアントコンピューターを自動的に特定しますLinuxおよびmacOSのクライアントコンピューター(および[ハードウェア検出](#)が無効であるWindowsクライアント)のみで、複製されたコンピューターを分割するためにタスクが必要です。

タスクを作成するには、**タスク > 新規 > クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

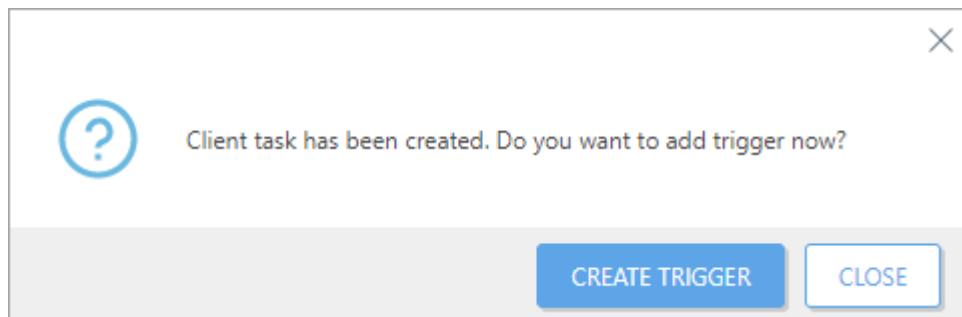
⚠ 注意してタスクを実行します。現在のESET Managementエージェントをリセットした後は、エージェントで実行中のすべてのタスクは破棄されます。

i このタスクの**設定**はありません。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

Rogue Detection Sensorデータベースリセット

Rogue Detection Sensorデータベースリセットタスクは、RD Sensor検索キャッシュをリセットするために使用されます。このタスクによって、キャッシュが削除され、検索結果がもう一度保存されます。検出されたコンピューターは削除されません。検出されたコンピューターがまだキャッシュにあり、サーバーに報告されていない場合に便利です。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

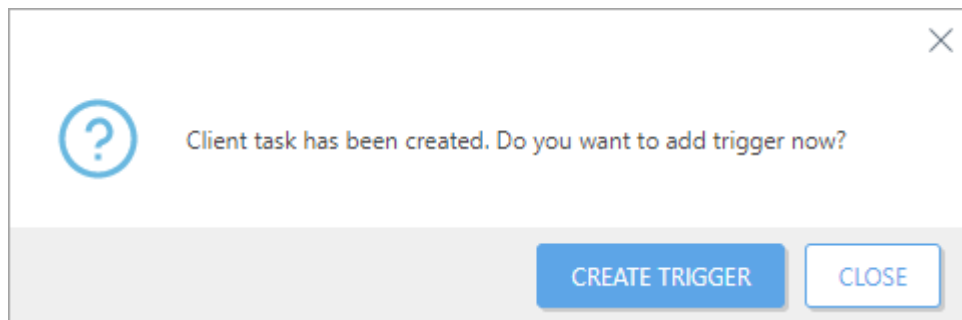
i このタスクの**設定**はありません。

このタスクのトリガーを作成するときには、**RD Sensor**がインストールされているコンピューターを対象にします。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[[トリガーの作成](#)(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

コマンドの実行

コマンドの実行タスクを使用すると、クライアントの特定のコマンドライン命令を実行できます。管理者は実行するコマンドライン入力を指定できます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

! コマンドはデスクトップ環境にアクセスせずに実行されます。結果として、アプリケーションのGUIに必要なコマンド実行はこのために失敗する場合があります。

コマンドの実行タスクでは、ecmd コマンドを使用できます。詳細については、次の[ナレッジベース記事](#)をご覧ください。

OS	コマンドはユーザーとして実行されます	既定の作業ディレクトリ	アクセス可能なネットワークロケーション	コマンドは次の場所で実行されます
Windows	Local System	C:\Windows\Temp	現在のドメインとローカルシステムユーザーが使用できる場所のみ	コマンドプロンプト (cmd.exe)
LinuxとMac OS	root	/tmp	場所がマウントされ、ルートユーザーが使用できる場合のみ	コンソール

基本

基本セクションで、**名前や説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

- **実行するコマンドライン** - クライアントで実行するコマンドラインを入力します。
- **作業ディレクトリ** - 上記のコマンドラインを実行するディレクトリを入力します。

複数行コマンドを入力できます。

最大コマンド長に関する制限:



- Webコンソールは最大32,768文字を処理できます。これよりも長いコマンドをコピーして貼り付けると、最後の部分が切り捨てられます。ユーザーへの確認はありません。
- LinuxおよびMacはコマンドの全長を処理できます。Windowsには、最大8,191文字の制限があります(詳細については、[こちら](#)をお読みください)。

• C:\Users\user\script.batでクライアントにあるローカルスクリプトを実行するには、次の手順に従います。

1.新しいクライアントタスクを作成し、[コマンドの実行]を選択します。

2.[設定]セクションで次の項目を入力します。

実行するコマンドライン: call script.bat



作業ディレクトリ: C:\Users\user

3.[完了]をクリックし、トリガーを作成して、ターゲットクライアントを選択します。

- 複数行コマンドを実行してWindowsサービスをリモートで再起動するには(Windows Updateサービスのwuauexecなどのサービス名でservice_nameを置換します):

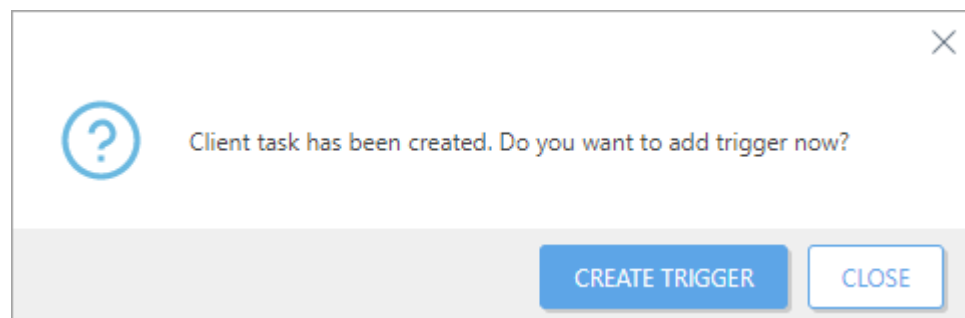
```
net stop service_name
```

```
net start service_name
```

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- [\[トリガーの作成\]](#)(推奨)]をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

SysInspectorスクリプトの実行

SysInspectorスクリプトの実行タスクを使用すると、システムから不要なオブジェクトを削除します。このタスクを実行する前に、SysInspectorスクリプトをESET SysInspectorからエクスポートする必要があります。スクリプトをエクスポートした後は、削除するオブジェクトを選択し、修正されたデータでスクリプトを実行できます。設定されたオブジェクトが削除されます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

i タスクが完了したら、レポートの結果を確認できます。

基本

基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

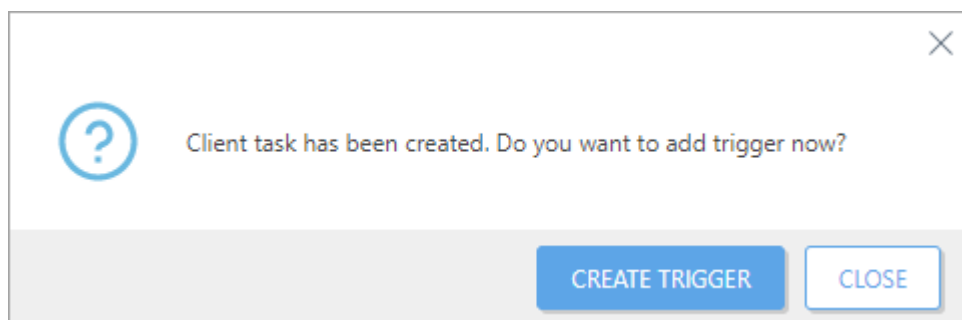
設定

- **SysInspector スクリプト** - [参照]をクリックすると、サービススクリプトに移動します。このタスクを実行する前に、このサービススクリプトを作成する必要があります。
- **アクション** ESET PROTECT コンソールからスクリプトを**アップロード**または**ダウンロード**できます。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から**トリガー**を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

ESET PROTECT コンポーネントのアップグレード

ESET PROTECT コンポーネントアップグレードタスクは、ESET PROTECT コンポーネント(ESET Management エージェント、ESET PROTECT サーバ、Web コンソール、MDM、Apache Tomcat および Apache HTTP Proxy は対象外)をアップグレードするために使用されます。アップグレードタスクは、ESET Management 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でのみ実行できます。エージェントは ESET PROTECT サーバでも必要です。

ESET PROTECT9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。

- ❗ ESET PROTECTバージョン7.0以降からのみ9.0 ESMCにアップグレードできます。詳細な手順については、[インストールガイド](#)を参照してください。
[ESET PROTECTを最新バージョンにアップグレード](#)する他の方法も参照してください。

インストールエラーを防止するためESET PROTECTは、ESET製品のインストールまたはアップグレード前に、次のチェックを実行します。

- リポジトリにアクセスできるかどうか
- クライアントコンピューターで十分な空き領域(1 GB)があるかどうか(Linuxでは使用できません)

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明 (任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

[**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。詳細については、[ESET製品のエンドユーザーライセンス契約\(EULA\)と利用規約、およびプライバシーポリシー](#)を参照してください。

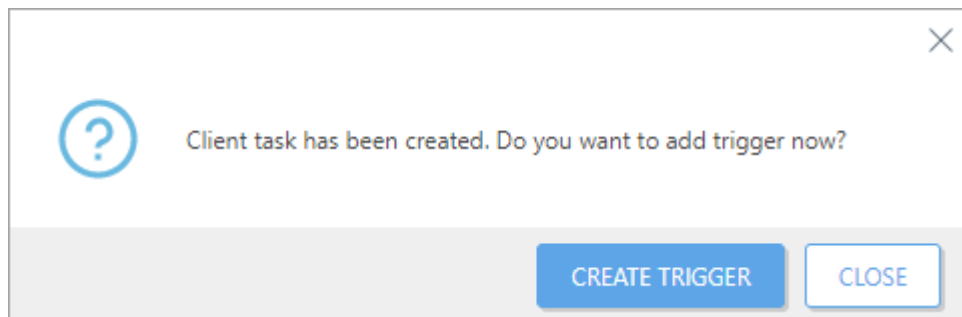
- **ESET PROTECTサーバーの参照** – リストからESET PROTECTサーバーバージョンを選択します。すべてのESET PROTECTコンポーネントは、選択したサーバーと互換性があるバージョンにアップグレードされます。

[**必要なときに自動的に再起動**]の横のチェックボックスを選択し、インストール後にクライアントコンピュータを強制的に自動再起動します。あるいは、このオプションをオフにし、クライアントコンピュータを手動で再起動できます。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- [**トリガーの作成** (推奨)]をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

EDTDにファイルを送信

このタスクを実行するには、[検出](#)に移動します。

✉**EDTDにファイルを送信**は、🔒[ブロックされたファイル](#)でのみ使用できます。ESET Dynamic Threat Defense Webコンソールからマルウェア分析のファイル([ESET PROTECT](#))を送信できます。[提出されたファイル](#)では、ファイル分析の詳細を確認できます。ESET Dynamic Threat Defenseで分析のために手動で他の実行ファイルを送信する場合は、ESETエンドポイント製品から実行できます(ESET Dynamic Threat Defense ライセンスが必要です)。

サーバー検査

サーバー検査タスクを使用してESETサーバーソリューションがインストールされているクライアントを検査できます。検査実行のタイプはインストールされているESETソリューションによって異なります。

製品	検査	説明
ESET Server Security for Windows (旧称ESET File Security for Microsoft Windows Server)	Hyper-V 検査	このタイプの検査では、 Microsoft Hyper-V Server のディスクを検査できます。これはVMにESET Managementエージェントをインストールしない仮想マシン(VM)です。
ESET Security for Microsoft SharePoint Server	SharePointデータベース検査、Hyper-V 検査	この機能では、ESET Securityがあるサーバーで サーバー検査 クライアントタスクを実行するときにESET PROTECT for Microsoft SharePointが適切な検査対象を使用できます。
ESET Mail Security for Microsoft Exchange Server	オンデマンドメールボックスデータベース検査、Hyper-V 検査	この機能ではESET PROTECTが適切な検査対象を使用できます。ESET PROTECTが サーバー検査 クライアントタスクを実行するときには、対象のリストを収集します。その特定のサーバーでオンデマンドメールボックスデータベース検査の検査対象を選択するように指示されます。
ESET Mail Security for IBM Domino	オンデマンドデータベース検査、Hyper-V 検査	この機能では、ESET Mail Securityがあるサーバーで サーバー検査 クライアントタスクを実行するときにESET PROTECT for IBM Dominoが適切な検査対象を使用できます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

- **検査されたサーバー**の下で**選択**をクリックし、バージョン6以降のサーバーセキュリティ製品がインストールされているコンピューターを選択します。そのコンピューターで検査する特定のドライブ、フォルダー、ファイルを指定する必要があります。
- このタスクの[トリガー](#)を選択し、必要に応じて調整を設定できます。既定では、タスクは即時実行されます。

検査対象

ESETPROTECTは選択したサーバーで使用可能な対象のリストを表示します。このリストを使用するには、ツール>ERA/ESMC検査対象で、**対象リストの生成**を、サーバー製品の[ポリシー](#)で有効にする必要があります。

- **対象リストを生成** - この設定を有効にすると、ESET PROTECT が対象リストを生成できます。
- **アップデート期間[分]** - 初めて対象リストを生成するには、この期間の約半分の時間がかかります。

リストから検査対象を選択します。詳細については、「[ESET PROTECT検査対象](#)」を参照してください。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

コンピューターをシャットダウンする

コンピューターのシャットダウンタスクを使用し、クライアントコンピューターをシャットダウンまたは再起動できます。

タスクを作成するには、**タスク>新規>+** クライアントタスクをクリックするか、コンピューターで目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

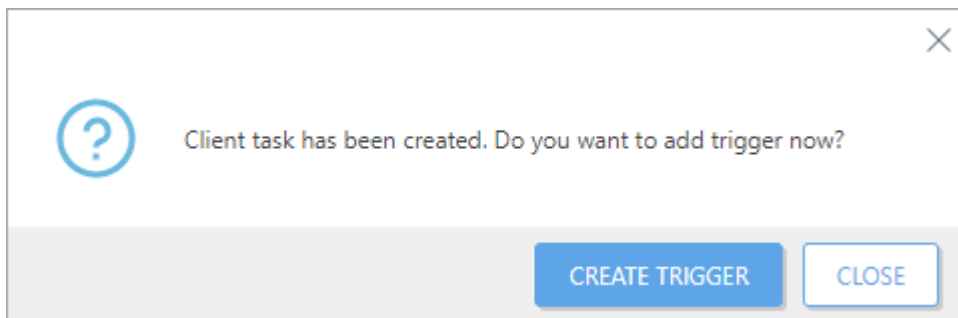
設定

- **コンピューターの再起動** – タスク完了後にクライアントコンピューターを再起動する場合は、このチェックボックスを選択します。コンピューターをシャットダウンする場合は、オフにします。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- [\[トリガーの作成\]](#) (推奨) をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から [トリガー](#) を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから **実行** を選択します。



タスクには、作成した各タスクの [進行状況インジケータバー](#)、[ステータスアイコン](#)、および [詳細](#) が表示されます。

ソフトウェアインストール

ソフトウェアインストールタスクを使用して、クライアントコンピューターにソフトウェアをインストールします。

- ESETセキュリティ製品のインストール
- ESETセキュリティ製品のアップグレード – 最新のインストーラーパッケージを使用してタスクを実行し、既存のソリューションの上にインストールします。ESET製品のアップグレードは、**ダッシュボード** から [ワンクリック操作](#) ですぐに実行できます。このアップグレードを完了するには、[ESET Security for Microsoft SharePointのアップグレード手順](#) を参照してください。
- [サードパーティソフトウェアをインストールします](#)

リポジトリにアクセスしてインストールを実行するにはESET PROTECTサーバーもESET Management エージェントもインターネットにアクセスする必要があります。インターネットに接続していない場合は、クライアントソフトウェアをローカルでインストールする必要があります。リモートインストールが失敗するためです。 インストールエラーを防止するためESET PROTECTは、ESET 製品のインストールまたはアップグレード前に、次のチェックを実行します。

- リポジトリにアクセスできるかどうか
- クライアントコンピューターで十分な空き領域(1 GB)があるかどうか(Linuxでは使用できません)

ESET Management エージェントが実行中のドメインのコンピューターでソフトウェアインストールタスクを実行するときには、ユーザーはインストーラーがあるフォルダーの読み取り権限が必要です。必要に応じて、次の手順に従って権限を付与します。



- 1.タスクを実行するコンピューターでActive Directoryコンピューターアカウントを追加します(たとえば `NewComputer$`)
- 2.インストーラーがあるフォルダーを右クリックし、コンテキストメニューから**プロパティ** > **共有** > **共有**を選択し、`NewComputer$`に**読み取り**権限を付与します。`$`記号は、コンピューター名文字列の最後に必要です。
共有ロケーションからのインストールは、クライアントコンピューターがドメインにある場合にのみ可能です。
ソフトウェアインストールタスクを使用してESET PROTECTコンポーネント(エージェント、サーバESET MDM)をアップグレードしないでください。[コンポーネントアップグレードタスク](#)を使用してください。ソフトウェアインストールタスクを使用してRogue Detection Sensorコンポーネントのみをアップグレードできます。

タスクを作成するには、**タスク** > **新規** > **クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明**(任意)などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

インストールするパッケージ - 2つのオプションがあります。

- **リポジトリからパッケージをインストール** - **パッケージの選択**をクリックし、リポジトリからインストーラーパッケージを選択します。ポップアップウィンドウに、利用可能なESETセキュリティ製品パッケージが一覧表示されます。任意のインストーラーパッケージ(ESET Endpoint Securityなど)を選択し、**OK**をクリックしますESET製品をアップグレードするには、リポジトリから最新バージョンを選択します。
- **直接パッケージURLでインストール** - インストールパッケージとURLを指定するにはURLを入力するか、コピーしてテキストフィールドに貼り付けます(認証が必要なURLは使用しない)。

`ohttp://server_address/ees_nt64_ENU.msi` - 公開Webサーバーまたは独自のHTTPサーバーからインストールしている場合。

`ofile://\\pc22\install\ees_nt64_ENU.msi` - ネットワークパスからインストールしている場合。

`ofile://C:\installs\ees_nt64_ENU.msi` - ローカルパスからインストールしている場合。

ESETライセンス – 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。

- アクティブではない製品をインストールまたはアップグレードするとき、または現在使用中のライセンスを別のライセンスに変更する場合にのみ、ライセンスを選択します。
- 既にアクティベーションされた製品をアップグレードする場合は、ライセンスを選択しないでください。

ESET Dynamic Threat Defense (EDTD)をアクティベーション - ESET Dynamic Threat Defenseライセンスがあり、[ESET Dynamic Threat Defenseと製品ライセンスに対応するESETセキュリティ製品](#)を選択した場合は、このチェックボックスを使用できます。チェックボックスを選択すると、ソフトウェアインストールタスクのターゲットコンピューターでESET Dynamic Threat Defenseがアクティベーションされます。アクティベーション後、[ポリシー](#)を使用してESET Dynamic Threat Defense設定を管理できます。

[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。詳細については、[ESET製品のエンドユーザーライセンス契約\(EULA\)と利用規約、およびプライバシーポリシー](#)を参照してください。

Windows版のESETセキュリティ製品を選択した場合：**保護設定** – 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。

インストールパラメータ (任意):

- コマンドラインインストールパラメーターは、ユーザーインターフェイス設定の**簡易**と**基本**およびなしで使用します。
- 該当するコマンドラインスイッチで 사용되는 **msiexec** バージョンについては、[マニュアル](#)を参照してください。
- [ESET Endpoint製品](#) および [ESETサーバー製品](#) のコマンドラインインストールについては、それぞれのオンラインヘルプをお読みください。

[**必要なときに自動的に再起動**]の横のチェックボックスを選択し、インストール後にクライアントコンピュータを強制的に自動再起動します。あるいは、このオプションをオフにし、クライアントコンピュータを手動で再起動できます。

[サードパーティソフトウェアのインストール](#)

ソフトウェアのインストールタスクを使用し、非ESET(サードパーティ)ソフトウェアをインストールできます。

OS	サポートされているインストールファイルタイプ	インストールパラメータのサポート
Windows	.msi	ソフトウェアのインストールタスクは、常に、.msiパッケージのサイレントインストールを実行します。 msiexecパラメーターは指定できません。インストールパッケージ自体で使用するパラメーターのみを指定できます(各ソフトウェアインストールパッケージで一意)。

OS	サポートされているインストールファイルタイプ	インストールパラメータのサポート
Linux	<code>.deb</code> , <code>.rpm</code> , <code>.sh</code>	<code>.sh</code> ファイルのみパラメーターを使用できます(<code>.deb</code> および <code>.rpm</code> はパラメーターをサポートしません)。
macOS	<code>.pkg</code> と <code>.dmg</code> (<code>.pkg</code> ファイル)を含む	インストールパラメーターはサポートされていません。
Android	<code>.apk</code>	
iOS	<code>.ipa</code>	

2つのパラメーターの`install_script.sh`ファイルを使用してLinuxにソフトウェアをインストールできます。`-a`は1つ目のパラメーター、`-b`は2番目のパラメーターです。

端末でのインストール(`install_script.sh`があるフォルダーのルートユーザーを使用):

```
./install_script.sh -a parameter_1 -b parameter_2
```

ソフトウェアインストールタスクを使用したインストール:

- **直接パッケージURLでインストール**にファイルパスを入力します。例:

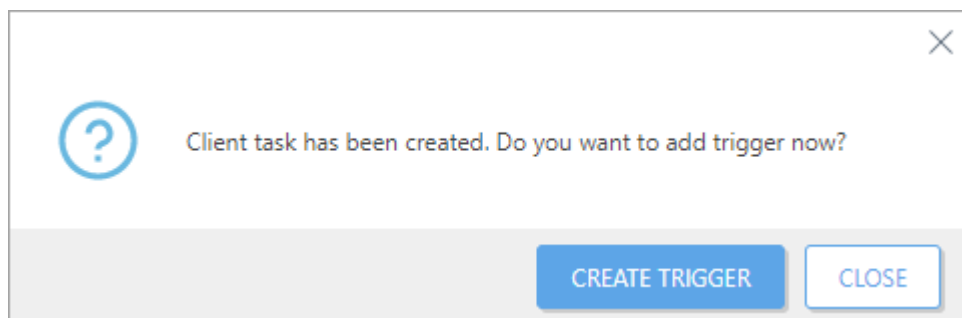
```
file:///home/user/Desktop/install_script.sh
```

- **インストールパラメータ**: `-a parameter_1 -b parameter_2`を入力します。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます:

- [\[トリガーの作成\(推奨\)\]](#)をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

インストールの失敗に関する問題の一覧

- インストールパッケージが見つかりません。
- 新しいバージョンのWindowsインストーラーサービスが必要です。
- 別のバージョンまたは競合する製品が既にインストールされています。
- 別のインストール既に実行中です。そのインストールを完了してから、このインストールを続行してください。

- インストールまたはアンインストールは正常に完了しましたが、コンピュータの再起動が必要です。
- タスクが失敗しました - エラーがあります。[エージェントトレースログ](#)を確認して、インストーラの戻りコードをチェックする必要があります。

Safeticaソフトウェア

Safeticaの概要

[Safetica](#)はサードパーティのソフトウェア会社でありESET技術アライアンスのメンバーです。Safeticaは、データ損失防止ITセキュリティソリューションを提供し、ESETセキュリティ製品を補完します。主要なSafeticaソフトウェア機能:

- データ損失防止 - すべてのハードドライブ、USBドライブ、ネットワークファイル転送、電子メールとプリンター、アプリケーションファイルアクセスの監視
- レポートおよびアクティビティブロック - ファイル操作、Webサイト、電子メール、インスタントメッセージング、アプリケーション使用状況、検索されたキーワード

Safeticaの仕組み

Safeticaはエージェント(Safeticaエンドポイントクライアント)を任意のエンドポイントに展開し、サーバ(Safetica管理サービス)経由で定期的な接続を維持します。このサーバは、ワークステーションアクティビティのデータベースを構築し、新しいデータ保護ポリシーと規制を各ワークステーションに配布します。

ESET PROTECTでのSafetica統合

ESET Managementエージェントは、[コンピューター詳細 > インストールされたアプリケーション](#)でESETソフトウェアとしてSafeticaソフトウェアを検出して報告します。ESET PROTECT Webコンソールは、新しいバージョンが利用可能な場合に、Safeticaエージェントをアップデートします。

Safeticaエージェントの展開

ESETソフトウェアリポジトリからESET PROTECT Webコンソールで直接Safeticaエージェントを展開するには、[ソフトウェアインストールタスク](#)を使用するか、`STSERVER=Server_name`をインストールパラメーター(Server_nameをSafetica Management Serviceがインストールされているサーバのホスト名/IPアドレスです)入力します。

あるいは、[クライアントタスク - コマンドの実行](#)でSafeticaエージェントをインストールできます。

^ [コマンドの実行タスクの使用](#)

```
msiexec /i safetica_agent.msi STSERVER=Server_name
```

コマンドの最後で/silentパラメーターを使用して、リモートで、「サイレント」モードでインストールを実行できます: `msiexec /i safetica_agent.msi STSERVER=Server_name /silent`

上記のインストールでは、`.msi`パッケージがデバイスに既に存在している必要があります。共有された場所で、`.msi`パッケージのインストールを実行するには、次のように、コマンドで場所を指定します。`msiexec /i Z:\sharedLocation\safetica_agent.msi STSERVER=Server_name`

Safeticaエージェントのアップグレード

管理されたコンピューターでSafeticaエージェントをアップグレードするには、[コンピューター詳細 > インストールされているアプリケーション](#)に移動し、**Safeticaエージェント**を選択して、**ESET製品**のアップデートをクリックします。

Safeticaエージェントのアンインストール

管理されたコンピューターでSafeticaエージェントをアンインストールするには、[コンピューター詳細 > インストールされているアプリケーション](#)に移動し、**Safeticaエージェント**を選択して、**アンインストール**をクリックします。

ソフトウェアアンインストール

ソフトウェアアンインストールタスクを使用すると、必要がなくなったESET製品をクライアントからアンインストールできます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、コンピューターで目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

設定

ソフトウェアアンインストール設定

アンインストール - リストのアプリケーション:

- **パッケージ名** - ESET PROTECTコンポーネントまたはクライアントセキュリティ製品またはサードパーティアプリケーションを選択します。選択したクライアントからアンインストールできるすべてのパッケージがこのリストに表示されます。

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。

- エージェントがパスワードで保護されている場合は、アンインストールできません。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。

- **パッケージバージョン** – 特定のバージョンのパッケージを削除(特定のバージョンが問題の原因となることがあります)したり、**すべてのバージョンのパッケージをアンインストール**したりできます。

- **アンインストールパラメーター** – アンインストールのパラメーターを指定できます。

- **[必要ときに自動的に再起動]**の横のチェックボックスを選択し、インストール後にクライアントコンピューターを強制的に自動再起動します。あるいは、このオプションをオフにし、クライアントコンピューターを手動で再起動できます。

アンインストール – 他社製の脅威対策ソフトウェア(OPSWATで構築)

対応するウイルス対策ソフトウェアの一覧については、[ナレッジベース記事](#)を参照してください。この削除は、**プログラムの追加と削除**アンインストールとは異なります。これは別の方法を使用して、常駐レジストリエントリまたは他のトレースを含む他社製のウイルス対策ソフトウェアを徹底的に削除します。

記事「[ESET PROTECTを使用しているクライアントコンピューターからサードパーティのウイルス対策ソフトウェアを削除する](#)」の段階的な手順に従い、クライアントコンピューターからサードパーティのウイルス対策ソフトウェアを削除するタスクを送信してください。

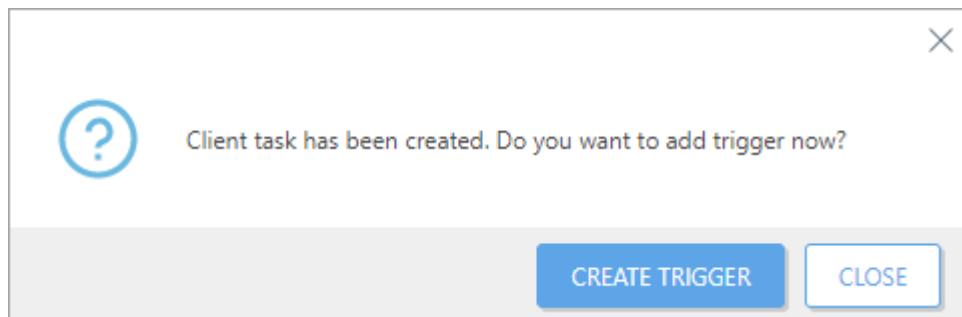
パスワードで保護されたアプリケーションをアンインストールできるようにする場合は、[ナレッジベース記事](#)を参照してください。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- **[トリガーの作成(推奨)]**をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。

- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。



ESETセキュリティ製品のアンインストールタスクは、次のようなパスワード関連エラーで失敗する場合があります。**製品:ESET Endpoint Security -- エラー5004。アンインストールを続行するには有効なパスワードを入力してください。**これはESETセキュリティ製品のパスワード保護設定が有効なためです。[ポリシー](#)をクライアントコンピューターに適用し、パスワード保護を削除します。ソフトウェアのアンインストールタスクを使用してESETセキュリティ製品をアンインストールできます。

管理の停止(ESET Managementエージェントのアンインストール)

このタスクは、選択したターゲットデバイスからESET Managementエージェントをアンインストールします。デスクトップが選択されている場合は、ESET Managementエージェントが削除されます。モバイルデバイスが選択されている場合は、デバイスのMDM登録がキャンセルされます。



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。
- エージェントがパスワードで保護されている場合は、アンインストールできません。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。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本


基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

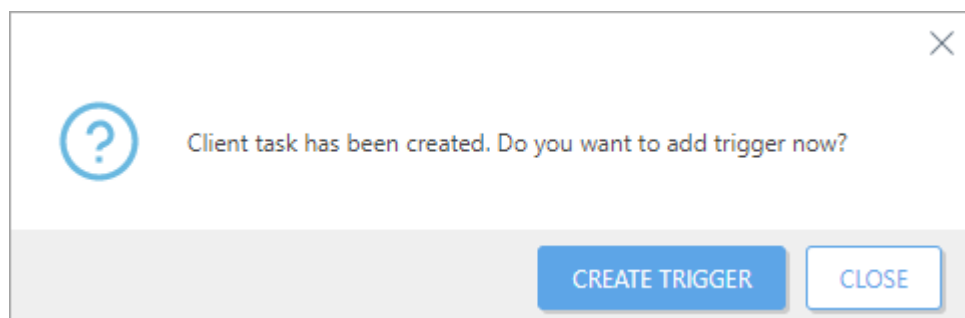
タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

i このタスクの設定はありません。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：


- [\[トリガーの作成\]](#) (推奨) をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から [トリガー](#) を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから  **実行** を選択します。



タスクには、作成した各タスクの [進行状況インジケータバー](#)  [ステータスアイコン](#)、および [詳細](#) が表示されます。

SysInspector ログ要求 (Windows のみ)

SysInspector ログ要求 タスクを使用すると、この機能を備えたクライアントセキュリティ製品から SysInspector ログを要求できます。


タスクを作成するには、**タスク > 新規 >  クライアントタスク** をクリックするか、**コンピューター** で目的のクライアント デバイスをクリックし、**新しいタスク** を選択します。

基本

基本 セクションで、**名前** や **説明 (任意)** などのタスクに関する基本情報を入力します。 **タグを選択** をクリックして、[タグを割り当て](#) ます。

タスク ドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク** があらかじめ選択されます。**タスク** ([すべてのタスク](#) の一覧を参照) は、タスクの設定と動作を定義します。

設定

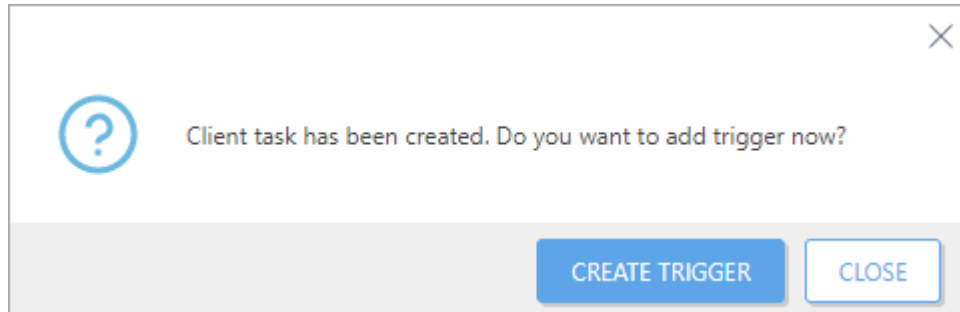
- **クライアントにログを保存** – クライアントと ESET PROTECT サーバーに SysInspector ログを保存する場合は選択します。例えば  ESET Endpoint Security がクライアントにインストールされている場合、通常、ログは `C:\Program Data\ESET\ESET Security\SysInspector\` にあります。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップ

プウィンドウが開きます:

- [\[トリガーの作成\(推奨\)\]](#)をクリックし、クライアントタスクターゲット(コンピューターまたはグループ)とトリガーを指定します。
- **閉じる**をクリックすると、後から[トリガー](#)を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから**実行**を選択します。



タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

隔離ファイルのアップロード

隔離ファイルのアップロードタスクを使用すると、クライアントで隔離されたファイルを管理できます。詳細な調査のため、隔離から特定の場シヨンに隔離されたファイルをアップロードできます。

タスクを作成するには、**タスク > 新規 > + クライアントタスク**をクリックするか、**コンピューター**で目的のクライアント デバイスをクリックし、**新しいタスク**を選択します。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。


設定

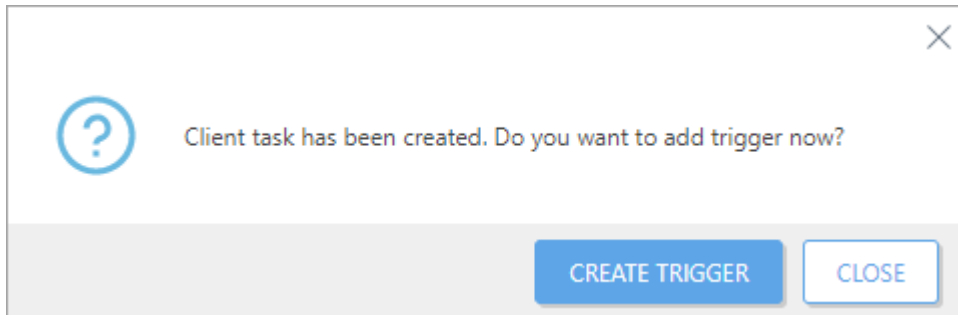
- **隔離されたオブジェクト** - [隔離](#)から特定のオブジェクトを選択します。
- **オブジェクトパスワード** - セキュリティの理由からオブジェクトを暗号化するパスワードを入力します。このパスワードは対応するレポートに表示されます。
- **アップロードパス** - オブジェクトをアップロードする場所へのパスを入力します。次の構文を使用します。 `smb://server/share`
- **アップロードのユーザー名/パスワード** - 認証が必要な場合(ネットワーク共有など)、このパスにアクセスするための認証情報を入力します。ユーザーがドメインにある場合は、形式 `DOMAIN\username` を使用します。

i トリガーで、ファイルが隔離される対象を選択してください。

概要

構成された設定の概要を確認し、**終了**をクリックします。クライアントタスクが作成され、ポップアップウィンドウが開きます：

- [\[トリガーの作成\]](#) (推奨) をクリックし、クライアントタスクターゲット (コンピューターまたはグループ) とトリガーを指定します。
- **閉じる** をクリックすると、後から [トリガー](#) を作成できます。クライアントタスクインスタンスをクリックし、ドロップダウンメニューから  **実行** を選択します。



タスクには、作成した各タスクの [進行状況インジケータバー](#)  [ステータスアイコン](#)、および [詳細](#) が表示されます。



隔離されたファイルが選択した **アップロードパス** の場所にアップロードされた後：

- ファイルはパスワードで保護された **.zip** アーカイブに保存されます。パスワードは **.zip** ファイル名 (隔離されたファイルのハッシュ) です。
- 隔離されたファイルにはファイル拡張子があります。ファイルを復元するには、元のファイル拡張子を追加します。

サーバータスク

サーバータスクは、サーバーまたは他のデバイスで ESET PROTECT サーバーによって実行されます。サーバータスクを、特定のクライアントまたはクライアントグループに割り当てることはできません。各サーバーは1つの [トリガー](#) のみを設定できます。さまざまなイベントでタスクを実行する必要がある場合は、各トリガーに個別のサーバータスクが必要です。

サーバータスクと権限

タスクとトリガーは両方実行ユーザーが必要です。これはタスク (とトリガー) を修正するユーザーです。このユーザーは選択したアクションに対する十分な権限が必要です。実行中、タスクは常にトリガーから実行ユーザーを取得します。**完了後にただちにタスクを実行** 設定を使用してタスクを実行する場合、実行ユーザーは ESET PROTECT Web コンソールにログインしたユーザーです。権限設定 ([詳細 > 権限設定](#)) で選択した権限があり、サーバータスクがある静的グループに対して権限が設定されている場合は、ユーザーは選択した **サーバータスク** インスタンスの権限 ([読み取り](#)  [使用](#)  [書き込み](#)) があります。アクセス権の詳細については、[権限の一覧](#) を参照してください。

JohnのホームグループはJohn's Groupで、Server Task 1:レポートの作成を削除しようとしています。タスクは最初にLarryによって作成されたため、自動的にLarryのホームグループのLarry'sGroupグループに含まれています。Johnがタスクを削除するには、次の条件を満たす必要があります。

- Johnにはサーバータスクとトリガー-レポートの生成の書き込み権限がある権限設定を割り当てる必要があります。
- 権限設定は静的グループの下でLarry's Groupを含む必要があります。

特定のサーバータスクアクションに必要な権限

- 新しいサーバータスクを作成するには、ユーザーは選択したタスクタイプに対する書き込み権限と参照されたオブジェクト(コンピューター、ライセンス、グループ)に対する適切なアクセス権が必要です。
- サーバータスクを修正するには、ユーザーは選択したサーバータスクに対する書き込み権限と参照されたオブジェクト(コンピューター、ライセンス、グループ)に対する適切なアクセス権が必要です。
- サーバータスクを削除するには、ユーザーは選択したサーバータスクインスタンスの書き込み権限が必要です。
- サーバータスクを実行するには、ユーザーは選択したサーバータスクインスタンスの使用権限が必要です。

サーバータスクを新規作成する

1. 新しいサーバータスクを作成するには、タスク > 新規作成 > +サーバータスクをクリックするか、左側で任意のタスクタイプを選択して、新規作成 > +サーバータスクをクリックします。
2. 基本セクションで、名前や説明(任意)などのタスクに関する基本情報を入力します。タグを選択をクリックして、タグを割り当てます。タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、タスクがあらかじめ選択されます。タスク(すべてのタスクの一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- 完了後ただちにタスクを実行 - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- トリガーの設定 - チェックボックスをオンにし、トリガーセクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

3. [設定]セクションでタスク設定を構成します。
4. 必要に応じて、トリガーセクションでトリガーを設定します。
5. サマリーセクションでこのタスクのすべての設定を確認し、[トリガー]をクリックします。

i 定期的にサーバータスクを使用する場合は、他のユーザーと共有するのではなく、独自のタスクを作成することをお勧めします。タスクを実行するたびに、実行ユーザーの権限を使用します。これによって、一部のユーザーは混乱する場合があります。

エージェント展開

エージェント展開サーバータスクは、ESET Managementエージェントのリモート展開を実行します。

i エージェント展開タスクは、ターゲットコンピューターで、1つずつ(順次に)ESET Managementエージェントのインストールを実行します。結果として、多数のクライアントコンピューターでエージェント展開タスクを実行するときには、完了までに時間がかかる場合があります。このため、代わりに[ESET Remote Deployment Tool](#)を使用することをお勧めします。同時に(並列で)すべてのターゲットコンピューターでESET Managementエージェントのインストールを実行し、ローカル保存されたインストーラーファイルを使用することでネットワーク帯域幅を節約します。オンラインリポジトリにはアクセスしません。

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク(すべてのタスク)**の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、**トリガー**セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

エージェント展開設定

ターゲット - これをクリックして、このタスクを受信するクライアントを選択します。

i ターゲットコンピューターが[静的グループ同期](#)タスクによってESET PROTECTに追加された場合は、コンピューター名が完全ドメイン名であることを確認します。これらの名前は展開中にクライアントのアドレスとして使用されます。これらが正しくないと、展開が失敗します。dNSHostName属性を**コンピューターホスト名属性**として、エージェント展開の目的で同期中に使用します。

サーバーホスト名(オプション) - クライアント側とサーバー側で異なる場合は、サーバーホスト名を入力できます。

ターゲットコンピューター資格情報

ユーザー名/パスワード - エージェントのリモートインストールを実行する十分な権限を持つユーザーのユーザー名とパスワード。

証明書設定

ピア証明書:

- **ESET PROTECT証明書** – エージェントインストールのセキュリティ証明書と認証機関。既定の証明書と認証機関を選択するか、カスタム証明書を使用できます。
- **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、エージェントのインストール時に証明書に移動して選択します。詳細については、[証明書](#)の章を参照してください。

証明書パズフレーズ – 証明書のパスワードESET PROTECTサーバーインストール中に入力したパスワード(認証機関を作成した手順)か、カスタム証明書のパスワード。



証明書パズフレーズには、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。

ESET PROTECTサーバーは、オペレーティングシステムに合ったエージェントインストールパッケージを自動的に選択できます:

- **Linux - sudo** コマンドまたは **root** ユーザーを使用するアクセス権をもつユーザーを選択します。rootを使用する場合は、sshサービスがrootとしてのログインを許可する必要があります。
- **Linux** または **macOS** - コンピューターにインストールする場合は、ターゲットコンピューターでSSHデーモンが有効で、ポート22で実行され、ファイアウォールがこの接続をブロックしていないことを確認します。次のコマンド(IPアドレスをESET PROTECTサーバーのIPで置換)を使用してLinuxファイアウォールの例外を追加します。
`iptables -A INPUT -s 10.0.0.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT`
- エージェント展開タスクの失敗を防止するには、[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。

他の設定

クラッシュレポートと匿名のテレメトリデータ(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に送信することに同意しない場合は、**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フにします。チェックボックスがオンの場合、テレメトリデータとクラッシュレポートがESETに送信されます。

トリガー

[トリガー](#) セクションには、タスクを実行するトリガーの情報が 있습니다。各サーバータスクは、トリガーのみを設定できます。各トリガーは1つの**サーバータスク**のみを実行できます。**トリガーの設定が基本**セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 – 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。


概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

トラブルシューティング

エージェント展開タスクが失敗する場合は、[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。

 ESET Management エージェントを再展開するには、現在インストールされているエージェントを絶対に削除しないでください。現在インストールされているエージェントでエージェント展開タスクを実行します。エージェントを削除するときに、新しい展開の後に、新しいエージェントが古いタスクを実行し始めることがあります。

接続していないコンピューターの削除

未接続のコンピューターを削除タスクでは、指定された条件に従い、コンピューターを削除できます。たとえば、クライアントコンピューターの ESET Management エージェントが 30 日間接続していない場合 [ESET PROTECT Web](#) コンソールから削除できます。

[\[コンピューター\]](#) に移動します。 **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。

○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。

○赤(警告) - コンピューターは 14 日以上接続されていません。

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク** をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク** をクリックします。

基本

基本 セクションで、**名前や説明(任意)** などのタスクに関する基本情報を入力します。 **タグを選択** をクリックして、**タグを割り当て** ます。

タスク ドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク** があらかじめ選択されます。 **タスク** ([すべてのタスク](#) の一覧を参照) は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了] をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#) セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

グループ名 - 静的グループを選択するか、新しい静的グループを作成されます。名前は変更されます。

コンピューターが接続していない日数 - コンピューターが削除されるまでの日数を入力します。

ライセンスのアクティベーション解除 – 削除されたコンピューターのライセンスをアクティベーション解除するには、このチェックボックスをオンにします。

管理されていないコンピューターの削除 – このチェックボックスを使用すると、管理されていないコンピューターも削除されます。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報が 있습니다。各サーバータスクは、[トリガー](#)のみを設定できます。各トリガーは1つの**サーバータスク**のみを実行できます。[トリガーの設定](#)が**基本**セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 – 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

レポートの作成

レポートの**生成**タスクは、以前に作成または定義された[レポートテンプレート](#)からレポートを生成します。

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。**タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** – このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** – チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

レポートテンプレート – レポートテンプレートの追加をクリックし、リストからレポートテンプレートを選択します。タスクを作成するユーザーは、グループで利用できるレポートテンプレートのみを表示および選択できます。1つのレポートで複数のレポートテンプレートを選択できます。

[電子メールを送信](#)または[ファイルに保存](#)を選択し、生成されたレポートを取得します。

レポート配信

電子メールを送信

メールメッセージを送受信するには、[サーバー設定](#) > [詳細設定](#)でSMTP設定を構成する必要があります。

- **送信先** – レポート電子メールの受信者の電子メールアドレスを入力します。カンマ(,)を使用して複数のアドレスを区切ります。CCとBCCフィールドを追加することもできます。これらは、メールクライアントのように正確に動作します。

- ESET PROTECTでは、選択したレポートテンプレートに基づいて、電子メールの件名と本文があらかじめ入力されます。**メッセージをカスタマイズ**の下チェックボックスを選択して、**件名とメッセージ**をカスタマイズできます。

o件名 – レポートメッセージの件名。識別できる件名を入力し、受信メッセージを並べ替えられるようにします。これはオプションの設定ですが、空欄にしないことをお勧めします。

oメッセージ – レポートメッセージの本文を定義します。

- **レポートが空の場合にメールを送信** – レポートにデータがない場合でも、レポートを送信する場合は、このオプションを使用します。

[印刷オプションを表示]をクリックすると、次の設定が表示されます。

- **出力形式** – 適切なファイル形式を選択します。 **.pdf**または**.csv**を選択できます。CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します

i CSVを選択すると、レポートの日時値がUTC形式で保存されます。PDFを選択すると、レポートでローカルサーバー時刻が使用されます。

- **出力言語** – メッセージの言語を選択します。既定の言語はESET PROTECT Webコンソールで選択された言語に基づきます。

- **ページサイズ/解像度/用紙の向き/色形式/余白単位/余白** – 印刷環境設定に基づいて、該当するオプションを選択します。これらのオプションは、レポートを印刷する場合にのみ有効です。CSV形式ではなくPDF形式にのみ適用されます。


ファイルに保存

- **相対ファイルパス** – 次のような特定のディレクトリにレポートが生成されます。

oWindowsでは、一般的に、レポート

は `C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports\` にあります。


Linuxでは、一般的に、レポートは /var/opt/eset/RemoteAdministrator/Server/GeneratedReports/ にあります。

 Windowsでは、一部の特殊文字(: ? \)は保存されたファイル名で正しく解釈されません。

- **レポートが空の場合にファイルを保存** – レポートにデータがない場合でも、レポートを送信する場合は、このオプションを使用します。

[印刷オプションを表示]をクリックすると、次の設定が表示されます。

- **出力形式** – 適切なファイル形式を選択します。 `.pdf`または`.csv`を選択できます。CSVはテーブルデータにのみ適していて、; (セミコロン)を区切り文字として使用します。

 CSVを選択すると、レポートの日時値がUTC形式で保存されます。PDFを選択すると、レポートでローカルサーバー時刻が使用されます。

- **出力言語** – メッセージの言語を選択します。既定の言語はESET PROTECT Webコンソールで選択された言語に基づきます。
- **ページサイズ/解像度/用紙の向き/色形式/余白単位/余白** – 印刷環境設定に基づいて、該当するオプションを選択します。これらのオプションは、レポートを印刷する場合にのみ有効です。CSV形式ではなくPDF形式にのみ適用されます。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報が含まれています。各サーバータスクは、トリガーのみを設定できます。各トリガーは1つのサーバータスクのみを実行できます。トリガーの設定が基本セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 – 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、完了をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

コンピューター名の変更

コンピューター名の変更タスクを使用するとESET PROTECTでFQDN形式でコンピュータ名を変更できます。ESET PROTECTでインストールされる既定の既存のサーバータスクを使用できます。クライアントデバイス名がデバイス詳細で報告された名前と異なる場合、このタスクを実行すると正しい名前を復元できます。

このタスクは、**Lost + found**グループにある同期されたコンピューターの名前を1時間ごとに自動的に変更します。

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前や説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

グループ名 - 静的または動的グループを選択するか、新しい静的または名前が変更されたコンピューターの動的グループを作成します。

次に基づいて名前を変更

- **コンピューター名** - 各コンピューターは一意のコンピューター名でローカルネットワークで特定されます。
- **コンピューターFQDN (完全修飾ドメイン名)** - これは、ホスト名で始まり、最上位のドメイン名まですべてのドメイン名まで続きます。

名前の解決は、すでにESET PROTECTにあるコンピューターと同期によって追加されたコンピューターと競合します(名前は一意でなければなりません)。同期対象のサブツリー外のコンピューター名にのみ適用されることを確認してください。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報がありません。各サーバータスクは、**トリガー**のみを設定できます。各トリガーは1つの**サーバータスク**のみを実行できます。**トリガーの設定**が**基本**セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 - 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

静的グループの同期

静的グループの同期タスクは、ネットワーク(Active DirectoryとOpen DirectoryとLDAPとローカルネットワークとVMware)のコンピューターを検索し、[静的グループ](#)に配置します。[サーバーインストール](#)中に**Active Directory**と**同期**を選択すると、見つかったコンピューターがすべてグループに追加されます。Windowsドメインに参加したLinuxコンピューターを同期するには、[詳細手順](#)に従います。

i ESET PROTECTは[セキュリティで保護されたLDAP署名](#)をサポートしています。

3つの同期モードがあります。

- **Active Directory/Open Directory/LDAP** - 基本サーバー接続情報を入力します。[詳細については、ここをクリックしてください](#)
- **MS Windows ネットワーク** - 使用するワークグループ、ユーザーの認証情報を入力します。[詳細については、ここをクリックしてください](#)
- **VMware** - VMware vCenter Server 接続情報を入力します。[詳細については、ここをクリックしてください](#)

同期モード - Active Directory/Open Directory/LDAP

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。**タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。


後でトリガーを設定するには、このチェックボックスをオフにします。

設定

共通設定

静的グループ名の下で**選択**をクリックします。既定では、実行ユーザーのホームグループが同期されたコンピュータで使用されます。あるいは、**新しい静的グループ**を作成できます。

- **同期するオブジェクト - コンピュータとグループまたは コンピュータのみ**
- **コンピュータ作成の競合処理** - 同期によって既に静的グループのメンバーであるコンピュータが追加された場合、競合解決方法を選択できます。
 - o **スキップ** (重複するコンピュータは追加されません)
 - o **移動** (新しいコンピュータはサブグループに移動されます)
 - o **複製** (新しいコンピュータが修正された名前で作成されます)
- **コンピュータ消去処理** - コンピュータが存在しない場合は、このコンピュータを**削除**するか、**スキップ**できます。
- **グループ消去処理** - グループが存在しない場合は、このグループを**削除**するか、**スキップ**できます。

 **グループ消去処理**を**スキップ**に設定し、Active Directoryからグループ(組織単位)を削除する場合は、**コンピュータ消去処理**を**削除**に設定してもESET PROTECTグループに属するコンピュータは削除されません。

- **同期モード** - Active Directory/Open Directory/LDAP


ESET PROTECT9でActive Directory同期を使用したコンピュータの管理に関する[ナレッジベース記事](#)をお読みください。

サーバー接続設定

- **サーバー**: ドメインコントローラのサーバー名またはIPアドレスを入力します。
- **ログイン**: 次の形式でドメインコントローラーのユーザー名を入力します。

oDOMAIN\username (Windowsで実行中のESET PROTECT Server)

ousername@FULL.DOMAIN.NAMEまたはusername (Linuxで実行中のESET PROTECT Server)


 ドメイン名は必ず大文字で入力してください。クエリを正常にActive Directoryサーバーで認証するには、この形式が必要です。

- **パスワード** - ドメインコントローラにログインするためのパスワードを入力します。

既定ではWindowsのESET PROTECTサーバー9.0は、すべてのActive Directory (AD)接続で、暗号化されたLDAPS (SSLを使用したLDAP)プロトコルを使用します。[ESET PROTECT仮想アプライアンスでLDAPSを設定](#)することもできます。

Windowsコンピューターでバージョン7.0-7.1からESET PROTECT 9.0にアップグレードし、Active Directory同期を使用していた場合は、ESET PROTECT 9.0で同期タスクが失敗します。

LDAPSでAD接続を正常に実行するために、次の項目を設定します。

1. ドメインコントローラーには、コンピューター証明書をインストールしている必要があります。ドメインコントローラーの証明書を発行するには、次の手順を実行します。
 - a) サーバーマネージャーを開き、**管理 > 役割と機能の追加**をクリックして、**Active Directory証明書サービス > 認証局**をインストールします。新しい認証局が**信頼できるルート認証局**に作成されます。
 -  b) スタートからcertmgr.mscと入力し、**Enter**を押して、**証明書Microsoft管理コンソールスナップイン**を実行 > **証明書 - ローカルコンピューター > 個人**に移動して、空のウィンドウを右クリックし、**すべてのタスク > 新しい証明書の要求 > ドメインコントローラーの登録ロール**をクリックします。
 - c) FQDNのドメインコントローラーが発行された証明書に含まれていることを確認します。
 - d) ESMCサーバーで、生成したCAを証明書ストアにインポート(certmgr.mscツールを使用)し、信頼できるCAフォルダーにインポートします。
2. ADサーバーに接続設定を入力するときには、**サーバー**または**ホストフィールド**に、ドメインコントローラーのFQDNを(ドメインコントローラー証明書の記載のとおり)に入力します。LDAPSではIPアドレスは十分な情報ではありません。

LDAPプロトコルへのフォールバックを有効にする場合は、**Active Directoryの代わりにLDAPを使用する**の横のチェックボックスを選択し、サーバーと一致する固有の属性を入力します。あるいは、**選択**をクリックして**プリセット**を選択すると、属性が自動的に入力されます。

- **Active Directory**
- **Mac OS X Server Open Directory (コンピューターホスト名)**
- **Mac OS X Server Open Directory (コンピューターIPアドレス)**
- **SambaのOpenLDAPコンピューターレコード** - パラメーター[Active DirectoryのDNS名](#)を設定します。

Active Directoryの代わりにLDAPを使用と**Active Directoryプリセット**を選択すると、[コンピューター詳細](#)にActive Directory構造の属性を入力できます。タイプDirectoryStringの属性のみを使用できます。ツール(たとえばADExplorer)を使用して、ドメインコントローラーの属性を検査できます。以下の表の対応するフィールドを参照してください。

コンピューター詳細フィールド	同期タスクフィールド
名前	コンピューターホスト名属性
説明	コンピューター説明属性

同期設定

- **識別名** - Active Directoryツリーのノードへのパス(識別名)。このオプションを空欄にするとADツリー全体を同期します。**識別名**の横の**参照**をクリックします。Active Directoryツリーが表示されます。最上位のエントリを選択してすべてのグループをESET PROTECTと同期するか、追加する特定のグループのみを選択します。コンピューターと組織単位のみが同期されます。完了したら、**[OK]**をクリックします。
- **除外された識別名** - Active Directoryツリーの特定のノードを除外(無視)することを選択できます。

- 無効なコンピュータを無視(**Active Directoryのみ**) - Active Directoryで無効なコンピュータを無視できます。タスクはこれらのコンピュータをスキップします。

! エラーの場合: **Server not found in Kerberos database** [参照](#)をクリックした後、IPアドレスではなく、サーバーのAD FQDNを使用します。

Linuxサーバーからの同期

Linux上で実行されているESETPROTECTサーバーは、Windowsマシンとは異なる方法で同期を実行します。プロセスは次のとおりです。

1. ドメインコントローラーのホスト名と資格情報を入力する必要があります。
2. サーバーは資格情報を検証し、Kerberosチケットに変換します。
3. ドメインが存在しない場合、サーバーはドメインの識別名を検出します。
4. A) オプション**Active Directoryの代わりにLDAPを使用**がオンではない場合:
ldapsearchの複数の呼び出しはツリーを列挙します。コンピューターレコードを取得するプロセスの簡素化された例:
`kinit <username>`
(これは、2行に分割された1つのコマンドです)
`ldapsearch -LLL -Y GSSAPI -h ad.domain.com -b 'DC=domain,DC=com' \`
`'(&(objectCategory=computer))' 'distinguishedName' 'dNSHostName'`

B) オプション**Active Directoryの代わりにLDAPを使用**がオンである場合:
同じプロセスがオプション4Aで呼び出されますが、ユーザーはパラメーターを設定できます。
5. Kerberosはハンドシェイクメカニズムを使用して、ユーザーを認証し、クリアテキストでパスワードを送信せずに認証のために他のサービスで後から使用できるチケットを生成します(**簡易認証を使用オプションとは逆**)。
6. ldapsearchユーティリティはGSSAPIを使用して、取得されたKerberosチケットによってActive Directoryに対して認証します。
7. 暗号化されていないチャネル経由で検索結果が渡されます。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報が 있습니다。各サーバータスクは、トリガーのみを設定できます。各トリガーは1つの**サーバータスク**のみを実行できます。**トリガーの設定が基本**セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 - 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#) [ステータスアイコン](#)、および[詳細](#)が表示されます。

同期モード - MS Windows ネットワーク

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前**や**説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、[タグを割り当て](#)ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。


- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

共通設定

静的グループ名の下で**選択**をクリックします。既定では、実行ユーザーのホームグループが同期されたコンピューターで使用されます。あるいは、**新しい静的グループ**を作成できます。

- **同期するオブジェクト - コンピュータとグループ**または **コンピュータのみ**
- **コンピュータ作成の競合処理** - 同期によって既に静的グループのメンバーであるコンピュータが追加された場合、競合解決方法を選択できます。

☐ **スキップ** (重複するコンピューターは追加されません)

☐ **移動** (新しいコンピューターはサブグループに移動されます)

☐ **複製** (新しいコンピューターが修正された名前で作成されます)

- **コンピューター消去処理** - コンピューターが存在しない場合は、このコンピューターを**削除**するか、**スキップ**できます。
- **グループ消去処理** - グループが存在しない場合は、このグループを**削除**するか、**スキップ**できます。
- **同期モード - MS Windows ネットワーク**

[Microsoft Windows ネットワーク同期設定] セクションで、次の情報を入力します。

- **ワークグループ** - 同期されるコンピュータを含むドメインまたはワークグループを入力します。ワークグループを指定しない場合、すべての表示されるコンピュータが同期されます。
- **ログイン** - Windows ネットワークでの同期に使用するログイン資格情報を入力します。
- **パスワード** - Windows ネットワークにログインするために使用するパスワードを入力します。

i ESET PROTECT Serverはネットワークサービス権限で実行されます。これは、すべての付近のコンピュータを読み取るために十分ではない可能性があります。ユーザー資格情報が存在しない場合、サーバーは、オペレーティングシステムによって自動的に入力されたWindowsで使用可能なネットワークフォルダーから、すべての付近のコンピュータを読み取ります。資格情報が存在する場合、サーバーは直接同期でそれらを使用します。

トリガー

トリガー セクションには、タスクを実行するトリガーの情報がります。各サーバータスクは、トリガーのみを設定できます。各トリガーは1つのサーバータスクのみを実行できます。トリガーの設定が基本セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 - 調整

調整を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの**進行状況インジケータバー**、**ステータスアイコン**、および**詳細**が表示されます。

同期モード - VMware

VMware vCenter Serverで実行中の仮想マシンを同期できます。

i このタスクを正常に実行するには、ESET PROTECTサーバーでvCenter CAを**インポート**する必要があります。Webブラウザでエクスポートできます。
たとえばFirefoxを使用して証明書をエクスポートするには、アドレスバー **https://** で安全な接続のアイコンをクリックし、**接続詳細を表示 > 詳細 > 証明書の表示 > 詳細 > エクスポート > 保存**をクリックします。

新しいサーバータスクを作成するには、**タスク > 新規作成 > +サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成 > +サーバータスク**をクリックします。

基本

基本セクションで、**名前や説明(任意)**などのタスクに関する基本情報を入力します。 **タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作

成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

共通設定


静的グループ名の下で**選択**をクリックします。既定では、実行ユーザーのホームグループが同期されたコンピューターで使用されます。あるいは、**新しい静的グループ**を作成できます。

- **同期するオブジェクト - コンピュータとグループまたは コンピュータのみ**
 - o **スキップ** (重複するコンピューターは追加されません)
 - o **移動** (新しいコンピューターはサブグループに移動されます)
 - o **複製** (新しいコンピューターが修正された名前で作成されます)
- **コンピューター消去処理** - コンピューターが存在しない場合は、このコンピューターを**削除**するか、**スキップ**できます。
- **グループ消去処理** - グループが存在しない場合は、このグループを**削除**するか、**スキップ**できます。
- **同期モード - VMware**

サーバー接続設定

- **サーバー - VMware vCenter Server**のDNSまたはIPアドレスを入力します。アドレスは、インポートされたvCenter CAの値**CN**と正確に一致する必要があります。[詳細](#) > **認証局**ウィンドウの**件名**の列にこの値があります。
- **ログイン - VMware vCenter Server**のログイン資格情報を入力します。
- **パスワード - VMware vCenter Server**にログインするためのパスワードを入力します。

同期設定

- **構造ビュー** - 構造ビュー、**フォルダ**リソースプールのタイプを選択します。
- **構造パス** - [\[参照\]](#)をクリックし、同期するフォルダに移動します。フィールドが空欄の場合は、

構造全体が同期されます。

- **コンピュータービュー** – 同期後に**名前**、**ホスト名**、**IPアドレス**でコンピューターを表示するかどうかを選択します。

 エラーの場合: **Server not found in Kerberos database** [参照](#)をクリックした後、IPアドレスではなく、サーバーのAD FQDNを使用します。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報が 있습니다。各サーバータスクは、**トリガー**のみを設定できます。各トリガーは1つの**サーバータスク**のみを実行できます。**トリガーの設定**が**基本**セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 – 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、**完了**をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

静的グループ同期 - Linux コンピュータ

Windowsドメインに参加したLinuxコンピュータは、[コンピュータ]プロパティのActive Directory Users and Computers (ADUC)にテキストが表示されません。このため、手動でテキストを挿入する必要があります。

[サーバー前提条件](#)と次の前提条件を確認します。

- LinuxコンピュータがActive Directoryにある。
- ドメインコントローラにDNSサーバーがインストールされている。
- [ADSI Edit](#)がインストールされている。

1. コマンドプロンプトを開き、`adsiedit.msc`を実行します
2. **アクション > 接続先**に移動します。[接続設定]ウィンドウが表示されます。
3. **既知の命名コンテキストを選択**をクリックします。
4. 下のコンボボックスを展開し、**既定の命名コンテキスト**を選択します。
5. **OK**をクリックします。左側のADSI値は、ドメインコントローラの名前です。既定の命名コンテキスト(ドメインコントローラ)。
6. **ADSI値**をクリックし、サブグループを展開します。

7. **サブグループ**をクリックし、Linuxコンピュータが表示されるCN (共通名)とOU (組織単位)に移動します。
8. Linuxコンピュータの**ホスト名**をクリックし、コンテキストメニューから**プロパティ**を選択します。**dnsHostName**パラメータに移動し、**編集**をクリックします。
9. 値**未設定**を有効な値に変更します(例: ubuntu.TEST)回
10. **OK**>**OK**をクリックします。**ADUC**を開き、Linuxコンピュータの**プロパティ**を選択します。新しいテキストがここに表示されます。

ユーザー同期

このサーバータスクは、ActiveDirectoryLDAPパラメーターなどのソースのユーザーおよびユーザーグループ情報を同期します。

新しいサーバータスクを作成するには、**タスク**>**新規作成**>**サーバータスク**をクリックするか、左側で任意のタスクタイプを選択して、**新規作成**>**サーバータスク**をクリックします。

基本

基本セクションで、**名前や説明(任意)**などのタスクに関する基本情報を入力します。**タグを選択**をクリックして、**タグを割り当て**ます。

タスクドロップダウンメニューで、作成および設定するタスクタイプを選択します。新しいタスクを作成する前に、特定のタスクタイプを選択した場合、前回の選択に基づいて、**タスク**があらかじめ選択されます。**タスク**([すべてのタスク](#)の一覧を参照)は、タスクの設定と動作を定義します。

次のタスクトリガー設定から選択できます。

- **完了後ただちにタスクを実行** - このオプションをオンにし、[完了]をクリックした後にタスクを自動的に実行します。
- **トリガーの設定** - チェックボックスをオンにし、[トリガー](#)セクションを有効にして、トリガー設定を構成できます。

後でトリガーを設定するには、このチェックボックスをオフにします。

設定

共通設定

ユーザーグループ名 - 既定では、同期されたユーザーのルートが使用されます(既定ではこれは**すべてグループ**)。あるいは、新しいユーザーグループを作成できます。

ユーザー作成の競合処理 - 2つのタイプの競合が発生する可能性があります。

- 同じグループに同じ名前のユーザーが2人いる。
- 同じSIDの既存のユーザーがいる(システムの任意の場所)。

次の方法で競合処理を設定できます。

- **スキップ** - ユーザーは、Active Directoryとの同期中にESET PROTECT に追加されません。

- 上書き ESET PROTECT の既存のユーザーは Active Directory のユーザーによって上書きされます。SID 競合の場合 ESET PROTECT の既存のユーザーは前の場所から削除されます (ユーザーが別のグループにいた場合でも)。

ユーザー消去処理 - ユーザーが存在しない場合は、このユーザーを削除するか、スキップします。

ユーザーグループ消去処理 - ユーザーが存在しない場合は、このユーザーグループを削除するか、スキップします。

i ユーザーの **カスタム属性** を使用する場合は、[ユーザー作成の競合処理] を [スキップ] に設定します。そうでない場合、ユーザー (とすべての詳細) は、Active Directory のデータで上書きされ、カスタム属性が失われます。ユーザーを上書きする場合は、**ユーザー消去処理** を **スキップ** に変更します。

サーバー接続設定

- **サーバー**: ドメインコントローラのサーバー名または IP アドレスを入力します。
- **ログイン**: 次の形式でドメインコントローラーのユーザー名を入力します。

ODOMAIN\username (Windows で実行中の ESET PROTECT Server)

ouusername@FULL.DOMAIN.NAME または username (Linux で実行中の ESET PROTECT Server)

! ドメイン名は必ず大文字で入力してください。クエリを正常に Active Directory サーバーで認証するには、この形式が必要です。

- **パスワード** - ドメインコントローラーにログインするためのパスワードを入力します。

既定では Windows の ESET PROTECT サーバー 9.0 は、すべての Active Directory (AD) 接続で、暗号化された LDAPS (SSL を使用した LDAP) プロトコルを使用します。 [ESET PROTECT 仮想アプライアンスで LDAPS を設定](#) することもできます。

Windows コンピューターでバージョン 7.0-7.1 から ESET PROTECT 9.0 にアップグレードし、Active Directory 同期を使用していた場合は、ESET PROTECT 9.0 で同期タスクが失敗します。

LDAPS で AD 接続を正常に実行するために、次の項目を設定します。

1. ドメインコントローラーには、コンピューター証明書をインストールしている必要があります。ドメインコントローラーの証明書を発行するには、次の手順を実行します。

a) サーバーマネージャーを開き、**管理 > 役割と機能の追加** をクリックして、**Active Directory 証明書サービス > 認証局** をインストールします。新しい認証局が **信頼できるルート認証局** に作成されます。

! b) スタートから **certmgr.msc** と入力し、**Enter** を押して、**証明書 Microsoft 管理コンソール** スナップインを実行 > **証明書 - ローカルコンピューター > 個人** に移動して、空のウィンドウを右クリックし、**すべてのタスク > 新しい証明書の要求 > ドメインコントローラーの登録ロール** をクリックします。

c) FQDN のドメインコントローラーが発行された証明書に含まれていることを確認します。

d) ESMC サーバーで、生成した CA を証明書ストアにインポート (certmgr.msc ツールを使用) し、信頼できる CA フォルダーにインポートします。

2. AD サーバーに接続設定を入力するときには、**サーバー** または **ホストフィールド** に、ドメインコントローラーの FQDN を (ドメインコントローラー証明書の記載のとおり) に入力します。LDAPS では IP アドレスは十分な情報ではありません。


LDAP プロトコルへのフォールバックを有効にする場合は、**Active Directory** の代わりに **LDAP** を使用するの横のチェックボックスを選択し、サーバーと一致する固有の属性を入力します。あるいは、**選択** をクリッ

クしてプリセットを選択すると、属性が自動的に入力されます。

- **Active Directory**
- **Mac OS X Server Open Directory** (コンピューターホスト名)
- **SambaのOpenLDAPコンピューターレコード** - パラメーター [Active DirectoryのDNS名](#)を設定します。

同期設定

- **識別名** - Active Directoryツリーのノードへのパス(識別名)。このオプションを空欄にするとADツリー全体を同期します。識別名の横の参照をクリックします。Active Directoryツリーが表示されます。最上位のエントリを選択してすべてのグループをESET PROTECTと同期するか、追加する特定のグループのみを選択します。コンピューターと組織単位のみが同期されます。完了したら、**[OK]**をクリックします。
- **ユーザーグループとユーザー属性** - ユーザーの既定の属性は、ユーザーが属するディレクトリ固有です。Active Directory属性を同期する場合は、該当するフィールドのドロップダウンメニューからADパラメーターを選択するか、属性のカスタム名を入力します。同期された各フィールドの横にはESET PROTECTプレースホルダー(例:\${display_name})があり、特定のESET PROTECTポリシー設定のこの属性を表します。
- **詳細ユーザー属性** - 詳細カスタム属性を使用する場合は、**[新規追加]**を選択します。このフィールドはユーザー情報を継承し、iOS MDM用のポリシーエディターでプレースホルダとして処理できます。

 エラーの場合: **Server not found in Kerberos database** 参照をクリックした後、IPアドレスではなく、サーバーのAD FQDNを使用します。

トリガー

[トリガー](#)セクションには、タスクを実行するトリガーの情報が 있습니다。各サーバータスクは、トリガーのみを設定できます。各トリガーは1つのサーバータスクのみを実行できます。トリガーの設定が基本セクションで選択されていない場合、トリガーは作成されません。タスクはトリガーがなくても作成できます。このようなタスクは後から手動で実行するか、トリガーを後から追加できます。

詳細設定 - 調整

[調整](#)を設定すると、作成されたトリガーの詳細ルールを設定できます。調整の設定は任意です。

概要

すべての構成されたオプションはここに表示されます。設定を確認し、完了をクリックします。

タスクには、作成した各タスクの[進行状況インジケータバー](#)と[ステータスアイコン](#)、および[詳細](#)が表示されます。

タスクトリガータイプ

基本的にトリガーは、定義済みの方法で特定のイベントに反応するセンサーです。割り当てられたタスクを実行するために使用されます。トリガーはスケジュール(時間イベント)によって起動するか、特定のシステムイベントの発生時に起動します。

! トリガーの再利用はできません。各タスクは別のトリガーで実行する必要があります。各トリガーは1つのタスクのみを実行できます。

トリガーでは新しく割り当てられたタスクはただちに実行されません(即時トリガーを除く)。イベントに対するトリガーの感度は、[調整](#)によって下げることができます。

トリガータイプ:

- **即時** - クライアントタスクでのみ使用できます。タスクは **完了** をクリックするとすぐに実行されます。**有効期限 日付**の値は、タスクが実行されなくなる日を指定します。

スケジュール済み

スケジュールされたトリガーは、日時設定に基づいてタスクを実行します。タスクは、**1回だけ実行**するか、繰り返し実行するか、[CRON式](#)に基づいて実行するようにスケジュールできます。

- **一度だけ実行** - このトリガーはスケジュールされた日時に1回実行されます。ランダム間隔で遅延できます。
- **毎日** - このトリガーは選択した日に毎回実行されます。期間の開始日と終了日を設定できます。たとえば、10回連続して週末にタスクを実行できます。
- **毎週** - このトリガーは選択した曜日に毎回実行されます。たとえば、7月1日から8月31日までのすべての月曜日と金曜日にタスクを実行します
- **毎月** - このトリガーは選択した期間の選択した週の選択した日に実行されます。**繰り返し値**はタスクを実行する月の曜日(第2月曜日など)を設定します。
- **毎年** - このトリガーは毎年(または設定されている年ごとに)、指定した**開始日**に実行されます。

i **ランダム遅延間隔**設定はスケジュールされたタイプのトリガーで使用できます。タスク実行の最大遅延範囲を定義します。ランダムにすると、サーバーの過負荷を防止できます。

✓ Johnが**毎週**月曜日に実行し、2017年2月10日 8:00:00に**開始**するタスクを設定し、**ランダム遅延間隔**を 1時間に、**終了日**を 2017年4月6日 00:00:00に設定すると、指定された終了日まで、毎週月曜日8:00~9:00の間にランダムな1時間の遅延でタスクが実行されます。

- **設定した時間に実行されなかった場合は即時実行**チェックボックスを選択すると、定義した時刻に実行されなかった場合は、ただちにタスクを実行します
- トリガーを設定するときには **USESET PROTECT Web** コンソールのタイムゾーンが既定で使用されます。**サーバーのローカル時刻を使用**チェックボックスを選択すると **USESET PROTECT** コンソールタイムゾーンではなく、サーバーのローカルタイムゾーンを使用してトリガーを設定できます。

Use Server Local Time



動的グループ

動的グループトリガーは、サーバータスクでのみ使用できます。

- **動的グループメンバーが変更** – 動的グループの内容が変更されたときに起動します。例えば、クライアントが特定の動的グループに入った場合やグループから出た場合などです。
- **しきい値に従って動的グループサイズが変更** – 動的グループのクライアント数が指定したしきい値を上回った場合や下回った場合に、このトリガーが起動します。例えば、101台以上のコンピューターが特定のグループにある場合などです。
- **期間中に動的グループサイズが変更** – 動的グループのクライアント数が定義済みの期間に変化した場合に、このトリガーが起動します。例えば、特定のグループのコンピューター数が1時間に10%増加した場合などです。
- **比較グループを基準に動的グループサイズが変更** – このトリガーは、観察された動的グループのクライアント数が比較グループ(静的または動的)に合わせて変更された場合にトリガーされます。例えば、すべてのコンピューターの10%以上が感染した場合などです(グループ「すべて」とグループ「感染」を比較)。

その他

- **サーバー起動** – サーバータスクでのみ使用できます。サーバー起動時に実行されます。例えば、このトリガーは[静的グループ同期](#)タスクで使用されます。
- **結合された動的グループトリガー** – クライアントタスクでのみ使用できます。このトリガーはデバイスが動的グループに参加するときに実行されます。

i **結合された動的グループトリガー**は、ターゲットセクションで動的グループが選択されている場合にのみ使用できます。トリガーは、トリガーが作成された後に動的グループに参加したデバイスでのみタスクを実行します。既に動的グループにあるすべてのデバイスで、タスクを手動で実行する必要があります。

- **イベントログトリガー** – このトリガーは、特定のイベントがログで発生したときに呼び出されます。例えば、**検査**ログに検出がある場合などです。このタイプのトリガーは、[調整設定](#)で特殊な設定のセットを提供します。
- **CRON式** – このトリガーは特定の日に起動します。

CRON式間隔

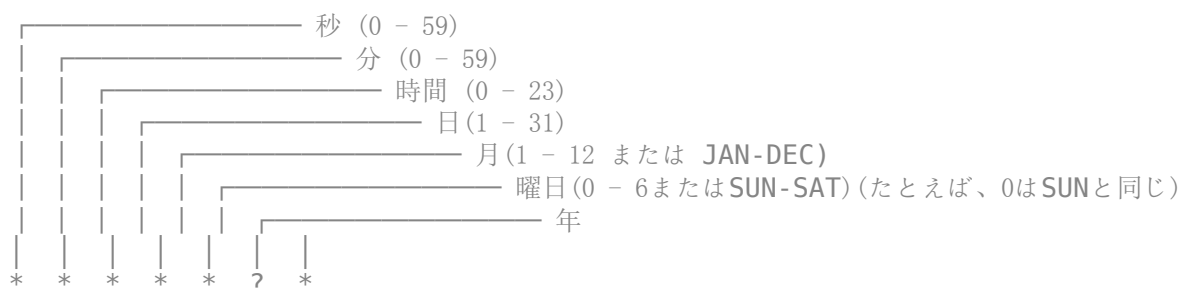
CRON式は、トリガーの特定のインスタンスを構成するために使用されます。ほとんどはスケジュールされた反復トリガー用です。これは、スケジュールの個別の値を表す6または7フィールドから構成される文字列です。これらのフィールドは、スペースで区切られます。また、任意の許容される値をさまざまに組み合わせて使用できます。

CRON式は次のように簡潔にすることができます。* * * * ? * または次のようにより複雑にできます。0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020

CRON式で利用できる値の一覧

名前	必要	値	許可された特殊文字
秒	はい	0-59	, - * / R
分	はい	0-59	, - * / R
時間	はい	0-23	, - * / R
月の日付	はい	1-31	, - * / ? L W
月	はい	1-12またはJAN-DEC	, - */
曜日	はい	0-6またはSUN-SAT	, - / ? L #
年	はい	1970-2099	, - * /

CRON式構文は次のとおりです。



- 0 0 0は深夜を意味します(秒、分、時間)。
- 他のフィールドで定義されているため値を定義できない場合は?を使用します(日または曜日)。
- *はすべてを意味します(秒、分、時間、日、月、曜日、年)。
- SUNは日曜日を意味します。

i 月の名前と曜日は大文字と小文字を区別しません。たとえばMONはmonと同じかJANはjanと同じになります。

特殊文字:

カンマ (,)

カンマはリストの項目を区切るために使用されます。たとえば、6番目のフィールドでMON,WED,FRI (曜日)を使用すると、月曜日、水曜日、金曜日を意味します。

ハイフン (-)

範囲を定義します。たとえば、2012-2020は2012年から2020年までの毎年を示します。

ワイルドカード (*)

フィールド内のすべての可能な値を選択するために使用されます。たとえば、分フィールドで*を使用すると毎分を意味します。ワイルドカードは曜日フィールドでは使用できません。

疑問符(?)

特定の日を選択するときには、日または曜日を指定できます。両方は指定できません。日を指定する場合は、曜日に?を使用する必要があります。逆も同様です。たとえば、特定の日(10日など)にトリガー

を実行し、実行される曜日を考慮しない場合は、日フィールドに10、曜日フィールドに?を入力します。

ハッシュ (#)

「N番目」の日を指定するために使用されます。たとえば、曜日フィールドの値4#3は、第3水曜日を意味します(第4日=木曜日、#3 = 月の第3木曜日)。#5を指定し、月に第5の曜日がない場合は、トリガーはその月に実行されません。

スラッシュ (/)

範囲の増分値を説明します。たとえば、2番目のフィールド(分)の3-59/15は、1時間のうちの3分目とその後15分間隔を意味します。

最後 (L)

曜日フィールドで使用すると、特定の月の最後の金曜日(5L)などのコンストラクトを指定できます。日フィールドでは、月の最後の日を指定します。たとえば、1月31日、2月28日(閏年を除く)です。

平日 (W)

W文字は日フィールドで使用できます。この文字は特定の日に最も近い平日(月曜日から金曜日)を指定するために使用されます。たとえば15Wを日フィールドの値として指定すると、15日に最も近い平日になります。15日が土曜日の場合、トリガーは14日の金曜日に実行されます。15日が日曜日の場合、トリガーは16日の月曜日に実行されます。ただし1Wを日の値に指定し、1日が土曜日の場合、トリガーは3日の月曜日に実行されます。月をまたいで実行されることはありません。

i LおよびW文字は、LWとして日フィールドで組み合わせることもできます。これは月の最後の平日を意味します。

ランダム (R)

Rは特殊な ESET PROTECT CRON式文字であり、ランダム化された時間を指定できます。たとえばR00*?*は毎日00:00に実行されますが、秒はランダムです(0-59)。

! すべてのESET Managementエージェントが同時にESET PROTECTサーバーに接続しないように、ランダム化された時間を使用することをお勧めします。

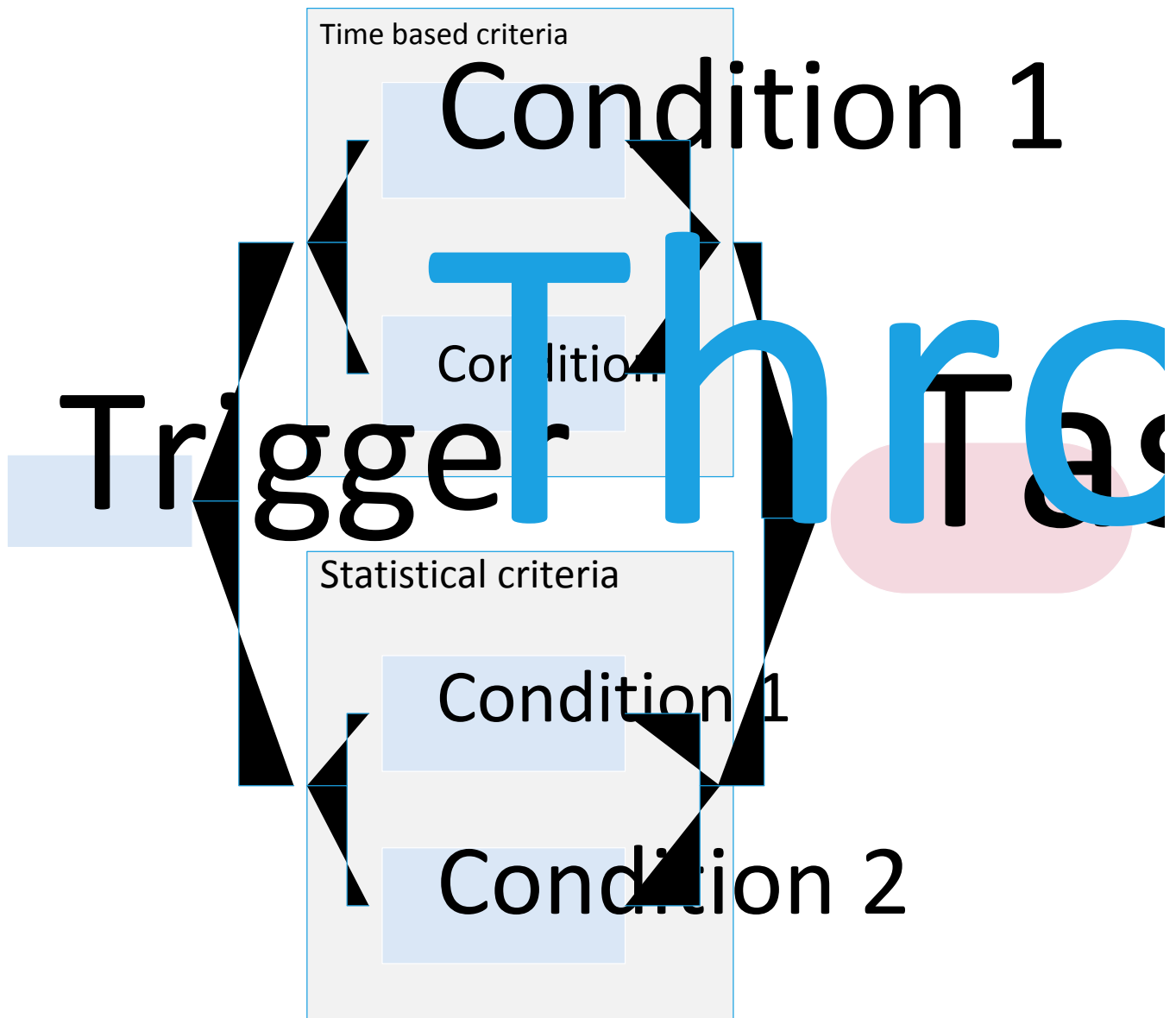
CRON式の一部のバリエーションを示す実際の例

CRON式	意味
0 0 12 * * ? *	毎日12時（正午）に起動します。
R 0 0 * * ? *	毎日00:00に実行されますが、秒はランダムです(0-59)。
R R R 15W * ? *	毎月15日のランダムな時間(秒、分、時間)に実行されます。15日が土曜日の場合、トリガーは14日の金曜日に実行されます。15日が日曜日の場合、トリガーは16日の月曜日に実行されます。
0 15 10 * * ? 2016	2016年中は毎日午前10時15分に起動します。
0 * 14 * * ? *	毎日午後2時から2時59分まで毎分起動します。
0 0/5 14 * * ? *	毎日午後2時から午後2時55分まで5分間隔で起動します。
0 0/5 14,18 * * ? *	毎日午後2時から午後2時55分まで5分間隔で起動、かつ午後6時から午後6時55分まで5分間隔で起動します。
0 0-5 14 * * ? *	毎日午後2時から午後2時5分まで毎分起動します。

CRON式	意味
0 10,44 14 ? 3 WED *	3月の水曜日午後2時10分と午後2時44分に起動します。
0 15 10 ? * MON-FRI *	毎平日(月曜日、火曜日、水曜日、木曜日、金曜日)の午前10時15分に起動します。
0 15 10 15 * ? *	毎月15日の午前10時15分に起動します。
0 15 10 ? * 5L *	毎月最後の金曜日の午前10時15分に起動します。
0 15 10 ? * 5L 2016-2020	2016年から2020年まで毎月の最後の金曜日の午前10時15分に実行されます。
0 15 10 ? * 5#3 *	毎月第3金曜日の午前10時15分に起動します。
0 0 * * * ? *	毎日1時間おきに実行します。

詳細設定 - 調整

調整はタスクが実行されないように制限するために使用されます。通常、タスクが頻繁に発生するイベントによってトリガーされるときに使用されます。特定の状況の下では、調整によってトリガーの実行ができない場合があります。トリガーが実行されるたびに、以下の方法に従って評価されます。指定された条件を満たすトリガーのみがタスクを実行します。調整条件されていない場合、すべてのトリガーイベントがタスクを実行します。



調整には、3種類の条件があります。

1.時間ベースの条件

2.統計条件

3.イベントログ条件

タスクを実行するには：

- すべての条件を満たす必要があります
- 条件を設定する必要があります。条件が空の場合は省略されます
- すべての時間ベースの条件を満たす必要がありますAND演算子で評価されるためです
- AND演算子で評価されるすべての統計条件を満たす必要がありますOR演算子の1つ以上の統計条件を満たす必要があります
- まとめて設定された統計および時間条件を満たす必要がありますAND演算子のみで評価され、タ

スクが実行されます


定義済みの条件のいずれかが満たされた場合、すべての監視側の蓄積された情報がリセットされます(カウントは0から開始します)。これは、時間ベースの条件と統計条件の両方に当てはまります。エージェントまたはESET PROTECTサーバーが再起動した場合にも、この情報はリセットされます。トリガーを変更すると、常にステータスがリセットされます。統計条件は1つだけ使用し、複数の時間ベースの条件を使用することをお勧めします。複数の統計条件を使用すると、不必要に複雑になり、トリガー結果が変わる可能性があります。




プリセット

3つのプリセットがあります。プリセットを選択するときには、現在の調整設定がクリアされ、プリセット値で置換されます。これらの値はさらに修正および使用できますが、新しいプリセットを作成することはできません。

時間ベースの条件

期間 (T2) - 指定された期間中に1回トリガーを許可します。たとえば、10秒に設定され、この期間中に10回呼び出しがあった場合、最初のトリガーのみがイベントを実行します。

時間ベースの条件で調整を設定し、タスク実行を15分に1回に制限する必要があります(ロックアイコン  は制限を示します)。

- サーバータスク ([レポート生成](#)を含む) - すべての [トリガータイプ](#) 
-  • クライアントタスク - [スケジュールされたCRON式トリガータイプ](#) 

ESET PROTECT 8.xからアップグレードした場合は、期間が15分未満に設定された既存のすべてのタスクに15分が自動的に適用されます。

最低の15分の期間は通知に適用されません。

スケジュール (T1) - 定義済みの範囲内でのみトリガーを許可します。**期間の追加**をクリックすると、ポップアップウィンドウが表示されます。選択した時間単位で**範囲期間**を設定します。**参照**リストから1つのオプションを選択し、フィールドを入力します。これは選択した繰り返しによって異なります。[CRON式](#)の形式で参照を定義することもできます。**OK**をクリックして範囲を保存します。複数の時間範囲をリストに追加できます。時間範囲は時系列順に表示されます。

タスクをトリガーするには、構成された条件のすべてが満たされる必要があります。

統計条件

条件 - 統計条件はいずれかを使用して結合できます。

- すべての統計条件が満たされたときに通知を送信する - **AND**論理演算子が評価で使用されます
- 1つ以上の統計条件が満たされたときに通知を送信する - **OR**論理演算子が評価で使用されます

発生数 (S1) - X番目のトリガーヒットのみを許可します。例えば、10を指定した場合、10番目のトリガーだけがカウントされます。

期間内の発生数

発生数 (S2) - 定義済みの期間内のトリガーのみを許可します。タスクをトリガーするイベントの最低頻度を定義します。たとえば、イベントが1時間に10回検出された場合に、この設定を使用して、タスク

の実行を許可します。トリガーの実行により、カウンターがリセットされます。

期間 – 上記のオプションの期間を定義します。

3番目の統計条件は特定のトリガータイプでのみ使用できます。トリガー>トリガータイプ>イベントログトリガーを参照してください。

イベントログ条件

これらの条件は第三の統計条件(S3)としてESET PROTECTによって評価されます。**統計条件の適用**演算子(AND / OR)は、すべての3つの統計条件をまとめて評価するために適用されます。**レポートの生成**タスクと組み合わせてイベントログ条件を使用することをお勧めします。すべての3つのフィールドは条件が動作するために必要です。トリガーが起動し、バッファ内に既にシンボルがある場合は、シンボルのバッファがリセットされます。

条件 – 条件をトリガーするイベントまたはイベントのセットを定義します。使用可能なオプションは次のとおりです。

- **行で受信** – 選択した数のイベントが連続して発生する必要があります。これらのイベントは個別である必要があります。
- **前回の発生以降に受信** – 条件は、選択した個別のイベント数に達したときにトリガーされます(前回のタスク実行以降)。

発生数 – タスクを実行するために選択されたシンボルがある個別のイベント数を入力します。

シンボル-ログタイプ(トリガーメニューで設定)に応じて、検索できるログのシンボルを選択できます。メニューを表示するには、**[選択]**をクリックします。選択したシンボルを削除するには、**削除**をクリックします。

i サーバータスクで使用されているときには、すべてのクライアントコンピューターが考慮されます。連続して多数の識別記号を受信する可能性は高くありません。合理的な場合にのみ、**連続受信**設定を使用してください。この時点で、見つからない値(n/a)は一意でないと見なされるため、バッファがリセットされます。

追加プロパティ

前述の通り、トリガーを実行しないイベントもあります。トリガーにならないイベントに対して実行されたアクション:

- 複数のイベントがスキップされた場合、最後の**N** イベントが1つにグループ化されます(抑制されたティックのデータを格納) [**N** <= 100]
- **N** == 0の場合、最後のイベントだけが処理されます(**N**は履歴の長さを意味します。最後のイベントは常に処理されます)。
- トリガーにならないイベントがすべてマージされます(最後のティックを**N** 履歴ティックとマージ)。

トリガー実行の頻度が高すぎる場合または通知の頻度を下げる場合、次の推奨事項を検討してください。

- 1つのイベントではなく複数のイベントがある場合にだけユーザーに対応させる場合は、統計条件S1を参照してください。
- 大量のイベントが発生した場合にだけトリガーを起動するには、統計条件S2を参照してください。
- 望ましくない値のイベントを無視する場合は、統計条件S3を参照してください。
- 関連する時間(業務時間など)外のイベントを無視する場合は、時間ベースの条件T1を参照してください。
- トリガー実行間隔を最小値に設定するには、時間ベースのT2条件を使用してください。

i 条件を組み合わせ、より複雑な調整シナリオに対応することもできます。詳細については、[調整の例](#)のセクションを参照してください。

調整例

調整の例では、調整条件(T1・T2・S1・S2・S3)が組み合わせられ、評価される方法を説明します。

i 「ティック」はトリガーからのパルスを意味します。T1・T2は時間ベースの条件です。S1・S2は統計条件です。S3はイベントログ条件です。

S1:発生条件(3ティックごとに許可)

時間	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13	14	15
ティック	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2:時間内の発生条件(3ティックが4秒以内に発生する場合に許可)

時間	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
ティック	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3:一意の記号値の条件(3つの一意の値が連続している場合に許可)

時間	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
値	A	B	B	C	D	G	H		J	K	N/A	L	M	N	N
S3					1									1	

S3:一意の記号値の条件(3つの一意の値が最後のティック以降の場合に許可)

時間	00	01	02	03	04	05	06	07	トリガーが修正される	08	09	10	11	12	13	14
値	A	B	B	C	D	G	H	I		J	K	N/A	L	M	N	N
S3				1			1						1			

T1:特定の時間範囲でティックを許可(8:10で始まる毎日を許可、期間は60秒)

時間	8:09:50	8:09:59	8:10:00	8:10:01	トリガーが修正される	8:10:59	8:11:00	8:11:01
ティック	x	x	x	x		x	x	x
T1			1	1		1		

この条件には状態がありません。このため、トリガー修正は結果に影響しません。

T2:時間間隔で1つのティックを許可(最大5秒に1回許可)

時間	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
ティック	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

S1+S2の組み合わせ

- S1:5ティックごと
- S2:4秒以内に3ティック

時間	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
ティック	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
結果			1				1								1		

結果は次のように列挙されます S1(論理 OR)S2

S1+T1組み合わせ

- S1:3ティックごとに許可
- T1:8:08から始まる毎日を許可、期間は60秒日時:

時間	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
ティック	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
結果						1			1	

結果は次の通り列挙されます S1(論理 AND)T1

S2+T1組み合わせ

- S2:10秒以内に3ティック
- T1:8:08から始まる毎日を許可、期間は60秒日時:

時間	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
ティック	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
結果							1			

結果は次のように列挙されます[S2(論理 AND)T1]

S2の状態は、グローバル結果が1の場合にだけリセットされます。

S2+T2組み合わせ

- S2:10秒以内に3ティック
- T2:最大20秒に1回許可

時間	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
ティック	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		
T2	1	1	1													1		
結果			1													1		

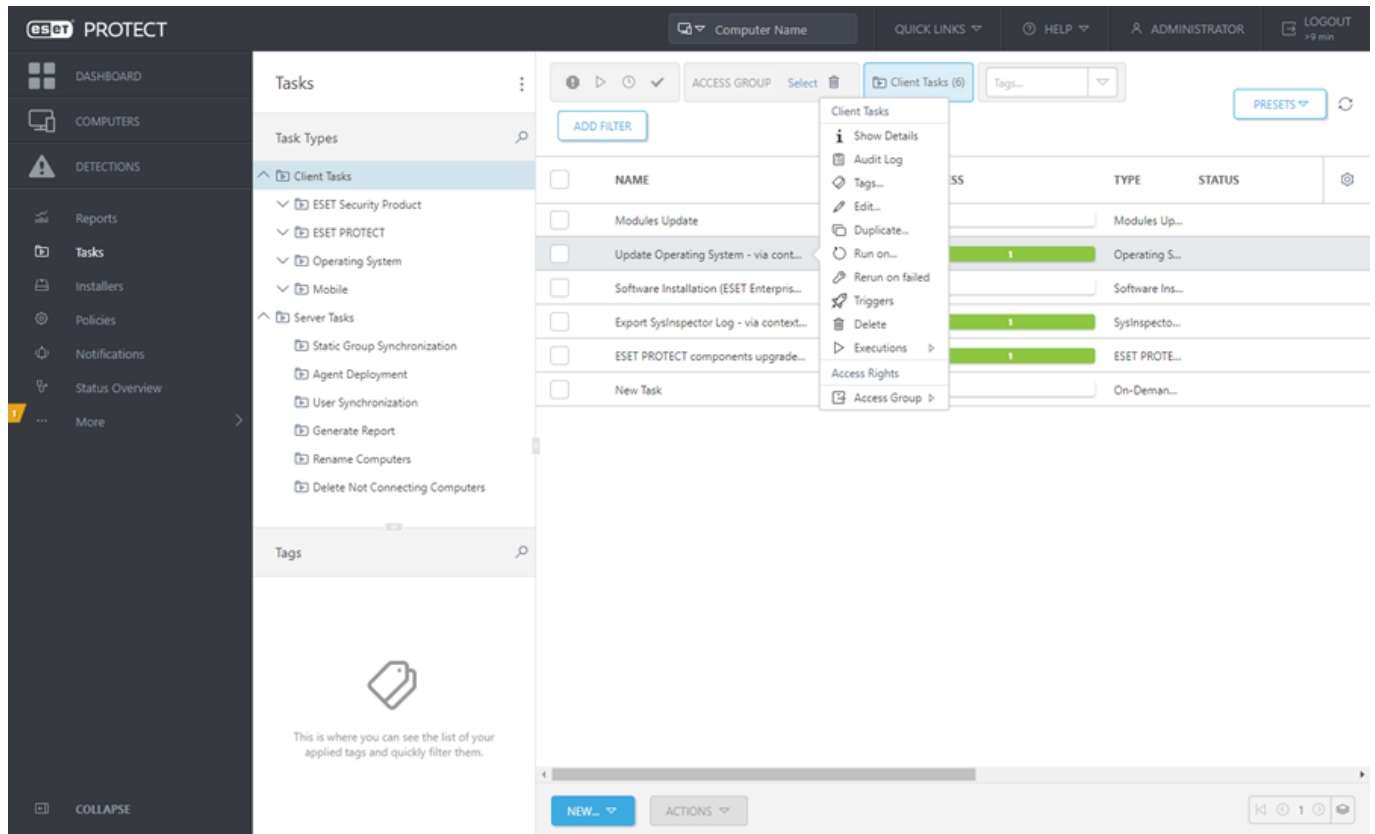
結果は次のように列挙されます[S2(論理 AND)T2]

S2の状態は、グローバル結果が1の場合にだけリセットされます。

タスク概要


タスクには、作成した各タスクの[進行状況インジケータバー](#)、[ステータスアイコン](#)、および[詳細](#)が表示されます。

! クライアントタスクを実行するには、[トリガー](#)を作成する必要があります。



タスクをクリックすると、さらにタスクアクションを実行できます。

詳細を表示	タスク詳細を表示 : 概要、実行、トリガー(トリガー詳細はクライアントタスクでのみ使用できます)。
監査ログ	選択した項目の 監査ログ を表示します。
タグ	タグ を編集します(割り当て、割り当て解除、作成、削除)。
実行	クライアントタスクのみ:タスク実行結果から選択し、必要に応じてさらにアクションを実行できます。詳細については、 タスク詳細 を参照してください。
トリガー	クライアントタスクのみ:選択したクライアントタスクの トリガー のリストを表示します。
編集	選択した タスク を編集します。若干の調整だけが必要な場合には、既存のタスクを編集すると便利です。より変更点の多いタスクについては、新しいタスクを作成した方がよい場合があります。
複製	選択したタスクに基づいて、新しいタスクが追加されます。重複するタスクの新しい名前が必要です。
今すぐ実行	サーバータスクのみ:選択したサーバータスクを実行します。
実行	クライアントタスクのみ: 新しいトリガー を追加し、クライアントタスクの対象コンピューターまたはグループを選択します。
失敗時に再実行する	クライアントタスクのみ:対象として設定された以前のタスク実行中に失敗したすべてのコンピューターを含む新しいトリガーを作成します。必要に応じてタスク設定を編集するか、[完了]をクリックして、タスクを変更せずに再実行できます。
削除	<p>選択したタスクを完全に削除します。</p> <ul style="list-style-type: none"> タスクが作成された後、開始がスケジュールされる前に削除された場合、タスクは削除され、実行されたり、開始されません。 タスクの実行のスケジュール後にタスクが削除された場合、タスクは完了しますがWebコンソールに情報は表示されません。

 アクセスグループ	タスクを別の静的グループに移動します。
---	---------------------

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

進捗状況のインジケータ

進行状況インジケータは色付きのバーであり、タスクの実行ステータスを示します。各タスクには独自のインジケータがあります(**進行状況**行に表示)。タスクの実行ステータスには異なる色でタスクの実行ステータスが示され、特定のタスクの該当する状態にあるコンピューター数が表示されます。

実行中 (青)



正常終了 (緑)















失敗 (オレンジ)



新しく作成されたタスク(白) - インジケータの色が変わるまでに時間がかかる場合があります。実行ステータスを表示するためにESET PROTECTサーバーはESET Managementエージェントからの応答を受け取る必要があります。進行状況インジケータは、トリガーが割り当てられていない場合は、白で表示されます。



上記の組み合わせ:

様々なアイコンタイプとステータスの詳細については、「[ステータスアイコン](#)」を参照してください。



進行状況インジケータには、タスクが最後に実行されたときのタスクのステータスが表示されます。これはESET Managementエージェントからの情報です。進行状況インジケータにはESET Managementエージェントがクライアントコンピュータから報告する内容と同じ情報が表示されます。

ステータスアイコン

[プロジェクトインジケータ](#)の横のアイコンは、詳細情報を示します。特定のタスクで予定された実行があるかどうかと、完了した実行の結果を示します。この情報はESET PROTECTサーバーによって列挙されます。次のステータスが表示されます。

実行	タスクは1つ以上のターゲットで実行中です。スケジュールされたタスクと失敗した実行はありません。これは、タスクが既に一部のターゲットで完了している場合にも該当します。
成功	タスクはすべてのターゲットで正常に完了しました。スケジュールされたタスクまたは実行中のタスクはありません。
エラー	タスクはすべてのターゲットで実行されましたが、1つ以上のターゲットで失敗しました。今後の実行は計画(スケジュール)されていません。
計画済み	タスクの実行が計画されていますが、まだ実行されていません。
計画済み/実行中	タスクの実行がスケジュールされています(過去または将来)。失敗した実行はなく、1つ以上のタスクが現在実行中です。
計画済み/成功	タスクには一部の計画された実行(過去または将来)がありますが、失敗した実行または実行中のタスクはなく、1つ以上の実行が正常に完了しました。
計画済み/エラー	タスクには一部の計画された実行(過去または将来)がありますが、実行中のタスクはなく、1つ以上の実行が失敗しました。一部の実行が正常に完了しても、適用されます。

タスク詳細

タスクをクリックし、**詳細を表示**を選択して、次のタブでタスク詳細を表示します。

概要

このタブには、タスク設定の概要が表示されます。

実行

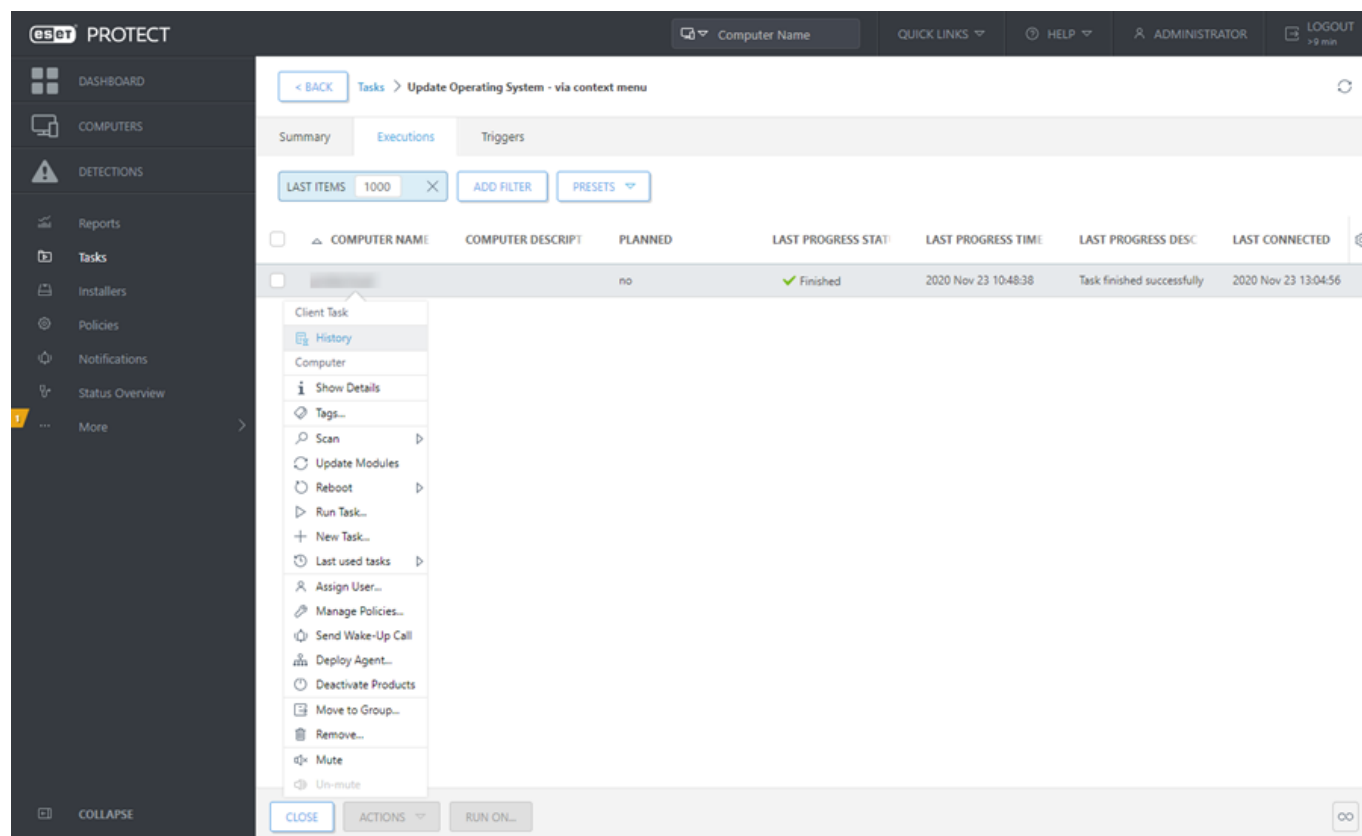
実行タブをクリックすると、ビューを切り替えて、各実行結果を表示できます。実行が多すぎる場合は、ビューをフィルタリングして、結果を絞り込むことができます。

クライアントタスクの**実行**には、選択した結果(フィルターを使用)のコンピューターが一覧表示されます。**フィルターの追加**をクリックすると、選択した実行をステータス別にフィルタリングします。

- **待機中** - はい (クライアントタスクの実行が計画されています)、いいえ (クライアントタスク実行が完了しました)。
- **前回のステータス** - ステータスなし **実行中** **完了** **失敗**

選択したコンピューター以外の結果のコンピューターは表示されません。フィルターを修正するか、オフにすると、最新のステータスに関係なく、すべてのコンピューターが表示されます。

また、さらにドリルダウンすることもできます。たとえば、**[履歴]**を選択して、**実行日時**、現在の**ステータス**、**進行状況**、**追跡メッセージ**(該当する場合)など、クライアントタスク実行の詳細を確認できます。**コンピューター名**または**コンピューターの説明**をクリックして、必要に応じてその他のアクションを実行するか、特定のクライアントの**コンピューター詳細**を表示します。複数のコンピューターでアクションを実行するには、チェックボックスを使用して、コンピューターを選択し、**アクション**ボタンをクリックします。

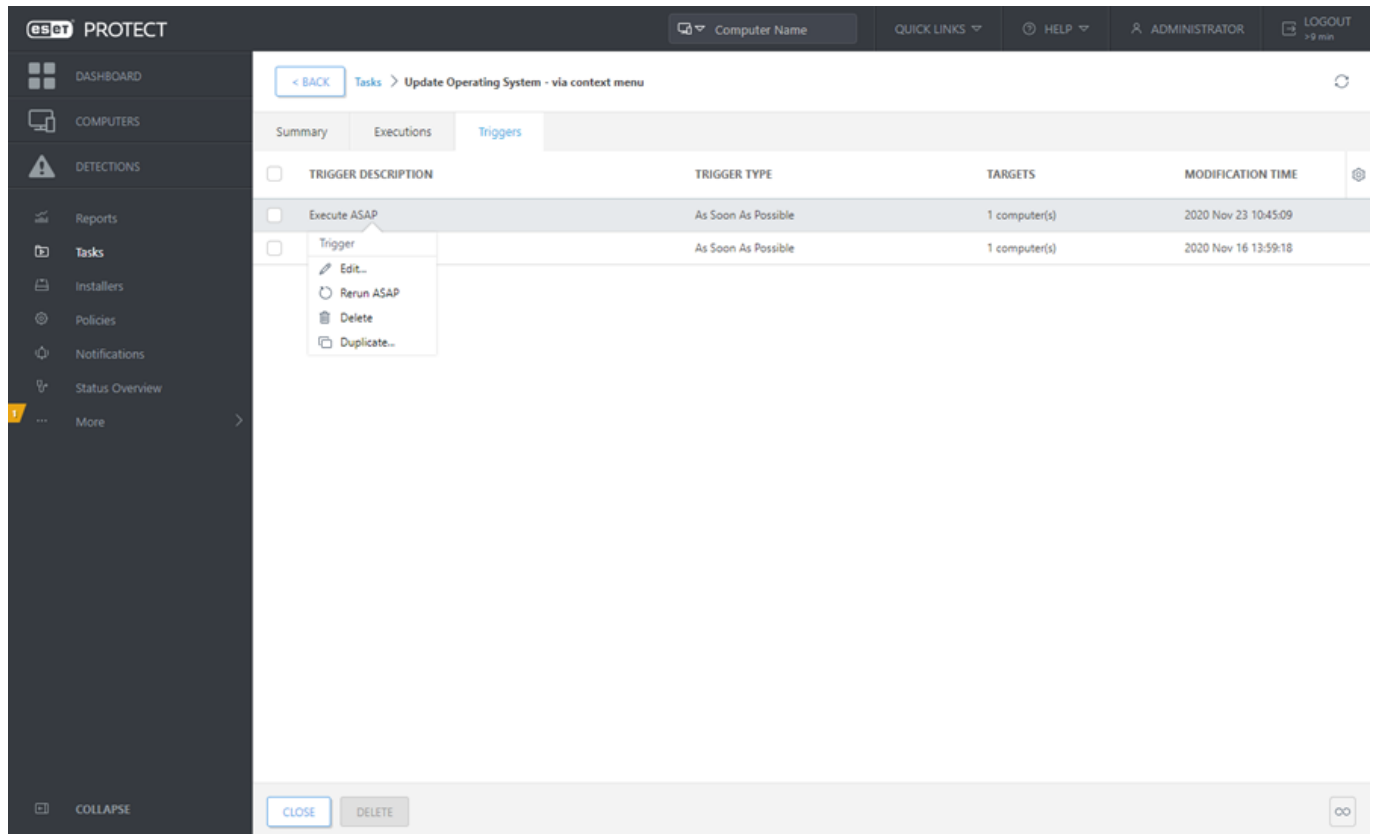


- 実行履歴テーブルにエントリがない場合は、**実行**フィルターの期間を長く設定してみてください。
- 古いESET製品をインストールするときには、クライアントタスクレポートが表示されます。管理された製品に配信されるタスク

トリガー

トリガータブは、クライアントタスクでのみ使用できます。選択したクライアントタスクのトリガーの一覧が表示されます。トリガーを管理するには、トリガーをクリックして、次の項目のいずれかを選択します。

編集	選択した トリガー を編集します。
すぐに再実行	既存の トリガー を修正せずにそのまま使用して、クライアントタスクを即時再実行します。
削除	選択したトリガーを完全に削除します。複数のトリガーを削除するには、左側のチェックボックスを選択して、 削除 ボタンをクリックします。
複製	選択したトリガーに基づいて、新しいトリガーが作成されます。重複するトリガーの新しい名前が必要です。



インストーラー

このセクションでは、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するためのエージェント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 PROTECT Webコンソールに保存され、必要に応じて[編集](#)および[再度ダウンロード](#)できます。

1. **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。

2.作成するインストーラーの種類を選択します:

- **エージェントおよびESETセキュリティ製品インストーラー** パッケージではESET ManagementエージェントおよびESET製品のポリシー設定ESET PROTECTサーバーホスト名とポート、親グループの選択機能など、詳細設定オプションを利用できます。

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](#)
- [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。

- **エージェントライブインストーラー** – このタイプのエージェント展開は、リモートおよびローカル展開オプションが適していない場合に使用できます。このような場合、電子メールでエージェントライブインストーラを配布し、ユーザーに展開させることができます。また、エージェントライブインストーラは、リムーバブルメディア(USBフラッシュドライブなど)から実行することもできます。

- **GPOまたは SCCM** スクリプト

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

インストーラーと権限

ユーザーは、ユーザーが**グループとコンピューター**および**保存されたインストーラー**の**書き込み**権限があるグループに含まれるインストーラーを作成または編集できます。

既に作成されたインストーラーをダウンロードするには、**グループとコンピューター**および**保存されたインストーラー**の**使用**権限が必要です。

- オールインワンインストーラー、GPOインストーラー、またはSCCMスクリプトを作成するときには、**[詳細]>[初期インストーラー設定]>[設定タイプ]**で選択されたポリシーの**使用**権限をユーザーに割り当てる必要があります。
- 静的グループのライセンスが指定される場合は、**ライセンスの使用**アクセス権をユーザーに割り当てる必要があります。
- i** • ユーザーがインストーラーを作成するときには、[証明書](#)を操作できます。証明書が含まれる静的グループへのアクセス権を持つ**証明書の使用**権限を割り当てる必要があります。ユーザーがESET Managementエージェントを展開する場合、実際のサーバー証明書が署名される**認証機関の使用**権限が必要です。証明書と認証局へのアクセスを分割する方法については、この[例](#)をお読みください。

ユーザーがインストーラーを作成できるようにする方法

管理者はユーザー *John* が *John's Group* の新しいインストーラーを作成または編集できるようにします。管理者は次の手順に従います。

1. 新しい **静的グループ** の *John's Group* を作成します。

2. 新しい **権限設定** を作成します。

a. *Permissions for John - Create Installers* という名前を付けます。

b. グループ *John's Group* を **静的グループ** セクションで追加します。

c. **機能** セクションで次の項目を選択します。

- 保存されたインストーラーの書き込み

- 証明書の使用

- グループとコンピューターの書き込み

d. **[完了]** をクリックして権限設定を保存します。

3. 新しい **権限設定** を作成します。

a. *Permissions for John - Certificates* という名前を付けます。

b. グループすべてを **静的グループ** セクションで追加します。

c. **[機能]** セクションで、 **証明書の使用** を選択します。

d. **[完了]** をクリックして権限設定を保存します。

これらの権限は完全 (作成および編集) インストーラー使用のための最低要件です。

4. 新規 **ユーザー** の作成

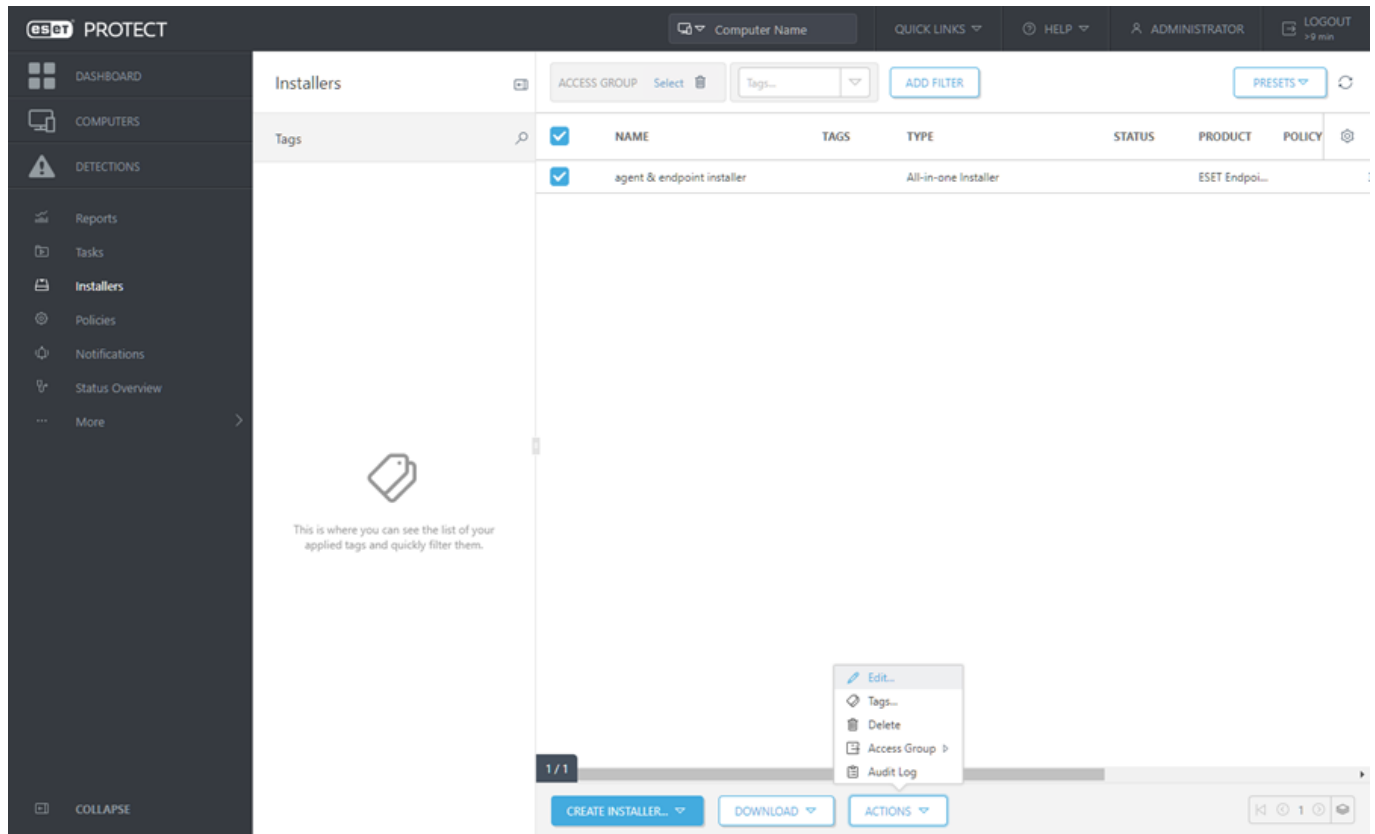
a. *John* という名前を付けます。

b. **基本** セクションで *John's Group* をホームグループとして選択します。

c. ユーザー *John* のパスワードを設定します。

d. **権限設定** セクションで、 *Permissions for John - Certificates* と *Permissions for John - Create Installers* を選択します。

e. **[完了]** をクリックしてユーザーを保存します。



インストーラーメニューからインストーラーをダウンロードする方法

1. [インストーラー]をクリックします。
2. ダウンロードするインストーラーの横のチェックボックスをオンにします。
3. ダウンロードをクリックし、正しいバージョンのインストールパッケージを選択します。

インストーラーメニューからインストーラーを編集する方法

1. [インストーラー]をクリックします。
2. 編集するインストーラーの横のチェックボックスをオンにします。
3. [アクション] > [編集]をクリックして、インストーラーパッケージを修正します。

ポリシー

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、特定の構成をプッシュするために使用されます。これにより、各クライアントのESET製品を手動で構成せずに済みます。個別の[コンピューター](#)とグループ([静的](#)と[動的](#))に直接適用できます。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。

ポリシーと権限

ユーザーにはポリシーを作成して割り当てるための十分な[権限](#)が必要です。特定のポリシーアクションに必要な権限:

- ポリシーと設定のリストを読むには、ユーザーは**読み取り**権限が必要です。
- ポリシーをターゲットに割り当てるには、ユーザーは**使用**権限が必要です。
- ポリシーを作成、修正または編集するには、ユーザーに**書き込み**権限が必要です。

アクセス権の詳細については、[権限の一覧](#)を参照してください。

ロックされた🔒 (編集できない) ポリシー (特定のビルトインポリシー ([自動アップデート](#) ポリシーや ESET Dynamic Threat Defense ポリシーなど)、またはユーザーに**読み取り**権限がありますが、**書き込み**権限ではないポリシーの横にはロックアイコンがあります。


- ユーザー *John* が自分が作成したポリシーのみを読み取る必要がある場合、ポリシーの**読み取り**権限が必要です。
- ✓ ユーザー *John* が特定のポリシーをコンピューターに割り当てる場合、ポリシーの**使用**権限と**グループとコンピューターの使用**権限が必要です。
- *John* にポリシーのフルアクセスを許可するには、管理者はポリシーの**書き込み**権限を設定する必要があります。

ポリシー適用

ポリシーは、静的グループの配置順に適用されます。これは、動的グループの場合には該当せず、動的グループでは子の動的グループが最初に網羅されます。これにより、グループツリーの最上位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提供できます。[フラグ](#)を使用すると、ツリーの上位にあるグループにアクセスできる ESET PROTECT ユーザーは、下位のグループのポリシーを上書きできます。アルゴリズムの詳細については、「[ポリシーをクライアントに適用する方法](#)」を参照してください。

ポリシー削除ルール

ポリシーを適用し、後で削除するときには、ポリシーを削除しても、クライアントコンピューターの結果の構成は、管理対象のコンピューターにインストールされた ESET セキュリティ製品のバージョンによって異なります。

- ESET セキュリティ製品バージョン 6 以前: ポリシーが削除されると、クライアントコンピューターの構成が自動的に元の設定に戻りません。クライアントに適用された最後のポリシーに従って、構成が維持されます。コンピューターが、コンピューターの設定を変更する特定のポリシーが適用された [動的グループ](#) のメンバーになった場合も、同じことが発生します。コンピューターが動的グループから削除されても、設定は保持されます。このため、既定の設定でポリシーを作成し、ルートグループ (**すべて**) に割り当て、このような状況では既定の設定に戻すことをお勧めします。この方法では、コンピューターが、設定を変更した動的グループから解除されても、既定の設定を使用できます。
- ESET セキュリティ製品バージョン 7 以降: ポリシーが削除されると、構成は、クライアントに適用された以前のポリシーに自動的に戻されます。コンピューターが、特定のポリシー設定が適用されている動的グループから外れると、これらのポリシー設定がコンピューターから削除されます。
 **未適用** フラグは、個別のポリシー設定を、クライアントコンピューターの既定の状態に変更します。

ポリシーのマージ

通常、クライアントに適用されたポリシーは、複数のポリシーが 1 つの最終ポリシーに [マージ](#) されたものです。

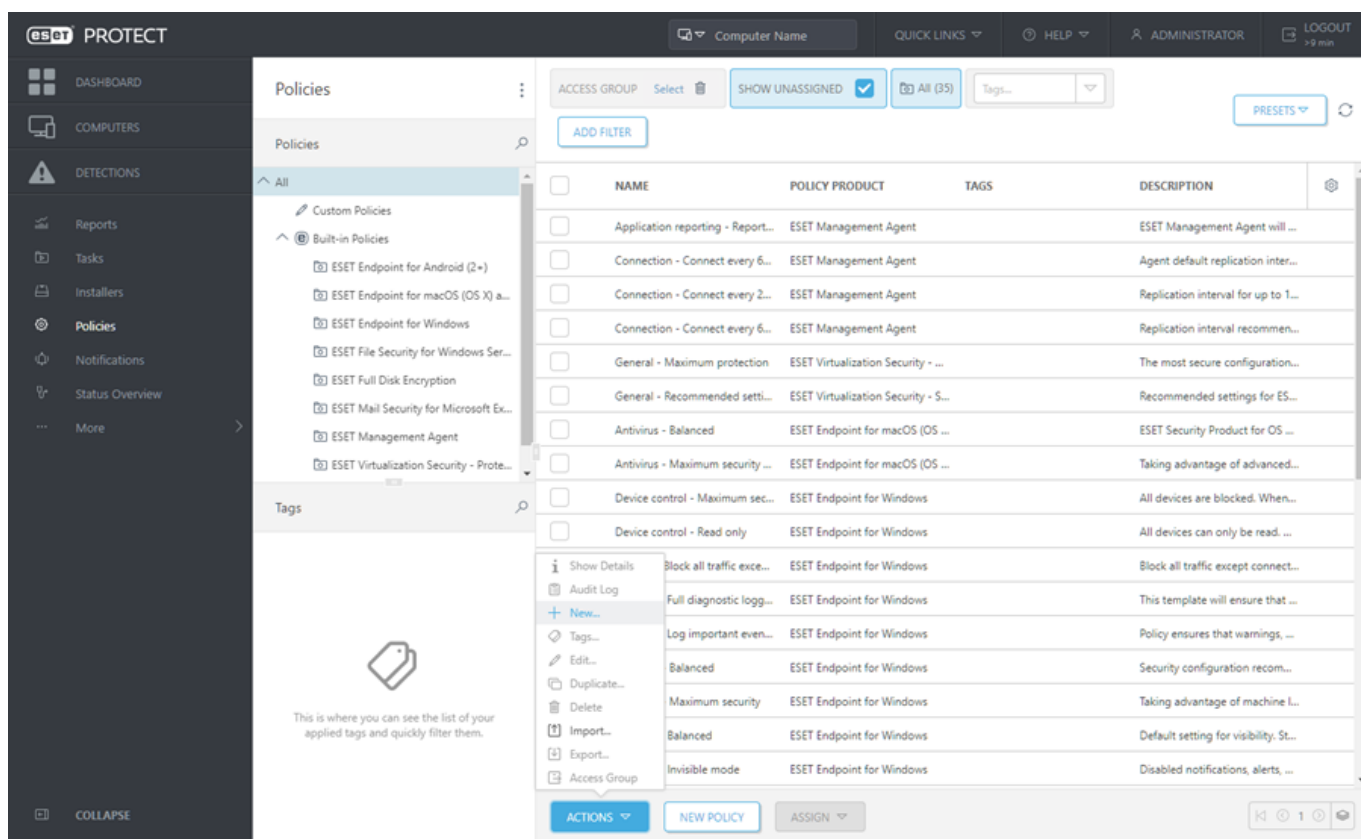


グループツリーの上位にあるグループには、より汎用的なポリシー(アップデートサーバーなど)を割り当てておくことをお勧めします。より特定のポリシー(デバイスコントロール設定など)はグループツリーの下位に割り当てられます。通常、マージ時に下位のポリシーが上位の設定を上書きします([ポリシーフラグ](#)で定義されている場合を除く)。

ポリシーウィザード

ポリシーはESET製品別にグループ化/分類されます。ビルトインポリシーには、定義済みのポリシーと、手動で作成したすべてのポリシーの**カスタムポリシー**リストカテゴリが含まれます。

ポリシーを構成して、製品GUIの詳細設定ウィンドウを使用する場合と同様に、ESET製品を構成します。Active Directoryのポリシーとは異なりESET PROTECTポリシーはスクリプトまたはコマンドを実行できません。詳細設定で入力して項目を検索します(HIPSなど)。すべてのHIPS設定が表示されます。右上端の(?)アイコンをクリックすると、特定の設定のオンラインヘルプページが表示されます。



フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

新しいポリシーの作成

1. **アクション > 新規**をクリックします。
2. **名前**と**説明**(オプション)などのポリシーに関する基本情報を入力します。 **タグを選択**をクリッ

クして、[タグを割り当て](#)ます。

3.[設定]セクションで正しい製品を選択します。

4.[フラグ](#)を使用して、ポリシーによって処理される設定を追加します。


5.このポリシーを受信するクライアントを指定します。**[割り当て]**をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。ポリシーを適用するコンピューターを選択し、**OK**をクリックします。


6.このポリシーの設定を確認し、**[完了]**をクリックします。


フラグ

ポリシーをマージするときには、ポリシーフラグを使用して動作を変更できます。フラグは、ポリシーによって設定が処理される方法を定義します。

各設定に対して、次のフラグのいずれかを選択できます。



 **未適用** – このフラグの設定はポリシーによって設定されていません。この設定は適用されないため、他のポリシーによって後から変更できます。

 **適用** – このフラグの設定がクライアントに送信されます。ただし、ポリシーのマージの場合には、後のポリシーによって上書きされます。ポリシーがクライアントコンピュータに適用され、特定の設定にこのフラグがある場合、クライアントでローカルに構成されていた内容に関係なく、この設定が変更されます。この設定は適用されないため、他のポリシーによって後から変更できます。



 **強制** – 強制フラグの設定には優先度があり、後のポリシーに強制フラグがある場合でも、後のポリシーによって上書きできません。マージ中に後のポリシーでこの設定が変更されないことを保証します。

操作をより簡単にするために、すべてのルールがカウントされます。特定のセクションで定義したルール数が自動的に表示されます。また、左側のツリーのカテゴリ名の横にも数字が表示されます。これは、すべてのセクションのルールの合計数を示します。このように、設定またはルールが数が定義されている場所と、定義済みの設定またはルール数が簡単にわかります。

また、次の候補を使用して、ポリシーを簡単に編集できます。

-  を使用して、現在のセクションのすべての項目に適用フラグを設定します。
-  を使用して、現在のセクションの項目に適用されたすべてのルールを削除します。

ESETセキュリティ製品バージョン7以降:

  **未適用**フラグは、個別のポリシー設定を、クライアントコンピューターの既定の状態に変更します。

管理者によってユーザーがすべてのポリシーを表示できるようにする方法

管理者はユーザー *John* がホームグループのポリシーを作成または編集できるようにし、*John* が管理者によって作成されるポリシーを表示できるようにします。管理者が作成したポリシーには **強制** フラグがあります。ユーザー *John* はすべてのポリシーを表示できますが、管理者が作成したポリシーを編集できません。静的グループすべてへのアクセス権がある **ポリシーの読み取り** 権限が設定されているためです。ユーザー *John* はホームグループ *San Diego* のポリシーを作成または編集できます。

管理者は次の手順に従います。

環境の作成

1. 新しい **静的グループ** の *San Diego* を作成します。
2. 静的グループすべてへのアクセスと **ポリシーの読み取り** 権限がある新しい **権限設定** の *Policy - All John* を作成します。
3. 静的グループ *San Diego* へのアクセスと **グループとコンピューターとポリシーの書き込み** 権限がある新しい **権限設定** の *Policy John* を作成します。この権限により、*John* はホームグループ *San Diego* のポリシーを作成または編集できます。
4. 新しい **ユーザー** *John* を作成し、 **権限設定** セクションで、*Policy - All John* と *Policy John* を選択します。

ポリシーの作成

5. 新しい **ポリシー** *All- Enable Firewall* を作成し、 **設定** セクションを展開し、 **ESET Endpoint for Windows** を選択して、 **パーソナルファイアウォール > 基本** に移動して、 **強制** フラグですべての設定を適用します。 **割り当て** セクションを展開し、静的グループすべてを選択します。
6. 新しい **ポリシー** *John Group- Enable Firewall* を作成し、 **設定** セクションを展開し、 **ESET Endpoint for Windows** を選択して、 **ネットワーク保護 > ファイアウォール > 基本** に移動して、 **適用** フラグですべての設定を適用します。 **割り当て** セクションを展開し、静的グループ *San Diego* を選択します。

結果

管理者が作成したポリシーは、グループすべてに割り当てられているため、最初に適用されます。**強制** フラグがある設定は優先され、後のポリシーで上書きできません。次に、ユーザー *John* が作成したポリシーが適用されます。

詳細 > グループ > San Diego に移動し、コンピューターをクリックして、 **詳細の表示** を選択します。**設定 > 適用されたポリシー** は、最終的なポリシーアプリケーション順序です。

△	POLICY ORDER	POLICY PRODUCT	POLICY NAME
1 (applied first)		ESET Endpoint for Windows	Antivirus - Balanced
2		ESET Management Agent	Replicate every 10s

最初のポリシーは管理者によって作成され、次のポリシーは *John* が作成します。

ポリシーの管理

ポリシーはESET製品別にグループ化/分類されます。**ビルトインポリシー**には、定義済みのポリシーと、手動で作成または修正したすべてのポリシーのカスタムポリシーリストカテゴリが含まれます。

ポリシーで使用可能なアクション:

i 詳細を表示	ポリシー詳細を表示します。
目 監査ログ	選択した項目の 監査ログ を表示します。
+ 新規	新しいポリシーを作成します。
タグ	タグ を編集します (割り当て、割り当て解除、作成、削除)。
編集	既存のポリシーを修正します。

複製	選択した既存のポリシーに基づいて新しいポリシーを作成します。ポリシーの複製には新しい名前が必要です。
割り当ての変更	グループまたはクライアントにポリシーを割り当てます。
削除	ポリシーを削除します。 ポリシー削除ルール も参照してください。
インポート	[ポリシー]>[インポート]をクリックしてから、[ファイルの選択]をクリックして、インポートするファイルを参照します。ESET PROTECT Web コンソールからエクスポートされたポリシーを含む .dat ファイルのみをインポートできます。ESET セキュリティからエクスポートされたポリシーを含む .xml ファイルのみはインポートできません。インポートされたポリシーは、 カスタムポリシー の下に適用されます。
エクスポート	リストからエクスポートするポリシーの横にあるチェックボックスを選択し、 アクション>エクスポート をクリックします。ポリシーは .dat ファイルとしてエクスポートされます。選択したカテゴリからすべてのポリシーをエクスポートするには、テーブルヘッダーのチェックボックスを選択します。
アクセスグループ	別のグループにポリシーを移動します。

ポリシーがクライアントに適用される方法

グループとコンピューターには複数のポリシーを割り当てることができます。さらに、コンピューターを深いネストされたグループに配置し、親には固有のポリシーを割り当てることができます。

ポリシーの適用で最も重要なのは順序です。これはグループの順序とグループに割り当てられたポリシーの順序に基づきます。

選択したコンピューターに適用されるすべてのポリシーを表示するには、コンピューター詳細で[適用されたポリシー](#)を参照してください。

次の手順に従い、クライアントで有効なポリシーを決定します。

1. [クライアントが配置されているグループの順序を確認](#)
2. [割り当てられたポリシーでグループを置換](#)
3. [ポリシーを統合して最終設定を取得](#)

グループの順序

ポリシーはグループに割り当てることができ、**特定の順序で適用**されます。以下のルールは、**ポリシーがクライアントに適用される順序を決定**します。

ルール1: 静的グループはルート静的グループ「すべて」から走査されます。

ルール2: すべてのレベルで、そのレベルの静的グループはまずツリーの表示順に走査されます。これは、横型検索と言います。

ルール3: 特定のレベルのすべての静的グループが考慮された後、動的グループが走査されます。

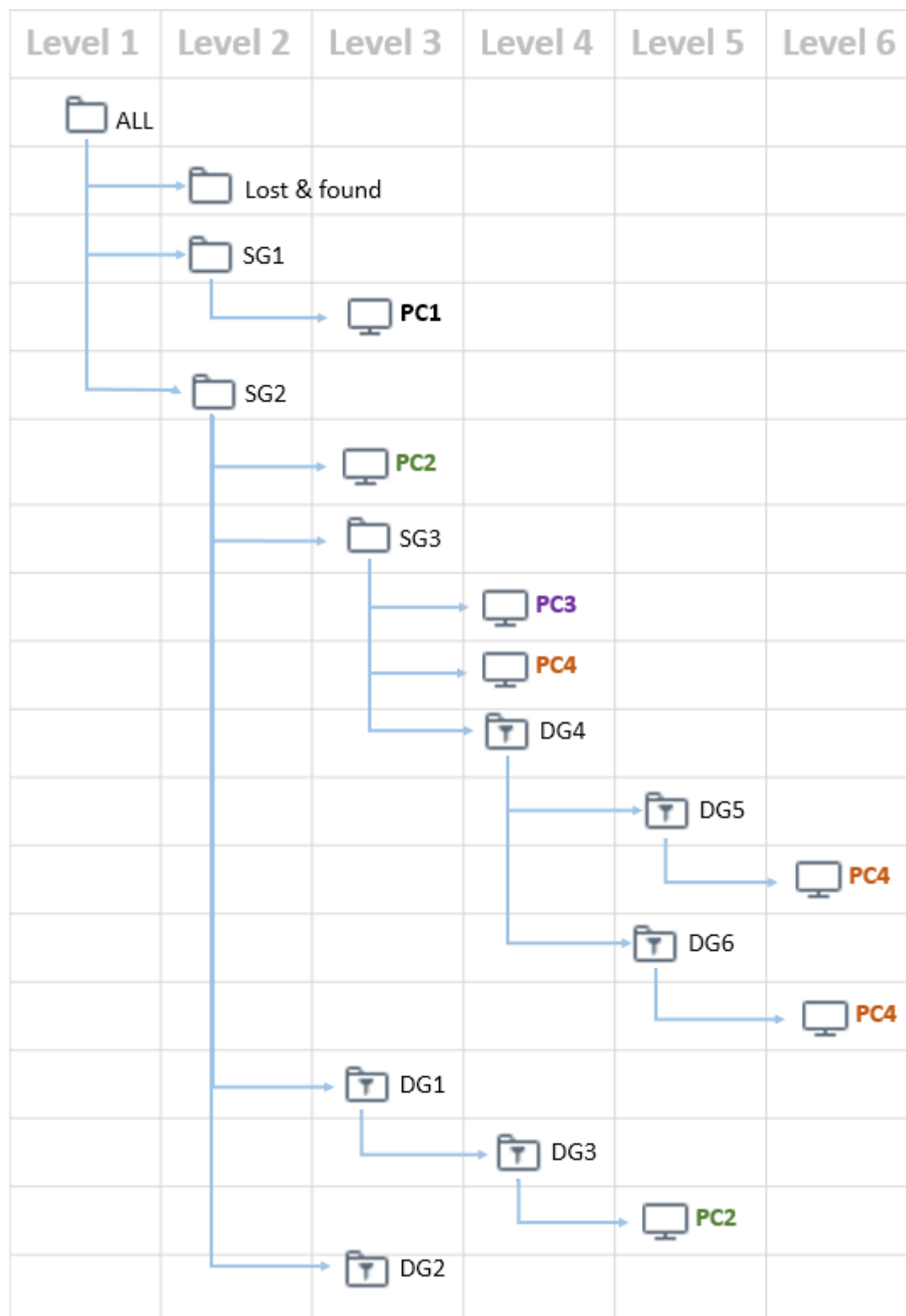
ルール4: すべての動的グループで、すべての子がリストの表示順に走査されます。

ルール5: 任意のレベルの動的グループで、すべての子がリストされ、子が検索されます。子がなくなると、親レベルの次の動的グループがリストに入ります。これは縦型検索と言います。

ルール6: コンピューターで走査が終了します。



ポリシーはコンピューターに適用されます。つまり、ポリシーを適用するコンピューターで走査が終了します。



上記のルールを使用すると、個別のコンピュータにポリシーが適用される順序は次のとおりです。

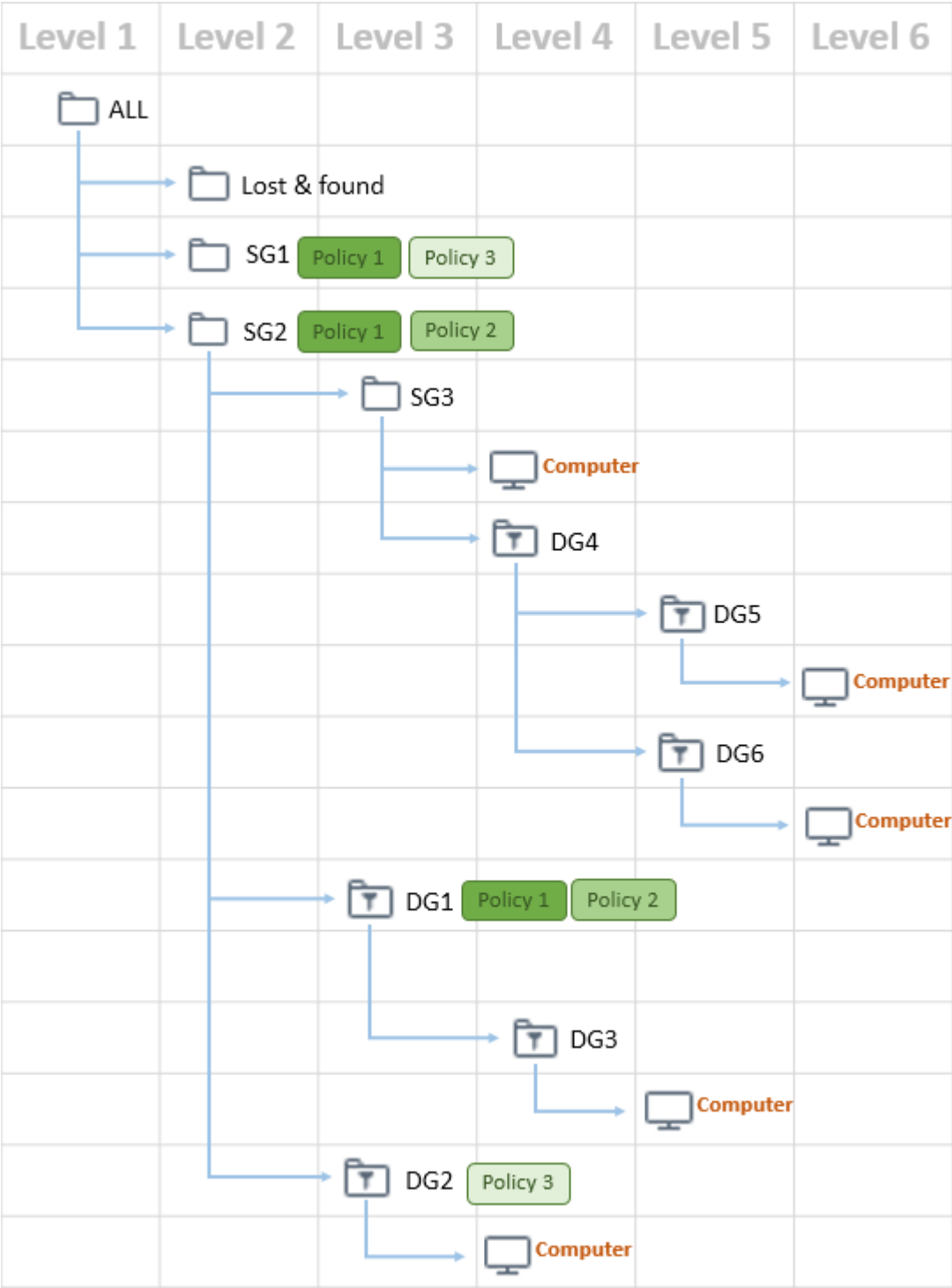
PC1:	PC2:	PC3:	PC4:
1.ALL	1.ALL	1.ALL	1.ALL
2.SG1	2.SG2	2.SG2	2.SG2
3.PC1	3.DG1	3.SG3	3.SG3
	4.DG3	4.PC3	4.DG4
	5.PC2		5.DG5
			6.DG6
			7.PC4

ポリシーの列挙

グループの順序を把握したら、次に、グループに割り当てられたポリシーで各グループを置換します。ポリシーは、グループに割り当てられた順序で一覧表示されます。複数のポリシーが割り当てられたグループのポリシーの優先度を編集できます。各ポリシーは1つの製品(ESET ManagementエージェントとEESなど)だけを構成します。

i ポリシーがないグループはリストから削除されます。

静的グループと動的グループの両方に3つのポリシーが適用されています(次の図を参照)。



ポリシーがコンピューターに適用される順序。

次の一覧は、適用されるグループとポリシーを示します。

- 1.すべて -> 削除、ここにはポリシーなし
- 2.SG 2 -> ポリシー1、ポリシー2
- 3.SG 3 -> ポリシーがないため削除
- 4.DG 1 -> ポリシー1、ポリシー2
- 5.DG 3 -> ポリシーがないため削除
- 6.DG 2 -> ポリシー3
- 7.DG 4 -> ポリシーがないため削除
- 8.DG 5 -> ポリシーがないため削除
- 9.DG 6 -> ポリシーがないため削除
10. コンピューター -> ポリシーがないため削除

ポリシーの最終リスト：

- 1.ポリシー1
- 2.ポリシー2
- 3.ポリシー1
- 4.ポリシー2
- 5.ポリシー3

ポリシーのマージ

別のポリシーが既に適用されているESETセキュリティ製品にポリシーを適用すると、重複するポリシー設定がマージされます。ポリシーは1つずつマージされます。ポリシーをマージするときの原則は、後のポリシーによって、前のポリシーで構成された設定が必ず置換されるということです。この動作を変更するには、[ポリシーフラグ](#) (すべての設定で使用可能)を使用できます。一部の設定には設定できる別の[ルール](#) (置換/後に追加/前に追加)があります。

[グループ](#) (階層)の構造とポリシーの順序によって、ポリシーのマージ方法が決まります。任意の2つのポリシーをマージしても、順序によっては結果が異なる場合があります。



ポリシーを作成するときには、一部の設定には設定できる追加ルールがあります。これらのルールでは、さまざまなポリシーで同じ設定を配置できます。

- **置換**: ポリシーのマージで使用する既定のルール。前のポリシーで設定された設定を置換します。

- **最後に追加:**複数のポリシーで同じ設定を適用するときに、このルールを設定を後に追加できます。この設定は、ポリシーのマージで作成されたリストの最後に配置されます。
- **前に追加:**複数のポリシーで同じ設定を適用するときに、このルールを設定を前に追加できます。この設定は、ポリシーのマージで作成されたリストの先頭に配置されます。

ローカルリストとリモートリストのマージ

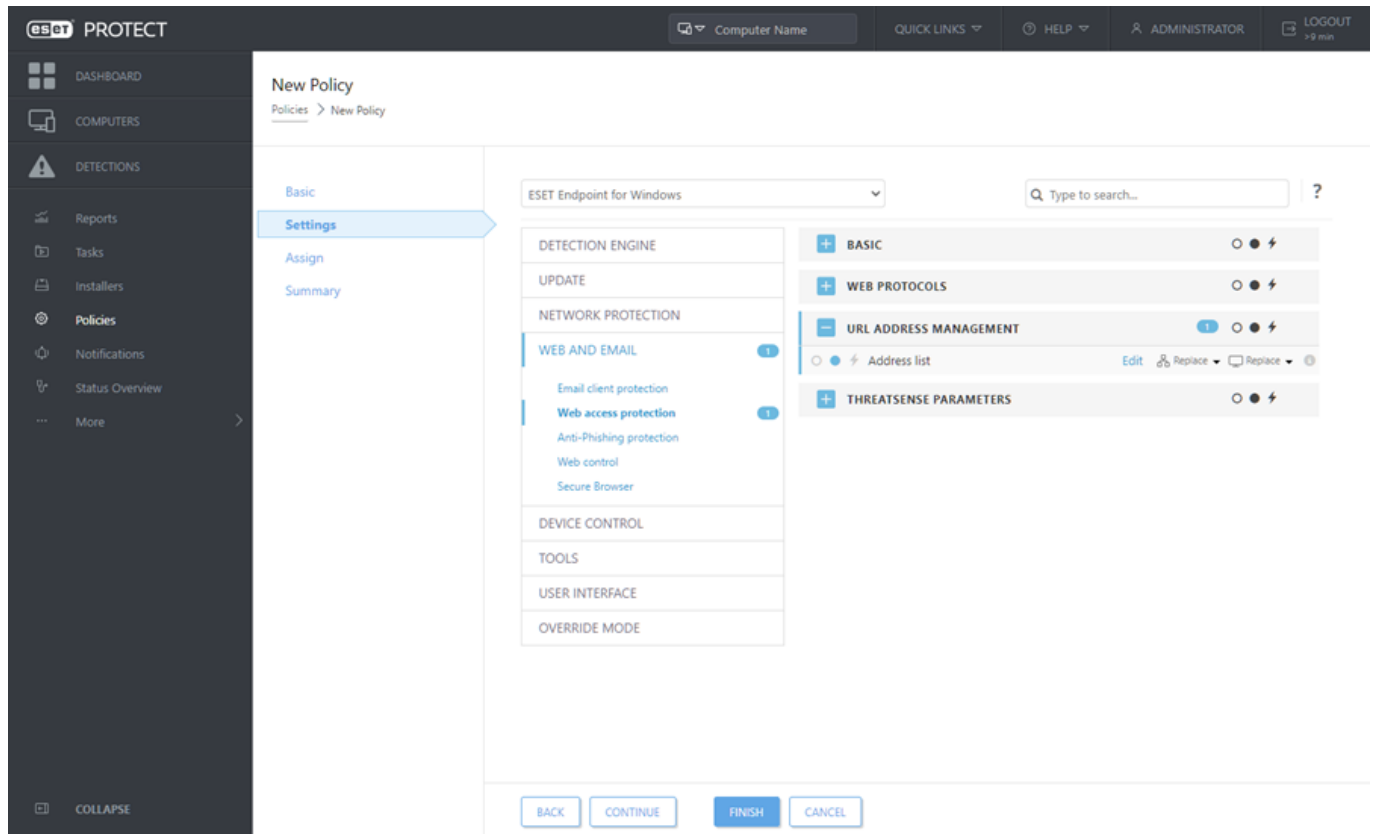
最近のESETセキュリティ製品(以下の表のサポートされたバージョンを参照)は、ローカル設定とリモートポリシーのマージを新しい方法でサポートします。設定がリスト(Webサイトのリストなど)で、ポリシーが既存のローカル設定と競合している場合、リモートポリシーが優先されます。ローカルリストとリモートリストを結合する方法を選択できます。次のマージルールを選択できます。

-  リモートポリシーの設定のマージ。
-  リモートおよびローカルポリシーのマージ - ローカル設定を結果のリモートポリシーでマージ。

オプションは上記と同じです。置換^②後ろに追加^②前に追加

ローカルリストとリモートリストをサポートする製品の一覧:

ESETセキュリティ製品	バージョン
ESET Endpoint for Windows	7+
ESET Server Security for Windows	8+
ESET File Security for Linux	8.1+
ESET Mail Security for Microsoft Exchange	6+
ESET File Security for Windows Server	6+
ESET Mail Security for IBM Domino	6+
ESET Security for Kerio	6+
ESET Security for Microsoft SharePoint Server	6+



ESETセキュリティ製品バージョン7以降でのポリシー削除

ポリシーが削除されると、構成は、クライアントに適用された以前のポリシーに自動的に戻されます。

未適用フラグは、個別のポリシー設定を、クライアントコンピューターの既定の状態に変更します。

ポリシーの統合シナリオの例

この例の内容:

- ESET Endpointセキュリティ製品にポリシー設定を適用する手順
- フラグとルールを適用するときにポリシーをマージする方法

管理者が次のことをしたい場合:

- サンディエゴ事業所がWebサイト www.forbidden.uk、www.deny-access.com、www.forbidden-websites.uk、www.forbidden-website.comにアクセスすることを拒否する
- マーケティング部がWebサイト www.forbidden.uk、www.deny-access.comにアクセスすることを許可する

Edit list ? □ ×

Address list type: Blocked

List name: List of blocked addresses

List description:

List active: ☒

Notify when applying: ☐

Logging severity: e ≥ 6.6 Information

Address list	
www.forbidden.uk	
www.deny-access.com	
www.forbidden-websites.uk	
www.forbidden-website.com	

3. [ポリシー]に移動し、次のように新しいポリシーを作成します。

i. *Marketing department*

ii. [設定]を展開し、[ESET Endpoint for Windows]を選択します。

iii. [Webとメール] > [Webアクセス保護] > [URLアドレス管理]に移動します。

iv. ボタンポリシーの適用をクリックし、[\[ルール追加\]](#)を選択してから、**編集**をクリックして、アドレスリストを編集します。[ルールを最後に追加]により、ポリシーのマージ時にアドレスリストが最後に配置されます。

v. [許可されたアドレスのリスト] > [編集]を選択します。

vi. 次のWebアドレスを追加します。www.forbidden.uk@www.deny-access.com。許可されたアドレスのリストとアドレスリストを保存します。

vii. [割り当て]を展開し、ポリシーを *Marketing department*に割り当てます。

viii. [完了]をクリックしてポリシーを保存します。

このポリシーは *Marketing department*に適用され、以下のWebサイトへのアクセスを許可します。

Edit list ? □ ×

Address list type: Allowed

List name: List of allowed addresses

List description:

List active: ☒

Notify when applying: ☐

Logging severity: ☒ ≥ 6.6 Diagnostic

Address list

www.forbidden.uk

www.deny-access.com

4.最後のポリシーには、*San Diego office*と*Marketing Department*とに適用される両方のポリシーが含まれます。エンドポイントセキュリティ製品を開き、[設定] > [Webとメール] > [詳細設定]に移動し、[Webとメール]タブ > [Webアクセス保護]を選択して、[URLアドレス管理]を展開します。最終エンドポイント製品設定が表示されます。

Advanced setup - ESET Endpoint Security — □ ×

Address list ?

List name	Address types	List description
List of allowed addresses	Allowed	
List of blocked addresses	Blocked	
List of addresses excluded from content scan	Found malware is ignored	

Add View Delete

Add a wildcard (*) to the list of blocked addresses to block all URLs except those included in a list of allowed addresses.

Show merged rules

Show merged rules

Show policy rules

Show local rules

OK Cancel

最終設定には次の内容が含まれます。

1.San Diego officeポリシーのアドレスリスト

2.Marketing departmentポリシーのアドレスリスト

ESET PROTECTからの製品の構成

ポリシーを構成して、製品GUIの詳細設定ウィンドウを使用する場合と同様に、ESET製品を構成できます。Active Directoryのポリシーとは異なりESET PROTECTポリシーはスクリプトまたはコマンドを実行できません。

バージョン6以降のESET製品の場合、特定のステータスを設定し、クライアントまたはWebコンソールで報告できます。これはv6製品ポリシーの、**ユーザーインターフェイス > ユーザーインターフェイス要素 > ステータス**で設定できます。

- **表示** – ステータスはクライアントGUIで報告されます
- **送信** – ステータスはESET PROTECTに報告されます

ESET製品を設定するためのポリシー使用の例:

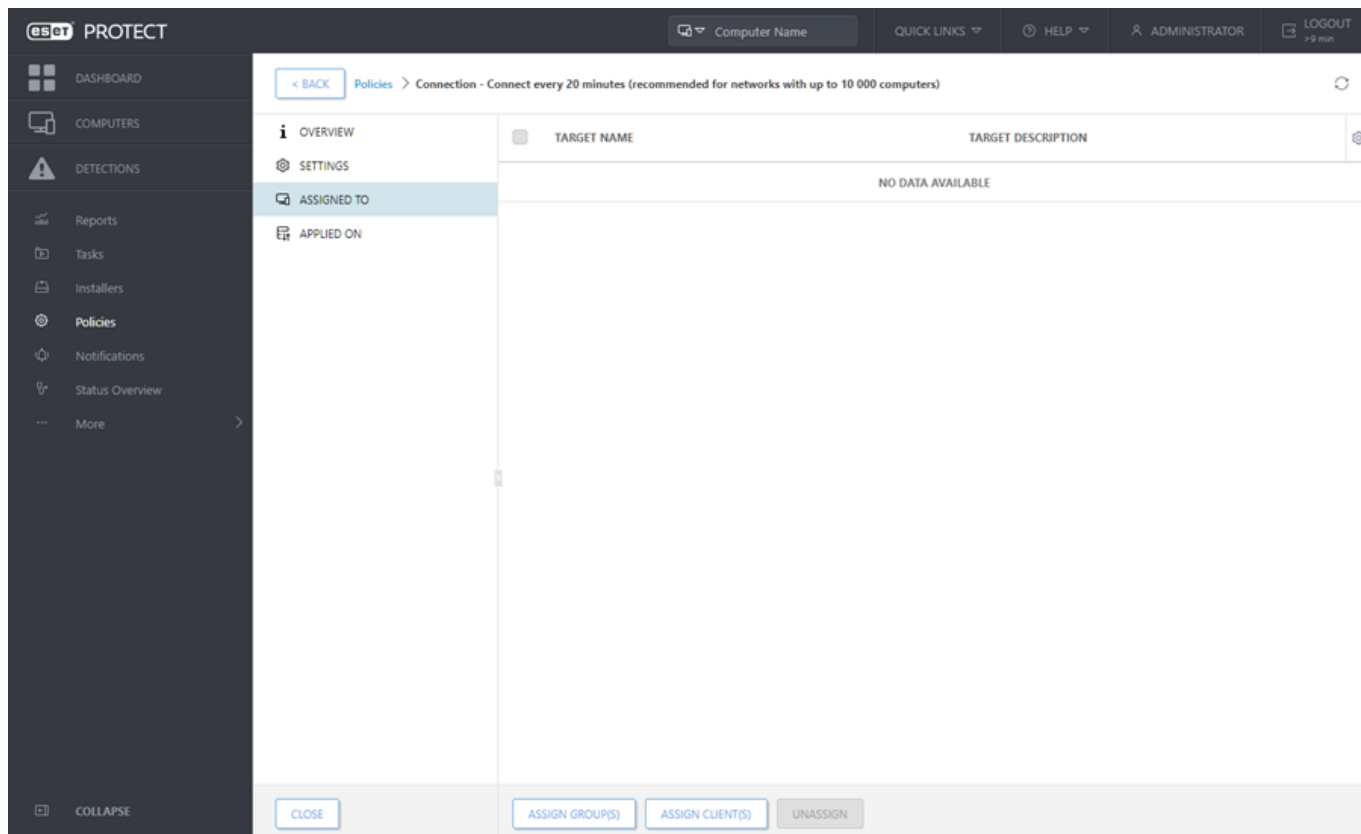
- [ESET Management エージェントポリシー設定](#)
- [ESET Rogue Detection Sensor ポリシー設定](#)
- [iOS MDMのポリシーの作成 - Exchange ActiveSyncアカウント](#)
- [MDCのポリシーを作成してiOS登録でAPNSを有効にする](#)

グループへのポリシーの割り当て

ポリシーが作成された後、**静的**または**動的**グループに割り当てることができます。ポリシーは2つの方法で割り当てることができます。

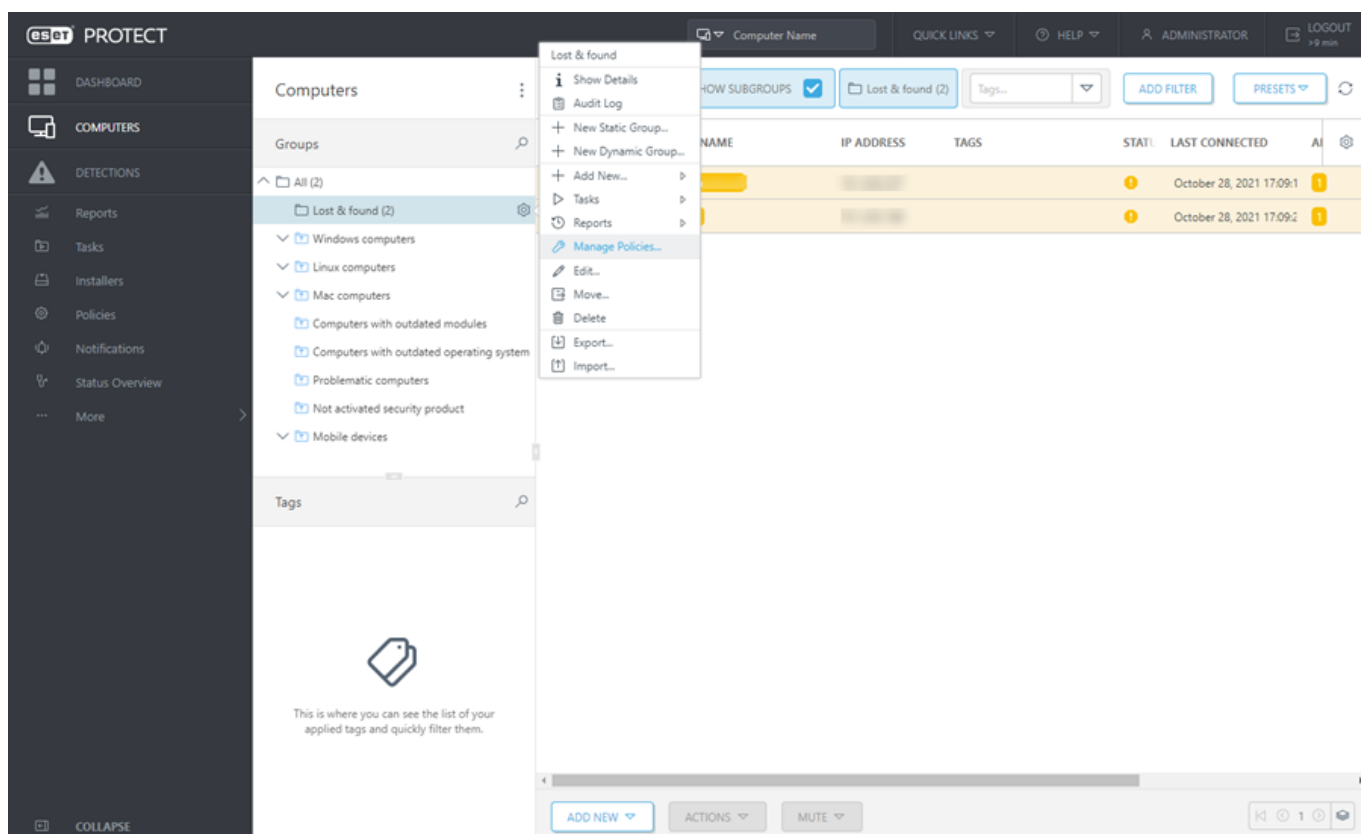
方法I.

ポリシーの下、**アクション > 詳細を表示 > 割り当て先 > グループの割り当て**をクリックします。リスト(その他のグループを選択できます)静的または動的グループを選択し、**[OK]**をクリックします。



方法II.

1. コンピューターをクリックし、グループ名の横の歯車アイコンをクリックして、ポリシーの管理を選択します。



2. ポリシーアプリケーション順序ウィンドウで、ポリシーの追加をクリックします。

3. このグループに割り当てるポリシーの横にあるチェックボックスをオンにし、**OK**をクリックします。

4. **[閉じる]**をクリックします

特定のグループに割り当てられたポリシーを確認するには、グループを選択し、**ポリシータブ**をクリックして、グループに割り当てられたポリシーのリストを表示します。

特定のポリシーに割り当てられたグループを表示するには、ポリシーを選択し、**詳細を表示 > 割り当て先**を表示します。

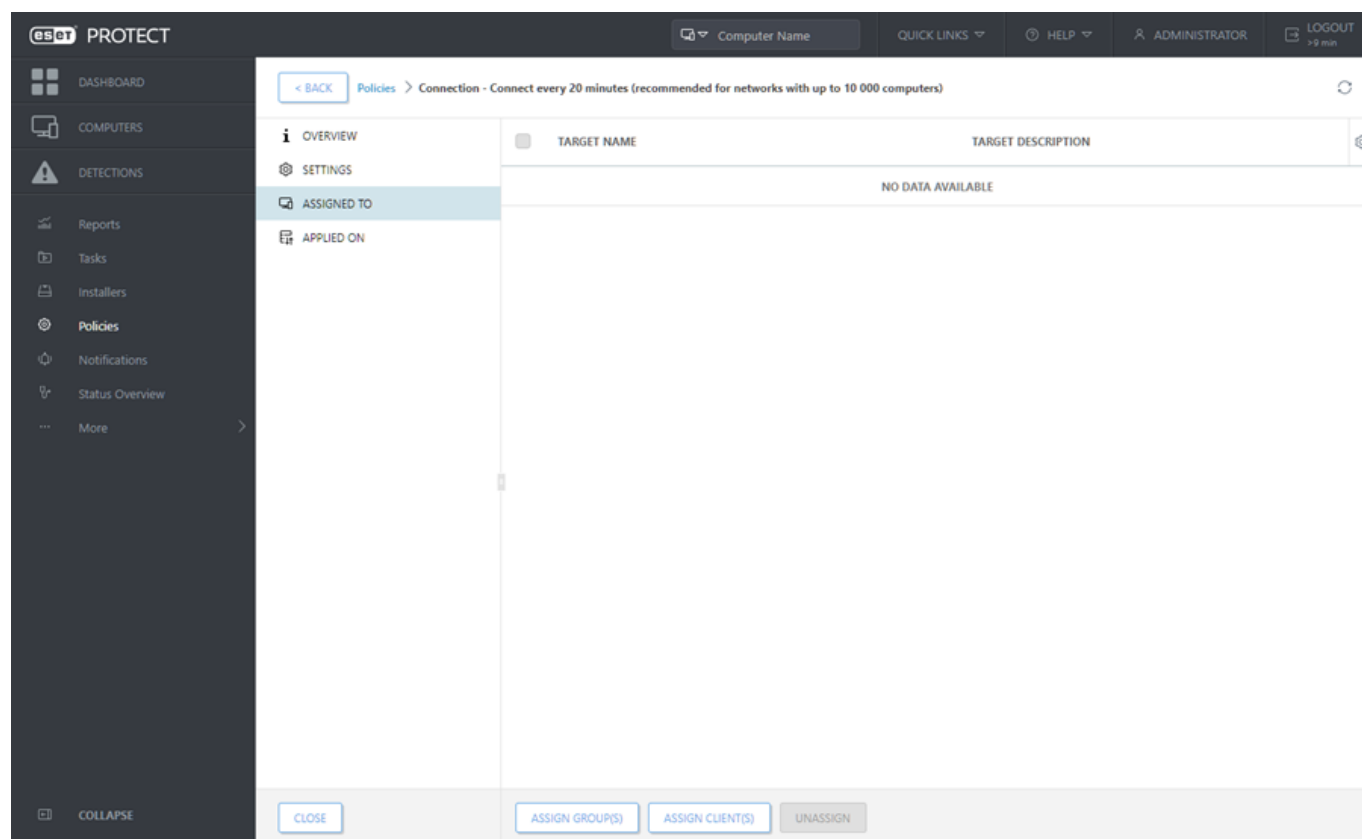
i ポリシーの詳細については、[ポリシー](#)の章を参照してください。

クライアントへのポリシーの割り当て

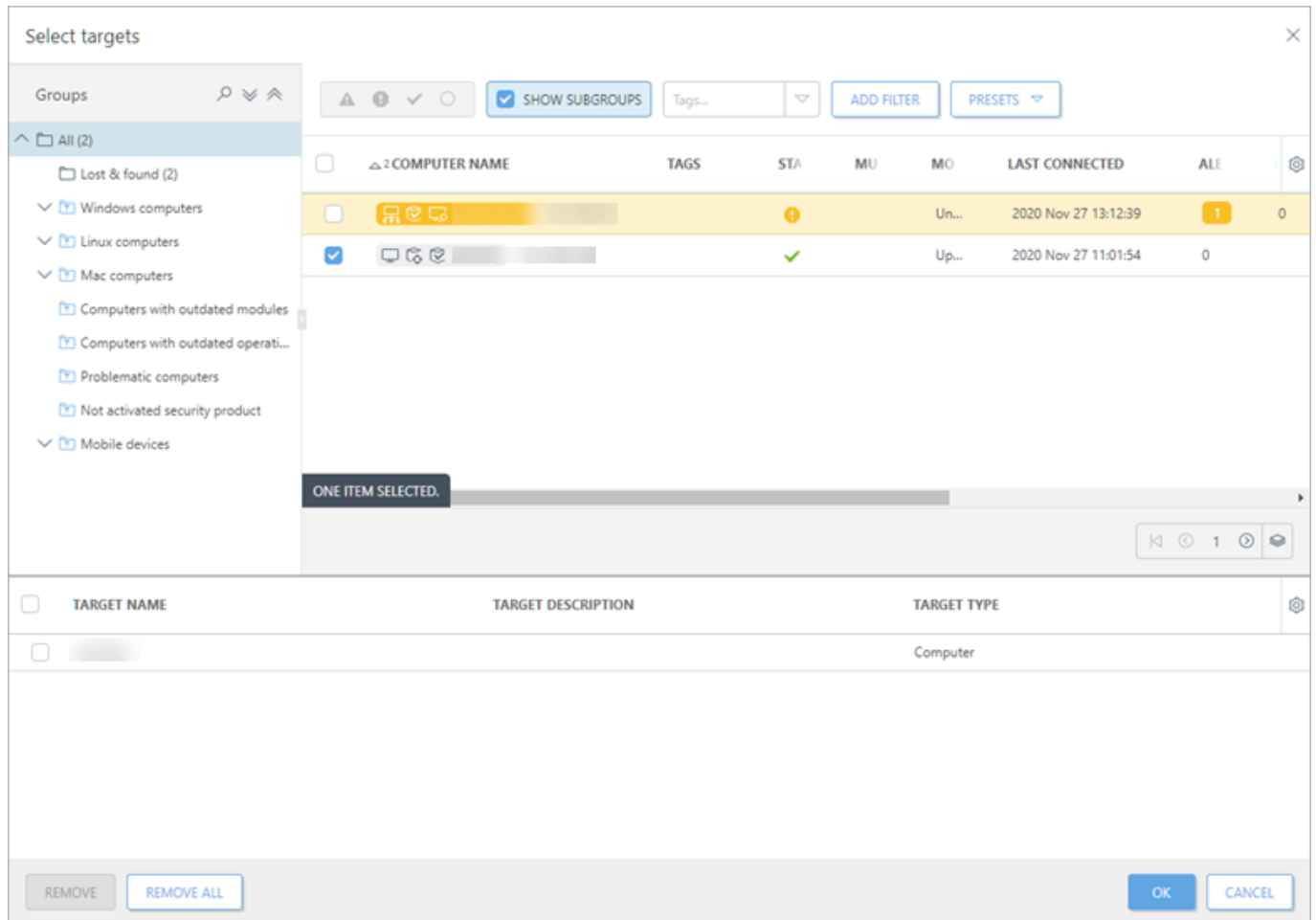
クライアントワークステーションにポリシーを割り当てるには、**ポリシー**をクリックし、**アクション > 詳細を表示 > 割り当て先 > クライアントの割り当て**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、**Webコンソール**の速度低下を防止します。
多数のコンピューターを選択すると**Webコンソール**に警告が表示されます。



ターゲットクライアントコンピューターを選択し、**[OK]**をクリックします。選択したすべてのコンピューターにポリシーが割り当てられます。



特定のポリシーに割り当てられたクライアントを表示するには、ポリシーを選択し、最初のタブ**割り当て先**を表示します。

上書きモードを使用する方法

Windows用のESETEndpoint製品(バージョン6.5以上)がコンピューターにインストールされている場合は、上書き機能を使用できます。上書きモードでは、設定が適用されたポリシーがある場合でも、クライアントコンピューターレベルで、インストールされたESET製品の設定を変更できます。上書きモードは、ADユーザーで有効にするか、パスワードで保護できます。この機能は、1回で4時間を超えると有効にできません。

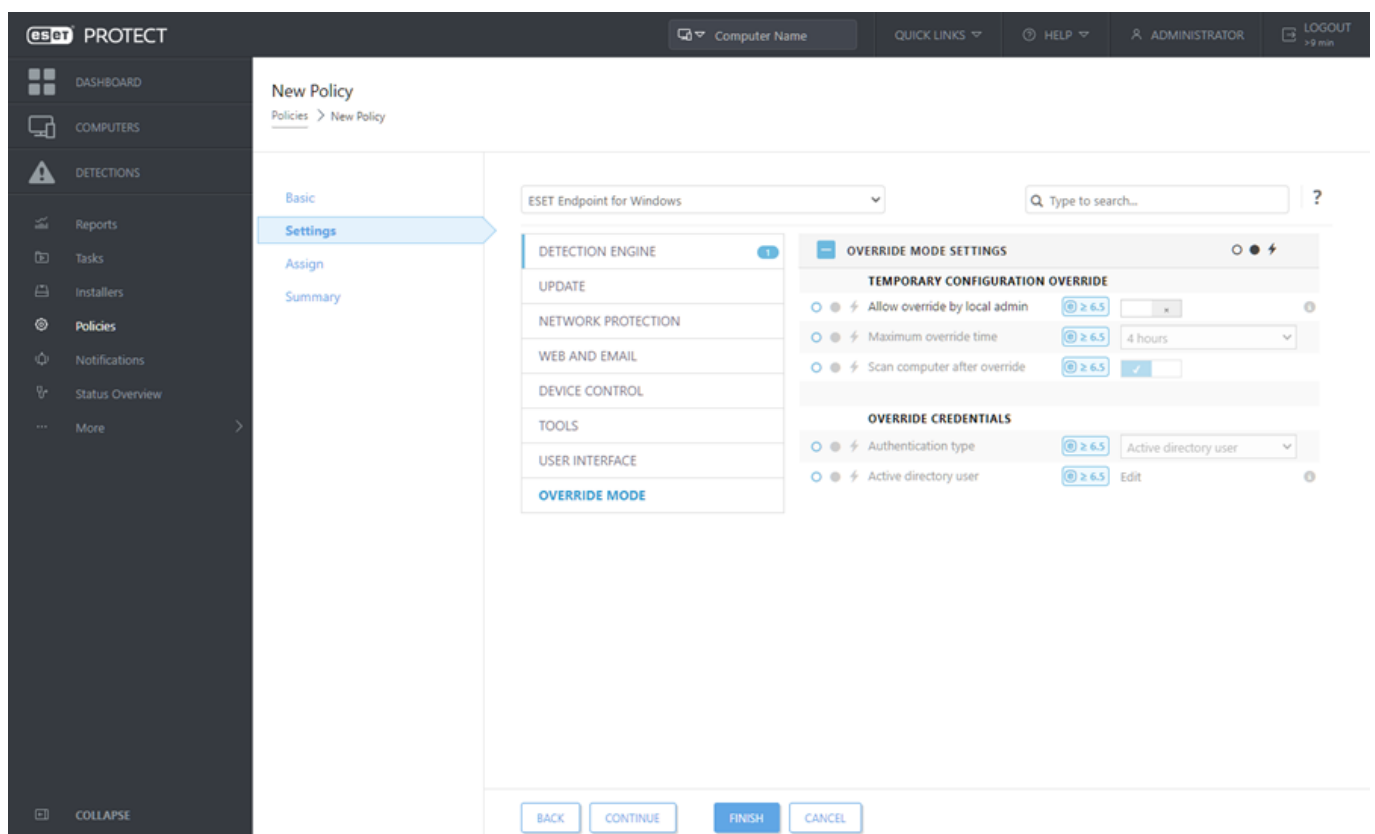
上書きモードの制限

- 上書きモードは、有効にした後、ESET PROTECT Webコンソールから停止することはできません。上書き時間が終了した後、またはクライアント側でオフにした場合にのみ、上書きが無効にされます。
- 上書きモードを使用しているユーザーも、Windows管理者権限が必要です。そうでないと、ユーザーはESET製品設定の変更を保存することはできません。
- Active Directoryグループ認証は、次のバージョンの選択した管理対象の製品でサポートされています。

ESET Endpoint Security	7. 0. 2100. 4以降。
ESET File Security for Microsoft Windows Server	6. 5. 12013. 0以降。
ESET Mail Security for IBM Domino	6. 5. 14020. 0以降。
ESET Mail Security for Microsoft Exchange Server	6. 5. 10019. 1以降。
ESET Server Security for Windows	8. 0以降。

上書きモードを設定するには

- [ポリシー] > [新しいポリシー]に移動します。
- [基本]セクションに、このポリシーの**名前**と**説明**を入力します。
- [設定]画面で、**[ESET Endpoint for Windows]**を選択します。
- [上書きモード]をクリックし、上書きモードのルールを設定します。
- [割り当て]セクションで、このポリシーが適用されるコンピューターまたはコンピューターのグループを選択します。
- [サマリー]セクションで、**[完了]**をクリックしてポリシーを適用します。



*John*のエンドポイント設定に問題があり、一部の重要な機能またはWebアクセスがコンピュータでブロックされる場合、管理者は*John*が既存のエンドポイントポリシーを上書きし、コンピュータで手動で設定を調整できるようにすることができます。後から、これらの新しい設定はESET PROTECTで要求されるため、管理者はそこから新しいポリシーを作成できます。

手順は次のとおりです。

1. [ポリシー] > [新しいポリシー]に移動します。
2. 名前および説明フィールドを入力します。[設定]画面で、[ESET Endpoint for Windows]を選択します。
3. [上書きモード]をクリックし、1時間上書きモードを有効にしADユーザーとして*John*を選択します。
4. *John*のコンピュータにポリシーを割り当て、[完了]をクリックしてポリシーを保存します。
5. *John*はESETエンドポイントで上書きモードを有効にし、コンピュータで手動で設定を変更する必要があります。
6. ESET PROTECT Webコンソールで、[コンピューター]に移動し、*John*のコンピューターをクリックして、[詳細を表示]をクリックします。
7. [設定]セクションで、[設定の要求]をクリックして、クライアントタスクをスケジュールして、クライアントから設定をすぐに取得します。
8. 少し待った後、新しい設定が表示されます。設定を保存する製品をクリックし、[設定を開く]をクリックします。
9. 設定を確認し、[ポリシーに変換]をクリックできます。
10. 名前および説明フィールドを入力します。
11. [設定]セクションでは、必要に応じて設定を変更できます。
12. [割り当て]セクションで、このポリシーを*John*のコンピュータ(またはその他)に割り当てることができます。
13. [完了]をクリックして設定保存します。
14. 必ず、必要がなくなった時点で、上書きポリシーを削除してください。

通知

通知はネットワーク上の全体的な状態を追跡するために非常に重要です。通知設定に基づいて新しいイベントが発生するときには、定義済みの方法([SNMPトラップ](#)または電子メールメッセージ、またはsyslogサーバーに送信)で通知され、それに応じて対応できます。検出された脅威、古いエンドポイントなどの特定のイベントに基づいて、自動通知を構成できます。特定の通知およびトリガーの詳細については、通知説明を参照してください。

	NAME	TAGS	ENABLED	STATUS	NOTIFICATION DESCRIPTION	LAST M
<input type="checkbox"/>	Malware outbreak alert (count per time criteria)		<input type="radio"/> Disabled		Notification is sent when count of antivirus detection events in d...	Administrator
<input type="checkbox"/>	Network attack alert		<input checked="" type="radio"/> Enabled	✓	Notification is sent when count of firewall events in defined perio...	Administrator
<input type="checkbox"/>	Computers report problems alert		<input type="radio"/> Disabled		Notification is sent when at least 5% of managed computers hav...	Administrator
<input type="checkbox"/>	Outdated modules alert		<input checked="" type="radio"/> Enabled	✓	Notification is sent when at least 5% of managed computers hav...	Administrator
<input type="checkbox"/>	Managed clients not connecting alert		<input type="radio"/> Disabled		Notification is sent when at least 5% of all managed clients have ...	Administrator
<input type="checkbox"/>	Outdated ESET software alert		<input type="radio"/> Disabled		Notification is sent when outdated ESET software is detected on ...	Administrator
<input type="checkbox"/>	Malicious file detected (trojan / worm / virus / application)		<input type="radio"/> Disabled		Notification is sent when a malicious file is detected (trojan / wor...	Administrator
<input type="checkbox"/>	Notification has invalid configuration and will not be triggered		<input type="radio"/> Disabled		At least one of the enabled notifications became invalid and will ...	Administrator
<input type="checkbox"/>	Outdated version of ESET Endpoint Antivirus detected		<input checked="" type="radio"/> Enabled	✓	Notification is sent every day when at least one outdated instanc...	Administrator
<input type="checkbox"/>	At least one computer has not connected for more than 14 ...		<input type="radio"/> Disabled		Notification is sent, when at least one computer has not been co...	Administrator
<input type="checkbox"/>	Potentially unsafe application detected		<input type="radio"/> Disabled		Notification is sent when a potentially unsafe application is detec...	Administrator
<input type="checkbox"/>	At least one infected file that was not cleaned automatically ...		<input type="radio"/> Disabled		Executed computer scan has detected at least one infected file th...	Administrator
<input type="checkbox"/>	Detection occurred in memory		<input type="radio"/> Disabled		Notification is sent, when a detection event is detected by advan...	Administrator
<input type="checkbox"/>	Potentially unwanted application (PUA) detected		<input type="radio"/> Disabled		Notification is sent when PUA (potentially unwanted application) ...	Administrator
<input type="checkbox"/>	High severity alert detected by HIPS occurred		<input type="radio"/> Disabled		Notification is sent when a high severity detection triggered by H...	Administrator
<input type="checkbox"/>	Suspicious application detected		<input checked="" type="radio"/> Enabled	✓	Notification is sent when a suspicious application is detected in y...	Administrator
<input type="checkbox"/>	Client task has invalid configuration and therefore will fail		<input type="radio"/> Disabled		At least one of the created client tasks has invalid configuration a...	Administrator
<input type="checkbox"/>	New computer connected for the first time		<input type="radio"/> Disabled		This notification is triggered when and ESET Management Agent ...	Administrator

[新しい通知](#)を作成するには、ページの下にある[\[新しい通知\]](#)をクリックします。

既存の通知を選択し、[アクション](#)をクリックして、[通知を管理します。](#)

フィルタリング条件を追加するには、[フィルターの追加](#)をクリックし、リストから項目を選択します。検索文字列を入力するか、フィルターフィールドでドロップダウンメニューから項目を選択して、**Enter**を押します。アクティブなフィルターは青でハイライト表示されます。

通知、ユーザー、権限

通知の使用は現在のユーザーの権限によって制限されます。通知を実行するたびに、権限が考慮される実行ユーザーが存在します。実行ユーザーは常に通知を最後に編集したユーザーです。ユーザーは、**読み取り**権限があるグループに含まれる通知のみを表示できます。



通知が適切に機能するには、実行ユーザーはすべての参照されたオブジェクト(デバイス、グループ、テンプレート)に対する十分な権限がある必要があります。一般的に、**読み取り**および**使用**権限が必要です。ユーザーにこれらの権限がないか、後から失う場合は、通知が失敗します。失敗した通知はオレンジ色でハイライトされ、電子メールによってユーザーに通知されます。

通知の作成 - 通知を作成するには、ユーザーはホームグループに対する通知の**書き込み**権限が必要です。新しい通知はユーザーのホームグループに作成されます。

通知の修正 - 通知を修正するには、ユーザーは通知があるグループに対する通知の**書き込み**権限が必要です。

通知の削除 - 通知を削除するには、ユーザーは通知があるグループに対する通知の**書き込み**権限が必要です。

JohnのホームグループはJohn's Groupで、Notification 1を削除(修正)しようとしています。通知は最初にLarryによって作成されたため、自動的にLarryのホームグループのLarry's Groupグループに含まれています。JohnがNotification 1を削除(修正)するには、次の条件を満たす必要があります。

- Johnには通知の書き込み権限がある権限設定を割り当てる必要があります。
- 権限設定は静的グループの下でLarry's Groupを含む必要があります。

複製とVDI

3つの準備された通知があり、複製関連のイベントをユーザーに通知するか、ユーザーが新しいカスタム通知を作成できます。

フィルターとレイアウトのカスタマイズ











現在のWebコンソール画面ビューをカスタマイズできます。

- サイドパネルとメインテーブルを管理します。
- フィルターとフィルタープリセットを追加します。 タグを使用して、表示される項目をフィルタリングできます。

通知の管理

通知は[通知]セクションで管理されます。次のアクションを実行できます。

- 新しい通知をクリックして、新しい通知を作成します。
- 既存の通知をクリックして、ドロップダウンメニューからアクションを選択します。



 詳細を表示	構成や配布設定を含む通知詳細を表示します。メッセージプレビューを表示をクリックすると、通知プレビューが表示されます。
 監査ログ	選択した項目の監査ログを表示します。
 タグ	タグを編集します(割り当て、割り当て解除、作成、削除)。
 有効化 /  無効化	通知のステータスを変更します。無効な通知は評価されません。すべての通知は既定で無効に設定されます。
 編集	通知の設定と配布を構成します。
 複製	ホームグループで重複する通知を作成します。
 削除	通知を削除します。
 アクセスグループ >  移動	通知を別の静的グループに移動します。

新しい通知

電子メールで通知を送信する場合は、SMTPサーバーを設定します。

基本

通知の名前と説明を入力し、異なる通知の間でフィルタリングを容易にできます。

有効な通知を編集し、通知を無効にする場合は、スライダー  をクリックし、ステータスが無効  に変更されます。

設定

• イベント

通知をトリガーできるイベントの基本タイプがあります。**[設定]**セクションで各イベントタイプのオプションを指定します。次のイベントタイプのいずれかを選択します。

- [管理されたコンピューターまたはグループのイベント](#)
- [サーバーステータス変更](#)
- [動的グループ変更](#)

詳細設定 – 調整

調整により、通知がトリガーされるべきことを決定する高度なルールを設定できます。詳細については、[調整](#)を参照してください。

配布

通知の[配布](#)設定を構成します。

管理されたコンピューターまたはグループのイベント

このオプションは、動的グループに関連付けられた通知で使用されますが、イベントログから除外されたシステムイベントに基づきます。通知の基になるログタイプとフィルタリング用の論理演算子を選択します。

カテゴリ – 次のイベントカテゴリから選択します。

- ファイアウォール検出
- ウイルス対策の検出
- 検査
- HIPS
- [Enterprise Inspectorアラート](#)
- [ブロックされたファイル](#)
- 最初に接続したコンピューター
- コンピューターのIDが取り戻されました
- コンピューターの複製の質問が作成されました
- 新しいMSP顧客が見つかりました

選択したカテゴリに応じて、**設定 > フィルタリング条件**の下に、使用できるイベントのリストが表示されます。フィルターの値はクライアントによって送信されたイベントと直接比較されます。使用可能な

値の限定リストはありません。

監視された静的グループ – 監視されるデバイスがある静的グループを選択します。

ミュートされたデバイスをスキップ – このチェックボックスをオンにすると、ミュートされたコンピューターから通知を受信しません(ミュートされたコンピューターは通知から除外されます)。

設定

設定の下で、**演算子**フィルターの値(**フィルタリング条件**)を選択します。1つの演算子のみを選択できます。すべての値はその演算子を使用して評価されます。**フィルターの追加**をクリックし、フィルターの新しい値を追加します。

サーバーステータス変更

このオプションは、オブジェクト状態変更を通知します。通知間隔は、選択した**カテゴリ**によって異なります。既存の設定を1つ選択するか、独自のパラメーターを設定できます。


設定プリセットの読み込み – 選択をクリックし、既存の設定から選択するか、空欄にします。クリアをクリックし、設定セクションをクリアします。

カテゴリ – オブジェクトのカテゴリを選択します。選択したカテゴリに従って、以下の設定セクションにオブジェクトが表示されます。

監視された静的グループ – 通知がクライアントに関連するカテゴリ(管理クライアント、インストールされたソフトウェア)では、監視する静的グループを選択できます。何も選択されていない場合は、実行ユーザーに十分な権限があるすべてのオブジェクトが監視されます。

設定

演算子とフィルターの値(**フィルタリング条件**)を選択します。1つの演算子のみを選択できます。すべての値はその演算子を使用して評価されます。**フィルターの追加**をクリックし、フィルターの新しい値を追加します。その他のフィルターが選択される場合は、通知の実行は、**AND**演算子で評価されます(すべてのフィルターフィールドが**true**と評価される場合にのみ通知が送信されます)。

 一部のフィルターでは通知の頻度が多すぎる場合があります。[調整](#)を使用して、通知を集約することをお勧めします。

使用可能なフィルター値のリスト

カテゴリ	値	コメント
CA証明書 ピア証明書	相対的な時間間隔	相対的な時間間隔(認証局の有効期限)を選択します。
管理クライアント	接続していないコンピューターの割合	0から100の値。 相対的な時間間隔 フィルターと組み合わせてのみ使用できます。

カテゴリ	値	コメント
ライセンス	相対的な時間間隔	ライセンス有効期限を監視する時間間隔を選択します。
	ライセンス使用状況の割合	アクティベーションで使用されるライセンス 単位 に基づいて計算された0～100 の値。ESET Mail Security製品の場合、ライセンス使用状況はアクティベーションで使用される サブ単位 に基づいて計算されます。
クライアントタスク	タスク	有効期間フィルターのタスクを選択します。何も選択しない場合、すべてが考慮されます。
	タスクが有効です	はい/いいえ を選択します。 いいえ を選択した場合、選択(フィルタータスク)からの1つ以上のタスクが無効なときに通知がトリガーされます。
サーバータスク	カウント(失敗)	選択したタスクの失敗数。
	前回のステータス	選択したタスクの最後に報告されたステータス。
	タスク	このフィルターのタスクを選択します。何も選択しない場合、すべてが考慮されます。
	タスクが有効です	はい/いいえ を選択します。 いいえ を選択した場合、選択(フィルタータスク)からの1つ以上のタスクが無効なときに通知がトリガーされます。
	相対的な時間間隔	監視する時間間隔を選択します。
インストールされたソフトウェア	アプリケーション名	完全なアプリケーション名。その他のアプリケーションが監視される場合は、 in 演算子を使用し、その他のフィールドを追加します。
	アプリケーションベンダー	完全なベンダー名。その他のベンダーが監視される場合は、 in 演算子を使用し、その他のフィールドを追加します。
	バージョンチェックステータス	古いバージョン が選択される場合、1つ以上のアプリケーションが古くなったときに、通知がトリガーされます。
ネットワークピア	ピア	
	サーバー状態	ESET PROTECTサーバーがログの書き込みで過負荷の場合は、状態が変更されます。 <ul style="list-style-type: none"> • 標準 – サーバーからの即時応答 • 制限 – サーバーは、1時間に1回エージェントに応答します • 過負荷 – サーバーはエージェントに応答していません
通知	通知	このフィルターの通知を選択します。何も選択しない場合、すべてが考慮されます。
	通知がオンです	はい/いいえ を選択します。 いいえ を選択した場合、選択(フィルター通知)した1つ以上の通知が無効なときに通知がトリガーされます。
	通知の構成が正しい	はい/いいえ を選択します。 いいえ を選択した場合、選択(フィルター通知)した1つ以上の通知の構成が正しくないときに通知がトリガーされます。

動的グループ変更

条件が満たされたときに通知が送信されます。特定の動的グループに対して監視される条件を1つのみ選択できます。

動的グループ – 評価する動的グループを選択します。

設定 - 条件

通知をトリガーする条件のタイプを選択します。

- **動的グループコンテンツが変更されるたびに通知**

有効にすると、選択したグループのメンバーが追加、削除、または変更されたときに通知されます。

ESET PROTECTは20分ごとに動的グループステータスを確認します。



たとえば、最初の確認が10:00に発生する場合、他の確認は10:20、10:40、11:00に実行されます。動的グループコンテンツが10:05に変更され、10:13に変更が戻る場合、10:20に実行される次のチェック中に、ESET PROTECTは前の変更を認識せず、通知しません。

- **グループのサイズが特定の数値を超えたときに通知する**

通知のグループサイズ演算子としきい値を選択します。

- **より多い** - グループサイズがしきい値より多いときに通知を送信します。

- **未満** - グループサイズがしきい値未満のときに通知を送信します。

- **グループの増加が特定の割合を超えたときに通知する**

通知の送信をトリガーするしきい値と期間を定義します。クライアント数またはクライアントの割合(動的グループのメンバー)を定義できます。新しい状態と比較するための期間(分、時間、または日)を定義します。例えば、7日前、古いセキュリティ製品のクライアント数が10で、しきい値が20に設定されました。古いセキュリティ製品のクライアント数が30になると、通知されます。

- **動的グループのクライアント数が他のグループと比較して変更されたときに通知する**

- 動的グループのクライアント数が比較グループ(静的または動的)に従って変化した場合、通知が実行されます。しきい値 - 通知の送信をトリガーするしきい値を定義します。



十分な権限がある動的グループにのみ通知を割り当てることができます。動的グループを表示するには、親静的グループの**読み取り**権限が必要です。

配布

1つ以上の配布方法を選択する必要があります。

SNMPトラップの送信

SNMPトラップを送信します。SNMPトラップは未承諾SNMPメッセージを使用してサーバーに通知します。詳細については、「[SNMPトラップサービスの構成方法](#)」を参照してください。

電子メールを送信

[電子メール設定](#)に基づいて、電子メールメッセージを送信します。既定では、通知電子メールはHTML形式であり、フッターにはロゴがあります。[カスタマイズ設定](#)([カスタマイズ](#) > [明るい背景ロゴ](#))に基づいて、異なるロゴの位置を設定できます。

- **カスタマイズなし** - ESET PROTECT ロゴはフッターの左側です

- **共同ブランディング** - ESET PROTECTロゴは左側、自分のロゴはフッターの右側です

- ホワイトラベル - ESET PROTECT ロゴはありません。フッターの左にある自分のロゴのみです

電子メールを送信が選択されている場合は、1つ以上の電子メール受信者を挿入します。

- **電子メールアドレス** - 通知メッセージの受信者の電子メールアドレスを入力します。
- **+** をクリックして、新しいアドレスフィールドを追加します。
- **> 1度に複数のユーザーを追加するには、その他 > ユーザーの追加**([コンピューターユーザー](#)からユーザーのアドレスを追加)するか、**詳細 > CSVのインポート**または**クリップボードから貼り付け**(区切り文字で構造化されたCSVファイルからアドレスのカスタムリストを[インポート](#))をクリックします。
- **詳細 > クリップボードから貼り付け** - カスタム区切り文字で区切られたアドレスのカスタムリストをインポートします。この機能はCSVインポートと同様に機能します。

Syslogを送信

ESET PROTECTを使用して、通知とイベントメッセージを[Syslogサーバー](#)に送信できます。また、クライアントのESET製品から[ログをエクスポート](#)し、Syslogサーバーに送信できます。**Syslog重要度** - ドロップダウンメニューから重要度を選択します。通知は選択した重要度で[Syslogサーバー](#)に表示されます。


配布の基本フィールド

- **メッセージプレビュー** - 通知に表示されるメッセージのプレビュー。プレビューには構成された設定がテキスト形式で含まれます。メッセージの内容と件名の両方をカスタマイズし、変数を使用して、通知が生成されるときに実際の値に変換できます。これは任意ですが、通知と概要のフィルタリング効果を高めるために設定することをお勧めします。
- **o件名** - 通知メッセージの件名。🖋️ アイコンをクリックして、内容を編集します。正確な件名はメッセージの並べ替えとフィルタリングを改善できます。
- **o内容** - 🖋️ アイコンをクリックして、内容を編集します。内容を編集した後、↺️ アイコンをクリックして、既定のメッセージコンテンツをリセットできます。

件名とコンテンツに変数を追加し、通知に特定の情報を含めることができます。**変数の追加**をクリックするか、\$と入力し始めると、変数のリストが表示されます。

• 一般

- **oロケール** - 既定のメッセージの言語。メッセージの内容は変換されません。
- **oタイムゾーン - 発生時刻** \${timestamp} 変数のタイムゾーンを設定します。これはカスタムメッセージで使用できます。

 イベントがローカル時刻の3:00に発生し、ローカル時刻はUTC+2を選択したタイムゾーンがUTC+4の場合、通知で報告される時刻は5:00です。

[完了]をクリックすると、編集しているテンプレートに基づいて、新しいテンプレートを作成します。

SNMPトラップサービスの構成方法

SNMPメッセージを正常に受信するには、SNMPトラップサービスを構成する必要があります。オペレーティングシステムに応じて、以下の構成手順に従います。

WINDOWS

前提条件

- ESET PROTECTサーバーがインストールされているコンピュータと、SNMPトラップソフトウェアがインストールされる予定のコンピュータには、**簡易ネットワーク管理プロトコルサービス**をインストールする必要があります。
- 両方のコンピュータ(上記)は同じサブネットにある必要があります。
- SNMPサービスはESET PROTECTサーバーコンピュータで構成する必要があります。

SNMPサービス構成(ESET PROTECTサーバー)

- 1.Windows+Rキーを押して、ダイアログボックスを開きます。開くフィールドにServices.mscと入力し、**Enter**を押します。SNMP Serviceを検索します。
- 2.トラップタブを開き、コミュニティ名フィールドに**public**と入力し、リストに**追加**をクリックします。
- 3.**追加**をクリックし、該当するフィールドに、SNMPトラップソフトウェアがインストールされているコンピュータの**ホスト名**、**IP** または **IPXアドレス**を入力して、**追加**をクリックします。
- 4.セキュリティタブに移動します。**追加**をクリックして、**SNMPサービス構成**ウィンドウを表示します。コミュニティ名フィールドに**public**と入力し、**追加**をクリックします。権限は**読み取り専用**に設定されます。これで問題ありません。
- 5.すべてのホストからの**SNMPパケット**を許可が選択されていることを確認し、**OK**をクリックして確認します。SNMPサービスは構成されません。

SNMPトラップソフトウェア設定(クライアント)

- 1.SNMPサービスがクライアントコンピュータにインストールされていることを確認します。
- 2.トラップレシーバーアプリケーションをインストールします。
- 3.ESET PROTECTサーバーからSNMPトラップを受信するトラップレシーバーアプリケーションを設定します(これにはESET PROTECT サーバのIPアドレスとポート設定を含めることができます)。
- 4.クライアントマシンのファイアウォールが、前の手順で設定したSNMP通信のネットワーク通信を許可していることを確認してください。
- 5.トラップレシーバーアプリケーションでESET PROTECTサーバーからメッセージを受信できます。

Linux

1. 次のコマンドのいずれかを実行してsnmpdパッケージをインストールします。

```
apt-get install snmpd snmp(DebianUbuntuディストリビューション)
```

```
yum install net-snmp (Red HatCentOSディストリビューション)
```

2. /etc/default/snmpdファイルを開き、次の属性を編集します。

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
# を追加すると、この行が完全に無効になります。
```

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -
c /etc/snmp/snmpd.conf'
この行をファイルに追加します。
```

```
TRAPDRUN=yes
```

trapdrun属性をyesに変更します。

3. 元のsnmpd.confファイルのバックアップを作成します。このファイルは後から編集されます。

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. 新しいsnmpd.confファイルを作成し、次の行を追加します。

```
rocommunity public
syslocation "Testing ESET PROTECT"
syscontact admin@PROTECT.com
```

5. /etc/snmp/snmptrapd.confファイルを開き、次の行をファイルの最後に追加します。

```
authCommunity log,execute,net public
```


6. 次のコマンドを入力してSNMPマネージャサービスと受信トラップのロギングを開始します。

```
/etc/init.d/snmpd restart
または
service snmpd restart
```

7. トラップが動作し、メッセージを受信しているかどうかを確認するには、次のコマンドを実行します。

```
tail -f /var/log/syslog | grep -i TRAP
```

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。 **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。**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。

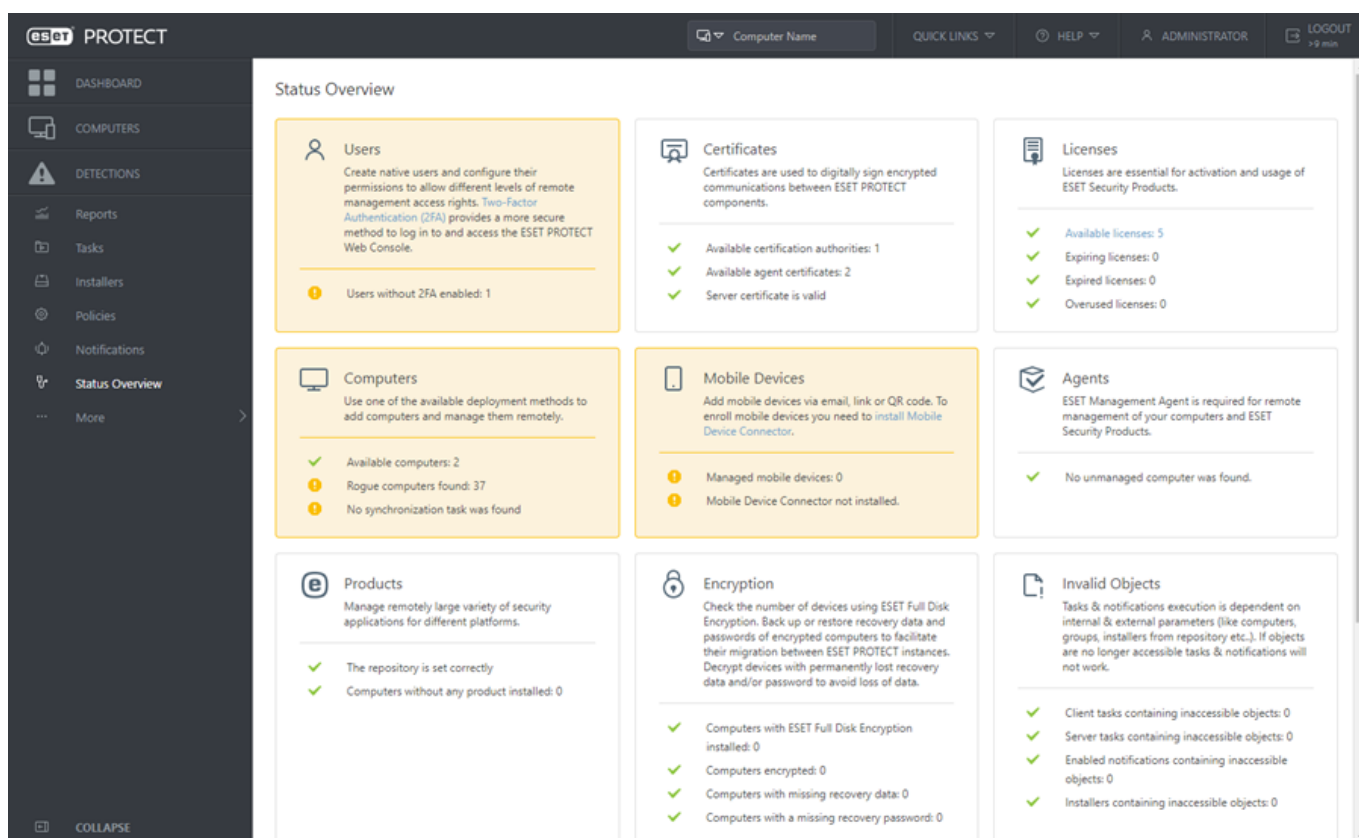
セクションタイトルをクリックし、アクションのある右側のタスクバーを表示します。各セクションタイトルには、複数の色の1つが設定されます。これは、含まれる項目の最高重要度ステータスに基づきます。

色	アイコン	アイコン凡例	説明
緑	✓	Ok	セクションのすべての項目には問題がありません。
イエロー	!	警告	セクションの1つ以上の項目には警告があります。
赤	△	エラー	セクションの1つ以上の項目にはエラーがあります
灰色	⊖	コンテンツは利用できません	コンテンツは、ESET PROTECTコンソールユーザーのアクセス権が不十分のため使用できません。管理者は、ユーザーが適切なアクセス権を持つ別のユーザーとしてログインできるように、追加の 権限 を設定する必要があります。
青	?	情報	接続されたコンピューターに関する質問があります(以下の 質問 セクションを参照)。

🔗 **ステータス概要**には次のセクションがあります。

ユーザー	別の ユーザー を作成し、ESET PROTECTで異なる管理レベルを実現するように 権限 を構成できます。既定のESET PROTECT管理者アカウントはインストール中に作成されています。 <div>! 標準ユーザーアカウントとして、既定のESET PROTECT管理者アカウントを使用することとは推奨されません。ユーザーの表示をクリックし、二要素認証を使用して新しい標準ユーザーアカウントを作成し、その既定のアカウントをESET PROTECTで使用します。</div>
証明書	ESET PROTECTで提供されている既定の証明書以外の証明書を使用する場合は、 認証局 と ピア証明書 を個別のESET PROTECTコンポーネントに作成し、ESET PROTECTサーバーとの通信ができます。
ライセンス	ESET PROTECTは ESETライセンスシステム を使用します。クライアントコンピューターでESET PROTECTコンポーネントとESETセキュリティ製品をアクティベーションするときに使用される ライセンス を追加する方法を選択します。
コンピューター	<ul style="list-style-type: none"> • コンピューターの追加 - ネットワーク上のコンピューターをESET PROTECT構造に追加します。コンピューターとモバイルデバイスを手動で追加するか、デバイスのリストをインポートできます。 • 管理対象外のコンピューターの追加 - ESET RD Sensorを使用して検出されたコンピューターを自動的にインポートします。 • 新しい同期タスク - 静的グループ同期を実行し、Active Directory®LDAP®VMwareなどと同期します。
モバイルデバイス	<ul style="list-style-type: none"> • ダウンロード - MDCがインストールされていない場合は、ESETのWebサイトからMobile Device Connectorインストーラーをダウンロードできます。 • モバイルデバイスの追加 - 電子メールあるいはリンクまたはQRコードを使用するか、デバイス所有者として、モバイルデバイスを登録できます。
エージェント	<ul style="list-style-type: none"> • 新しいポリシー - ESET Managementエージェントの新しいポリシーを作成して接続間隔を変更することもできます。 • エージェントの展開 - 複数の方法で、ネットワーク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できます。
製品	<ul style="list-style-type: none"> • 新しいポリシー - 新しいポリシーを作成し、クライアントコンピューターにインストールされたESETセキュリティ製品の設定を変更できます。 • リポジトリの構成 - サーバー設定を変更します。 • ソフトウェアのインストール - ESET Managementエージェントが展開されるとESETリポジトリから直接ソフトウェアをインストールするか、インストールパッケージの場所(URLまたは共有フォルダー)を指定できます。

無効なオブジェクト	クライアント と サーバー タスク、 トリガー 、 通知 、 インストーラー のリストと、到達できないまたは無効なオブジェクトへの参照が表示されます。任意の結果フィールドをクリックすると、選択したオブジェクトのリストがあるメニューが表示されます。
外部サービス	ESET PROTECTは、外部サービスに接続して完全な機能を提供するように構成できます。 <ul style="list-style-type: none"> • リポジトリの構成 - リポジトリには、インストールタスクを使用してインストールできる他のESETセキュリティ製品のインストーラーファイルがあります。リポジトリはサーバー設定で構成されます。必要に応じて、オフラインリポジトリを作成できます。 • アップデートの構成 - ESET PROTECTを最新に保つにはアップデートが必要です。アップデートは、ESET PROTECTが期限切れではないビジネス製品ライセンスをインポートした場合のみ使用できます。サーバー設定でアップデート設定を変更できます。 • SMTPの構成 - 電子メールメッセージ（例えば通知、モバイルデバイス登録メール、レポートなど）を送信するために既存のSMTPサーバーを使用するようにESET PROTECTを設定します。
質問	複製されたデバイスまたはハードウェアの変更がクライアントデバイスで検出されると、質問が一覧に表示されます。 複製されたコンピューター についての詳細をお読みください。
MSPステータス	MSPアカウントをインポート する場合は、利用可能な MSPステータス のタイルがあります。





詳細

*** [詳細] セクションはESET PROTECTの詳細設定コンポーネントです。このセクションには、管理者がクライアントセキュリティソリューションとESET PROTECT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。これらのツールを使用すると、ネットワーク環境を設定でき、少ないメンテナンス作業で済みます。

*** 詳細セクションには、次の項目があります。

検出 0 送信されたファイル 0 除外 0 隔離
コンピューター 0 コンピューターユーザー 0 動的グループテンプレート
ライセンス 0 ライセンス管理
アクセス権 0 ユーザー 0 権限設定
証明書 0 ピア証明書 0 認証局
サーバー 0 サーバー設定
アクティビティ 監査 0 監査ログ


送信されたファイル

ESET Dynamic Threat Defenseは、これまでにない検出からの高度な保護を提供するサービスです。ESET PROTECTユーザーはクラウド環境でマルウェア分析のためにファイルを送信し、サンプル動作に関するレポートを受信できます。段階的な手順については、[ESET Dynamic Threat Defenseユーザーガイド](#)を参照してください。ESET PROTECT Webコンソールの[検出](#)から直接リモートでファイルを送信できます。 >  [ブロックされたファイル](#) カテゴリ >  [ファイル](#) をEDTDに送信をクリックします。

送信されたファイルウィンドウにはESETサーバーに送信されたすべてのファイルのリストを確認できます。これらには、クライアントコンピューターからESET LiveGrid®に自動的に送信されたファイル(ESETセキュリティ製品でESET LiveGrid®が有効な場合)、およびESET Dynamic Threat Defense Webコンソールから手動でESET PROTECTに送信されたファイルが含まれます。

送信されたファイルウィンドウ

送信されたファイルと、ファイルを送信したユーザーや送信日などのファイルに関連する情報が一覧表示されます。送信されたファイルをクリックして、ドロップダウンメニューからアクションを選択します。

 詳細を表示	クリックすると、 最新の送信 タブを表示します。
 動作の表示	特定のサンプルの動作分析レポートを表示します。このオプションは、ESET Dynamic Threat Defenseに送信されたファイルでのみ使用できます。
 除外の作成	1つ以上のファイルを選択し、 除外の作成 をクリックして、選択したファイルの検出除外を既存のポリシーに追加します。

ファイル詳細ウィンドウ

ファイル詳細ウィンドウには、選択したファイルのファイル詳細が一覧表示されます。ファイルが複数回送信される場合、前回の送信の詳細が表示されます。

ステータス	マルウェア分析の結果。 不明 – ファイルは分析されませんでした。 未感染 – 検出エンジンのいずれもファイルをマルウェアとして評価しませんでした。 不審 不審な可能性が高い – ファイルは不審な動作を示していますが、マルウェアではない可能性もあります。 悪意 – ファイルは危険な動作を示します。
状態	分析の状態。ステータス 再分析 は、結果が利用可能であることを意味しますが、さらに分析すると変更される場合があります。
前回処理日	ファイルは、分析のために何回も、複数のコンピューターから送信できます。これは最終分析日時です。
送信日	送信日時。
動作	動作の表示 をクリックし、ESET Dynamic Threat Defenseから分析を表示します。これは、ファイルを送信したコンピューターにアクティブなESET Dynamic Threat Defenseライセンスがある場合にのみ有効です。
コンピューター	ファイルが送信されたコンピューターの名前。
ユーザー	ファイルを送信したコンピューターユーザー。
原因	ファイルが送信された理由。
送信先	ファイルを受信したESETクラウドの一部。一部の送信されたファイルはマルウェア分析が行われます。
ハッシュ	送信されたファイルのSHA1ハッシュ。
サイズ	送信されたファイルのサイズ。
カテゴリ	ファイルのカテゴリ。カテゴリはファイル拡張子に従わない場合があります。

ESET Dynamic Threat Defense動作レポートの詳細については、[ドキュメント](#)を参照してください。

フィルターとレイアウトのカスタマイズ







現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

除外

このセクションには、**ウイルス対策**検出および**ファイアウォールIDS**ルールのすべての[作成された除外](#)の一覧が表示されます。この新しいセクションには、すべての除外が含まれ、表示がわかりやすくなり、管理が簡素化されます。

除外を管理するには、除外を1つクリックするか、複数の除外を選択して**アクション**ボタンをクリックします。

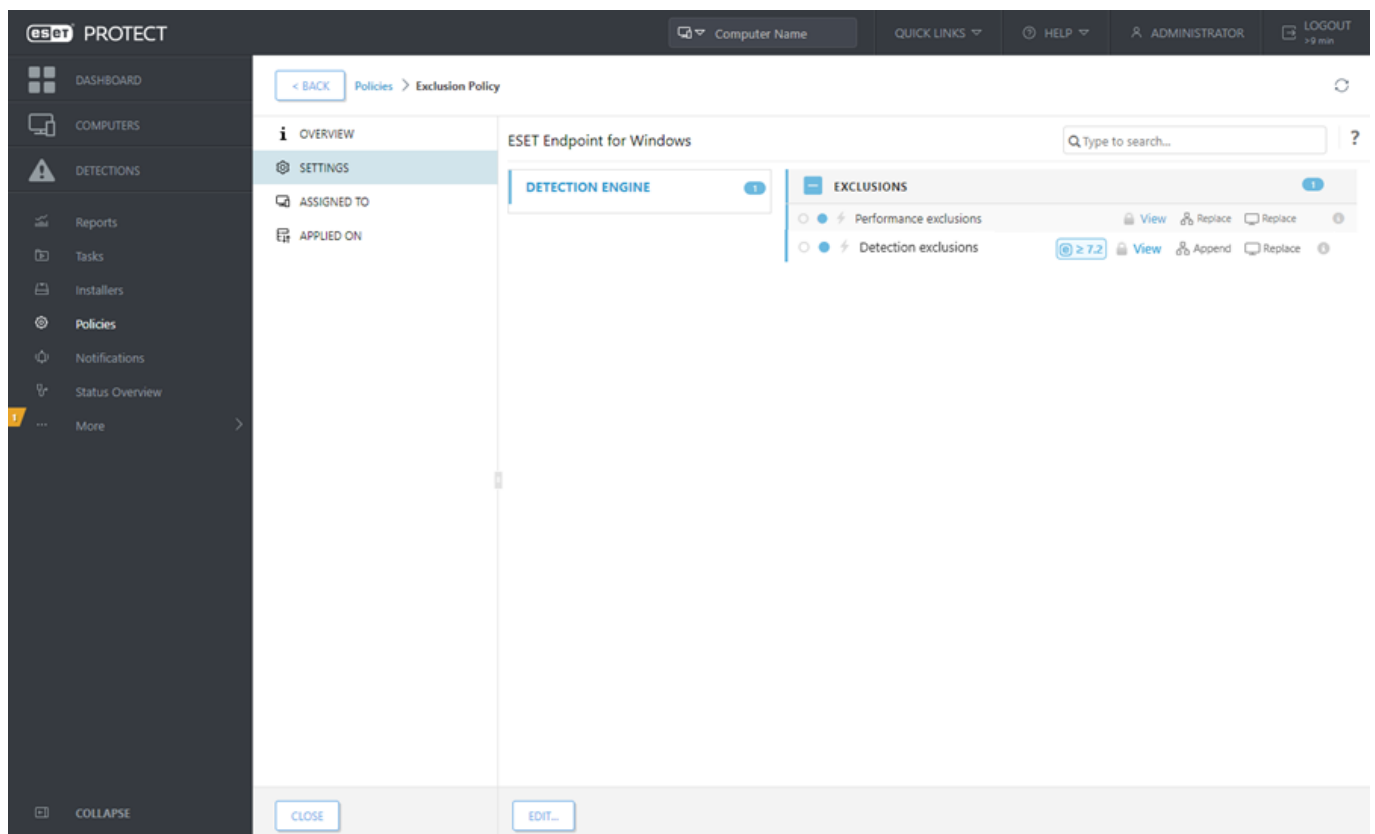
-  **割り当ての変更** – 除外が適用されるターゲットコンピューターを変更します。
-  **影響を受けるコンピューターを表示** – 除外が適用されるコンピューターを表示します。
-  **監査ログ** – 選択した除外の[監査ログ](#)を表示します。
-  **削除** – 選択した除外を削除します。
-  **アクセスグループ** >  **移動** – 除外を別の静的グループに移動します。

除外された検出またはファイアウォールアクションが管理されたコンピューターにもう一度表示される場合は、**ヒット数列**に除外が適用された回数が表示されます。

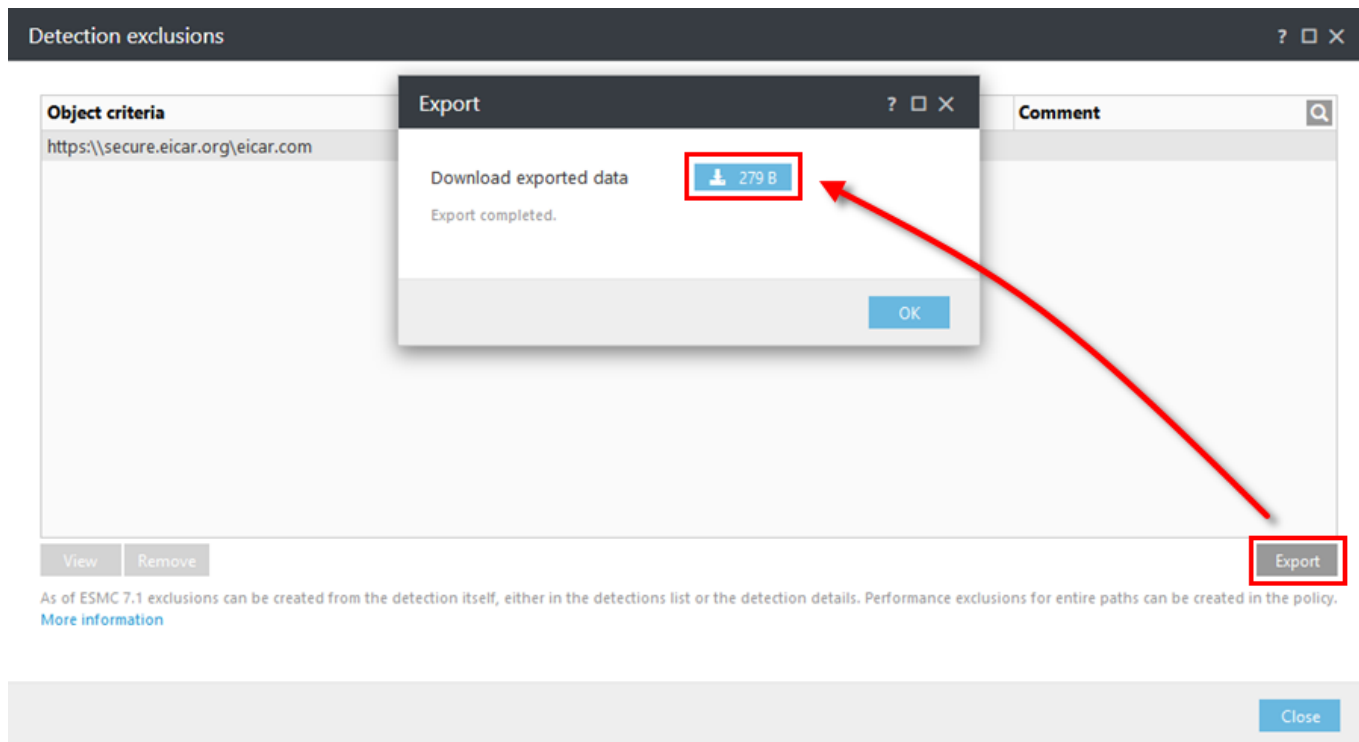
ポリシーから除外を移行する

ESET PROTECTでは、ポリシーを使用して、ウイルス対策検出除外を作成することはできません。以前にポリシーに除外が含まれていた場合は、以下の手順に従い、ESET PROTECTで、ポリシーから**除外**に除外を移行します。

1. ポリシーに移動し、除外が含まれるポリシーをクリックし、**詳細を表示**を選択します。
2. **設定 > 検出 エンジン**をクリックします。
3. **検出除外**の横の**表示**をクリックします。

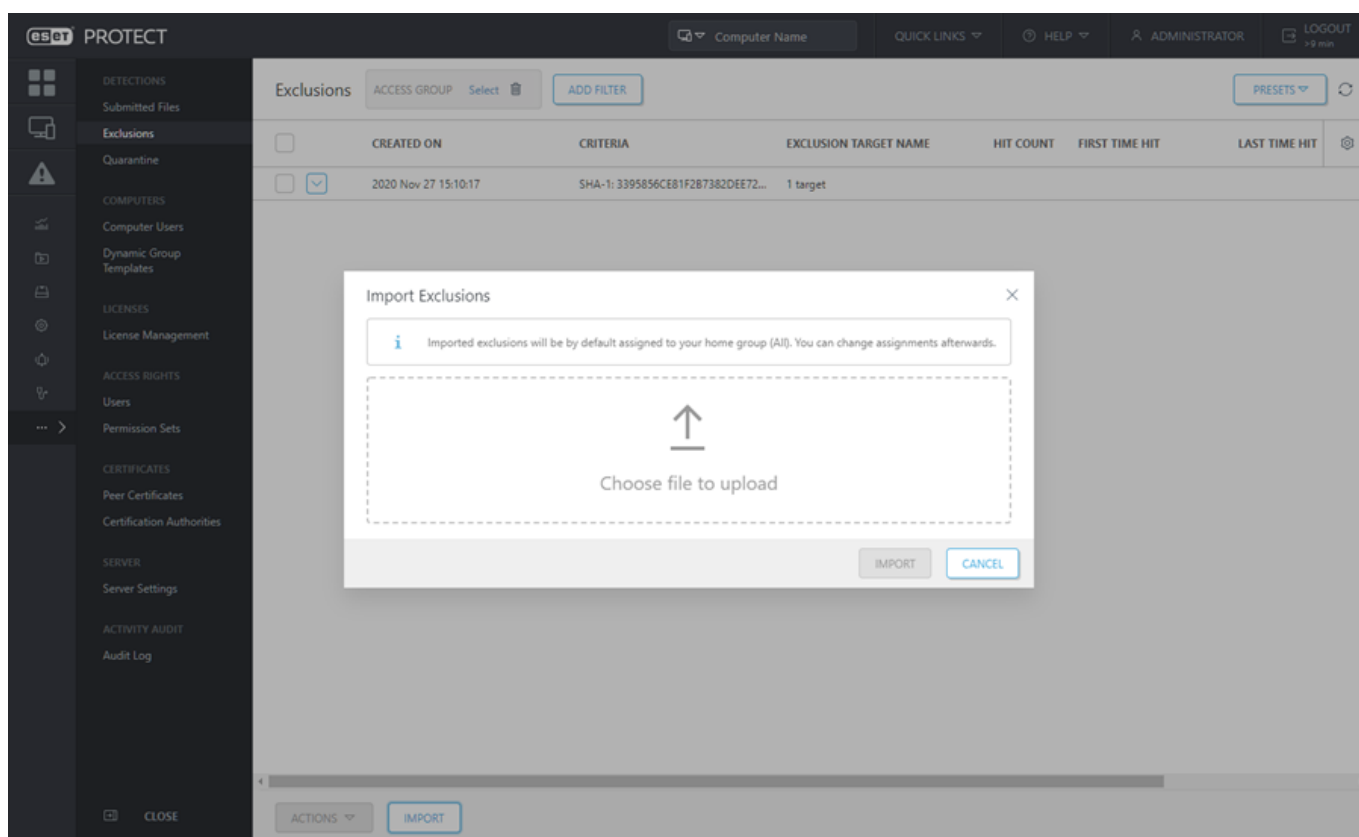


4. **エクスポート**ボタンをクリックしてから、**エクスポートされたデータのダウンロード**の横のボタンをクリックして、**export.txt**ファイルを保存します。**OK**をクリックします。



5. ESET PROTECT Webコンソールで、**詳細 > 除外**に移動します。

6. インポートボタンをクリックして、ファイルから検出除外をインポートします。**アップロードするファイルを選択**をクリックして、**export.txt**ファイルに移動するか、ファイルをドラッグアンドドロップします。



7. インポートボタンをクリックして、検出除外をインポートします。インポートされた検出除外は、除外リストに表示されます。

Import Exclusions

i

Imported exclusions will be by default assigned to your home group (All). You can change assignments afterwards.

export.txt

0.59 KB

×

IMPORT

CANCEL

除外の割り当て制限

- 元の除外割り当ては保持されません。既定では、インポートされた検出除外はホームグループのコンピューターに割り当てられます。除外の割り当てを変更するには、除外をクリックして、**割り当ての変更**を選択します。
- 検出除外(ウイルス対策検出およびファイアウォールIDSルール)は、[互換性があるESETセキュリティ製品](#)がインストールされているコンピューターにのみ割り当てることができます。除外は互換性のないESETセキュリティ製品には適用されず、無視されます。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

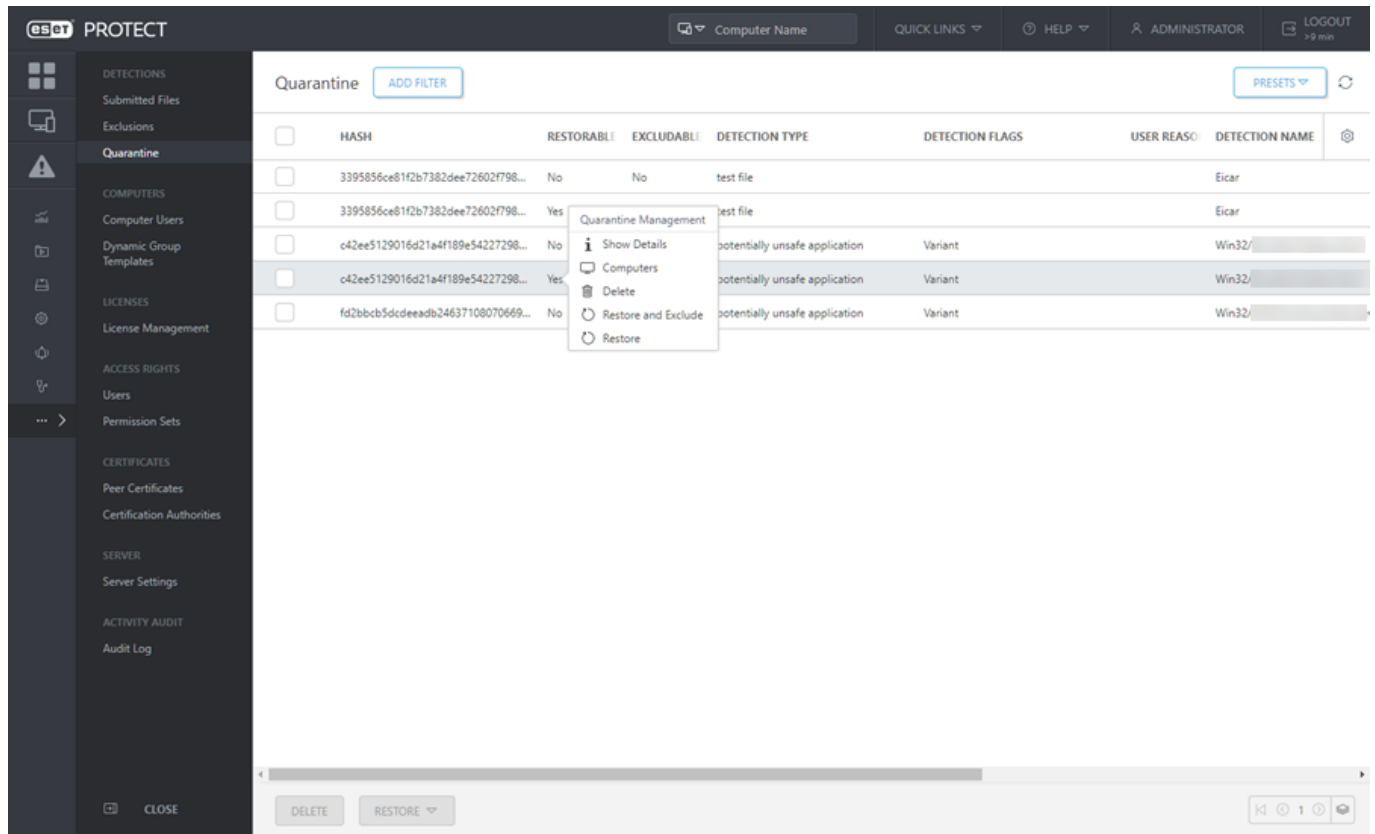
- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

隔離

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ないまたは推奨されない場合、あるいはESET製品で誤って検出された場合、ファイルを隔離する必要があります。

- i

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](#)



隔離されたファイルを削除するか、元の場所に復元できます。隔離されたファイルを復元して除外すると、次回以降にESET製品によって報告されないようにすることができます。

さまざまなフィルターを使用して、隔離のファイルのリストをフィルタリングできます。

2つの方法で隔離にアクセスできます。

1. 詳細 > 隔離

2. コンピューター詳細 > 検出と隔離 > 隔離タブ

[隔離] セクションの項目をクリックすると、[隔離管理] メニューが開きます。

i 詳細を表示 – ソースデバイス、検出名とタイプ、オブジェクト名(完全ファイル、ハッシュ、サイズなど付き)を表示します。

コンピューター – 隔離されたファイルがある接続されたフィルタリングされたデバイスの[コンピューター] セクションが開きます。

削除 – 隔離と影響するデバイスからファイルを削除します。

復元 – ファイルを元の場所に復元します。

復元と除外 – ファイルを元の場所に復元し、検査から除外します。

アップロード – [隔離されたファイルのアップロード](#) タスクを開きます。このアクションは、詳細を表示をクリックした後に使用できます。

! アップロード機能は上級者ユーザーにのみ推奨されます。隔離されたファイルをさらに調査する場合は、共有ディレクトリにアップロードできます。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

コンピューターユーザー

コンピューターユーザーセクションでは、ユーザーとユーザーグループを管理できます。一部のユーザー固有の設定を同期するために、ユーザーとデバイスをペアリングできます。最初に、[ユーザーをActive Directoryと同期](#)することをお勧めします。新しいコンピューターを作成するときに、そのコンピューターを特定のユーザーとペアリングできます。ユーザーを検索し、ユーザーとアクティビティに割り当てられたコンピューターの詳細を表示できます。

[iOSデバイスに割り当てられたポリシー](#)を使用して、[iOSモバイルデバイス管理](#)の目的で、ユーザーとユーザーグループを管理することもできます。ユーザーを修正したり、[カスタム属性](#)を追加できます。

! コンピューターユーザーは、[ESET PROTECT Webコンソールユーザー](#)とは異なります。ESET PROTECT Webコンソールと権限セットを管理するには、[\[詳細\] > \[ユーザー\]](#)に移動します。

- オレンジ色でハイライト表示されたユーザーにはデバイスが割り当てられていません。ユーザーをクリックし、[\[編集\]](#)を選択して、[\[割り当てられたコンピューター\]](#)をクリックして、ユーザーの詳細を表示します。[コンピューターの追加](#)をクリックして、デバイスをこのユーザーに割り当てます。

<input type="checkbox"/>	USER NAME	TAGS	USER DESCRIPTION	EMAIL ADDRESS
<input type="checkbox"/>	Amanda			amanda@company.com

- また、[コンピューター詳細](#)から、[割り当てられたユーザー](#)を追加または削除できます。コンピューター内で、デバイスを選択し、[i 詳細を表示](#)をクリックします。ユーザーは複数のデバイスに割り当てることができます。[\[ユーザーの割り当て\]](#)を使用して、選択したデバイスに直接ユーザーを割り当てることができます。デバイスがユーザーに割り当てられている場合は、デバイス名をクリックして、デバイスの詳細を表示できます。

- ユーザーとユーザーグループをドラッグアンドドロップできます。ユーザー(またはグループ)を選択し、マウスボタンを押しながら、他のグループに移動します。

ユーザー管理アクション

ユーザーを選択し、アクションを実行できるドロップダウンメニューを開きます。詳細については、[アイコン凡例](#)を参照してください。

i 詳細を表示 - メニューには、電子メールアドレス、オフィスまたはロケーション、および割り当てられたコンピューターなどの情報が表示されます。ユーザーは複数のデバイスに割り当てることができます。

す。ユーザーの**名前**の説明、または**親グループ**を変更できます。 [iOS MDMポリシーを作成](#)するとき
に使用できる**カスタム属性**がここに表示されます。

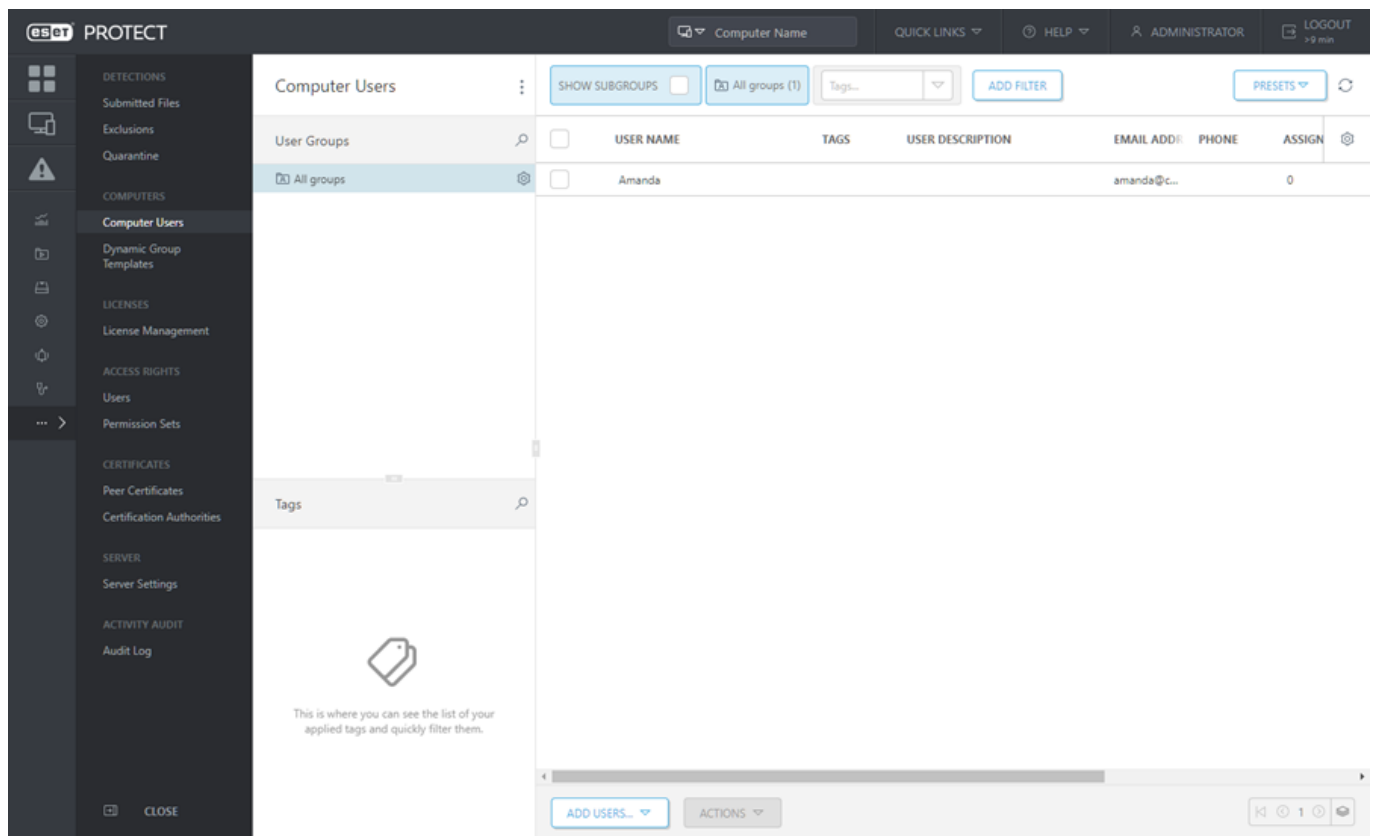
フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

新しいユーザーの追加

1. [コンピューターユーザー]>[ユーザーの追加]をクリックします。 このオプションを使用すると、[ユーザー同期](#)中に見つからなかったか自動的に追加されなかったユーザーを追加します。



2. [ユーザー名]フィールドに、追加するユーザーの名前を入力します。[追加]をクリックして、その他のユーザーを追加します。複数のユーザーを同時に追加する場合は、[CSVのインポート](#)をクリックして、追加するユーザーのリストを含む.csvファイルをアップロードします。コピーして貼り付けをクリックすると、カスタム区切り文字で区切られたアドレスのカスタムリストをインポートします(この機能はCSVインポートと同様に動作します)。必要に応じて、簡単に識別できるようにユーザーの[説明]を入力できます。
3. 既存の**親グループ**を選択するか、新しいグループを作成できます。
4. **タグを選択**をクリックして、[タグを割り当て](#)ます。
5. 追加するユーザーが既にESET PROTECTにある場合は、[競合の解決](#)ドロップダウンメニューを使用

して、実行するアクションを選択します。

- **競合が検出されたときに確認:** 競合が検出された場合、プログラムのアクション(以下のオプションを参照)を選択するように求められます。
- **競合するユーザーをスキップ:** 同じ名前のユーザーは追加されません。これは、既存のユーザーのESET PROTECTの [カスタム属性](#) が保持されることも保証します(Active Directoryのデータで上書きされない)。
- **競合するユーザーの上書き:** ESET PROTECTの既存のユーザーはActive Directoryのユーザーによって上書きされます。同じSIDのユーザーが2人いる場合の既存のESET PROTECTユーザーは前の場所から削除されます(ユーザーが別のグループにある場合でも削除されます)。

6. 変更が完了したら、[追加]をクリックします。ユーザーは指定した親グループに表示されます。

The screenshot shows the ESET PROTECT web interface. The left sidebar contains a navigation menu with categories like DETECTIONS, COMPUTERS, LICENSES, ACCESS RIGHTS, CERTIFICATES, SERVER, and ACTIVITY AUDIT. The 'COMPUTERS' section is expanded, showing 'Computer Users' as the selected option. The main content area is titled 'Add Users'. It includes a 'Users' section with a 'Conflict Resolution' dropdown set to 'Ask when conflicts are detected'. Below this is a 'Parent Group' section with a link to 'All groups or Create new group'. There is also a 'Tags' section with a 'Select tags' link. The 'List of Users' section features a table with columns: USER NAME, USER DESCRIPTION, EMAIL ADDRESS, PHONE, OFFICE, and JOB POSITION. The 'USER NAME' column has a red border and a warning icon. Below the table are buttons for '+ ADD', 'IMPORT CSV...', and 'COPY & PASTE'. At the bottom of the form are 'ADD' and 'CANCEL' buttons.

ユーザーの編集

基本情報、割り当てられたコンピューターなどのユーザー詳細情報を変更できます。

i カスタム属性が定義されているユーザーに対して [ユーザー同期](#) タスクを実行するときには、**ユーザー作成競合処理をスキップ**するように設定します。そうしないと、ユーザーデータがActive Directoryのデータによって上書きされます。

基本

[ユーザー同期](#) タスクを使用してユーザーを作成し、一部のフィールドを空欄にする場合は、必要に応じてこれらを手動で指定できます。

ここでは、次のようなユーザー詳細情報を編集できます。

- **ユーザー名と説明** - 情報提供のみを目的とします。
- **タグ**: [タグ](#)を編集します(割り当て、割り当て解除、作成、削除)。
- **電子メールアドレス** - 通知の配信用受信者アドレスとして使用できます。
- **電話番号とオフィスまたはロケーション** - 情報提供のみを目的とします。
- **SID**: このAD情報が必要な複数のESET PROTECT機能に関連付けることができます(エンドポイントポリシー [上書きモード](#)など)。

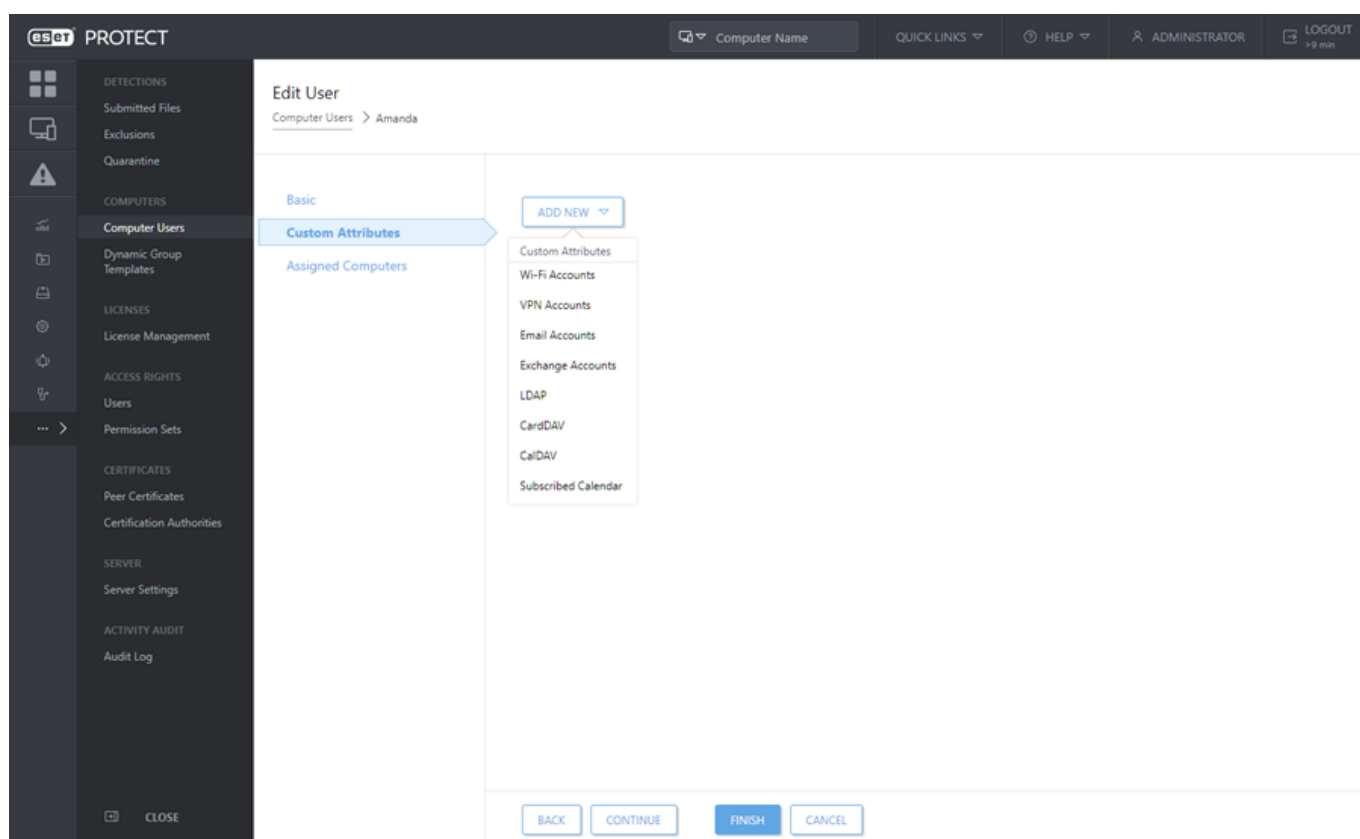
カスタム属性

既存のカスタム属性を編集するか、新しい属性を追加できます。新しい属性を追加するには、**[新規追加]**をクリックして、カテゴリから選択します。

- **Wi-Fiアカウント**: プロファイルを使用して、企業Wi-Fi設定を管理されたデバイスに直接プッシュします。
- **VPNアカウント**: 認証資格情報、証明書、およびその他の必要な情報とともにVPNを設定し、ユーザーが簡単にVPNにアクセスできるようにします。
- **電子メール アカウント**: これはIMAPまたはPOP3仕様を使用する電子メールアカウントで使用されます。Exchangeサーバーを使用する場合は、次のExchange ActiveSync設定を使用します。
- **Exchange アカウント**: 社内でMicrosoft Exchangeを利用している場合は、ここですべての設定を作成し、ユーザーの電子メール、カレンダー、および連絡先へのアクセスを設定する時間を最小化できます。

- **LDAP (属性エイリアス):** 社内で連絡先用にLDAPを使用している場合に特に便利です。連絡先フィールドを対応するiOS連絡先フィールドにマッピングできます。
- **CalDAV:** これにはCalDAV仕様を使用するすべてのカレンダーの設定が含まれます。
- **CardDAV:** CardDAV仕様で同期されるすべての連絡先の同期情報をここで確立できます。
- **登録されたカレンダー:** CalDAVカレンダーが設定されている場合は、ここで、他のカレンダーへの読み取りアクセスを定義できます。

一部のフィールドは、変数(プレースホルダー)として[iOSモバイルデバイスのポリシーを作成](#)するときを使用できる属性になります。たとえば、ログイン\${exchange_login/exchange}または電子メールアドレス\${exchange_email/exchange}です。

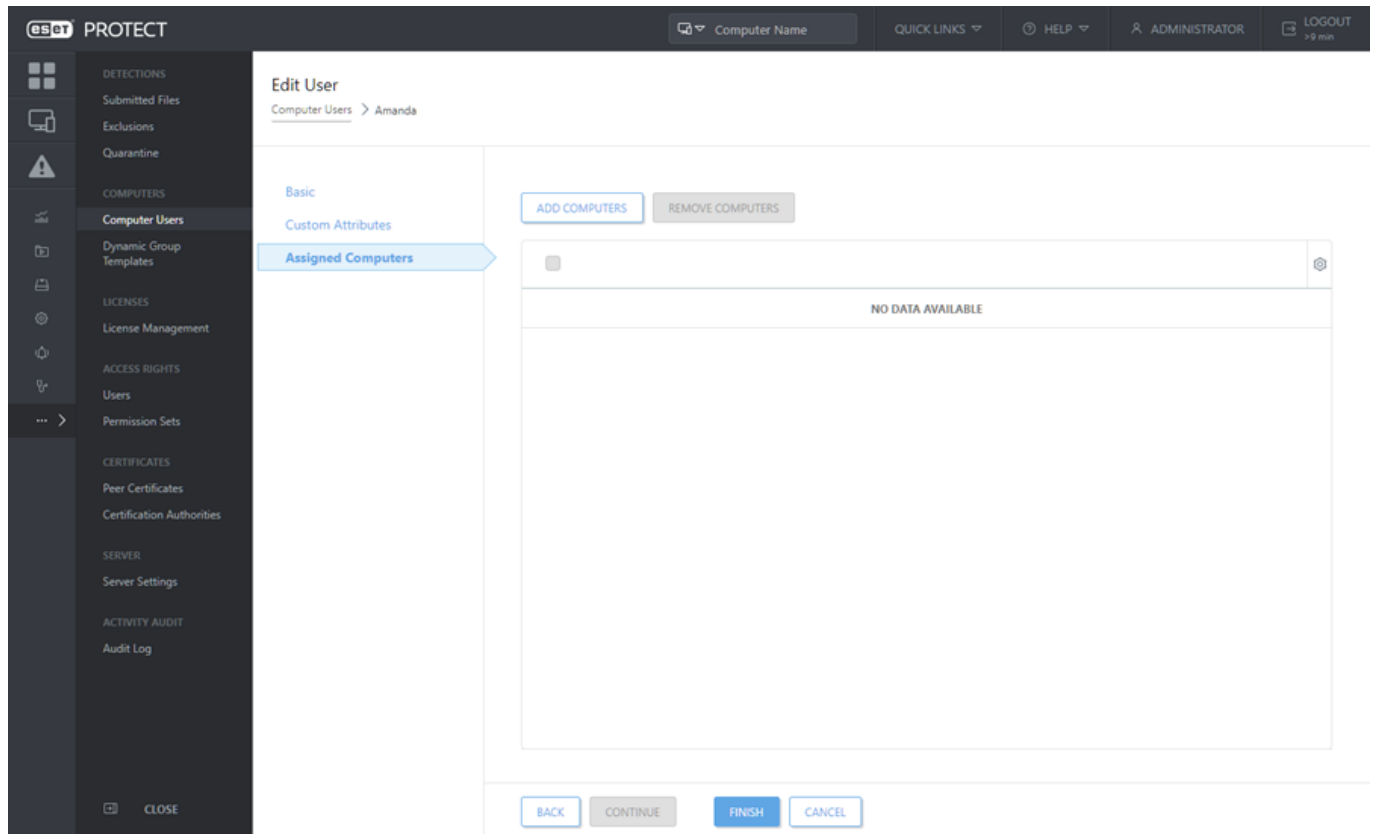


割り当てられたコンピューター


ここでは、個別のデバイスを選択できます。このためには、**コンピューターの追加** をクリックします。すべての静的および動的グループとそのメンバーが一覧表示されます。チェックボックスを使用して選択し、**[OK]** をクリックします。



ユーザーは1つの処理で最大200コンピューターにのみ割り当てることができます。

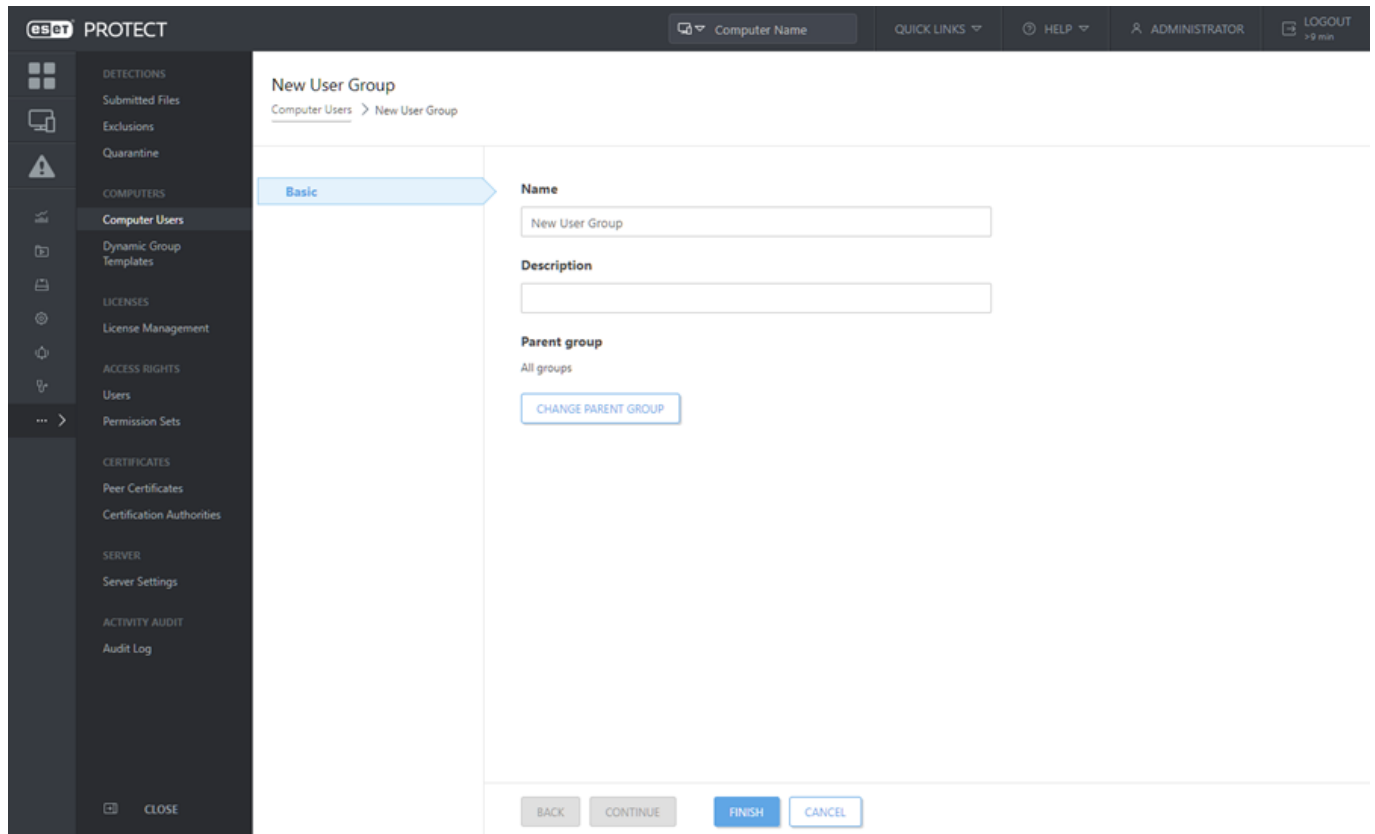


新しいユーザーグループの作成

[すべてのグループ] >  をクリックし、+ [新しいユーザーグループ] を選択します。

基本

新しいユーザーグループの**名前と説明**(任意)を入力します。既定では、親グループは、新しいユーザーグループの作成時に選択したグループです。親グループを変更する場合は、**親グループの変更**をクリックし、ツリーから親グループを選択します。**完了**をクリックして、新しいユーザーグループを作成します。



[アクセス権](#)から[権限設定](#)を使用して、このユーザーに特定の権限を割り当てることができます([ユーザーグループ](#)セクションを参照)。このように、特定のESET PROTECT コンソールユーザーが管理できる特定のユーザーグループを指定できます。必要に応じて、ポリシーを使用して、このようなユーザーのアクセスを他のESET PROTECT機能に制限することもできます。これらのユーザーはユーザーグループのみを管理します。

動的グループテンプレート









動的グループテンプレートは、コンピューターを[動的グループ](#)に配置するために満たす必要がある条件を確立します。これらの条件がクライアントで満たされると、自動的に該当する動的グループに移動されます。

i テンプレートは静的グループに保存される静的オブジェクトです。ユーザーはテンプレートにアクセスするために適切な[権限](#)が必要です。ユーザーが動的グループテンプレート进行操作するにはアクセス権が必要です。すべての定義済みテンプレートは静的グループすべてにあり、既定では管理者のみが使用できます。他のユーザーには[追加の権限を割り当てる必要があります](#)。結果として、ユーザーは既定のテンプレートを表示または使用できない可能性があります。テンプレートはユーザーが権限を持つグループに移動できます。テンプレートを複製するには、ソーステンプレートがあるグループ(動的グループテンプレート)に対する[使用権限](#)とユーザーのホームグループ(複製が保存される場所)に対する[書き込み権限](#)がユーザーに割り当てられている必要があります。[オブジェクトの複製の例](#)を参照してください。

- [新しい動的グループテンプレートの作成](#)
- [動的グループテンプレートのルール](#)
- [動的グループテンプレート - 例](#)

動的グループテンプレートの管理

テンプレートは、[詳細]>[動的グループテンプレート]から管理できます。

新しいテンプレート	クリックして、ホームグループで 新しいテンプレート を作成します。
 詳細を表示	選択したテンプレートの概要を参照してください。
 監査ログ	選択した項目の 監査ログ を表示します。
 タグ	タグ を編集します(割り当て、割り当て解除、作成、削除)。
 編集	選択したテンプレートを編集します。既存のテンプレートを保持し、編集集中のテンプレートに基づいて新しい名前を作成する場合は、[名前を付けて保存]をクリックします。確認されたら、新しいテンプレートの名前を指定します。
 複製	選択したテンプレートに基づいて、新しい動的グループテンプレートを作成します。複製タスクには新しい名前が必要です。重複するテンプレートはホームグループに保存されます。
 削除	テンプレートを完全に削除します。
インポート	ファイルから動的グループテンプレートをインポートします。インポート中には、ファイルが破損していないことを確認するために、ファイル構造が検証されます。
 エクスポート	バックアップまたは移行目的で、選択した動的グループテンプレートをファイルにエクスポートします。ファイルを編集することは推奨されません。データが利用できなくなる可能性があります。
 アクセス グループ	選択したテンプレートを別の静的グループに移動します。他の ユーザー でアクセスの問題を解決するときに有用です。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

新しい動的グループテンプレート

詳細>動的グループテンプレートの下の新規テンプレートをクリックします。

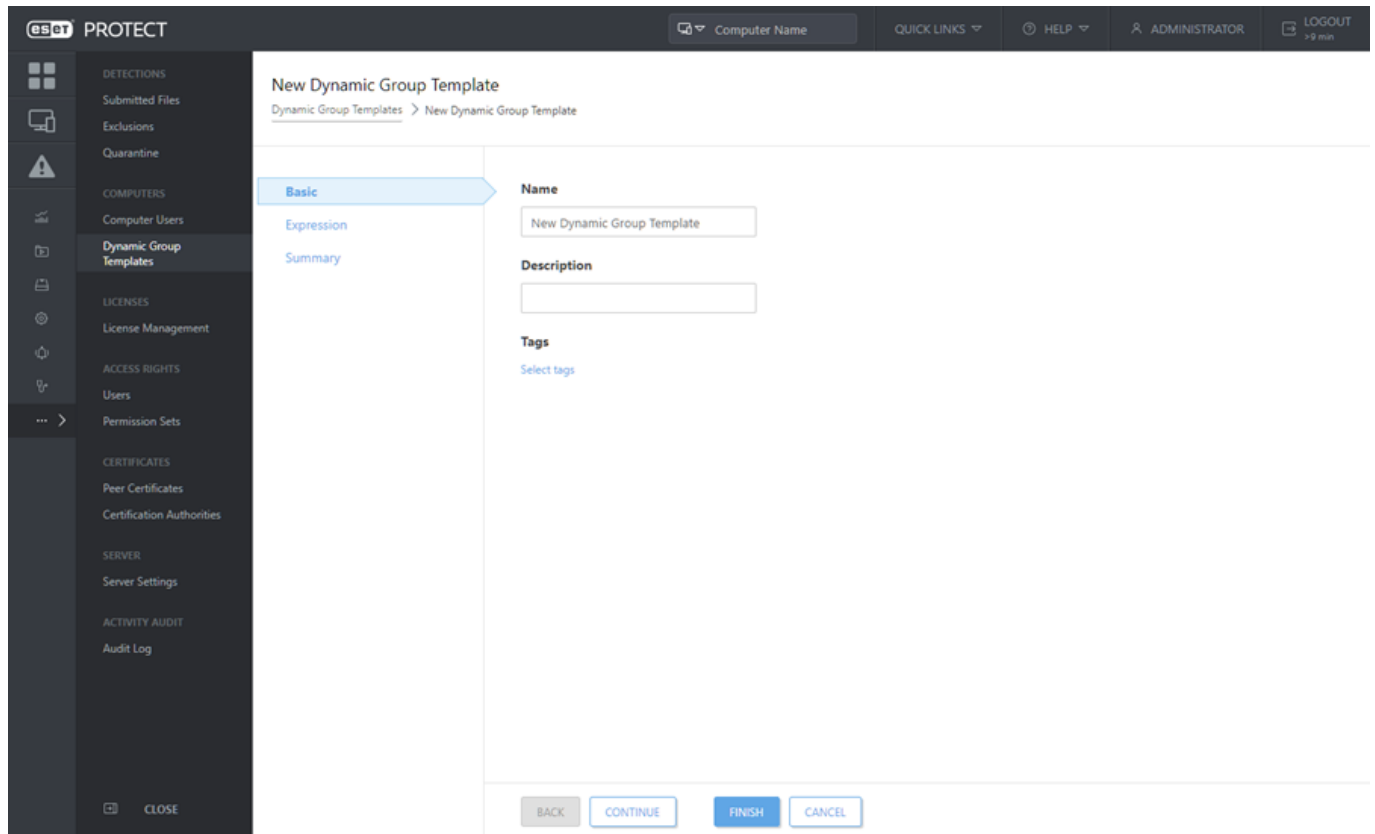
基本

新しい動的グループテンプレートの名前と説明を入力します。

タグを選択をクリックして、[タグを割り当て](#)ます。

式

ネットワーク上で動的グループを使用する方法の例については、[例](#)と図を使用した段階的な手順を参照してください。



概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

動的グループテンプレートのルール

動的グループテンプレートのルールを設定するときには、異なる条件でさまざまな演算子を使用し、目的のシナリオを実現できます。

次の章では、動的グループテンプレートで使用されるルールと処理を説明します。

- [演算子](#)
- [ルールと論理接続](#)
- [テンプレートルール評価](#)
- [ESET PROTECTで自動化を作成する方法](#)
- [動的グループテンプレート](#)
- [使用例 - 特定の動的グループテンプレートの作成](#)

演算子

複数のルール(条件)を指定する場合は、ルールを組み合わせるために使用される演算子を選択する必要があります。

があります。結果によっては、クライアントコンピューターが、このテンプレートを使用する動的グループに追加される場合とされない場合があります。

i

- 選択した演算子は、その他のルールを組み合わせるときにのみ動作しますが、1ルールしかないときにも動作します。
- 演算子の組み合わせはできません。動的グループにつき1つの演算子だけを使用し、すべてのルールに適用します。

AND（すべての条件が真であること）	すべての条件が真として評価されるかどうかを確認します。コンピューターはすべての必須パラメーターを満たす必要があります。
OR（1つ以上の条件が真でなければなりません）	条件の1つ以上が真として評価されるかどうかを確認します。コンピューターは必須パラメーターのいずれかを満たす必要があります。
NAND（1つ以上の条件が偽でなければなりません）	少なくとも条件の1つが真として評価できないかどうかを確認します。コンピューターは1つ以上の必須パラメーターを満たしていません。
NOR（すべての条件が偽でなければなりません）	すべての条件を真として評価できないかどうかを確認します。コンピューターはすべての必須パラメーターを満たしていません。

ルールと論理接続

ルールには、項目、論理コネクター(論理演算子)、定義済みの値があります。

[+ ルールの追加]をクリックすると、ポップアップウィンドウが開き、項目がカテゴリ別の一覧表示されます。例:

インストールされたソフトウェア>アプリケーション名

ネットワークアダプタ>MACアドレス

OSエディション>OS名

[このESETナレッジベース記事](#)で、すべての使用可能なルールの一覧を参照できます。

ルールを作成するには、項目を選択し、論理演算子を選択して、値を指定します。ルールは、指定した値と使用される論理演算子に従って評価されます。

指定できる値タイプには、数値、文字列、列挙型IPアドレス、製品マスク、コンピュータIDがあります。各値タイプには、異なる論理演算子が関連付けられESET PROTECT Webコンソールは自動的にサポートされたものだけを表示します。

- “= (等しい)” – シンボル値とテンプレート値が一致する必要があります。文字列は大文字と小文字を区別せずに比較されます。
- “> (より大きい)” – シンボル値はテンプレート値よりも大きくなければなりませんIPアドレスシンボルの範囲比較を作成するために使用することもできます。
- “≥ (以上)” – シンボル値はテンプレート値以上でなければなりませんIPアドレスシンボルの範囲比較を作成するために使用することもできます。
- “< (未満)” – シンボル値はテンプレート値よりも小さくなければなりませんIPアドレスシンボルの範囲比較を作成するために使用することもできます。
- “≤ (以下)” – シンボル値はテンプレート値以下でなければなりませんIPアドレスシンボルの範囲比較を作成するために使用することもできます。

囲比較を作成するために使用することもできます。

- **“含む”** – シンボル値はテンプレート値を含む必要があります。文字列の場合、サブ文字列を検索します。検索では大文字と小文字は区別されません。
- **“前方一致”** – シンボル値にはテンプレート値と同じテキストプレフィックスがあります。文字列は大文字と小文字を区別せずに比較されます。例えば `Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319` のプレフィックスは、`Microsoft` などです。
- **“後方一致”** – シンボル値にはテンプレート値と同じテキストポストフィックスがあります。文字列は大文字と小文字を区別せずに比較されます。検索された文字列から正確な最初の数文字を設定します。例えば `Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319` のポストフィックスは、「319」、「0.30319」などです。
- **“マスク”** – シンボル値はテンプレートで定義されたマスクと一致する必要があります。マスクの書式設定では、任意の文字と特殊記号「*」（ゼロ、1文字以上の文字）を使用できます。「?」は1文字を表します(例: “6.2.*” または “6.2.2033.?”)。
- **“正規表現”** – シンボル値はテンプレートの正規表現(regex)と一致する必要があります。正規表現はPerlで記述される必要があります。

i 正規表現として、*regex* または *regexpl* は、検索パターンを定義する文字の順序です。たとえば、*gray/grey* と *gr(a/e)y* は次の2つの単語と一致する同等のパターンです。 “gray” “grey”

- **“のいずれか”** – シンボル値はテンプレートのリストの任意の値と一致する必要があります。項目を追加するには、+ **追加** をクリックします。リストの新しい項目の各行。文字列は大文字と小文字を区別せずに比較されます。
- **“のいずれか(文字列マスク)”** – シンボル値はテンプレートのリストの任意のマスクと一致する必要があります。文字列は大文字と小文字を区別して比較されます。例: `*endpoint-pc*`, `*Endpoint-PC*`
- **“値がある”**

否定演算子:

! 否定演算子は注意して使用する必要があります。「インストールされたアプリケーション」などの複数行のログの場合には、すべての行がこれらの条件によって評価されます。本書の例([テンプレートルール評価](#)および[動的グループテンプレート - 例](#))を参照し、否定演算子または否定演算を使用して、想定された結果を得る方法について確認してください。

- **“≠ (等しくない)”** – シンボル値とテンプレート値が一致してはなりません。文字列は大文字と小文字を区別せずに比較されます。
- **“含まない”** – シンボル値にはテンプレート値が含まれません。検索では大文字と小文字は区別されません。
- **“前方一致しない”** – シンボル値にはテンプレート値と同じテキストプレフィックスがありません。文字列は大文字と小文字を区別せずに比較されます。
- **“後方一致しない”** – シンボル値にはテンプレート値と同じテキストポストフィックスがありません。文字列は大文字と小文字を区別せずに比較されます。
- **“マスクがない”** – シンボル値はテンプレートで定義されたマスクと一致してはなりません。

- “正規表現ではない” – シンボル値はテンプレートの正規表現(regex)と一致してはなりません。正規表現はPerlで記述される必要があります。否定演算は、再作成せずに、正規表現との一致を否定できるように提供されました。
- “のいずれかではない” – シンボル値はテンプレートのリストの任意の値と一致してはなりません。文字列は大文字と小文字を区別せずに比較されます。
- “のいずれかではない(文字列マスク)” – シンボル値はテンプレートのリストの任意のマスクと一致しない必要があります。
- “値がない”

テンプレートルール評価

テンプレートルール評価はESET ManagementサーバーではなくESET PROTECTエージェントによって処理されます(結果のみがESET PROTECTサーバーに送信されます)。評価処理は、テンプレートで構成されている[ルール](#)に従って実行されます。以下に、テンプレートルール評価プロセスの例をいくつか示します。

存在のテスト(その値で何も存在しない)および差異のテスト(何かが存在するが値が異なる)を識別する必要があります。これを識別する基本ルールは以下のとおりです。

- 存在を検証するには:否定なしの演算子(**AND**および否定なしの演算子(=, ><含む...))
- 異なる値の存在を検証するには:演算子**AND**および1つ以上の否定演算子を含む演算子(=><含む...)

- ✓ 値が存在しないことを検証するには否定の演算子(**NAND**および否定なしの演算子=><含む...)

項目のリスト(コンピューターにインストールされているアプリケーションの特定のリストなど)の存在を検証するには、リストの各項目に対して個別の動的グループテンプレートを作成し、そのテンプレートを個別の動的グループに割り当てます。各動的グループは、別の動的グループのサブグループです。コンピューターと項目のリストは最後のサブグループにあります。

状態はさまざまな情報が集約されたものです。各コンピューターの1次元的な状態(オペレーティングシステムRAMサイズなど)を提供するソースと、多次元的な状態(IPアドレス、インストール済みのアプリケーションなど)を提供するものがあります。

次に、クライアントの状態を視覚的に示します。

ネットワークアダプタ - IPアドレス	ネットワークアダプタ - MACアドレス	OS名	OSバージョン	HW - RAMサイズ(MB)	インストール済みアプリケーション
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

ステータスは情報のグループです。1つのグループのデータは常に一貫した情報を行に整理して提供します。各グループの行数は異なる場合があります。

条件はグループ単位、行単位で評価されます。1つのグループの列に関する条件が多い場合は、同じ行の値だけが考慮されます。

例1:

この例では、次の条件が考慮されます。

ネットワークアダプタ .IPアドレス = 10.1.1.11 ANDネットワークアダプタ .MACアドレス = 4A-64-3F-10-FC-75

このルールには一致するコンピューターがありません。両方の条件が真になる行がないためです。

ネットワークアダプタ -IPアドレス	ネットワークアダプタ -MACアドレス	OS名	OSバージョン	HW - RAMサイズ(MB)	インストール済みアプリケーション
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

例2:

この例では、次の条件が考慮されます。

ネットワークアダプタ .IPアドレス = 192.168.1.2 ANDネットワークアダプタ .MACアドレス = 4A-64-3F-10-FC-75

ここでは、両方の条件が同じ行のセルと一致したため、ルール全体が真であると評価されます。コンピューターが選択されます。

ネットワークアダプタ -IPアドレス	ネットワークアダプタ -MACアドレス	OS名	OSバージョン	HW - RAMサイズ(MB)	インストール済みアプリケーション
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

例3:

OR演算子(1つ以上の条件が真である)の場合

ネットワークアダプタ .IPアドレス = 10.1.1.11 ORネットワークアダプタ .MACアドレス = 4A-64-3F-10-FC-75

2つの行のルールが真です。条件のいずれかだけが満たされる必要があるためです。コンピューターが選択されます。

ネットワークアダプタ -IPアドレス	ネットワークアダプタ -MACアドレス	OS名	OSバージョン	HW - RAMサイズ(MB)	インストール済みアプリケーション

ネットワークアダプタ - IPアドレス	ネットワークアダプタ - MACアドレス	OS名	OSバージョン	HW - RAMサイズ(MB)	インストール済みアプリケーション
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

動的グループテンプレート - 例

詳細>動的グループテンプレートで、便利な定義済みの動的グループテンプレートを見つけることができます。

このガイドの動的グループテンプレートの例は、動的グループを使用してネットワークを管理する方法のいくつかを示します。

[セキュリティ製品がインストールされているかどうかを検出する動的グループ](#)

[特定のバージョンのソフトウェアがインストールされているかどうかを検出する動的グループ](#)

[特定のバージョンのソフトウェアがインストールされていないかどうかを検出する動的グループ](#)

[特定のバージョンのソフトウェアがインストールされていないか、別のバージョンが存在するかどうかを検出する動的グループ](#)

[コンピューターが特定のサブネットにあるかどうかを検出する動的グループ](#)

[インストールされ、アクティベーションされていないサーバーセキュリティ製品のバージョンを検出する動的グループ](#)

[新しく接続されたWindowsデスクトップで自動的にESET製品を展開する方法](#)

[ロケーションに基づくポリシーを強制する方法](#)

動的グループテンプレートと使用の例に関するナレッジベース記事も参照してください。

[ESET PROTECT9](#)で役に立つ動的グループテンプレートの例 - たとえば、[HW インベントリ](#)詳細を使用して、選択したHW条件を満たすデバイスを含む動的グループのルールを作成できます。

[ESET PROTECTを設定し、ESETエンドポイント製品を自動的に保護されていないコンピューターに展開する](#)

[ESET PROTECTを使用して接続しているネットワークに応じて、異なるアップデート設定を使用するようにエンドポイントを構成する](#)

[ESET PROTECTの動的グループに自動的に参加するように新しいワークステーションの新しい証明書を作成する](#)

i 言語によっては、ナレッジベース記事が提供されていない場合があります。

当然、ルールを組み合わせ、動的グループテンプレートを使用すると、その他の目的も実現できます。さまざまな可能性があります。

動的グループ – セキュリティ製品がインストールされている

この動的グループを使用すると、ESETセキュリティ製品がコンピューターにインストールされた後すぐに、認証、カスタム検査などのタスクを実行できます。

詳細 > 動的グループテンプレートの下で新しいテンプレートを作成し、テンプレートと新しい動的グループを作成します。

基本

新しい動的グループテンプレートの名前と説明を入力します。

式

1. [\[処理\]](#) メニューの論理演算子を選択します。 **AND** (すべての条件が真であること)
2. +ルールの追加をクリックして、[条件](#)を選択します。 [コンピューター] > [管理された製品マスク] > [のいずれか] > [ESET保護: デスクトップ]を選択します。別のESET製品を選択することもできます。

概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

動的グループ – 特定のソフトウェアバージョンがインストールされている

この動的グループを使用すると、コンピューターにインストールされているESETセキュリティソフトウェアを検出できます。これらのコンピューターでは、アップグレードタスクなどを実行したり、カスタムコマンドを実行できます。「含む」や「前方一致」などの異なる演算子を使用できます。

詳細 > 動的グループテンプレートの下で新しいテンプレートを作成し、テンプレートと新しい動的グループを作成します。

基本

新しい動的グループテンプレートの名前と説明を入力します。

式

1. [\[処理\]](#) メニューの論理演算子を選択します。 **AND** (すべての条件が真であること)
2. +ルールの追加をクリックして、[条件](#)を選択します。
 - [インストールされたソフトウェア] > [アプリケーション名] > [= (等しい)] > [ESET Endpoint Security]

•[インストールされたソフトウェア]>[アプリケーションバージョン]>[=(等しい)]>
[6.2.2033.0]

概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

動的グループ – 特定のバージョンのソフトウェアがインストールされていない

この動的グループを使用すると、コンピューターにインストールされていないESETセキュリティソフトウェアを検出できます。この例の設定には、ソフトウェアがまったくインストールされていないコンピューターまたは指定されたバージョン以外のコンピューターが含まれます。

このグループは便利であり、これらのコンピューターでは、ソフトウェアインストールタスクを実行して、インストールまたはアップグレードができます。「含む」や「前方一致」などの異なる演算子を使用できます。

詳細> 動的グループテンプレートの下の新規テンプレートをクリックします。

基本

新しい動的グループテンプレートの名前と説明を入力します。

式

1.[\[処理\]](#)メニューの論理演算子を選択します。**NAND** (1つ以上の条件が偽でなければなりません)

2.+ルールの追加をクリックして、[条件](#)を選択します。

•[インストールされたソフトウェア]>[アプリケーション名]>[=(等しい)]>[ESET Endpoint Security]

•[インストールされたソフトウェア]>[アプリケーションバージョン]>[=(等しい)]>
[6.2.2033.0]

概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

動的グループ – 特定のバージョンのソフトウェアがインストールされてなく、他のバージョンが存在

する

この動的グループを使用すると、要求しているバージョンとは別のバージョンのソフトウェアがインストールされていることを検出します。このグループは便利で、必要なバージョンがインストールされていないコンピュータでアップグレードタスクを実行できます。別の演算子を使用できますが、バージョンテストが否定演算子を使用して完了していることを確認してください。

詳細 > 動的グループテンプレートの下の **新規テンプレート** をクリックします。

基本

新しい動的グループテンプレートの **名前** と **説明** を入力します。

式

1. [\[処理\]](#) メニューの論理演算子を選択します。 **AND** (すべての条件が真であること)
2. **+ルールの追加** をクリックして、 [条件](#) を選択します。
 - [インストールされたソフトウェア] > [アプリケーション名] > [= (等しい)] > [ESET Endpoint Security]
 - [インストールされたソフトウェア] > [アプリケーションバージョン] > [≠ (等しくない)] > [6.2.2033.0]

概要

構成された設定を確認し、**[完了]** をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から [新しい動的グループを作成](#) するために使用できます。

動的グループ – コンピュータが特定のサブネットにある

この動的グループを使用して、特定のサブネットを検出できます。次に、これを使用して **Web** コントロールまたはアップグレード用のカスタムポリシーを適用できます。別の範囲を指定できます。

詳細 > 動的グループテンプレートの下の **新規テンプレート** をクリックします。

基本

新しい動的グループテンプレートの **名前** と **説明** を入力します。

式

1. [\[処理\]](#) メニューの論理演算子を選択します。 **AND** (すべての条件が真であること)
2. **+ルールの追加** をクリックして、 [条件](#) を選択します。
 - [ネットワークIPアドレス] > [アダプタIPアドレス] > [\geq (以上)] > [10.1.100.1]

- [ネットワークIPアドレス] > [アダプタIPアドレス] > [≤ (以下)] > [10.1.100.254]
- [ネットワークIPアドレス] > [アダプタサブネットマスク] > [= (等しい)] > [255.255.255.0]

概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

動的グループ – インストールされ、アクティベーションされていないバージョンのサーバーセキュリティ製品

この動的グループを使用して、アクティベーションされていないサーバー製品を検出できます。これらの製品が検出されると、クライアントタスクをこのグループに割り当て、適切なライセンスでクライアントコンピュータをアクティベーションできます。この例ではESET Mail Security for Microsoft Exchange Serverのみが指定されていますが、複数の製品を指定できます。

詳細 > 動的グループテンプレートの下の新規テンプレートをクリックします。

基本

新しい動的グループテンプレートの名前と説明を入力します。

式

1. [\[処理\]](#) メニューの論理演算子を選択します。AND (すべての条件が真であること)
2. +ルールの追加をクリックして、[条件](#)を選択します。
 - [コンピューター] > [管理された製品マスク] > [のいずれか] > [ESET保護: メールサーバー]
 - [機能/保護の問題] > [ソース] > [= (等しい)] > [セキュリティ製品]
 - [機能/保護の問題] > [問題] > [= (等しい)] > [アクティベーションされていない製品]

概要

構成された設定を確認し、[完了]をクリックして、テンプレートを作成します。この新しいテンプレートはすべてのテンプレートのリストに追加され、後から[新しい動的グループを作成](#)するために使用できます。

ESET PROTECTを自動化する方法

以下に示す例のような手法を使用すると、製品とOSのアップデート、検査、およびあらかじめ選択されたライセンスによる新しく追加された製品の自動アクティベーションから高度なインシデントの解決まで、さまざまなアクションを自動化できます。

新しく接続されたWindowsデスクトップで自動的にESET製品を展開する方法



この例は、サードパーティのセキュリティソフトウェアまたはホームセグメントのESETセキュリティソフトウェア（例：ESET Smart Security[®]）がないクライアントでのみ実行する必要があります。サードパーティセキュリティソフトウェアがあるクライアントでESET製品をインストールすることは推奨されません。[ESET AV Remover](#)を使用して、コンピューターから他のウイルス対策プログラムを削除できます。

1. セキュリティ製品なしという動的グループを作成します。
 - a. 定義されたグループ **Windows コンピューター > Windows (デスクトップ)** の子グループにします。
 - b. **新規テンプレート** をクリックします。
 - c. 次のルールを追加します。[**コンピューター**] > [**管理された製品マスク**] を選択します。
 - d. 演算子として **等しくない** を選択します。
 - e. マスク ☐ **ESET保護: デスクトップ**
 - f. [**完了**] をクリックしてグループを保存します。
2. **タスク > 新規 > + クライアントタスク** に移動します。
 - a. [タスク] ドロップダウンメニューから **ソフトウェアインストール** を選択し、**名前** にタスクの名前を入力します。
 - b. [**設定**] セクションでパッケージを選択し、必要に応じて他のパラメーターを設定します。
 - c. [**完了**] > [**トリガーの作成**] をクリックします。
 - d. [**ターゲット**] セクションで、[**グループの追加**] をクリックし、[**セキュリティ製品なし**] を選択します。
 - e. [**トリガー**] セクションで、[**結合された動的グループトリガー**] を選択します。
 - f. [**完了**] をクリックしてタスクとトリガーを保存します。

このタスクは、この時点以降に動的グループに接続されたクライアントで実行されます。タスクが作成される前に動的グループにあったクライアントでこのタスクを手動で実行する必要があります。

ロケーションに基づくポリシーを強制する方法

1. **Subnetwork 120** という動的グループを作成します。
 - a. すべてのグループの子グループにします。
 - b. **新規テンプレート** をクリックします。
 - c. ルールを追加します。ネットワークIPアドレス > IPサブネットワーク[®]
 - d. 演算子として **等しい** を選択します。
 - e. 10. 1. 120. 0などのフィルタリングするサブネットワークを入力します（最後の数値は0にし、10. 1. 120. サブネットワークからすべてのIPアドレスをフィルタリングする必要があります）。
 - f. [**完了**] をクリックしてグループを保存します。
2. [**ポリシー**] に移動します。
 - a. [**新しいポリシー**] をクリックし、ポリシーに **名前** を付けます。
 - b. [**設定**] セクションで **ESET Management エージェント** を選択します。
 - c. ポリシーを変更します。たとえば、**接続間隔** を5分に変更します。
 - d. [**割り当て**] セクションで、[**割り当て**] をクリックし、**Subnetwork120**グループの横のチェックボックス ☒ をオンにして、**OK** をクリックして確認します。
 - e. [**完了**] をクリックしてポリシーを保存します。

このポリシーは、この時点以降に動的グループに接続されたクライアントで適用されます。



クライアントコンピューターが動的グループから移動するとき（動的グループメンバーシップと一致する条件が有効ではなくなるとき）、適用されたポリシー設定がどうなるかを確認するには、[ポリシー削除ルール](#)を参照してください。

[ここで](#)他の例の一覧を参照してください。

ライセンス管理

ESETビジネス製品のライセンスを購入すると、自動的にESET PROTECTにアクセスできるようになります。ESET PROTECTを使用して、メインメニューの[詳細 > ライセンス管理](#)の下で、ライセンスを簡単に管理できます。ESETが発行したユーザー名とパスワードがあり、製品認証キーに変換する場合は、「[レガシーライセンス資格情報の変換](#)」を参照してください。ユーザー名とパスワードは製品認証キー/ライセンスIDに置き換えられました。製品認証キーは、ライセンス所有者とアクティベーション自体を識別するために使用される一意の文字列です。

ESET PROTECTを使用して[ESETビジネス製品](#)を[アクティベーション](#)できます。

ライセンス管理の権限

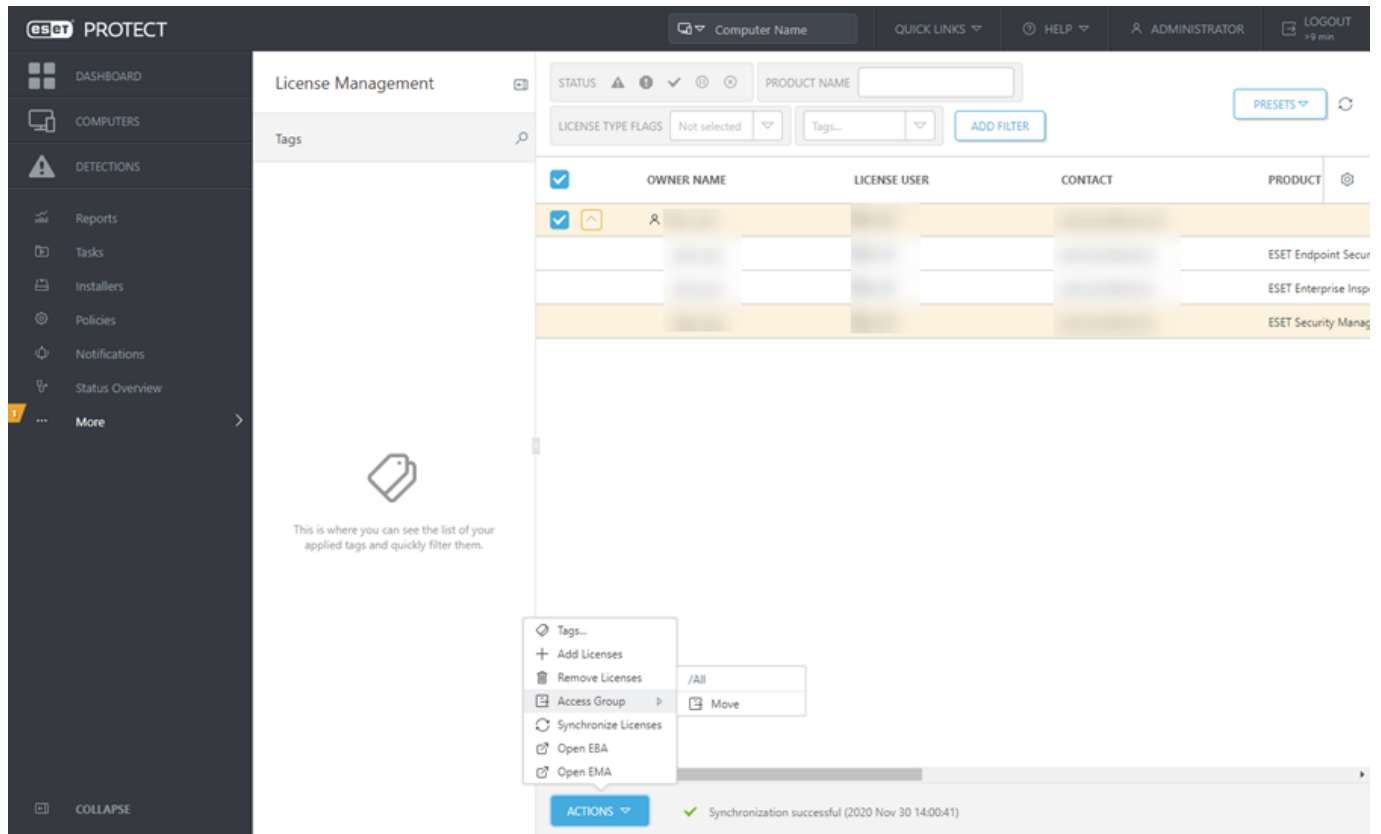
各ユーザーにはライセンスの[権限](#)を割り当てることができます。権限は、権限設定が割り当てられている静的グループに含まれているライセンスでのみ有効です。各タイプの権限で、ユーザーは[異なるアクション](#)ができます。



ホームグループが[すべて](#)に設定され、ホームグループのライセンスに対する[書き込み](#)権限がある管理者のみが、ライセンスを追加または削除できます。各ライセンスは[ライセンスID](#)で特定され、1つ以上の単位を含めることができます。ライセンスは管理者によってのみ十分な[権限](#)がある他のユーザーに配布できます。ライセンスは減らすことはできません。

MSPアカウントをインポートするときには、すべてのライセンスが1つのライセンスプールに保存されます。プールからライセンスを移動することはできません。ライセンスプール全体は移動できます。プールを移動するには、プール > [アクション > アクセスグループ > 移動](#)を選択し、新しいアクセスグループを選択します。後からMSPアカウントを同期する場合は、新しいライセンスがプールの実際の場所に表示されます。

Webコンソールのライセンス管理



同じESET Business Accountユーザーまたは同じ会社のライセンスは、ライセンスプールにグループ化されます。☒をクリックすると、ライセンスプールを展開し、ライセンス詳細が表示されます。

ESET Business AccountとESET PROTECTでは、各ライセンスは次の方法で識別されます。

- **ライセンスID**

- **ライセンスタイプ** - ビジネス(正規ライセンス)、**試用版**(試用ライセンス)、**MSP** (マネージドサービスプロバイダーライセンス)、および**NFR** (非再販ライセンス)です。

追加のライセンス情報:

- **所有者名と連絡先**
- **ライセンスユーザー名とタイプ**: **会社** **サイト** **MSP顧客**
- **ライセンス対象となるセキュリティ製品名**
- **ライセンスのステータス**(ライセンス有効期限が切れや使用超過、または有効期限切れや使用超過の危険がある場合、警告メッセージがここに表示されます)
- このライセンスでアクティベーションできる**単位数**と、オフライン単位数。ESET Mail Security製品の場合、ライセンス使用状況はアクティベーションで使用される**サブ単位**に基づいて計算されます。
- ESETサーバー製品の**サブ単位数**(メールボックス、ゲートウェイ保護、接続)。
- **ライセンスの有効期限**。

○サブスクリプションライセンスには有効期限がない場合があります。

ステータスでライセンスをフィルタリングできます。

✓ OK - 緑	ライセンスは正常にアクティベーションされました。
▲ エラー - 赤	ライセンスは登録されていないか、有効期限切れか、使用超過です。
⚠ 警告 - オレンジ	ライセンスはすべて使用されているか、まもなく期限切れです(30日以内に期限切れ)。
⏸ アクティベーション解除または一時停止	ライセンスはアクティベーション解除または一時停止されました。
🕒 古い	ライセンスは期限切れです。

アクションボタンをクリックして、選択したライセンスプールを管理します。

🏷 タグ	タグ を編集します(割り当て、割り当て解除、作成、削除)。
➕ ライセンスの追加	<p>[ライセンスの追加]をクリックして、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。</p> <p>1.ESET Business AccountまたはESET MSP Administrator - ESET Business AccountまたはEMA 2およびすべてのライセンスをライセンス管理セクションに接続します。ESET PROTECTは、ESET License AdministratorおよびESET MSP Administratorと後方互換性があるためESET Business Accountではなく、セキュリティ管理者認証情報を使用できます。</p> <p>2.製品認証キー-有効なライセンスの製品認証キーを入力して、ライセンスの追加をクリックします。製品認証キーは、アクティブなサーバーに対して検証され、リストに追加されます。</p> <p>3.オフラインライセンスファイル-ライセンスファイル(.lic)を追加して、ライセンスの追加をクリックします。ライセンスファイルが検証され、ライセンスがリストに追加されます。</p> <p>所有者名列のアイコンに基づいて、ライセンスの追加方法を確認できます。 オフラインライセンスファイル 製品認証キー、または ESET Business AccountまたはESET MSP Administrator</p>
🗑 ライセンスの削除	選択したライセンスプールを削除します。このアクションの確認が要求されます。ライセンスを削除しても、製品のアクティベーションは解除されませんESET PROTECT ライセンス管理 でライセンスを削除してもESET製品はアクティベーションされたままです。
📁 アクセスグループ	選択したライセンスプールを別の静的グループに移動します。
🔄 ライセンスの同期	ESET PROTECTのライセンス情報をただちに更新します。ライセンスは、1日1回、自動的にESETライセンスサーバーと同期されますESET Business Accountを使用している場合ESET License AdministratorまたはESET MSP Administratorライセンスは、1日1回、自動的にこれらのサービスと同期されます。
🔗 EBAを開く	ESET Business Accountポータル を開きます。
🔗 EMAを開く	ESET MSP Administratorポータル を開きます。

ライセンスプールを展開し、ライセンスをクリックして、次のアクションを実行します。アクションセットは、選択したライセンスのタイプによって異なります。

▶ アクティベーションでライセンスを使用する	このライセンスを使用して、 製品のアクティベーションタスク を実行します。
📄 オールインワンインストーラーの作成	オールインワンエージェントインストーラー で選択したライセンスを使用します。

 タグ	タグ を編集します(割り当て、割り当て解除、作成、削除)。
 ライセンスを管理	ライセンスがESET Business AccountまたはESET MSP Administratorから同期されている場合は、ライセンスを管理できます。ライセンスが使用超過の場合は、ライセンス数を増やしたり、一部のデバイスをアクティベーション解除できます。
 ライセンスの更新	ESET Business AccountまたはESET MSP Administratorで、期限切れ、一時停止またはアクティベーション解除されたライセンスを更新します。
 ライセンスのアップグレード	ESET Business AccountまたはESET MSP Administratorの試用ライセンスをアップグレードします。
 監査ログ	選択した項目の 監査ログ を表示します。
 公開ライセンスIDのコピー	公開ライセンスIDをクリップボードにコピーします。

サブスクリプションライセンス

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またはESET MSP Administrator](#)、あるいは [製品認証キー](#)を使用してこのような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](#) または [コンピューター > 詳細を表示](#) の下で、サブスクリプションの有効期限を確認できます。サブスクリプションライセンスから [オフラインライセンス](#) ファイルを作成することはできません。

ESET Business Accountサイトのサポート

[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。


ESETビジネス製品のアクティベーション

次の2つのタスクを使用して、ライセンスをESET PROTECTからESET製品に配布できます。

- [ソフトウェアインストールタスク](#)
- [製品アクティベーションタスク](#)

ESETビジネス製品のアクティベーション解除

ESET PROTECT Webコンソールを使用すると、次の複数の方法で、ESETビジネス製品をアクティベーション解除(製品からライセンスを削除)できます。

- コンピューターでコンピューターを選択し、 **製品のアクティベーション解除**を選択するとESETライセンスサーバー経由で選択したすべてのデバイスから削除されますESET PROTECTからアクティベーションされていない場合や、ライセンスがESET PROTECTによって管理されていない場合でも、製品がアクティベーション解除されます。

i

複数のESET製品(ESETエンドポイント製品とESET Enterprise Inspectorエージェントなど)がインストールされている1つのコンピューターのみを選択する場合は、個別の製品をアクティベーション解除することを選択できます。

- [コンピューターを管理から削除する](#)
- ライセンスのアクティベーション解除オプションで、[接続していないコンピューターの削除](#)タスクを作成します。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

支店の管理者間でライセンスを共有する

3人のユーザーと管理者があり、各ユーザーには独自のホームグループがあります。

- John San Diego
- Larry Sydney
- Makio Tokyo

管理者は3つのライセンスを [インポート](#) します。これらは静的グループすべてに含まれ、他のユーザーはこれらを使用できません。

✓ ライセンスを別のユーザーに割り当てるには、管理者は、別のユーザーに割り当てるライセンスプールの横のチェックボックスをクリックし、**アクション**ボタンをクリックしてから、 **アクセスグループ** > **移動** をクリックして、ユーザーが権限を持つグループを選択します。ユーザー John では、グループ San Diego を選択します。ライセンスを使用するには、John は、グループ San Diego のライセンスの [使用権限](#) が必要です。

ユーザー John がログインすると、自分のグループに移動されたライセンスのみを表示および使用できます。管理者は Larry と Makio に対してこのプロセスを繰り返します。その後で、ユーザーは自分のライセンスのみを表示できます。管理者はすべて表示できます。

ESET Business Account または ESET MSP Administrator

ホームグループがすべてに設定され、ホームグループのライセンスに対する **書き込み** 権限がある管理者のみが、ライセンスを追加または削除できます。各ライセンスは **ライセンスID** で特定され、1つ以上の単位を含めることができます。ライセンスは管理者によってのみ十分な [権限](#) がある他のユーザーに配布できます。ライセンスは減らすことはできません。

ESET Business Account または ESET MSP Administrator 2 認証情報

ESET Business Account または ESET MSP Administrator 2 資格情報 (ESET PROTECT は ESET PROTECT License Management ですべての委任ライセンスを表示します) を入力、**ライセンスの追加** をクリックします。

Add License

×

You can add your license using one of the following options:

☒ ESET Business Account or ESET MSP Administrator

☐ License Key

☐ Offline License File

ESET Business Account or ESET MSP Administrator Login

Password

Show password

Note: You can use ESET License Administrator Security Admin account credentials as well, however we do recommend to migrate your licenses to the new [ESET Business Account](#).

ADD LICENSES

CANCEL

ESET License Administrator, セキュリティ管理者

ESET PROTECTは、ESET License AdministratorおよびESET MSP Administratorとの後方互換性があります。ログインの代わりに、**セキュリティ管理者**資格情報(ESET Business AccountERA 6.xと同様)を入力できます。

ライセンスの追加 – ライセンスキー



ホームグループが**すべて**に設定され、ホームグループのライセンスに対する**書き込み**権限がある管理者のみが、ライセンスを追加または削除できます。各ライセンスは**ライセンスID**で特定され、1つ以上の単位を含めることができます。ライセンスは管理者によってのみ十分な**権限**がある他のユーザーに配布できます。ライセンスは減らすことはできません。

ライセンスキー

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**製品認証キー**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、**ライセンスの追加**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、認証情報を製品認証キー

に変換します。ライセンスが登録されていない場合は、登録処理が実行されます。ライセンスが登録されていない場合、登録処理が開始します。これはEBAポータルで実行されます(ESET PROTECTは、ライセンスの発行元に基づいて登録用の有効なURLを提供します)。

Add License

You can add your license using one of the following options:

☐ ESET Business Account or ESET MSP Administrator

☒ License Key

☐ Offline License File

License Key

[I have a Username and Password, what do I do?](#)

ADD LICENSES

CANCEL

オフラインアクティベーション

ESET Business Accountポータルからライセンスファイルを使用してESET PROTECTおよび他のESETセキュリティ製品をアクティベーションできます。各オフラインライセンスファイルは、ESET Endpoint Securityなどの1つの製品でのみ生成されます。オフラインライセンスファイルは、ESETライセンスサーバーにアクセスすることがないクライアントでのみ使用してください(クライアントが、ESETサービスへのアクセスが制限されたプロキシ経由でインターネットに接続されている場合でも、オフラインライセンスを使用しないでください)。サブスクリプションライセンスからオフラインライセンスファイルを作成できません。

既存のオフラインライセンスを置換するには、

- 1.ESET PROTECTで古いライセンスを削除し、ESET Business Accountでライセンスファイルを削除します。

- 2.ESET Business Accountで新しいオフラインライセンスを[作成](#)します。
- 3.新しいライセンスをESET PROTECTにインポートする
- 4.[***](#)新しいライセンスで製品を再アクティベーションします。



ホームグループが**すべて**に設定され、ホームグループのライセンスに対する**書き込み**権限がある管理者のみが、ライセンスを追加または削除できます。各ライセンスは**ライセンスID**で特定され、1つ以上の単位を含めることができます。ライセンスは管理者によってのみ十分な**権限**がある他のユーザーに配布できます。ライセンスは減らすことはできません。

オフラインライセンスファイル

オフラインライセンスファイルを作成してインポートするには、次の手順に従います。

- 1.ESET PROTECT**ライセンス管理**を開き、**アクション>ライセンスの追加**をクリックします。
- 2.オフラインライセンスファイルを選択し、特定の**ライセンスファイルトークン**をコピーします。

Add License

You can add your license using one of the following options:

☐ ESET Business Account or ESET MSP Administrator

☐ License Key

☒ Offline License File

License File Token ?

Offline License File

Choose File

No file chosen

UPLOAD

ADD LICENSES

CANCEL

- 3.ライセンスをインポートした[ESET Business Account](#)にログインします。

- 4.エクスポートするライセンスを選択し、**オフラインファイルの作成**を選択します。
- 5.このライセンスファイルの製品を選択し、ファイルの**名前**と**単位数**(ライセンスファイルにエクスポートされたシート数)を入力します。
- 6.**ESET PROTECT**による**管理を許可する**の横のチェックボックスをオンにして、**ESET PROTECT**トークンを入力します(ESET PROTECTのライセンスファイルトークン)[②](#)

Create offline license file

Product

ESET Endpoint Antivirus for Windows

Name

My custom name

Units count

1 /3

Username and password

☐ Include Username and Password
When included it is possible to update from ESET servers

ESET PROTECT

☒ Allow management with ESET PROTECT

ESET PROTECT token

GENERATE CANCEL

- 7.生成をクリックします。

ファイルをダウンロードするには、以下の手順に従います。

- 1.ライセンスを選択し、**詳細を表示**をクリックします。
- 2.オフラインファイルタブを選択します。
- 3.名前で識別できる作成したライセンスファイルをクリックし、**ダウンロード**を選択します。

ESET PROTECTライセンス管理に戻ります。

- 1.ファイルの**選択**をクリックし、ESET Business Accountでエクスポートしたオフラインライセンスファイルを選択 します。
- 2.**アップロード**をクリックし、**ライセンスの追加**をクリックします。

Add License

You can add your license using one of the following options:

☐ ESET Business Account or ESET MSP Administrator

☐ License Key

☒ Offline License File

License File Token ?

Offline License File

Choose File

Offline license.lf

UPLOAD

ADD LICENSES

CANCEL

アクセス権

アクセス権によりESET PROTECT Webコンソール [ユーザー](#)とその[権限](#)を管理できます。

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るグループです。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	オブジェクトは 静的グループ に配置されます。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）。 サーバータスクと通知 は「実行」ユーザーを必要とする例外です。
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ようにする静的グループとして機能します。
管理者	グループに対して完全な権限設定で すべて をホームグループに持つユーザーは、事実上管理者です。
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。詳細については、すべてのアクセス権と機能の 一覧 を参照してください。
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。ESET PROTECT Webコンソールでユーザーが実行または表示できる内容を定義します。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 は定義されたグループのオブジェクトにのみ適用されます。これらの 静的グループ は、権限設定の作成または編集時に、 静的グループ セクションで設定されます。
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 、 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。

アクセス権関連の例の一覧

アクセス権に関連する管理ガイドにはさまざまな例があります。次に一覧を示します。

- [ポリシーの複製方法](#)
- [使用と書き込みの違い](#)
- [支店の管理者用のソリューションを作成する方法](#)
- [複製によってオブジェクトを共有する方法](#)
- [証明書と権限へのアクセスを分割する方法](#)
- [ユーザーがインストーラーを作成できるようにする方法](#)
- [通知を削除する方法](#)
- [ポリシーの作成方法](#)
- [ユーザーがすべてのポリシーを表示できるようにする](#)
- [支店の管理者間でライセンスを共有する](#)

ユーザー

ユーザー管理はESET PROTECT Webコンソールの[詳細](#)セクションにあります。

- [ネイティブユーザーの作成](#)
- [ユーザーアクションとユーザー詳細](#)

- [ユーザーパスワードの変更](#)
- [マッピングされたユーザー](#)
- [権限設定をユーザーに割り当てる](#)
- [二要素認証](#)

ユーザータイプには次の2種類があります。

- [ローカルユーザー](#) ESET PROTECT Webコンソールから作成および管理されるユーザーアカウント。
- [マッピングされたドメインセキュリティグループ](#) - Active Directoryによって管理および認証されるユーザーアカウント。

新規のESET PROTECTの設定には、唯一のユーザーとして**管理者(すべてをホームグループに持ちすべてにアクセスできるローカルユーザー)**があります。

- このユーザーアカウントを定期的に使用しないことをお勧めします。[別の管理者アカウントを作成](#)するか、[マッピングされたドメインセキュリティグループ](#)から管理者権限設定が割り当てられた管理者を作成することを強くお勧めします。既定の管理者アカウントはバックアップオプションとしてのみ使用してください。
- 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。
- 任意で、ローカルユーザーとマッピングされたドメインセキュリティグループの[二要素認証](#)を設定できます。これによりESET PROTECT Webコンソールにログインしてアクセスするときのセキュリティが強化されます。

支店の管理者ソリューション

会社に2つの事業所があり、それぞれにローカル管理者がいる場合は、別のグループに対するその他の権限設定を割り当てる必要があります。

たとえば、管理者の *John* がサンディエゴに、*Larry* がシドニーにいます。両方がローカル管理者のみを管理し、コンピューターでダッシュボード、ポリシー、レポートおよび動的グループテンプレートを必要があります。メインの管理者は次の手順に従う必要があります。

1. 新しい静的グループを作成する: サンディエゴ事業所とシドニー事業所。

2. 新しい権限設定を作成する:

a) 静的グループシドニー事業所と完全アクセス権限(サーバー設定を除く)があるシドニー権限設定という権限設定

b) 静的グループサンディエゴ事業所と完全アクセス権限(サーバー設定を除く)があるサンディエゴ権限設定という権限設定

c) 静的グループすべてと次の権限があるすべてのグループ/ダッシュボードという権限設定

- クライアントタスクの読み取り
- ✓ 動的グループテンプレートの使用
- レポートとダッシュボードの使用
- ポリシーの使用
- メールの送信の使用
- SNMPトラップの送信の使用
- レポートをファイルへ出力の使用
- ライセンスの使用
- 通知の書き込み

3. 新しいユーザー *John* を作成します。ホームグループサンディエゴ事業所には権限設定サンディエゴ権限設定とすべてのグループ/ダッシュボードが割り当てられます。

4. 新しいユーザー *Larry* を作成します。ホームグループシドニー事業所には権限設定シドニー権限設定とすべてのグループ/ダッシュボードが割り当てられます。

権限設定がこのように設定される場合は、*John* と *Larry* は同じタスクとポリシー、レポートとダッシュボードを使用し、制限なく動的グループテンプレートを使用できます。ただし、それぞれは自分のホームグループに含まれるコンピューターに対してのみテンプレートを使用できます。

オブジェクトの共有

管理者が動的グループテンプレート、レポートテンプレート、またはポリシーなどのオブジェクトを共有する場合は、次のオプションがあります。

- これらのオブジェクトを共有グループに移動する
- 複製オブジェクトを作成し、他のユーザーがアクセスできる静的グループに移動する(以下の例を参照)

オブジェクトの複製には、元のオブジェクトに対する読み取り権限と、この種類のアクションのホームグループに対する書き込み権限が必要です。

ホームグループがすべての管理者がユーザー *John* と特別なテンプレートを共有しようとしています。テンプレートは最初に管理者によって作成されたため、自動的にすべてグループに含まれています。管理者は次の手順に従います。

1. 詳細 > 動的グループテンプレートに移動します。

✓ 2. 特別なテンプレートを選択し、[複製]をクリックします。必要に応じて、名前と説明を設定し、[完了]をクリックします。

3. 複製されたテンプレートは管理者のホームグループ、グループすべてに含まれます。

4. 詳細 > 動的グループテンプレートに移動し、複製されたテンプレートを選択します。🔍 アクセスグループ > 📁 移動をクリックし、対象の静的グループ(*John*に権限がある場合)を選択します。OKをクリックします。

共有グループでその他のユーザーとオブジェクトを共有する方法

新しいセキュリティモデルの動作をさらに理解するには、次の方法を参照してください。管理者が2つのユーザーを作成する場合があります。各ユーザーには独自のホームグループがあり、作成したオブジェクトがあります。サンディエゴ権限設定は *John* に対して自分のグループのオブジェクトを操作する権限を付与します。この状況は *Larry* と似ています。これらのユーザーが一部のオブジェクト(コンピューターなど)を共有する必要がある場合、これらのオブジェクトを共有グループ(静的グループ)に移動します。両方のユーザーには **静的グループ** セクションでリスト化された共有グループを持つ共有権限を割り当てる必要があります。



フィルターとレイアウトのカスタマイズ

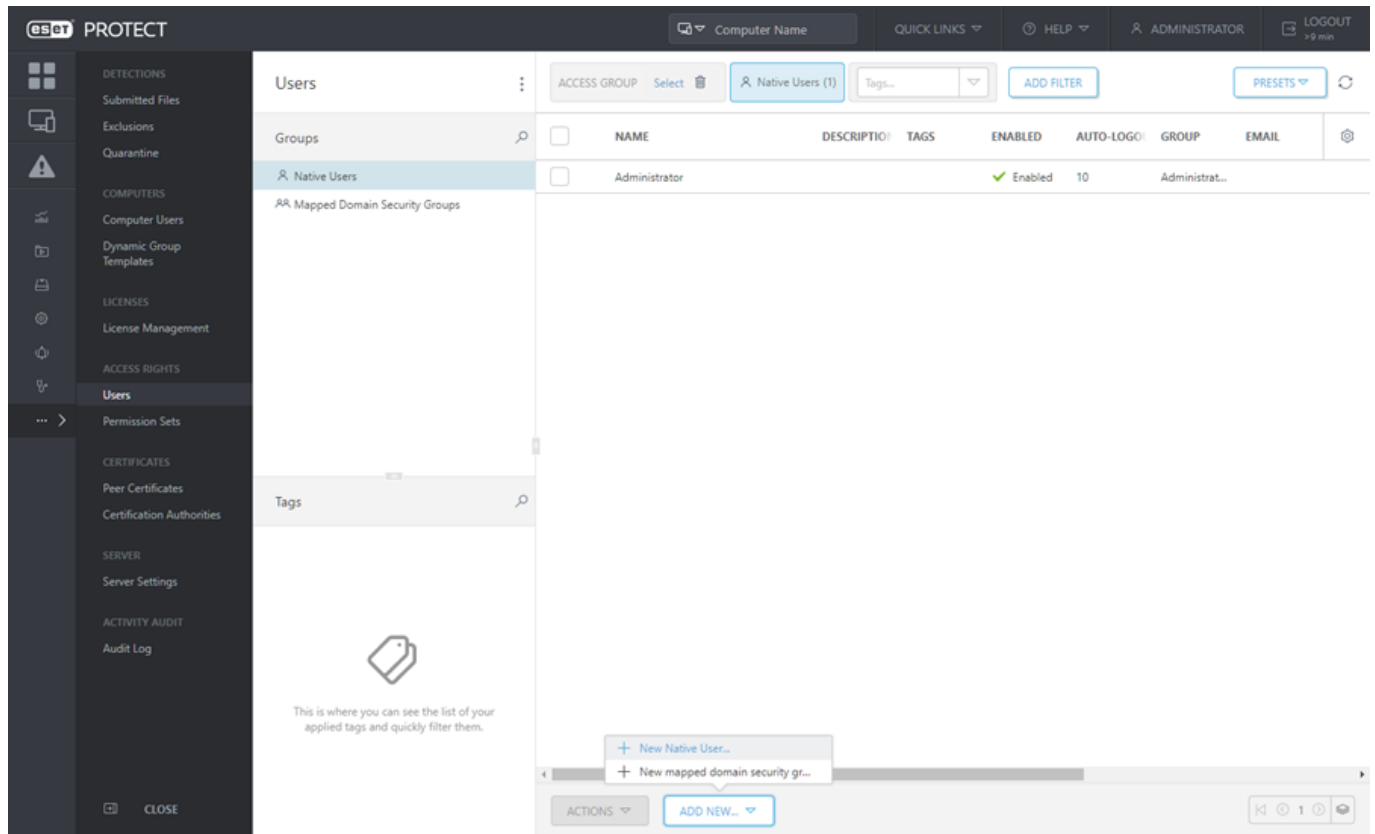
現在のWebコンソール画面ビューをカスタマイズできます。

- [フィルター](#)とフィルタープリセットを追加します。
- [タグ](#)を使用して、表示される項目をフィルタリングできます。

ローカルユーザーの作成

新しいローカルユーザーを作成するには、**詳細 > ユーザー > 新規追加 > 新しいローカルユーザー**をクリックします。

- i** ユーザーを正しく作成するには、次の手順に従うことをお勧めします。
1. ユーザーのホームグループになる静的グループを決定します。必要に応じて、[グループを作成](#)します。
 2. ユーザーに最適な権限設定を決定します。必要に応じて、[新しい権限設定を作成](#)します。
 3. この章に従い、ユーザーを作成します。



基本

新しいユーザーの**名前**と**説明**(任意)を入力します。

タグを選択をクリックして、[タグを割り当て](#)ます。

ホームグループを選択します。これは、このユーザーが作成したすべてのオブジェクトが自動的に含まれる静的グループです。

パスワードの設定

ユーザーのパスワードは、8文字以上である必要があります。パスワードにユーザー名を含めることはできません。

アカウント

有効 - アカウントを非アクティブにする場合を除き、このオプションを選択します(後で使用するため)。

パスワードの変更が必要 - これを選択するとESET PROTECT Webコンソールに初めてログインしたときにパスワードを変更する必要があります。

パスワードの有効期限(日) - このオプションは、パスワードが有効である日数を定義します(有効期限が切れた後にパスワードを変更する必要があります)。

自動ログアウト(分) - このオプションでは、ユーザーがWebコンソールからログアウトした後のアイドル期間(分単位)を定義します。ユーザーの自動ログアウトを無効にするには、**0** (ゼロ)を入力します。

フルネーム **メール連絡先**および**電話番号**を定義し、ユーザーの識別を容易にすることができます。

権限設定


ユーザーには複数の権限セットを[割り当てる](#)ことができます。

定義済みの権限(以下の一覧を参照)を選択するか、カスタム[権限設定](#)を使用できます。

- **確認者のアクセス権限設定** - すべてグループで読み取り専用権限。
- **管理者の権限設定** - すべてグループで完全アクセス権限。
- **サーバー支援インストール権限設定** - [サーバー支援インストール](#)に必要な最低アクセス権
- **Enterprise Inspector確認者権限設定** - ESET Enterprise Inspectorユーザーに必要な読み取り専用のアクセス権(すべてグループ)。
- **Enterprise Inspectorサーバー権限設定** - ESET Enterprise Inspectorインストール処理と、ESET Enterprise InspectorとESET PROTECTの間での自動同期の強化に必要な最小アクセス権(すべてグループ)。
- **Enterprise Inspectorユーザー権限設定** - ESET Enterprise Inspectorユーザーに必要な書き込みアクセス権(すべてグループ)。

各権限設定は、権限設定で選択される**静的グループ**に含まれるオブジェクトにのみ権限を提供します。

権限設定がないユーザーはWebコンソールにログインできません。

 すべての定義済み権限設定には、**静的グループ**セクションの**すべてグループ**があります。ユーザーに割り当てるときにはこれに注意してください。ユーザーはESET PROTECTのすべてのオブジェクトでこれらの権限があります。


概要








このユーザーに対する設定を確認し、**終了**をクリックして、ユーザーを作成します。

ユーザーアクションとユーザー詳細





ユーザーを管理するには、該当するユーザーを選択し、使用可能なアクションのいずれかを選択します。

アクション



-  **詳細を表示** - [ユーザー詳細](#)を表示します。

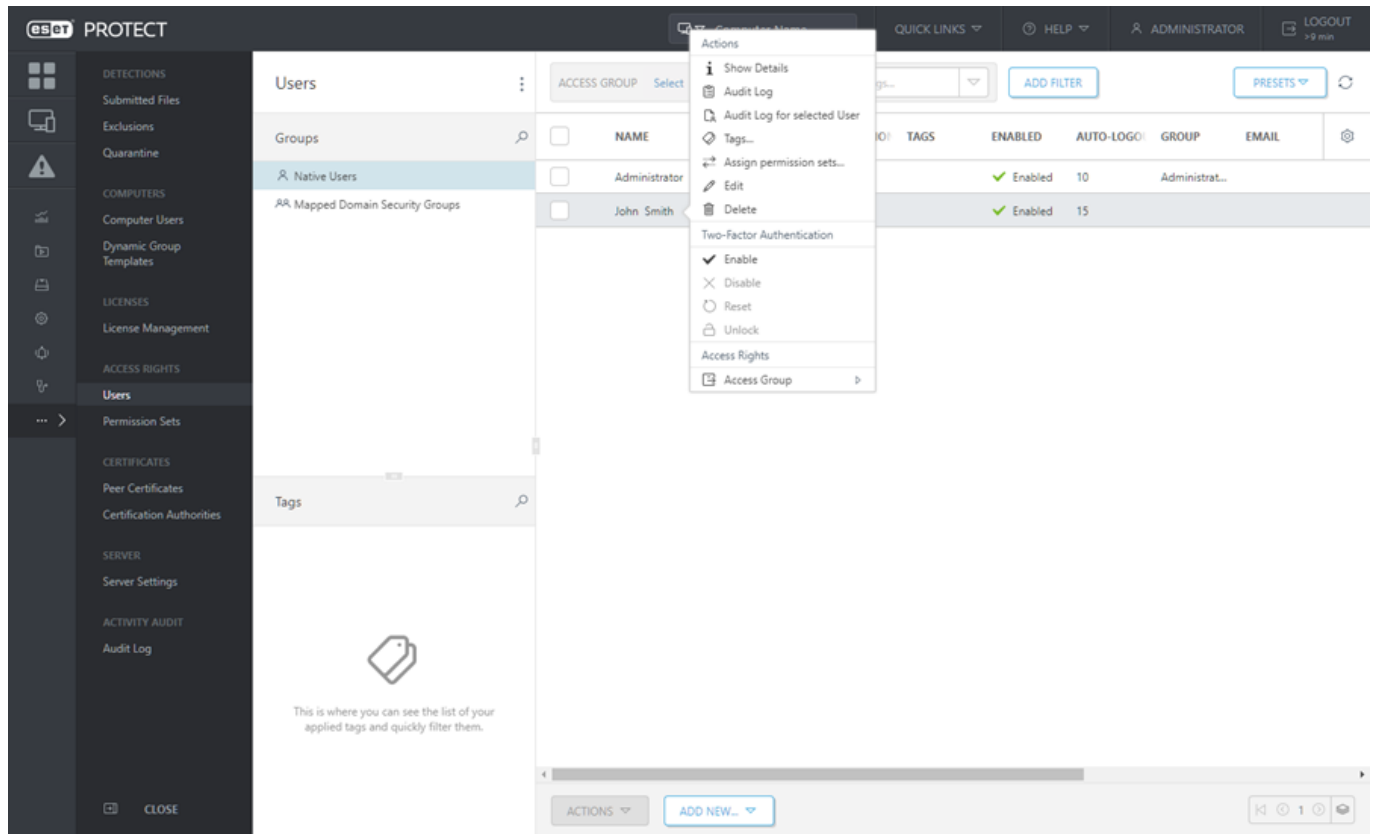
-  **監査ログ** - すべてのユーザーの [監査ログ](#) を表示します。
-  **選択したユーザーの監査ログ** - 選択したユーザーの [監査ログ](#) を表示します。
-  **タグ:** [タグ](#) を編集します (割り当て、割り当て解除、作成、削除)。
-  **権限セットの割り当て** - [権限セットをユーザーに割り当てます](#) 
-  **編集** - [ユーザー設定を編集](#) します。
-  **削除** - ユーザーを削除します。

二要素認証

-  **有効化** - ユーザーの [二要素認証](#) を有効にします。
-  **無効化** - ユーザーの既存の [二要素認証](#) を無効にします。
-  **リセット** - ユーザーの二要素認証設定をリセットします。
-  **ロック解除** - ユーザーがロックされている場合は、この設定を使用してユーザーのロックを解除できます。

アクセス権

-  **アクセスグループ** >  **移動** - ユーザーを別の静的グループに移動します。



ユーザー詳細

ユーザーの詳細には、次の2つのセクションがあります。

- **概要** – ユーザーに関する基本情報。 ユーザを管理するには、下部にある**アクション**ボタンと**二要素認証**ボタンを使用します。
- **権限設定** – ユーザーに割り当てられた権限設定の一覧。権限設定をクリックして[管理](#)します。

ユーザーパスワードの変更

アクセス権をもっているすべてのユーザーのパスワードを変更できます。ユーザーが保存されている静的グループに対する書き込み権限が必要です。ユーザーは、親ユーザーのホームグループに保存されます。

1. **アクセス権** > **ユーザー** をクリックします。
2. ユーザーを選択して、**編集** をクリックします。
3. **基本** セクションで、**パスワードを設定** にスクロールします。
4. サインインしたユーザーを編集している場合は、**現在のパスワード** を入力する必要があります。他のユーザーを編集するときには、**現在のパスワード** フィールドがあらかじめ入力されています。
5. **パスワードとパスワードの確認** フィールドに新しいパスワードを入力します。

6.[完了]をクリックします。

Edit Native User

Users > User

Basic

Permission Sets

Summary

Home group

All

Set Password

Current password

.....

Password

Confirm password

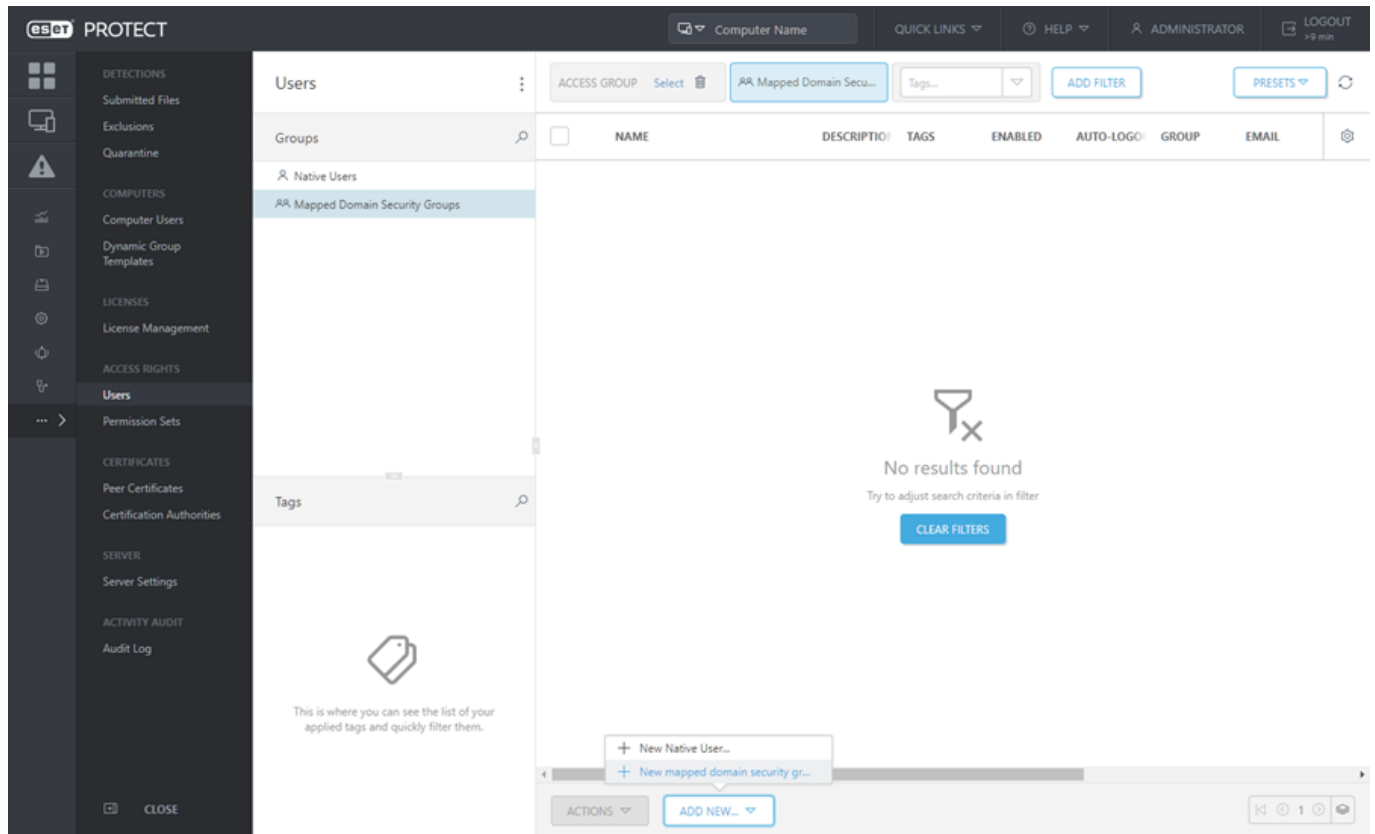
Show password

ドメインセキュリティグループユーザーのマッピング

ESET PROTECTサーバーにドメインセキュリティグループをマッピングすると、既存のユーザー(ドメインセキュリティグループのメンバー)がESET PROTECT Webコンソールユーザーになることができます。

i この機能は、Active Directoryのシステムでのみ使用できます。

マッピングされたドメインセキュリティグループのウィザードを実行するには、詳細 > ユーザー > 新規追加 > 新しいマッピングされたドメインセキュリティグループに移動します。



基本

ドメイングループ

このグループの**名前**を入力します。グループの**説明**も入力できます。

タグを選択をクリックして、[タグを割り当て](#)ます。

ホームグループを選択します。これは、このドメイングループのユーザーが作成したすべてのオブジェクトが自動的に含まれる静的グループです。

このドメイングループは**グループ SID**（セキュリティID）で定義されます。**[選択]**をクリックしてリストからグループを選択し、**[OK]**をクリックして確認します。ESET PROTECTサーバーはドメインに参加する必要がありますが、そうでない場合はリストにグループはありません。仮想アプライアンスを使用している場合は、[関連する章](#)を参照してください。

- LDAPSが使用できない場合は、次の方法でドメインセキュリティグループをマッピングできます。
- [サーバー設定](#) > 詳細設定 > Active DirectoryでActive Directory設定を一時的に無効にする。
- グループSIDを手動で入力する。
- 選択をクリックした後にエラーメッセージが表示され続け、ADが正しく設定されている場合は、バックグラウンド処理がタイムアウトしている可能性があります。次の対応を実施できます。
- 手動でSIDを入力して、問題を回避する
- [サーバー設定](#) > 詳細設定 > Active DirectoryにAD認証情報を入力する。ESET PROTECTは、別の高速な方法を使用してSIDのリストを取得します。

アカウント

有効 – アカウントを非アクティブにする場合を除き、このオプションを選択します（後で使用するため）。

自動ログアウト(分) - このオプションでは、ユーザーがWebコンソールからログアウトされるアイドル時間(分単位)を定義します。

メール連絡先および電話番号を定義し、グループの識別を容易にすることができます。

権限設定

このグループユーザーの資格(権限)を割り当てます。

i **権限セット**がActive Directoryドメインセキュリティグループに対して設定されます(ローカルユーザーの場合のように個人ユーザーには設定されません)。

ドメインセキュリティデバイスグループには複数の権限セットを**割り当てる**ことができます。

定義済みの権限(以下の一覧を参照)を選択するか、カスタム**権限設定**を使用できます。

- **確認者のアクセス権限設定** - すべてグループで読み取り専用権限。
- **管理者の権限設定** - すべてグループで完全アクセス権限。
- **サーバー支援インストール権限設定** - **サーバー支援インストール**に必要な最低アクセス権
- **Enterprise Inspector確認者権限設定** - ESET Enterprise Inspectorユーザーに必要な読み取り専用のアクセス権(すべてグループ)。
- **Enterprise Inspectorサーバー権限設定** - ESET Enterprise Inspectorインストール処理と、ESET Enterprise InspectorとESET PROTECTの間での自動同期の強化に必要な最小アクセス権(すべてグループ)。
- **Enterprise Inspectorユーザー権限設定** - ESET Enterprise Inspectorユーザーに必要な書き込みアクセス権(すべてグループ)。

各権限設定は、権限設定で選択される**静的グループ**に含まれるオブジェクトにのみ権限を提供します。

権限設定がないユーザーはWebコンソールにログインできません。

! すべての定義済み権限設定には、**静的グループ**セクションの**すべてグループ**があります。ユーザーに割り当てるときにはこれに注意してください。ユーザーはESET PROTECTのすべてのオブジェクトでこれらの権限があります。

概要

このユーザーに対する設定を確認し、**終了**をクリックして、グループを作成します。

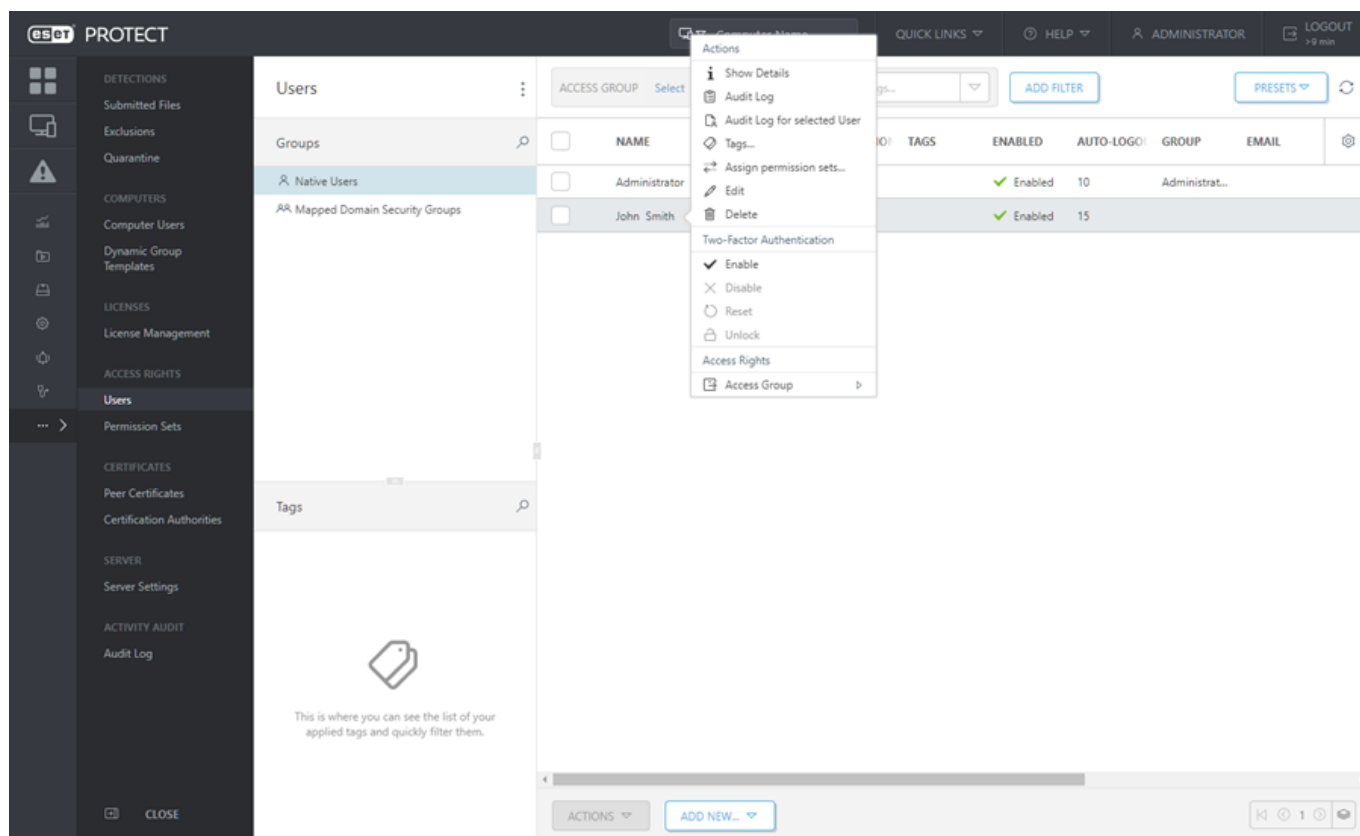
ユーザーは、最初にログインした後、マッピングされたドメインセキュリティグループに表示されます。

権限設定をユーザーに割り当てる

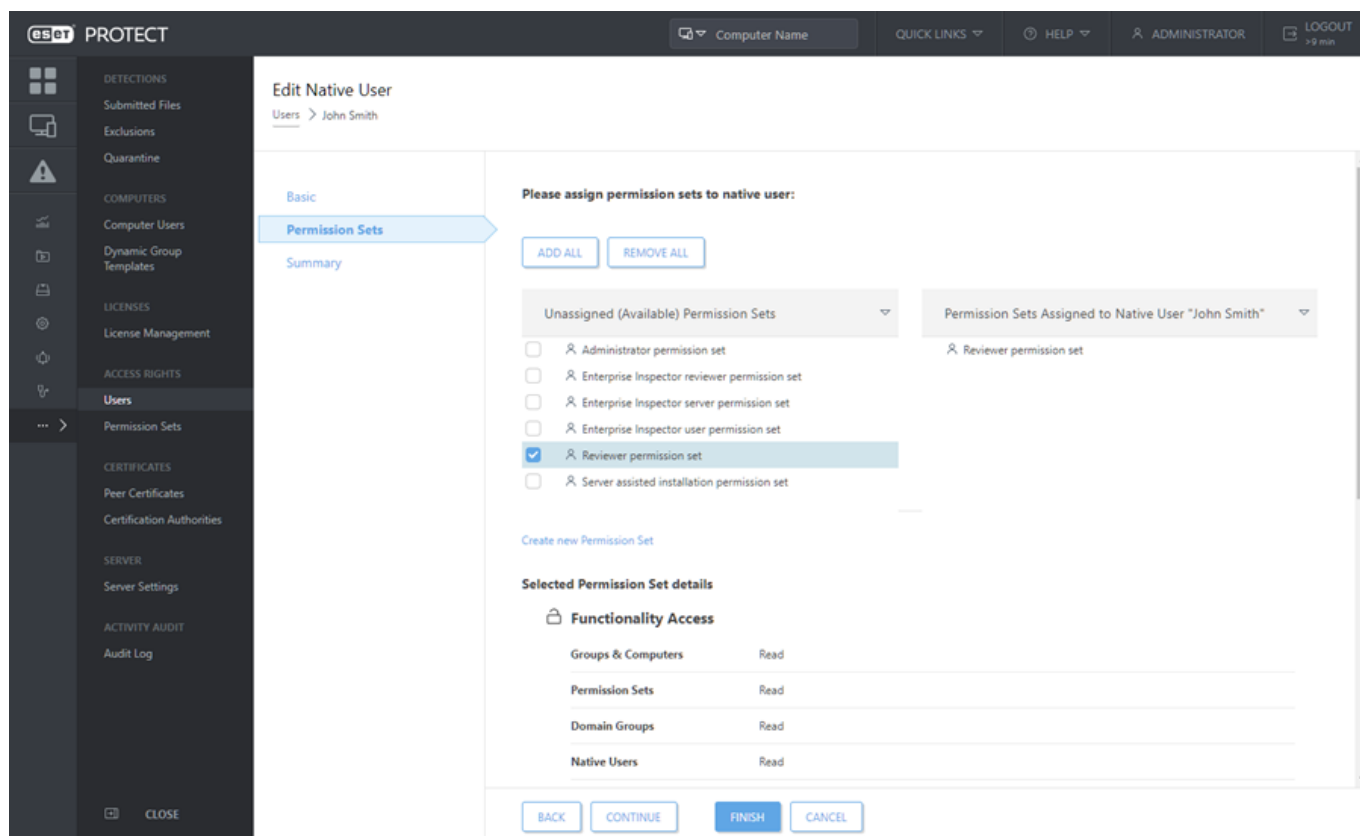
1. 権限設定をユーザーに割り当てるには、次の2つの方法があります。

a) **詳細 > ユーザー**をクリックして、ユーザーをクリックし、**権限セットの割り当て**を選択して、ユーザーに特定の権限セットを割り当てます。

b) ユーザーセクションで、編集をクリックして特定のユーザーを編集します。



2. 設定可能な権限セクションで、特定の権限設定の横にあるチェックボックスをオンにします。詳細については、「[権限設定の管理](#)」を参照してください。




二要素認証

- 二要素認証(2FA)は、ESET PROTECT Webコンソールにログインしてアクセスするためのより安全な方法です。
- 二要素認証はESETおよびESET Secure Authentication技術によって実現されています。環境内にESET Secure Authenticationを展開またはインストールする必要はありません。ESET PROTECTが自動的にESETサーバーに接続し、ESET PROTECT Webコンソールにログインしようとしているユーザーを認証します。
- 二要素認証が有効なユーザーは、[ESET Secure Authentication](#)を使用してESET PROTECTにログインする必要があります。
- 製品機能および利点の詳細については、[ESET Secure Authentication製品ガイド](#)をご覧ください。
- ESA 2FAを使用してESET PROTECTにログインできるユーザー数に制限はありません。
- HTTPプロキシ設定は、Secure Authenticationサーバー(2FA)との通信には適用されません。
- 管理者アカウントでも二要素認証を有効にできます。

前提条件

- 他のユーザーアカウントで2FAを有効にするには、そのユーザーに対する書き込み権限が必要です。有効にすると、ユーザーはログインする前に自分で2FAを構成する必要があります。ユーザーはテキストメッセージ(SMS)でリンクを受信し、電話のWebブラウザで開き、2FAを構成する手順を表示できます。
- 2FAは[ESET 2FAサーバー](#)への直接ネットワークアクセスなしで動作しません。ファイアウォールで少なくとも特定の2FAサーバーを許可する必要があります。プロキシが[詳細]>[サーバー設定]>[詳細設定]>[HTTPプロキシ]で設定されている場合、2FAには適用されません。

 サーバー支援インストールでは、二要素認証でユーザーを使用できません。

Webコンソールユーザーの二要素認証を有効にする方法

- 1.新しいユーザーを作成するか、既存のユーザーを使用します。
- 2.ESET PROTECT Webコンソールで**詳細>ユーザー**に移動します。
- 3.ユーザーをクリックし、**二要素認証>✔有効にする**を選択します。
- 4.ユーザーの次のログイン時に、メッセージが表示されたら、ユーザーの電話番号を入力します。
- 5.ユーザーの携帯電話で、SMSのリンクまたはQRコードを使用して、[ESET Secure Authenticationモバイルアプリ](#)をインストールします。
- 6.トークンを使用してアプリをインストールするときにはESET PROTECTインスタンスがアプリで追加されます。
- 7.ログインに進み、メッセージが表示されたら、モバイルアプリからのワンタイムパスワード

をWebコンソールに入力します。モバイルアプリで、各ログインの新しいパスワードが生成されます。

トラブルシューティング

Webコンソールユーザーが二要素認証でWebコンソールにログインできない場合は、次の手順に従います。


1. [ESET PROTECTデータをバックアップします](#)②

2. 該当するオプションを選択します。

- 二要素認証に設定された電話番号にアクセスできます。


a) Webコンソールログイン中に、二要素認証ポップアップウィンドウでトークンのリセットをクリックします。

b) 二要素認証用に設定された電話番号に確認SMSが送信されます。

 ESET PROTECTデータベースに保存されている電話番号は変更できません。電話にアクセスできない場合は、次の手順に従います。

- 二要素認証用に設定された電話番号にアクセスできない(電話が紛失、破損しているなど)

a) [Webコンソールパスワードをリセット](#)し、管理者アカウントで二要素認証を無効にします。

 他のESET PROTECTユーザーアカウントの二要素認証状態は影響を受けません。

b) ユーザーは二要素認証なしでWebコンソールにログインしてから、ログイン後に二要素認証を再有効化できます。

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②Webコンソールでユーザーが実行または表示できる内容を定義します。 [ローカルユーザー](#)は、自身の権限を保持することができます一方で、ドメインユーザーは、[マップされたセキュリティグループ](#)の権限を保持します。 各権限設定には適用の範囲(静的グループ)があります。**[機能]**セクションで選択した権限は、この権限設定で割り当てられた各ユーザーの**[静的グループ]**セクションで設定されたグループのオブジェクトに適用されます。特定の**静的グループ**へのアクセス権を保有すると、サブグループすべてに自動的にアクセスできます。静的グループの適切な設定では、ローカル管理者([例を参照](#))の個別の支店を作成できます。


表示できない場合でも、ユーザーに権限設定を割り当てることができます。権限設定は作成したユーザーのホームグループに自動的に保存されるオブジェクトです。ユーザーアカウントが作成されると、作成ユーザーのホームグループのオブジェクトとしてユーザーが保存されます。通常、管理者がユーザーを作成するため、グループすべてに保存されます。

権限設定は追加して付与されます。その他の権限設定を単一のユーザーに割り当てる場合は、すべての権限設定の合計は、ユーザーに付与される最終的なアクセス権です。

複数の権限設定の組み合わせ

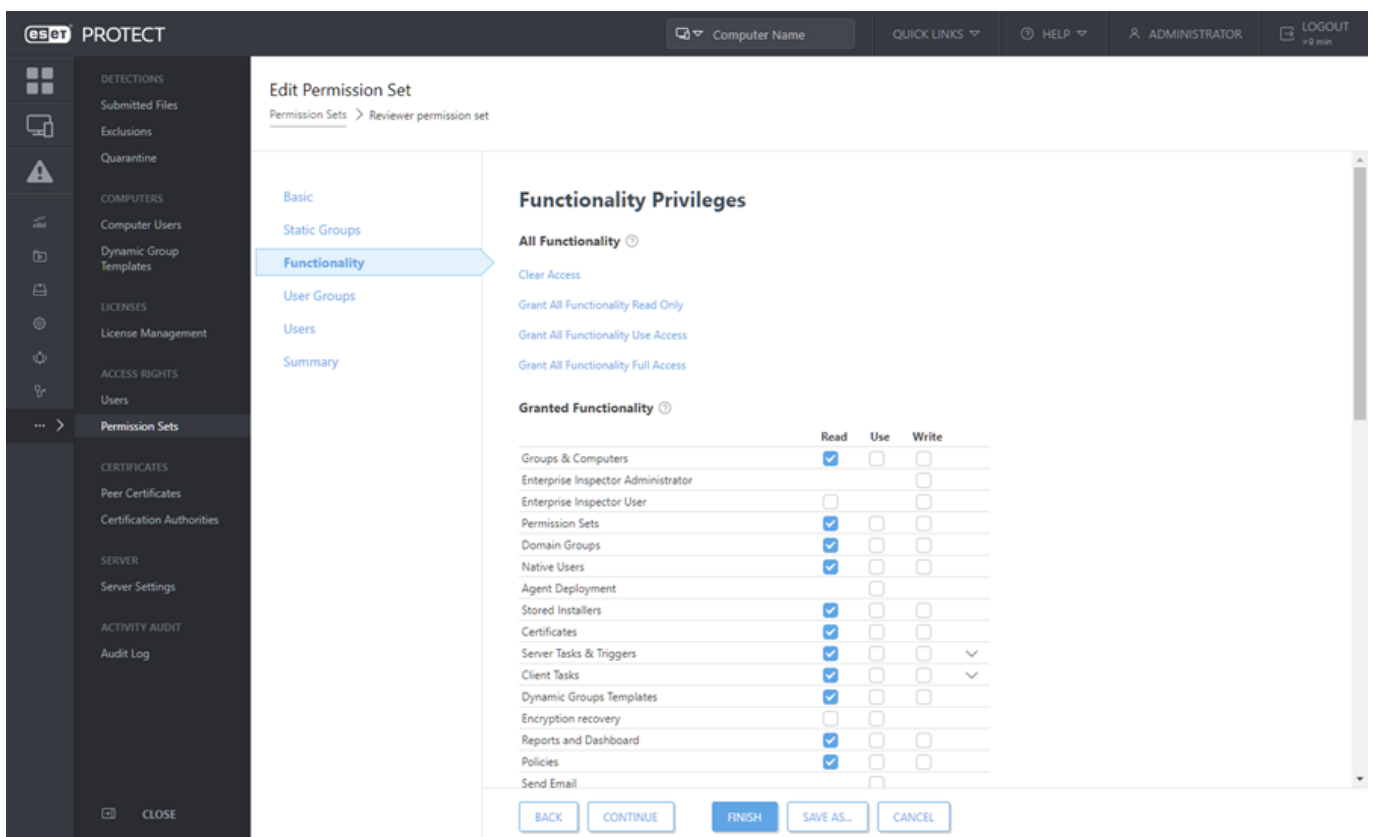
オブジェクトに対するユーザーの最終的なアクセス権は、ユーザーに割り当てられたすべての権限の組み合わせの結果となります。たとえば、ユーザーには2つの権限設定をもっているとします。1つはフル権限のホームグループ用です。もう1つは、コンピューターとグループの読み取り、使用権限のみを持つグループとコンピューターの権限設定です。このユーザーは、他のグループのコンピューターに、ホームグループからすべてのタスクを実行できます。

一般的に、ユーザーは、特定のグループの特定のオブジェクトタイプの権限が割り当てられている場合、別の静的グループのオブジェクトに対して、1つの静的グループからオブジェクトを実行できます。

ACCESS GROUP Select 

アクセスグループフィルターボタンでは、ユーザーが静的グループを選択し、属するグループに応じて、[表示されるオブジェクトをフィルタリング](#)できます。

[タグ](#)を使用して、表示される項目をフィルタリングできます。



	Read	Use	Write
Groups & Computers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise Inspector Administrator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise Inspector User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permission Sets	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Domain Groups	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Native Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Agent Deployment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stored Installers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server Tasks & Triggers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Client Tasks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Groups Templates	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption recovery	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reports and Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Send Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

権限の操作に関する最適な方法:

- [サーバー設定](#)へのアクセスは経験の浅いユーザーには絶対に付与しないでください。管理者のみにこのアクセス権を付与してください。
- [クライアントタスク>コマンドの実行](#)へのアクセスを制限することを検討してください。これは悪用される可能性がある非常に強力なタスクです。
- 管理者ではないユーザーには、[権限設定](#)、[ローカルユーザー](#)、[サーバー設定](#)の権限を付与しないでください。
- より複雑な権限のモデルが必要な場合、その他の権限設定を作成し、割り当ててください。

ESET PROTECT機能の権限の横では、[ユーザーグループ](#)への[読み取り](#)、[使用](#)、[書き込み](#)アクセスを付与できます。

複製

オブジェクトの複製には、元のオブジェクトに対する**読み取り**権限と、この種類のアクションの**ホームグループ**に対する**書き込み**権限が必要です。

*John*のホームグループは*John's Group*ですが、*Larry*が作成し、自動的に*Larry*のホームグループ*Larry's Group*に含まれる*Policy 1*を複製しようとしています。

- ✓ 1.新しい静的グループを作成します。共有ポリシーなどの名前を付けます。
- 2.*John*と*Larry*の両方に共有ポリシーグループの**ポリシー**の**読み取り**権限を付与します。
- 3.*Larry*は*Policy 1*を共有ポリシーグループに移動します。
- 4.ホームグループの**ポリシー**の**書き込み**権限を*John*に付与します。
- 5.*John*は*Policy 1*を**複製**できます。複製は自分のホームグループに表示されます。

使用と書き込みの違い

管理者がユーザー*John*が共有ポリシーグループのポリシーを修正することを許可しない場合は、次の権限設定を作成します。

- **機能ポリシー**:選択された**読み取り**および**使用**権限
- ✓ • **静的グループ**:共有ポリシー







これらの権限が*John*に割り当てられると、*John*はこれらのポリシーを実行できますが、編集、新規作成、削除はできません。管理者が**書き込み**権限を追加する場合、*John*は選択した静的グループ(共有ポリシー)内のポリシーを新規作成、編集、削除できます。

権限設定の管理



The screenshot shows the 'Permission Sets' management interface in the ESSENTIAL PROTECT application. The left sidebar contains navigation links for various system components. The main content area lists several permission sets, including 'Administrator permission set', 'Reviewer permission set', and 'Enterprise Inspector server permission set'. A context menu is displayed over the 'Administrator permission set', offering actions such as 'Show Details', 'Audit Log', 'Tags...', 'Edit...', 'Duplicate...', 'Delete', 'Assignments', 'AA: Show native users', 'Show mapped security groups', 'Access Rights', and 'Access Group'. The interface also includes a 'PRESETS' button and a 'CLOSE' button at the bottom.

権限設定を管理するには、権限設定をクリックし、次のいずれかのアクションを選択します。



権限設定


-  **詳細の表示** - 権限設定の詳細を表示します。
-  **監査ログ** - 選択した項目の[監査ログ](#)を表示します。
-  **タグ**: [タグ](#)を編集します(割り当て、割り当て解除、作成、削除)。
-  **編集** - 権限設定を[編集](#)します。
-  **複製** - 権限設定の複製を作成し、修正して特定のユーザーに割り当てます。複製は、複製したユーザーのホームグループに保存されます。
-  **削除** - 権限設定を削除します。

割り当て

-  **ネイティブユーザーを表示** - 割り当てられたネイティブユーザーのリストを表示します。
-  **マッピングされたセキュリティグループを表示** - 割り当てられた、マッピングされたドメインセキュリティデバイスグループの一覧を表示します。

アクセス権

-  **アクセスグループ** >  **移動** - 権限設定を別の静的グループに移動します。

 すべての定義済み権限設定には、**静的グループ**セクションの**すべてグループ**があります。ユーザーに割り当てるときにはこれに注意してください。ユーザーはESET PROTECTのすべてのオブジェクトでこれらの権限があります。

権限設定の作成または編集

新しい権限設定を作成するには、**新規**をクリックします。既存の権限設定を編集するには、該当する権限設定を選択し、**編集**をクリックします。

基本

設定の**名前**を入力します(必須設定)。**説明**と**タグ**を入力することもできます。

タグを選択をクリックして、[タグを割り当て](#)ます。

静的グループ

この資格を取得する静的グループ(または複数の静的グループ)を**選択**するか、**新しいグループを追加**できます。**[機能]**セクションで確認される権限は、このセクションで選択されたグループに含まれるオブジェクトに適用されます。

機能

アクセス権を付与する個別のモジュールを選択します。この権限のユーザーは、これらの特定のタスクにアクセスできます。[サーバータスク](#)と[クライアントタスク](#)ごとに別の権限を設定することもできます。4つの定義済み機能セットがあります。4つのいずれかを選択するか、機能チェックボックスを手動で選択します。

書き込み権限を付与すると、**使用**および**読み取り**権限が自動的に付与されます。**使用**権限を付与すると、**読み取り**権限が自動的に付与されます。

ユーザーグループ

ポリシー内でユーザーパラメーターを使用できる[ユーザーグループ](#)（または複数のユーザーグループ）を追加できます（例 [ESET MDM for iOS & iPadOS](#)または[上書きモード](#)）

ユーザー

この権限設定で割り当てられるユーザーを選択します。すべての使用可能な[ユーザー](#)は左側に一覧表示されます。特定のユーザーを選択するか、**[すべて追加]**ボタンを使用してすべてのユーザーを選択します。割り当てられたユーザーは右側に一覧表示されます。ユーザーを割り当てることは必須ではありません。後からできます。

概要

この権限に対する設定を確認し、**[完了]**をクリックします。権限設定は作成したユーザーのホームグループに保存されます。

[名前を付けて保存]をクリックすると、編集している権限セットに基づいて、新しい権限セットを作成します。新しい権限セットの名前を入力する必要があります。

権限の一覧

権限の種類

[詳細] > **[権限設定]** > **[新規作成 / 編集]** > **[機能]**で権限設定を作成または編集するときには、すべての使用可能な権限の一覧があります。ESET PROTECTのWebコンソールの権限は、**グループとコンピューター**、**ポリシー**、**クライアントタスク**、**レポート**、**通知**などのカテゴリに分類されています。特定の権限設定は、**読み取り**、**使用**、または**書き込み**アクセスで使用できます。一般:

読み取りの権限は、ユーザーの監査に適しています。データを表示できますが、変更はできません。

使用権限ではユーザーがオブジェクトを使用し、タスクを実行できますが、修正または削除はできません。

書き込み権限では、ユーザー該当するオブジェクトを修正または複製できます。

特定のタイプの権限(以下の一覧)は、オブジェクトではなく、プロセスを制御します。このためグローバルレベルで動作し、権限が適用されている静的グループに関係なく、動作します。プロセスがユーザーに許可されている場合、十分な権限があるオブジェクトでのみ使用できます。たとえば、**レポートをファイルに出力**権限はレポートのエクスポートを可能にしますが、レポートに含まれるデータは他の権限によって決定されます。

✓ [タスクの例と、そのタスクを正常に実行するために必要な権限設定に関するナレッジベース記事](#)をお読みください。

i 現在のユーザーにアクセス権がない機能は使用できません(灰色表示)。

ユーザーは次のプロセスの権限が割り当てられます。

- エージェント展開
- レポートとダッシュボード(ダッシュボードの機能のみが使用できます。ただし、使用できるレポートテンプレートはアクセス可能な静的グループに依存します)
- 電子メールを送信
- レポートをファイルへ出力
- SNMPトラップの送信
- サーバー設定
- Enterprise Inspector管理者
- Enterprise Inspectorユーザー

機能の種類:

グループとコンピューター

読み取り - コンピューター、グループ、グループ内のコンピューターを一覧表示します。

使用 - ポリシーまたはタスクのターゲットとしてコンピューター/グループを使用します。

書き込み - コンピューターを作成、修正、削除します。これには残りのコンピューターまたはグループも含まれます。

Enterprise Inspector管理者

書き込み - Enterprise Inspectorで管理機能を実行します。

Enterprise Inspectorユーザー

読み取り - Enterprise Inspectorへの読み取り専用アクセス。

書き込み - Enterprise Inspectorへの読み取り/書き込みアクセス。

権限設定

読み取り - 権限設定のリストと、その中のアクセス権のリストを読み取ります。

使用 - ユーザーの既存の権限設定を割り当て/削除します。

書き込み - 権限設定を作成、修正、削除します。



ユーザーに権限設定を割り当てる(割り当て解除する)ときには、**ドメイングループ**と**ネイティブユーザー**に**書き込み**権限が必要です。

ドメイングループ

読み取り - ドメイングループを一覧表示します。

使用

書き込み - 権限設定の付与/取り消しを許可します。ドメイングループを作成、修正、削除します。

ローカルユーザー

読み取り - ローカルユーザーを一覧表示します。

使用

書き込み - 権限設定の付与/取り消しを許可します。ネイティブユーザーを作成、修正、削除します。

エージェント展開

使用 - クイックリンクを使用してエージェントを展開するかESET PROTECT Webコンソールで手動でクライアントコンピュータを追加できます。

保存されたインストーラー

読み取り - 保存されたインストーラーを一覧表示します。

使用 - 保存されたインストーラーをエクスポートします。

書き込み - 保存されたインストーラーを作成、修正、削除します。

証明書

読み取り - ピア証明書と認証局のリストを読み取ります。

使用 - 認証局とピア証明書をエクスポートし、インストーラーまたはタスクで使用します。

書き込み - 新しいピア証明書または認証局を作成し、取り消します。

サーバータスクとトリガー

読み取り - タスクと設定のリストを読み取ります(パスワードなどの機密フィールドを除く)。

使用 - [今すぐ実行]で既存のタスクを実行します(現在Webコンソールにログインしているユーザー)。

書き込み - サーバータスクを作成、修正、削除します。

カテゴリを展開するには、記号▼をクリックすると、1つまたは複数の種類のサーバータスクを選択できます。

クライアントタスク

読み取り - タスクと設定のリストを読み取ります(パスワードなどの機密フィールドを除く)。

使用 - 既存のクライアントタスクの実行をスケジュールするか、実行をキャンセルします。ターゲット(コンピューターまたはグループ)へのタスクの割り当て(または割り当てキャンセル)の場合、影響を受けるターゲットで使用アクセスが必要です。

書き込み - 既存のクライアントタスクを作成、修正、削除します。ターゲット(コンピューターまたはグループ)へのタスクの割り当て(または割り当てキャンセル)の場合、影響を受けるターゲットオブジェクトで使用アクセスが必要です。

カテゴリを展開するには、プラス記号+をクリックすると、1つまたは複数の種類のクライアントタスクを選択できます。

動的グループテンプレート

読み取り - 動的グループテンプレートのリストを読み取ります。

使用 - 動的グループの既存のテンプレートを使用します。

書き込み - 動的グループテンプレートを作成、修正、削除します。

暗号化リカバリー

読み取り

使用 - [暗号化回復](#)プロセスを管理します。

レポートとダッシュボード

読み取り - レポートテンプレートとカテゴリを一覧表示します。レポートテンプレートに基づいてレポートを生成します。既定のダッシュボードに基づいて独自のダッシュボードを読み取ります。

使用 - 使用可能なレポートテンプレートでダッシュボードを修正します。

書き込み – 既存のレポートテンプレートとカテゴリを作成、修正、削除します。既定のダッシュボードを修正します。

ポリシー

読み取り – ポリシーと設定のリストを読み取ります。

使用 – 既存のポリシーをターゲットに割り当てます(あるいは割り当てをキャンセルします)。影響を受けるターゲットで、追加の**使用**アクセスが必要です。

書き込み – ポリシーを作成、修正、削除します。

電子メールを送信

使用 – 電子メールを送信します。(通知とレポートの生成のサーバータスクで使用可能)

SNMPトラップの送信

使用 - SNMPトラップの送信を許可します(通知で使用可能)。

レポートをファイルへ出力

使用 - ESET PROTECTサーバーマシンのファイルシステムにレポートを保存できます。レポートの生成サーバータスクで使用可能。

ライセンス

読み取り – ライセンスと使用統計情報のリストを読み取ります。

使用 – アクティベーションでライセンスを使用します。

書き込み – ライセンスを追加および削除します。(ユーザーのホームグループはすべてに設定する必要があります。既定では、管理者のみが実行できます。)

通知

読み取り – 通知と設定のリストを読み取ります。

書き込み – 通知を作成、修正、削除します。適切な通知処理のためには、通知設定に応じて、**SNMPトラップの送信**または**電子メールの送信の使用**アクセス権が必要な場合があります。

サーバーの設定

読み取り - [サーバー設定](#)を読み取ります。

書き込み - [サーバー設定](#)を修正します。

監査ログ


読み取り - [監査ログ](#)を表示し、[監査ログ](#)レポートを読み取ります。

付与されたESET Enterprise Inspector機能

これはユーザーがアクセスできる個別のESET Enterprise Inspector機能のリストです。詳細については、[ESET Enterprise Inspectorユーザーガイド](#)を参照してください。

証明書

証明書はESET PROTECTの重要な要素です。ESET PROTECTコンポーネントとESET PROTECTサーバーとの間の通信を保護し、ESET PROTECT Webコンソールの保護された接続を確立するために必要です。

 すべてのコンポーネントが正しく通信していることを確認するには、すべてのピア証明書が有効で、同じ認証局で署名されている必要があります。

[ナレッジベース記事](#)で、ESET PROTECTの証明書に関する詳細をお読みください。

証明書にはいくつかのオプションがあります。

- [ESET PROTECTのインストール](#)中に自動的に作成された証明書を使用できます。
- また、新しい[認証機関\(CA\)](#)を作成するか、[公開鍵](#)をインポートし、各コンポーネント(ESET Managementエージェント、ESET PROTECTサーバー、ESET PROTECT MDM)の[ピア証明書](#)を署名するために使用できます。
- [カスタム認証機関](#)と証明書を使用できます。



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場合は、使用しているすべての認証局とESET PROTECTサーバー証明書をエクスポート/バックアップする必要があります。そうしないと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 Webコンソールで新しい[認証機関](#)と[ピア証明書](#)を作成できます。このガイドの手順にしたがって次のことを行ってください。

- [新しい認証機関の作成](#)
- o [公開鍵のインポート](#)
- o [公開鍵のエクスポート](#)

o [BASE64形式での公開鍵のエクスポート](#)

- [新しいピア証明書の作成](#)

- o [証明書の作成](#)

- o [証明書のエクスポート](#)

- o [APN/ABM証明書の作成](#)

- o [証明書の取り消し](#)

- o [証明書の使用](#)

- o [新しいESET PROTECTサーバー証明書の設定](#)

- o [ESET PROTECTのカスタム証明書](#)

- o [期限切れの証明書 - 報告と置換](#)



macOS / OS Xは2038年1月19日以降に期限切れになる証明書をサポートしません。macOS / OS Xで実行されるESET ManagementエージェントはESET PROTECTサーバーに接続できません。



ESET PROTECTコンポーネントのインストール中に作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の2日前に設定されます。

ESET PROTECT Webコンソールで作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の1日前に設定されます。この理由は、影響を受けるシステム間のすべての考えられる時間の不一致に対応するためです。

たとえば、インストール中の2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値が2017年1月10日00:00:00です。ESET PROTECT Webコンソールで2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値は2017年1月11日00:00:00です。

ピア証明書

[認証局](#)がシステムに存在する場合は、個別のESET PROTECTコンポーネントのピア証明書を作成してください。各コンポーネント(ESET Managementエージェント、ESET PROTECTサーバー)には特定の証明書が必要です。

+ 新規

このオプションは、[新しい証明書を](#)作成するために使用されます。証明書はESET Managementエージェント、ESET PROTECTサーバーによって使用されます。

+ APN/ABM証明書

このオプションは、[新しいAPN/ABM証明書を](#)作成するために使用されます。この証明書はMDMで使用されます。このアクションには有効なライセンスが必要です。

証明書の使用

このESET PROTECT証明書を使用するクライアントもチェックできます。

タグ

[タグ](#)を編集します(割り当て、割り当て解除、作成、削除)。

編集

リストから既存の証明書の**説明**を編集するには、このオプションを選択します。

監査ログ

選択した項目の[監査ログ](#)を表示します。

エクスポート / Base64としてエクスポート

.pfxファイルまたは.txt(Base64)ファイルとして[証明書をエクスポート](#)します。このファイルは、ESET Management エージェントをコンピューターにローカルでインストールする場合、またはMDMをインストールする場合に必要です。


取り消し

証明書を使用しない場合は、**[取り消し]**を選択します。このオプションにより、証明書が無効になります。証明書は効果的にブラックリストに追加されます。この情報は、次の接続中にESET Management エージェントに送信されます。取り消された証明書は、ESET PROTECTによって許可されません。




取り消す前に、この証明書を使用しているESET Management エージェント(または他のコンポーネント)がないことを確認してください。証明書を取り消すと、コンポーネントはESET PROTECTサーバーに接続できなくなります。有効な証明書を使用したコンポーネントを再インストールし、機能を復元してください。

アクセス グループ

証明書または認証局は他のグループに移動できます。この後、このグループに対する十分な権限があるユーザーが使用できるようになります。証明書のホームグループを簡単に検索するには、証明書をクリックし、ドロップダウンメニューで **アクセスグループ**をクリックします。証明書のホームグループはポップアップメニューの最初の行に表示されます(例:証明書のホームグループは、ポップアップメニューの最初の行に表示されます(例: /All/San Diego))[証明書の共有](#)の詳細については、サンプルシナリオを参照してください)。



ホームグループの証明書のみを表示できます(証明書の**読み取り**権限がある場合) ESET PROTECTインストール中に作成される証明書は**すべて**グループにあり、管理者のみがアクセスできます。

取り消しを表示ボタンをクリックすると、すべての [取り消された証明書](#)が表示されます。

サーバー支援インストールのエージェント証明書 - この証明書は、**[証明書を生成する]**オプションを選択した場合に、サーバーインストール中に生成されます。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

新しい証明書の作成

インストール処理の一部としてESET PROTECTでは、エージェントのピア証明書を作成する必要があります。これらの証明書は、クライアントデバイスのエージェントとESET PROTECTサーバーの間の通信を認証するために使用されます。

i 例外として、サーバー支援インストールのエージェント証明書を手動で作成できません。[証明書
を生成]オプションを選択した場合、この証明書はサーバーインストール中に生成されます。

ESET PROTECT Webコンソールで新しい証明書を作成するには、**詳細 > ピア証明書**に移動し、**アクション > 新規作成**をクリックします。

基本

説明 - 証明書の説明を入力します。

タグを選択をクリックして、[タグを割り当て](#)ます。

製品 - ドロップダウンメニューから作成する証明書のタイプを選択します。

ホスト - [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。

! MDM証明書を作成するときにはMDMホストデバイスのIPアドレスまたはホスト名を入力します。既定値(アスタリスク)はこのタイプの証明書で有効ではありません。

パスフレーズ - このフィールドを空欄にすることをお勧めしますが、クライアントがアクティベートを試行するときに必要な証明書のパスワードを設定できます。

! 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。

属性(件名)

このフィールドは任意ですが、この証明書の詳細を入力できます。

共通名 - 選択した**製品**に従って、この値には文字列AgentProxyServerが含まれます。必要に応じて、証明書に関する説明情報を入力できます。**有効開始**と**有効終了**値を入力して、証明書が有効であることを保証します。

i ESET PROTECTコンポーネントのインストール中に作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の2日前に設定されます。
ESET PROTECT Webコンソールで作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の1日前に設定されます。この理由は、影響を受けるシステム間のすべての考えられる時間の不一致に対応するためです。
たとえば、インストール中の2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値が2017年1月10日00:00:00ですESET PROTECT Webコンソールで2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値は2017年1月11日00:00:00です。

署名

2つの署名方法から選択します。

- **認証局 - ESET PROTECT認証局** (ESET PROTECTインストール中に自己作成したCA)を使用して署名する場合。

o 認証局のリストから **ESET PROTECT認証局** を選択します。

o [新しい認証局](#) を作成する

- **カスタムpfxファイル** - カスタムファイルを使用するには、[\[参照\]](#)をクリックし、カスタムファイルに移動し、**OK**をクリックします。[アップロード](#)をクリックして、この証明書をサーバーにアップロードします。[カスタム証明書](#)は使用できません。



ESET PROTECT仮想アプライアンスでESET PROTECT CA (ESET PROTECTインストール中に作成)を使用して新しい証明書を署名する場合、[\[認証局パスフレーズ\]](#)フィールドを入力する必要があります。これは[ESET PROTECT VA設定](#)中に指定したパスワードです。

概要

入力した証明書情報を確認し、**完了**をクリックします。証明書が正常に作成され、エージェントをインストールするときに**証明書**リストで使用できます。証明書はホームグループで作成されます。



新しい証明書を作成する代わりに、[公開鍵のインポート](#)、[公開鍵のエクスポート](#)、または[ピア証明書のエクスポート](#)ができます。

ピア証明書のエクスポート

ピア証明書のエクスポート

1. リストから使用する**ピア証明書**を選択し、横のチェックボックスをオンにします。
2. コンテキストメニューから**[エクスポート]**を選択します。証明書は.pfxファイルとしてエクスポートされます(秘密鍵を含む)。証明書の名前を入力し、**[保存]**をクリックします。

ピア証明書からBase64としてエクスポート

ESET PROTECTコンポーネントの証明書はWebコンソールで使用できます。Base64形式の証明書の内容をコピーするには、[\[詳細\]](#) > [\[ピア証明書\]](#)をクリックし、証明書を選択して、**[Base64としてエクスポート]**を選択します。Base64エンコード証明書はファイルとしてもダウンロードできます。他のコンポーネント証明書と認証機関でもこの手順を繰り返します。

×

Export Public Key as Base64

You can copy the Base64 encoded certificate to clipboard. You can also download the Base64 encoded certificate as a file.

DOWNLOAD

CLOSE

i 証明書をエクスポートするには、**証明書の使用権限**が必要です。詳細については、[アクセス権の一覧](#)を参照してください。

APN/ABM証明書

APN (Apple Push Notification)/ABM (Apple Business Manager)証明書はESET PROTECT MDM for iOSデバイス登録で使用されます。**Apple社が提供するプッシュ証明書**を作成し、iOSデバイスをESET PROTECTに登録するにはApple社の署名を付ける必要があります。またに有効なESET PROTECTライセンスがあることを確認します。

[詳細]タブ > [ピア証明書]をクリックし、[新規]をクリックしてから[APN/ABM証明書]を選択します。

i APN証明書を取得するには、[Apple ID](#)が必要です。このIDはAppleが証明書に署名するために必要です。

i APN証明書には1年間の有効期間があります。証明書の有効期限が近い場合は、以下の手順と証明書パート手順2に従い、**更新**を選択します。

ABM登録トークンを取得するには、[Apple ABMアカウント](#)が必要です。

要求の作成

証明書の属性(国コード、組織名など)を指定し、[要求の送信]をクリックします。

ESET PROTECT

Computer Name QUICK LINKS HELP ADMINISTRATOR LOGOUT 9 min

DETECTIONS
Submitted Files
Exclusions
Quarantine

COMPUTERS
Computer Users
Dynamic Group
Templates

LICENSES
License Management

ACCESS RIGHTS
Users
Permission Sets

CERTIFICATES
Peer Certificates
Certification Authorities

SERVER
Server Settings

ACTIVITY AUDIT
Audit Log

Close

New APN/ABM Certificate

Peer Certificates > New APN/ABM Certificate

Create Request

Download
Certificate
Upload

Attributes (Subject)

Common name ⓘ
APN/ABM Certificate

Country code ⓘ

State or Province ⓘ

Locality name ⓘ

Organization name ⓘ

Organizational unit ⓘ

SUBMIT REQUEST

BACK CONTINUE CANCEL

ダウンロード

CSR (証明書署名要求) と秘密鍵をダウンロードします。

Create Request

Download

Certificate
Upload

Download Certification Signing Request (CSR) and Private Key to your disk

DOWNLOAD PRIVATE KEY

DOWNLOAD CSR

証明書

1. [Apple Push Certificates Portal](#)を開き、[Apple ID](#)を使用してログインします。
2. 証明書の作成をクリックします。
3. 備考(任意)を入力します。[ファイルの選択]をクリックし、前の手順でダウンロードしたCSRファイルをアップロードして、[アップロード]をクリックします。
4. しばらくすると、新しい確認画面に、ESET Mobile Device ManagementサーバーのAPNS証明書が正常に作成されたことを示す通知が表示されます。
5. ダウンロードをクリックして、.pemファイルをコンピューターに保存します。
6. Apple Push Certificateポータルを閉じ、以下のアップロードセクションに進みます。

[Create Request](#)
[Download](#)
[Certificate](#)
[Upload](#)

Open portal [Apple Push Certificates Portal](#) and follow the instructions on the portal

[OPEN APPLE PORTAL](#)

In order to optionally use the Apple Business Manager, open portal [business.apple.com](#) and follow the instructions on the portal. Use the signed MDM Certificate from Apple Portal as Public Key when requested.

[OPEN APPLE ABM PORTAL](#)

You will need Apple ID to use portal. You can create it on [appleid.apple.com](#)

⚠ APNS証明書はABMおよび非ABM MDCポリシーの両方で必要です。ABM登録証明書を作成する場合は、[ここ](#)に進んでください。

Apple Push Certificates Portal

Sign out

Certificates for Third-Party Servers

Create a Certificate

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	ESET, spol. s r.o.	Dec 16, 2017	Active	i Renew Download Revoke

*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

アップロード

上記のすべての手順が完了したら、[MDCのポリシーを作成し、iOS登録のためのAPNSを有効にします](#)任意のiOSデバイスを登録できます。デバイスのブラウザから https://<mdmcore>:<enrollmentport>/unique_enrollment_token にアクセスします。

[Create Request](#)
[Download](#)
[Certificate](#)
[Upload](#)

Upload your Apple Push Notification (APN) certificate and Private Key to the new ESET PROTECT Mobile Device Connector policy, or open and edit existing one. If you have created the ABM Authorization Token in the previous step, you may add it to the policy as well. ABM Authorization Token and APN Certificate share the same Private Key.

[OPEN POLICIES](#) [CREATE NEW POLICY](#)

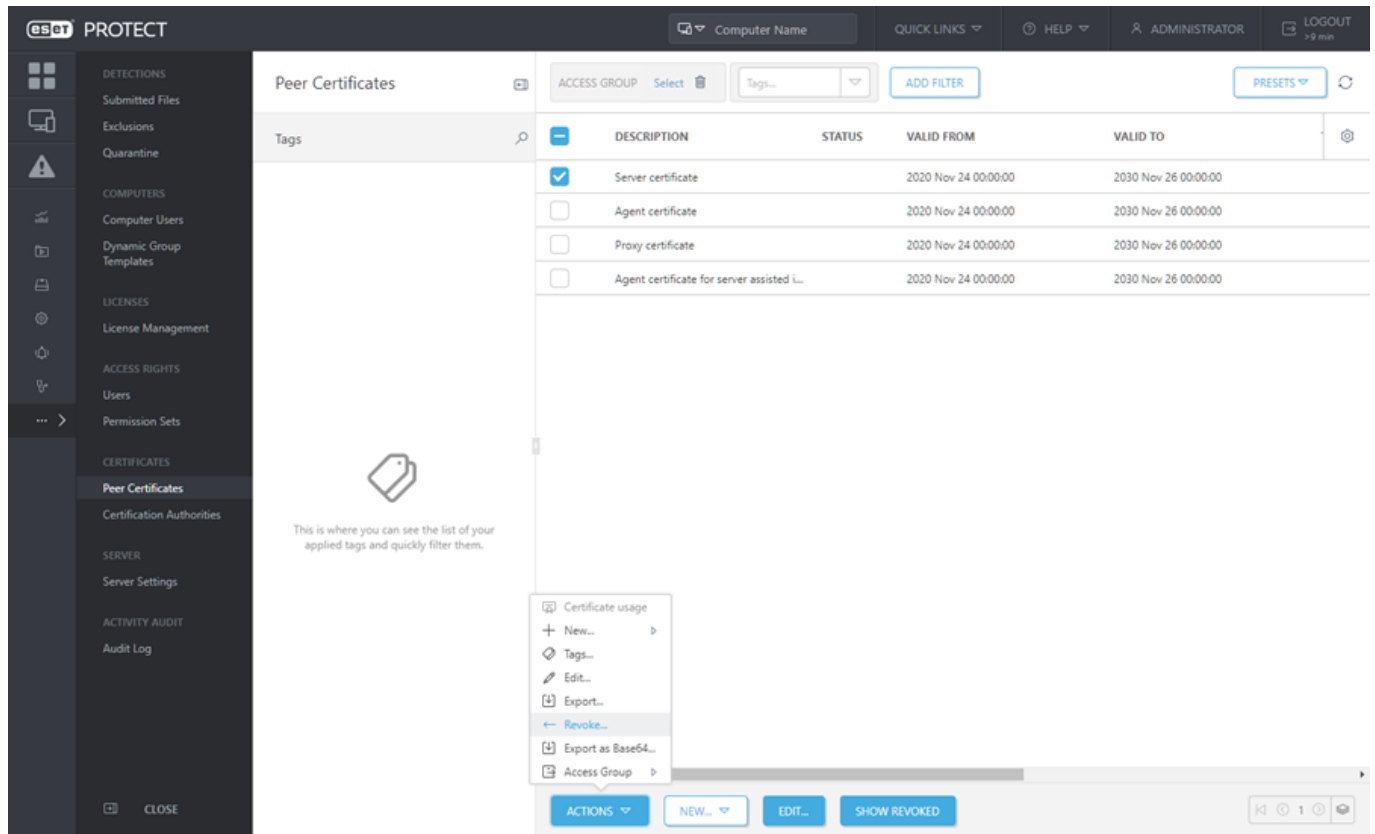
At least one applied ESET PROTECT Mobile Device Connector policy has to contain APN certificate and Private Key. This policy can be merged with other policies which do not contain them.

取り消しを表示

このリストにはESETPROTECTサーバーによって作成され、無効化されたすべての証明書が表示されます。取り消された証明書はメイン[ピア証明書]画面から自動的に削除されます。[取り消しを表示]をクリックすると、メインウィンドウから取り消された証明書が表示されます。

証明書を取消するには、次の手順に従います。

1. [詳細] > [ピア証明書] に移動し、証明書を選択して、[取消] をクリックします。



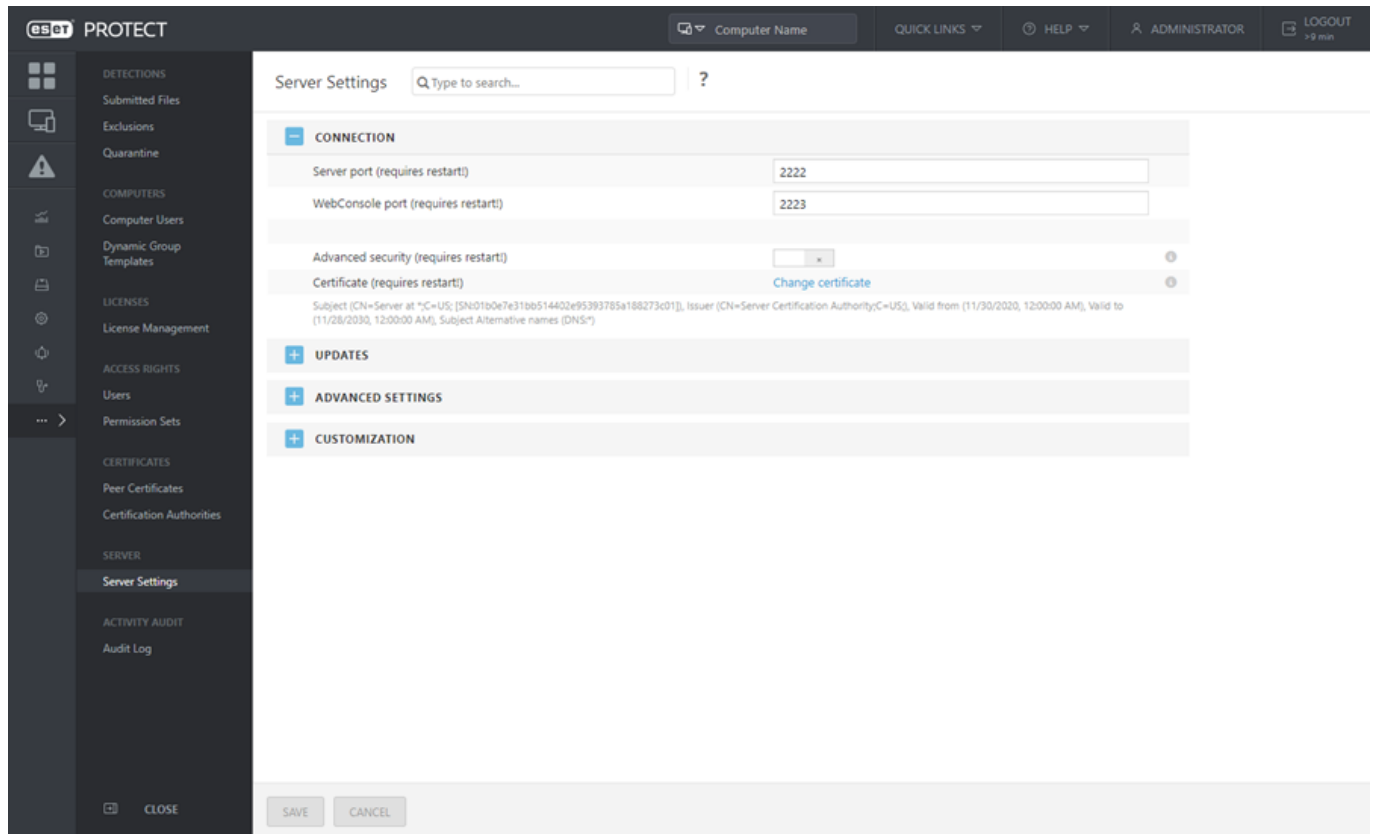
2. 取り消し理由を入力し、[取り消し]をクリックします。

3. **OK**をクリックします。証明書はピア証明書のリストに表示されなくなります。以前に取り消された証明書を表示するには、[取り消しの表示]ボタンをクリックします。

新しいESET PROTECTサーバー証明書の設定

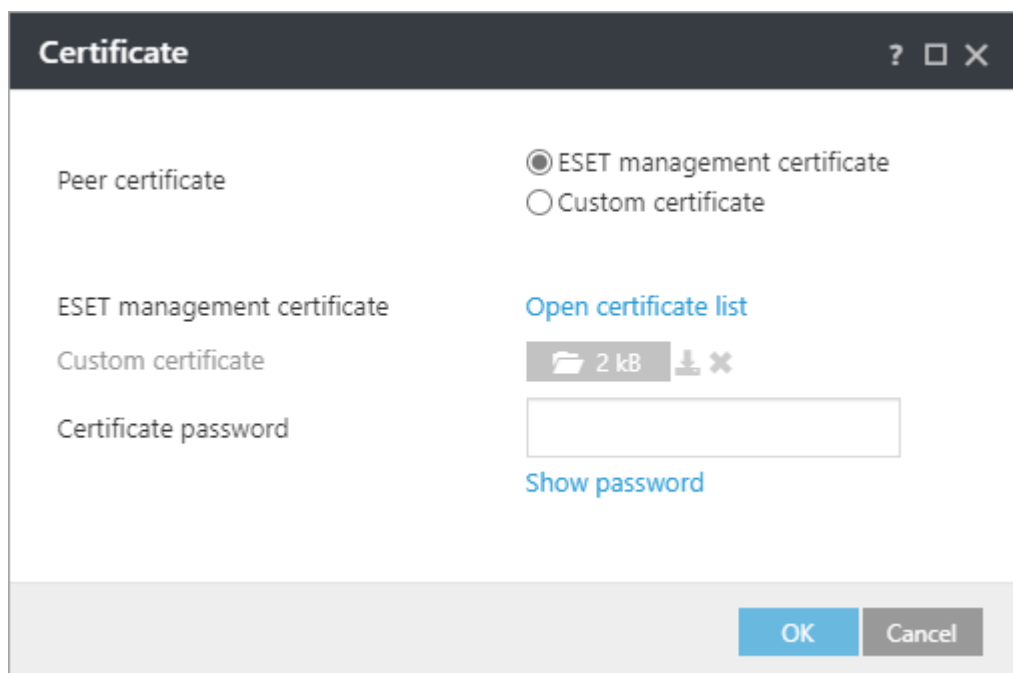
ESET PROTECTサーバー証明書はインストール中に作成され、ESET Managementエージェントおよびその他のコンポーネントに配布され、ESET PROTECTサーバーとの通信を可能にします。必要に応じてESET PROTECTサーバーを構成し、別のピア証明書を使用できます。ESET PROTECTサーバー証明書(インストール中に自動的に生成)または**カスタム証明書**を使用できます。安全なTLS接続と認証にはESET PROTECTサーバー証明書が必要です。サーバー証明書を使用してESET ManagementエージェントとESET PROTECTプロキシが非合法的なサーバーに接続しないことを保証します。

1. [詳細] > [サーバー設定]をクリックし、[接続]セクションを展開して、[証明書の変更]を選択します。



2.2つのピア証明書タイプから選択します。

- **ESET Management証明書** - [証明書リストを開く]をクリックして、使用する証明書を選択します。
- **カスタム証明書** - カスタム証明書を参照し、[OK]をクリックし、[保存]をクリックします。移行を実行している場合は、古いESET PROTECTサーバーからエクスポートしたESET PROTECTサーバー証明書.pfxファイルを選択します。



3.ESET PROTECTServer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。

ESET PROTECTのカスタム証明書

環境内に固有のPKI (公開鍵インフラストラクチャ)がありESET PROTECTでカスタム証明書を使用してコンポーネント間の通信を行う場合は、次の手順ですべて設定できます。この例はWindows Server 2012 R2で実行されます。スクリーンショットはWindowsのバージョンによって異なる場合がありますが、一般的な手順は同じです。

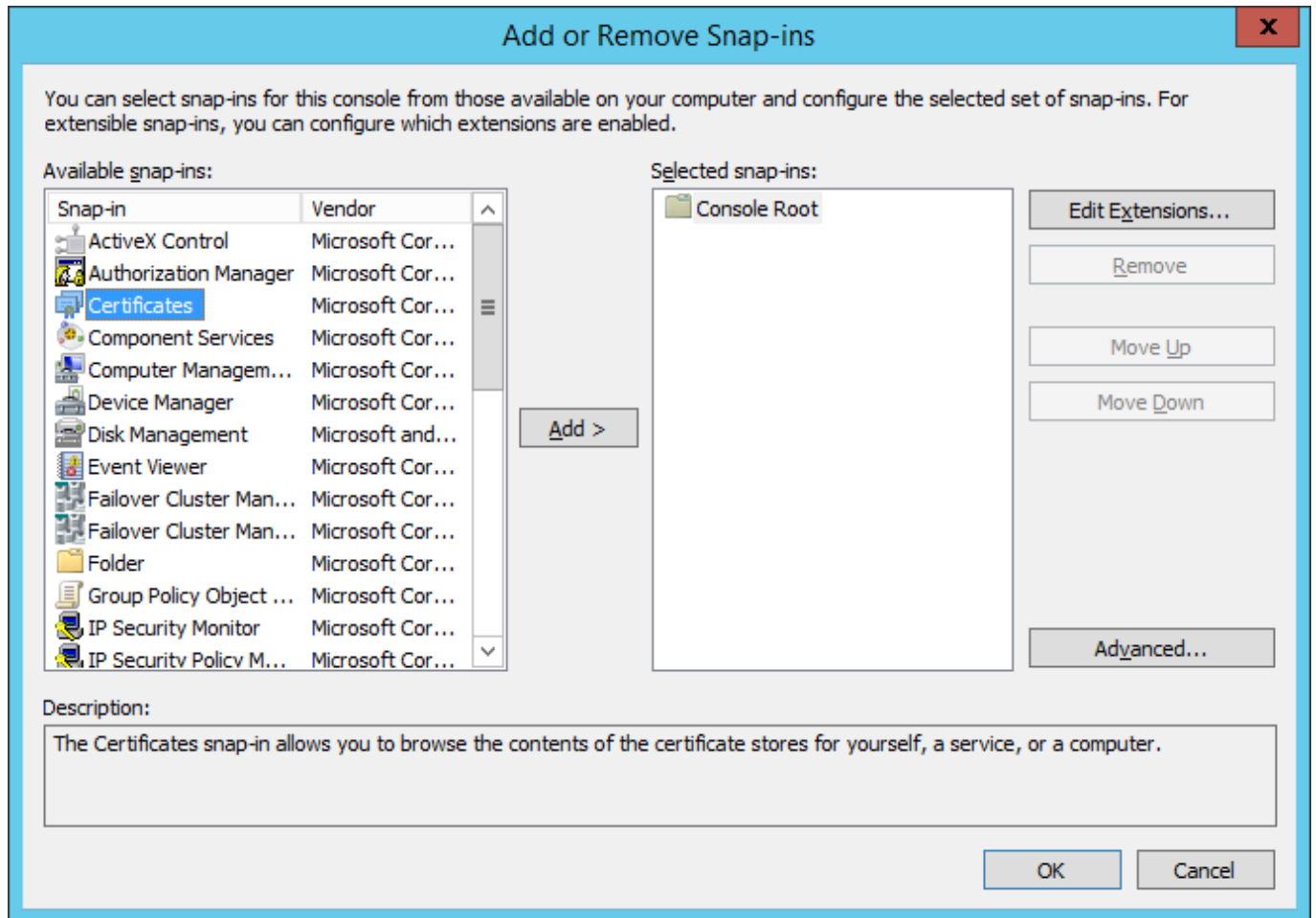
i OpenSSLを使用して、新しい証明書を作成できます。詳細については、「[ナレッジベース記事](#)」を参照してください。

必要なサーバーロール:

- Active Directory ドメインサービス。
- Active Directory Certificate ServicesとスタンドアロンRoot CAがインストールされます。

1. 管理コンソールを開き、証明書スナップインを追加します。

- a) ローカル管理者グループのメンバーとしてサーバーにログインします。
- b) mmc.exeを実行し、管理コンソールを開きます。
- c) ファイルをクリックし、スナップインの追加と削除...を選択(またはCTRL+Mを押下)します。
- d) 左のペインで証明書を選択し、追加をクリックします。



e) コンピューターアカウントを選択し、**次へ**をクリックします。

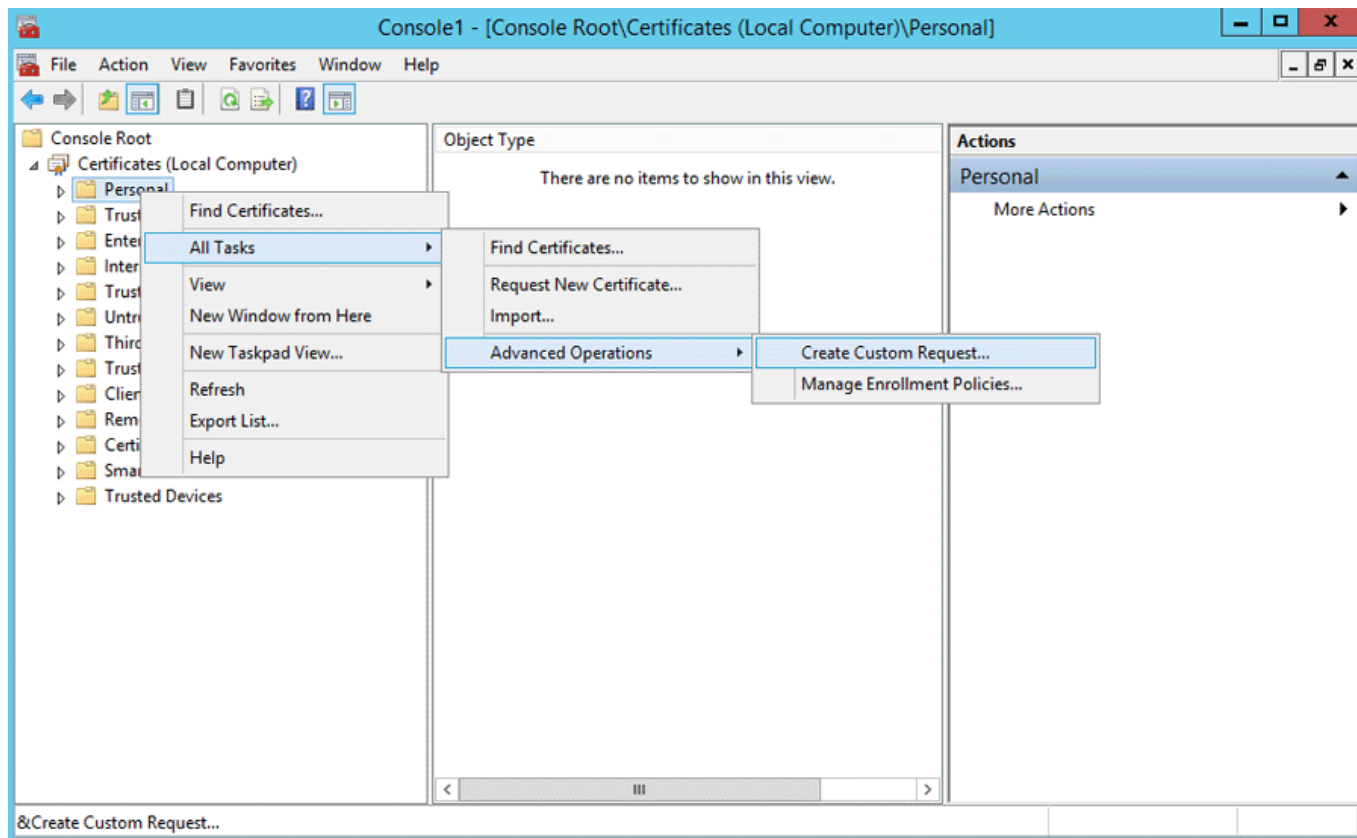
f) ローカルコンピューターが選択(既定)されていることを確認し、**完了**をクリックします。

g) **OK**をクリックします。

2. カスタム証明書要求を作成します。

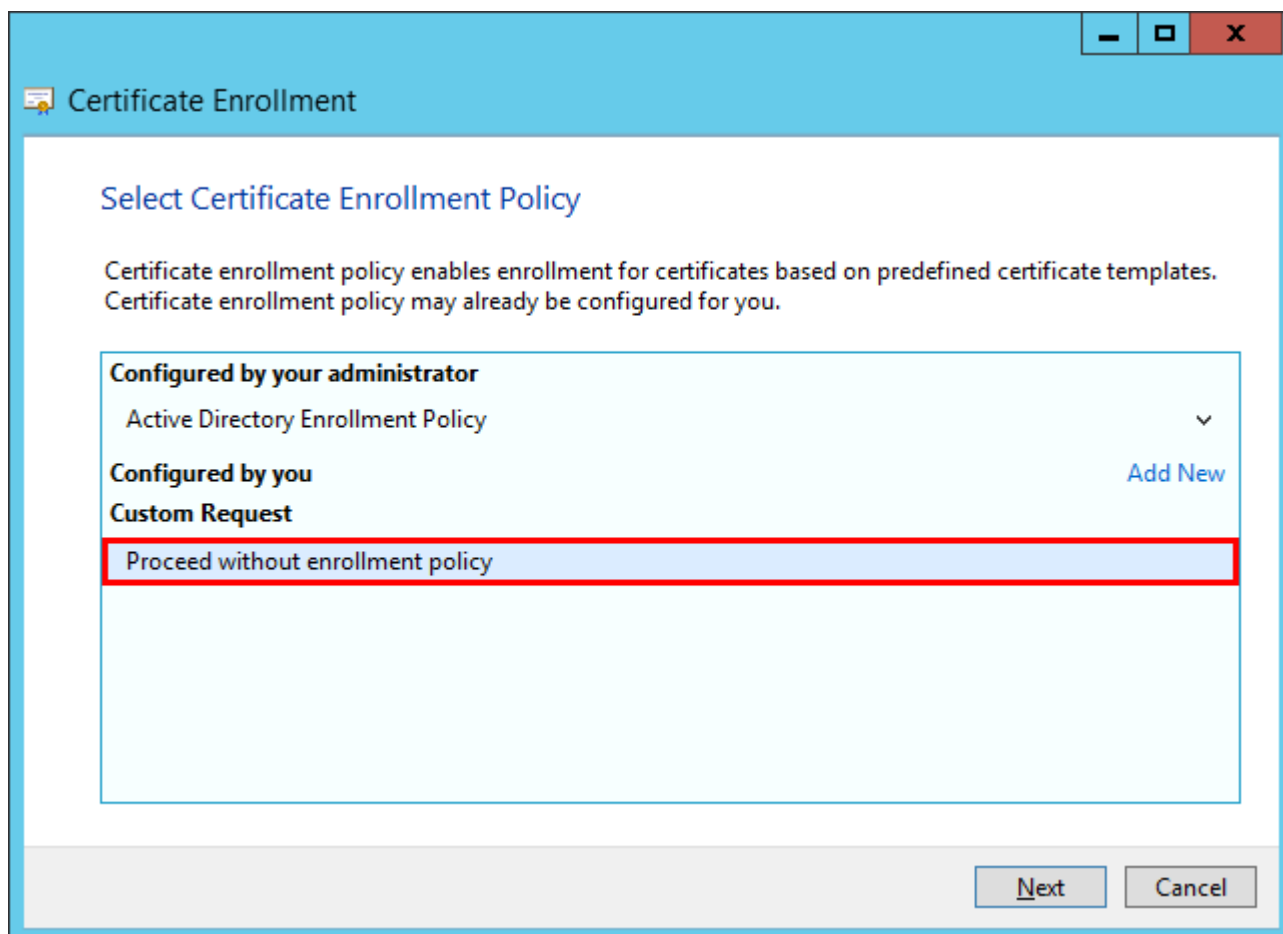
a) 証明書(ローカルコンピューター)をダブルクリックして展開します。

b) 個人をダブルクリックして展開します。証明書を右クリックし、すべてのタスク > 詳細オプションを選択し、カスタム要求の作成を選択します。

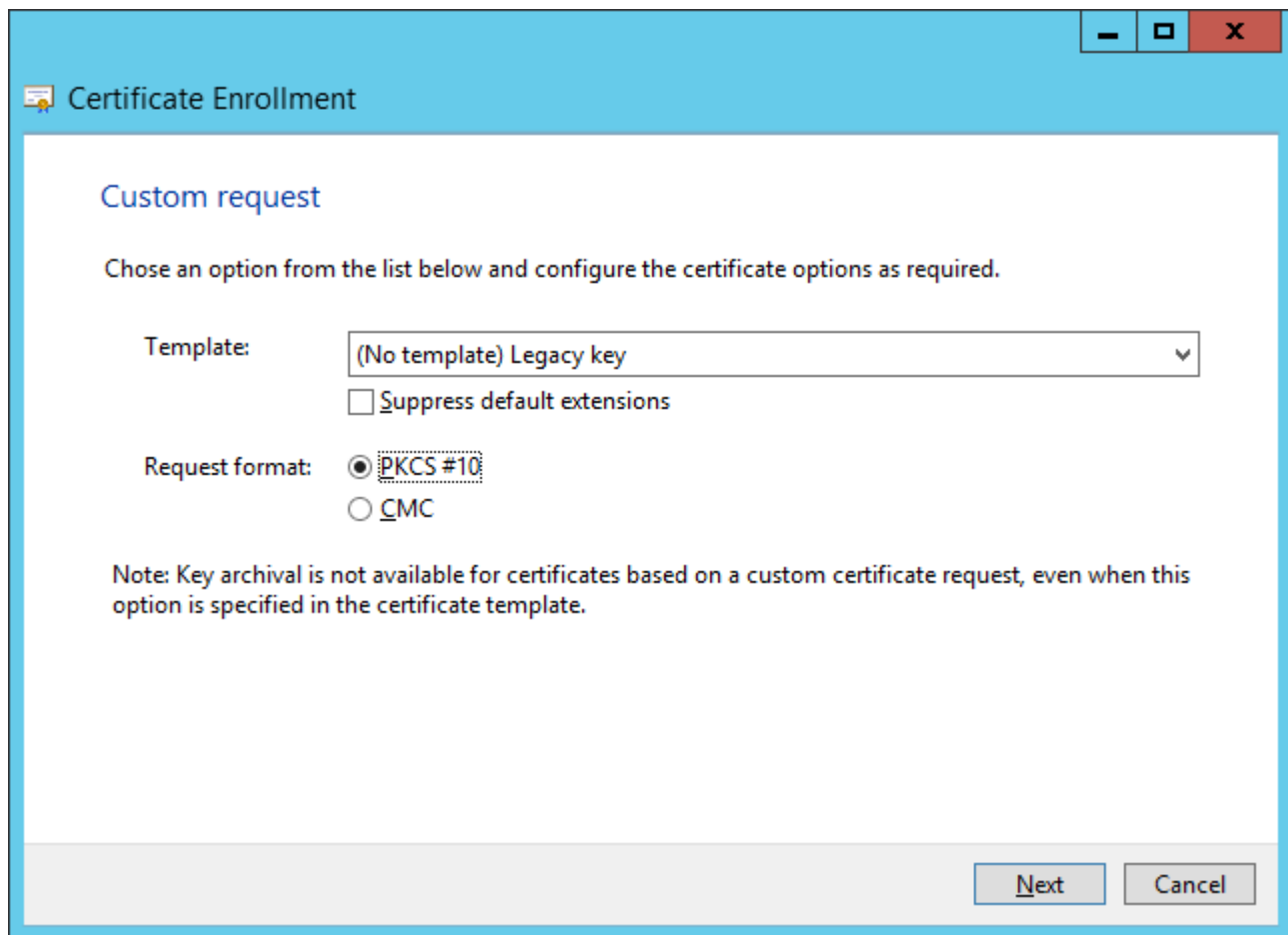


c)証明書登録ウィザードウィンドウが開きます。次へをクリックします。

d)登録ポリシーなしで続行するを選択し、次へをクリックして続行します。



e) ドロップダウンリストから(テンプレートなし)レガシーキーを選択し、PKCS #10要求形式が選択されていることを確認します。Next(次へ)をクリックします。



The image shows a Windows-style dialog box titled "Certificate Enrollment". It has a blue header bar with standard window controls (minimize, maximize, close) on the right. Below the header, the title "Certificate Enrollment" is followed by a small icon. The main content area is titled "Custom request" in blue. Below this, a instruction says "Chose an option from the list below and configure the certificate options as required." (Note the typo "Chose"). There are two main settings: "Template:" with a dropdown menu showing "(No template) Legacy key" and a small downward arrow, and "Request format:" with two radio buttons. The "Request format" section has "PKCS #10" selected (indicated by a filled circle) and "CMC" (indicated by an empty circle). Below these settings, a note states: "Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template." At the bottom right, there are two buttons: "Next" and "Cancel".

Template: (No template) Legacy key

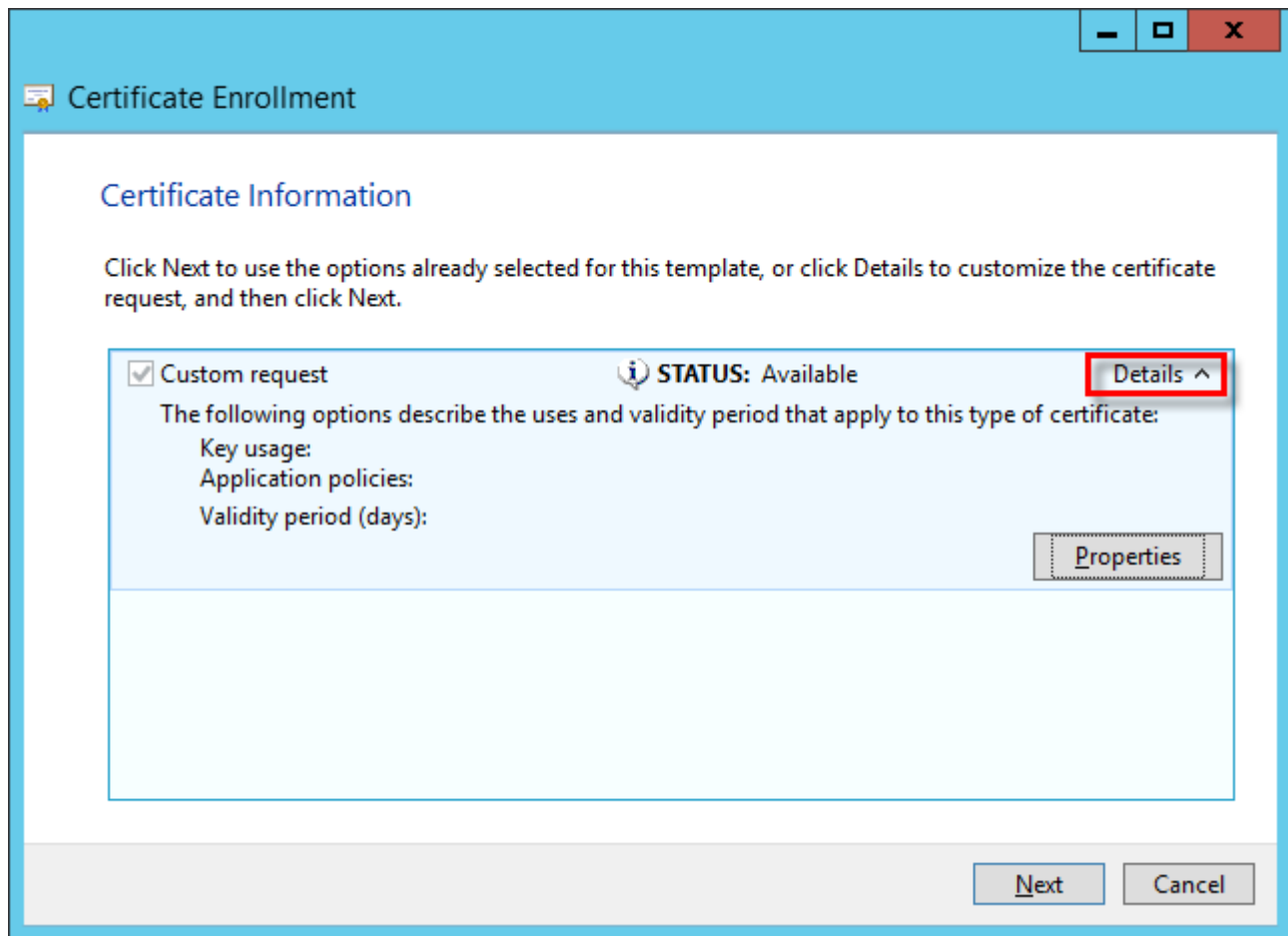
☐ Suppress default extensions

Request format: ☒ PKCS #10 ☐ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

Next Cancel

f) 矢印をクリックして詳細 セクションを展開し、プロパティをクリックします。



g)全般タブで証明書のフレンドリ名を入力します。説明(任意)も入力できます。

h)件名タブで次の手順を実行します。

件名セクションで**タイプ**の下ドロップダウンリストから**共通名**を選択し、era serverを**値**フィールドに入力します。次に、**追加**をクリックします。**CN=era server**が右側の情報ボックスに表示されます。ESET Managementエージェントの証明書要求を作成する場合は、共通名値フィールドでera agentを入力します。

⚠ 共通名には次の文字列のいずれかを含める必要があります。**"server"**と**"agent"**(作成する証明書要求によって異なる)。

i)代替名 セクションで、**タイプ**の下ドロップダウンリストから**DNS**を選択し、* (アスタリスク)を**値**フィールドに入力して、**追加**ボタンをクリックします。

⚠ 件名代替名(SAN)は、ESET PROTECTサーバーとすべてのエージェントの「DNS: *」として定義してください。

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:

Type:
Common name

Add >

Value:

< Remove

CN=era server

Alternative name:

Type:
DNS

Add >

Value:

< Remove

DNS
*

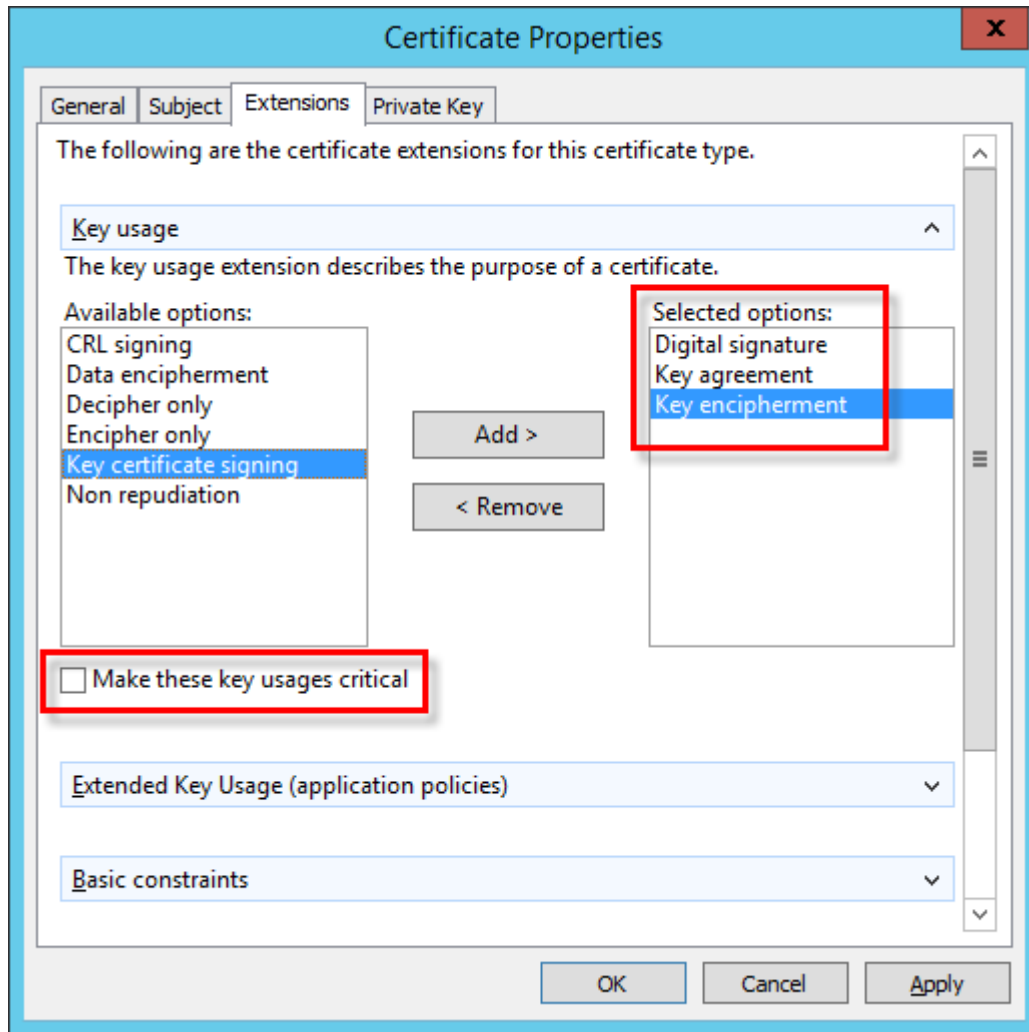
OK Cancel Apply

j) 拡張タブで矢印をクリックして、**鍵の使用**セクションを展開します。使用可能なオプションから次の項目を追加します。**デジタル署名**、**キーの承諾**、**キーの暗号化**。これらの**鍵使用を重要にする**をオフにします。

キーの使用 > **鍵証明書署名**の下の次の3つのオプションを選択していることを確認してください。



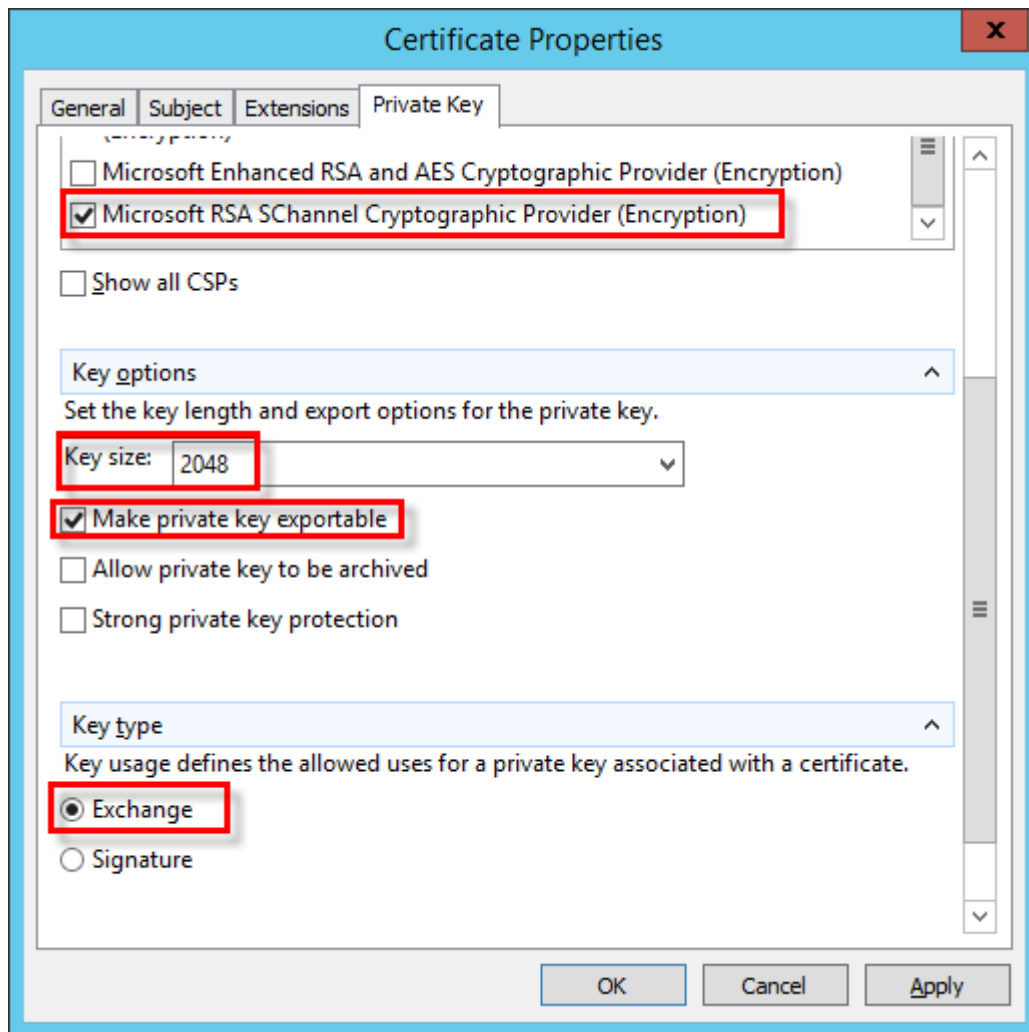
- デジタル署名
- キーの承諾
- キーの暗号化



k) **秘密鍵**タブで次の手順を実行します。

i. 矢印をクリックし、**暗号化サービスプロバイダー**セクションを展開します。すべての暗号化サービスプロバイダー(CSP)の一覧が表示されます。**Microsoft RSA SChannel暗号化プロバイダー(暗号化)**のみが選択されていることを確認します。

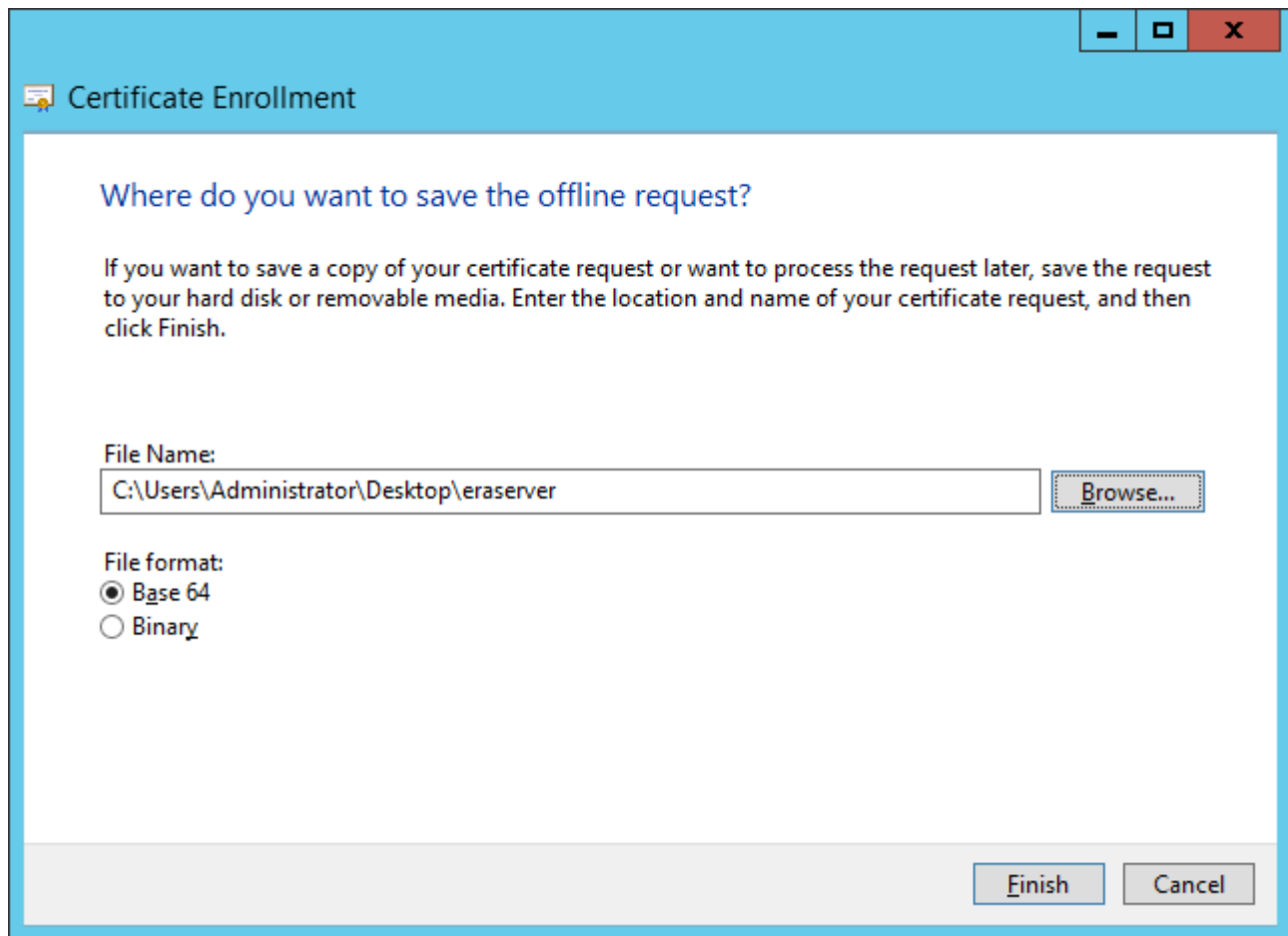
i Microsoft RSA SChannel暗号化プロバイダー(暗号化)以外のすべてのCSPをオフにします。



i. 鍵オプションセクションを展開します。鍵サイズメニューで、**2048**以上の値を設定します。秘密鍵をエクスポート可能にするを選択します。

ii. 鍵タイプセクションを展開し、**交換**を選択します。**適用**をクリックして設定を確認します。

l) **OK**をクリックします。証明書情報が表示されます。**次へ**ボタンをクリックして続行します。**参照**をクリックして、証明書署名要求(CSR)が保存される場所を選択します。ファイル名を入力し、**Base 64**が選択されていることを確認します。

A Windows-style dialog box titled "Certificate Enrollment" with a blue header bar. The main area is white and contains the text "Where do you want to save the offline request?" followed by instructions: "If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish." Below this is a "File Name:" label, a text input field containing "C:\Users\Administrator\Desktop\eraserver", and a "Browse..." button. Underneath is a "File format:" label with two radio buttons: "Base 64" (selected) and "Binary". At the bottom right are "Finish" and "Cancel" buttons.

Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:

C:\Users\Administrator\Desktop\eraserver

Browse...

File format:

☒ Base 64

☐ Binary

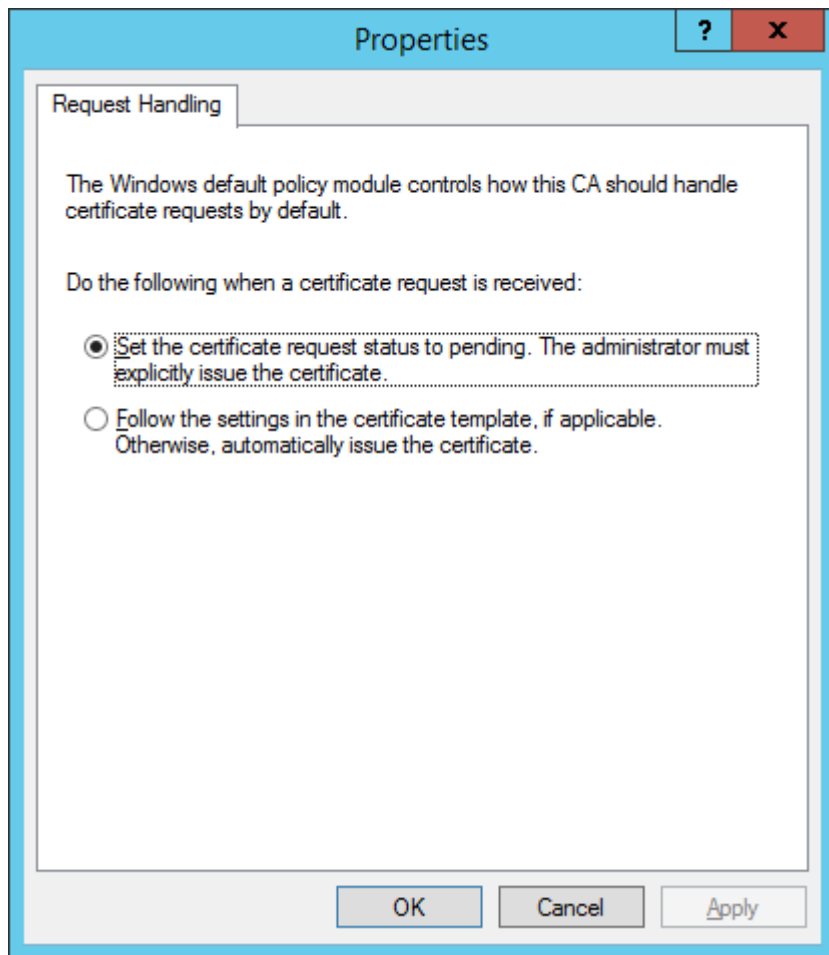
Finish Cancel

m)完了をクリックしてCSRを生成します。

3. カスタム証明書要求をインポートするには、次の手順に従います。

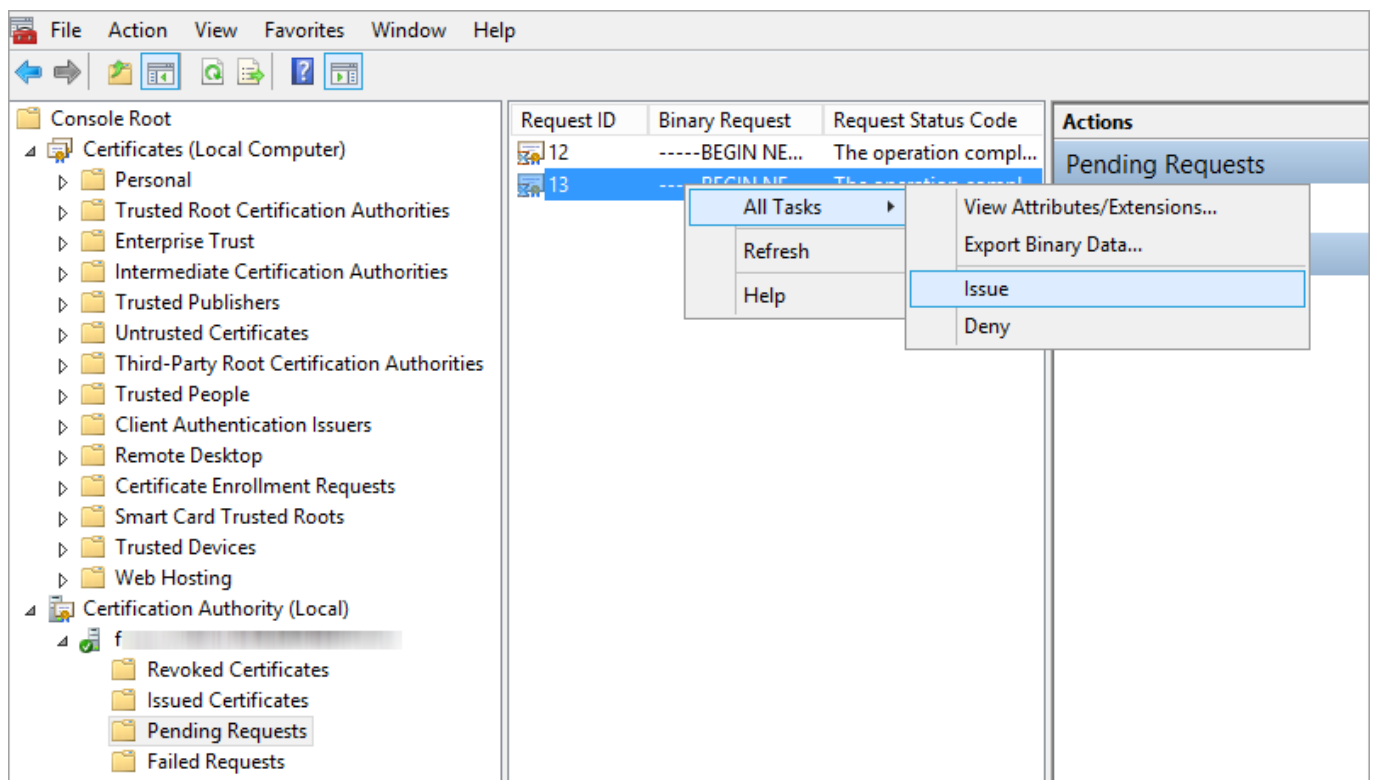
a)Server Managerを開き、ツール>認証局をクリックします。

b)認証局(ローカル)ツリーで、サーバー(通常はFQDN)>プロパティを選択し、ポリシーモジュールタブを選択します。プロパティをクリックし、[証明書要求ステータスを保留に設定する]を選択します。管理者は明示的に証明書を発行する必要があります。そうでない場合は、正常に動作します。この設定を変更する必要がある場合は、Active Directory証明書サービスを再起動する必要があります。



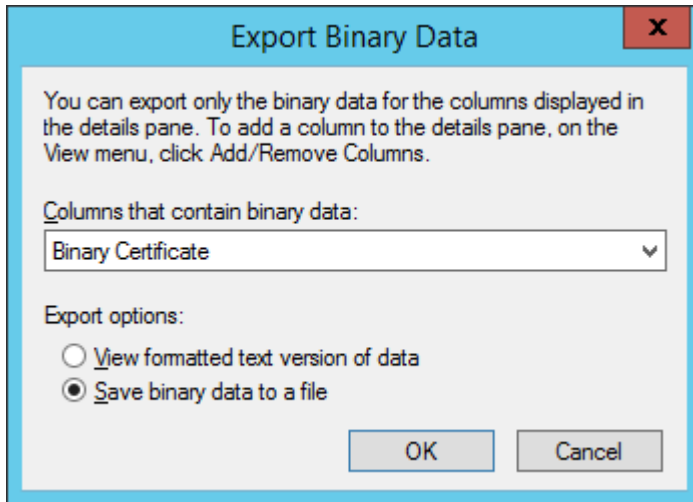
c) 認証局(ローカル)ツリーで、サーバー(通常はFQDN) > すべてのタスク > 新しい要求の送信... を選択し、手順2で生成されたCSRファイルに移動します。

d) 証明書は 保留中の要求 に追加されます。右のナビゲーションペインでCSRを選択します。アクションメニューで、 すべてのタスク > 発行 を選択します。



4. 発行されたカスタム証明書を.tmpファイルにエクスポートします。

- a) 左のペインで発行された証明書をクリックします。エクスポートする証明書を右クリックし、すべてのタスク > バイナリデータのエクスポートをクリックします。
- b) [バイナリデータのエクスポート] ダイアログで、ドロップダウンリストからバイナリ証明書を選択します。エクスポートオプションでバイナリデータをファイルに保存を選択し、OKをクリックします。



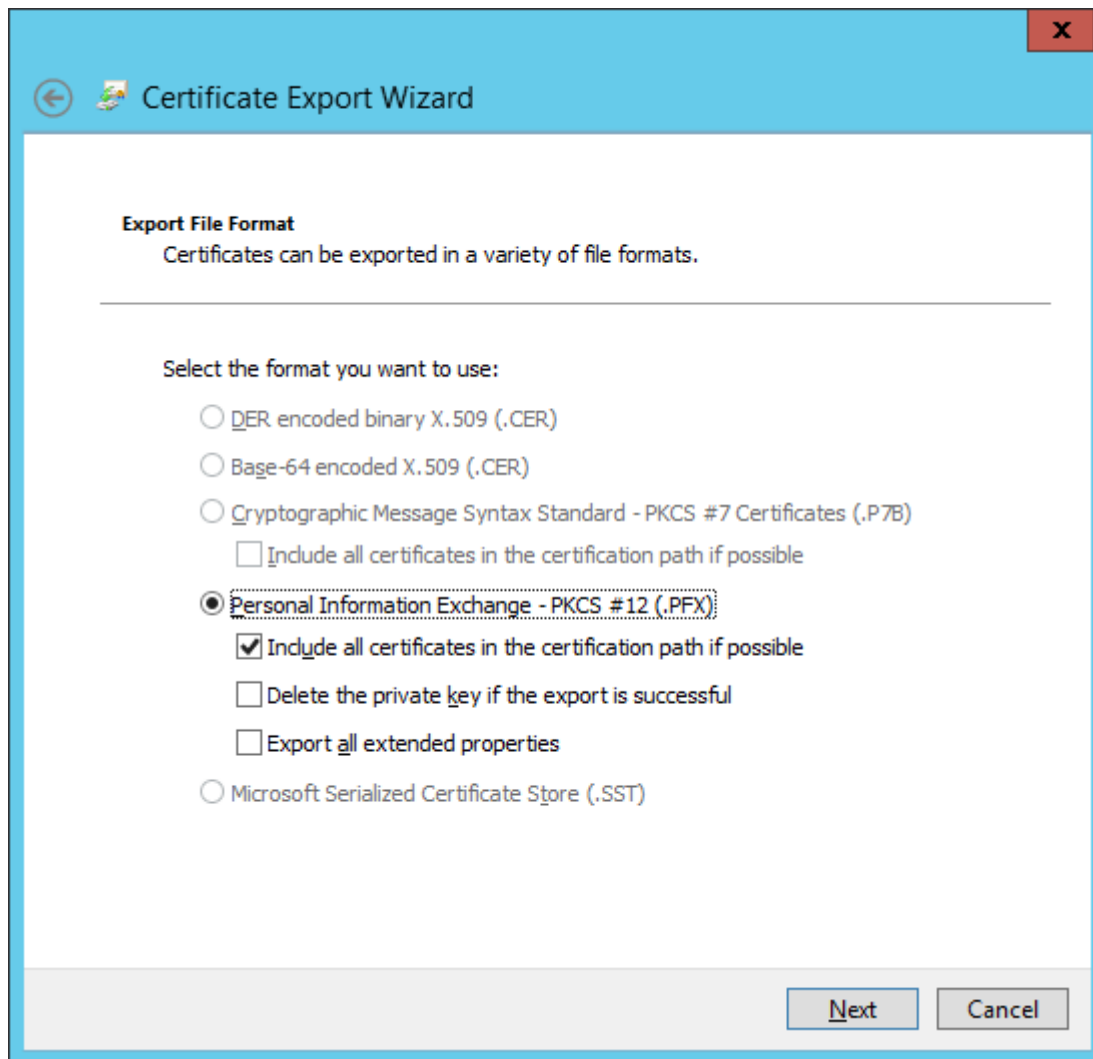
- c) [バイナリデータの保存] ダイアログボックスで、証明書を保存するファイルの場所に移動し、保存をクリックします。

5. .tmpファイルをインポートします。

- a) 証明書(ローカルコンピューター)に移動し、個人を右クリックして、すべてのタスク > インポートを選択します。
- b) **Next**(次へ)をクリックします。
- c) **参照**を使用して以前に保存された.tmpバイナリファイルを見つけ、**開く**をクリックします。すべての証明書を次のストアに配置する > **個人**を選択します。**Next**(次へ)をクリックします。
- d) **完了**をクリックし、証明書をインポートします。

6. .pfxファイルへの秘密鍵を含む証明書をエクスポートします。

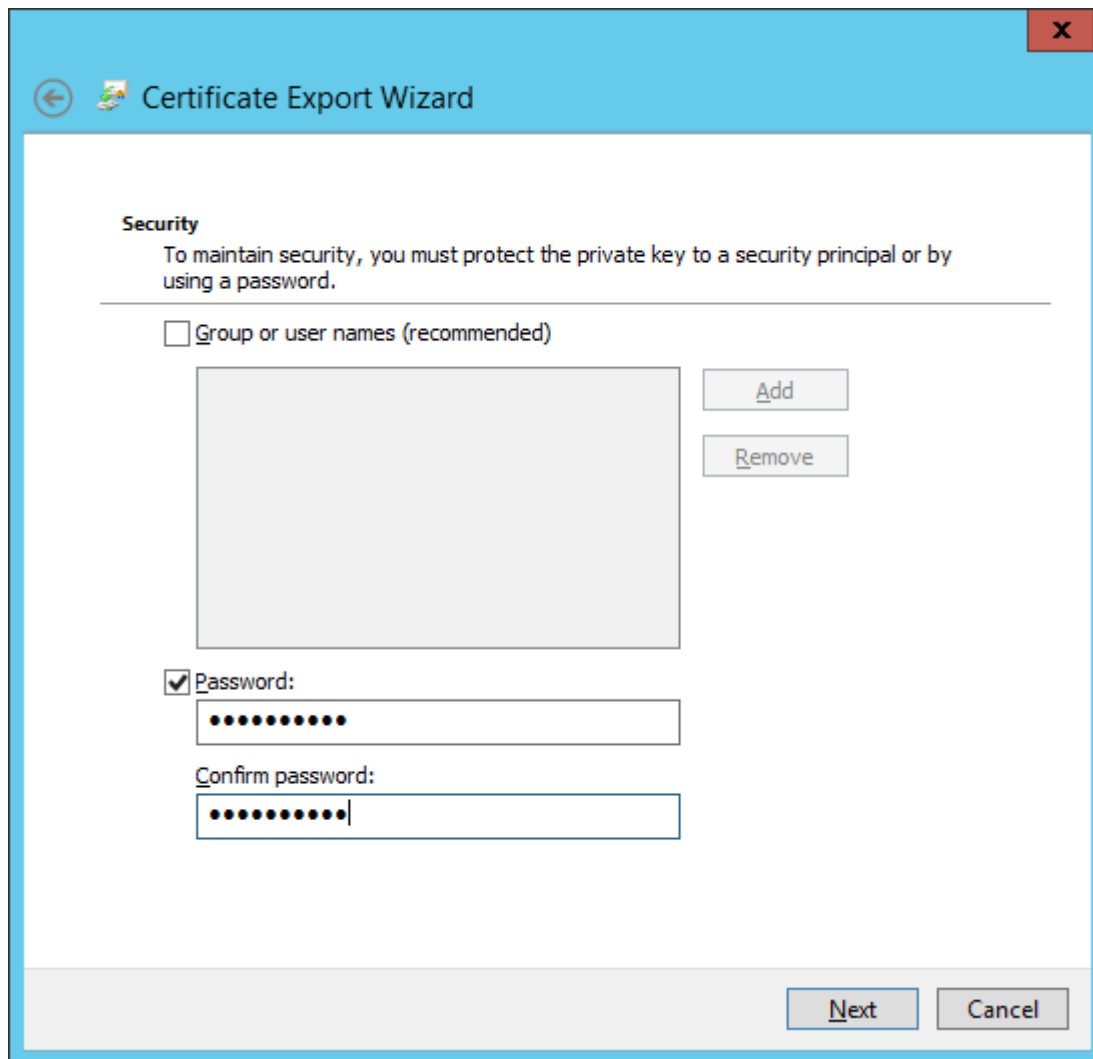
- a) 証明書(ローカルコンピューター)で個人を展開し、証明書をクリックして、エクスポートする新しい証明書を選択します。アクションメニューで**すべてのタスク > エクスポート...**を参照します。
- b) 証明書エクスポートウィザードでは、**秘密鍵をエクスポートします**をクリックします。(このオプションは、秘密鍵がエクスポート可能に設定され、秘密鍵にアクセスできる場合にのみ表示されます。)
- c) エクスポートファイル形式の下で、**Personal Information Exchange -PKCS #12 (.PFX)**を選択し、すべての証明書を認証パスに含めるには、可能な場合には認証パスのすべての証明書を含めることを選択するチェックボックスをオンにし、**次へ**をクリックします。



d)パスワード。エクスポートする秘密鍵を暗号化するパスワードを入力します。パスワードの確認フィールドで、同じパスワードをもう一度入力し、**次へ**をクリックします。



証明書パズフレーズには、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。



Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

☒ Password:

Confirm password:

e) **ファイル名**。エクスポートされた証明書と秘密鍵を保存する.pfxファイルのファイル名とパスを入力します。[次へ]をクリックし、[終了]をクリックします。

i 上記の例は、ESET Managementエージェント証明書の作成方法ですESET PROTECTサーバー証明書で同じ手順を繰り返します。
この証明書を使用してWebコンソールの別の新しい証明書に署名することはできません。

7. 認証機関のエクスポート:

- a) Server Managerを開き、ツール > **認証局**をクリックします。
- b) 認証局(ローカル)ツリーで、サーバー(通常はFQDN) > プロパティ > 一般タブを選択し、証明書の表示をクリックします。
- c) 詳細タブで、ファイルにコピーをクリックします。証明書エクスポートウィザードが開きます。
- d) エクスポートファイル形式ウィンドウで、DER暗号化バイナリX.509(.CER)を選択し、次へをクリックします。
- e) 参照をクリックして、.cerファイルが保存される場所を選択し、次へをクリックします。
- f) 完了をクリックし、認証局をエクスポートします。


ESETPROTECTでカスタム証明書を使用するための段階的な手順については、[次の章を参照](#)してください。

ESET PROTECTでのカスタム証明書の使用方法

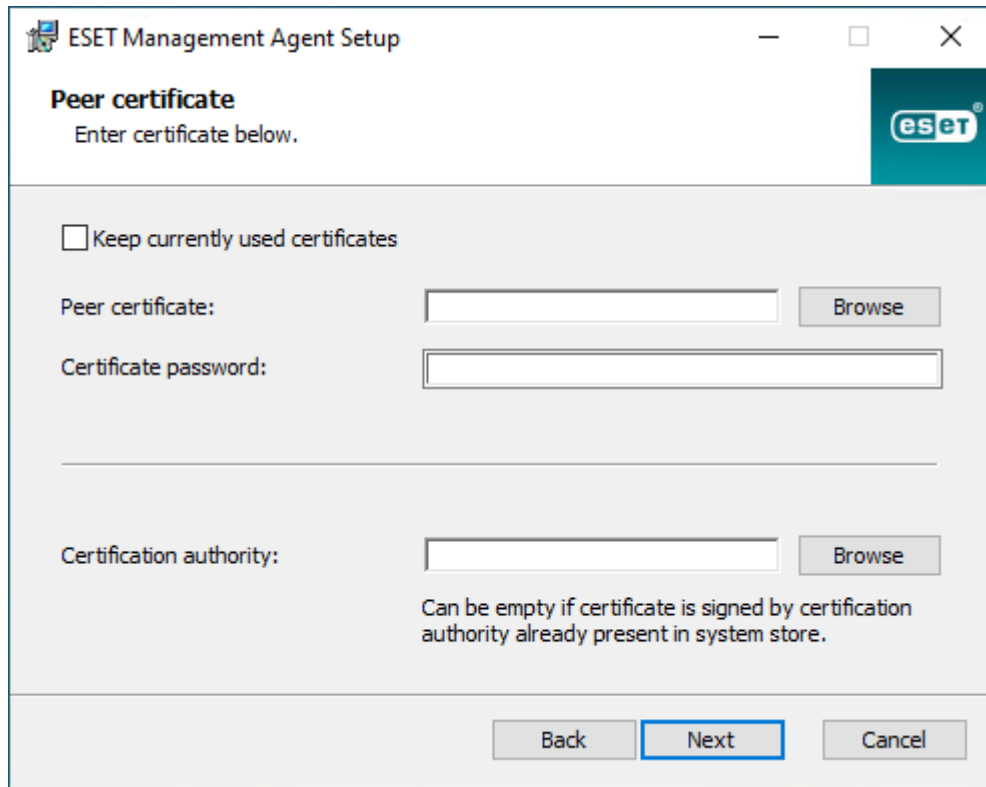
前の章の続き：

1. [サードパーティ認証局](#)をESET PROTECT Webコンソールにインポートします。
2. [新しいカスタムサーバー証明書](#)をESET PROTECT Webコンソールで設定します。

ESET Managementエージェントが既にESET PROTECTサーバーに接続している場合は、ポリシーを適用してESET Managementエージェントのカスタム証明書を変更します。

1. ESET PROTECT Webコンソールを開きます。
2. [管理] > [ポリシー] > [新規作成]をクリックします。ポリシーの名前を入力します。
3.  **設定**を展開し、ドロップダウンメニューから**ESET Managementエージェント**を選択します。
4. **接続**を展開し、**証明書の変更 (証明書の横)**をクリックします。
5. **カスタム証明書**をクリックし、ESET Managementエージェントのカスタム証明書を選択します。
6. 証明書パスワードを入力し、**OK**をクリックします。
7. [このポリシーを](#)すべてのクライアントに割り当てます。

3. **スタート > プログラムと機能**に移動し、**ESET Managementエージェント**を右クリックして、**変更**を選択します。
4. **次へ**をクリックし、**修復**を実行します。
5. サーバーホストとサーバーポートの設定をそのままにし、**次へ**をクリックします。
6. **ピア証明書**の横の**参照**をクリックし、カスタム.pfx証明書ファイルを見つけます。
7. 手順6で指定した証明書のパスワードを入力します。
8. **認証局の横の参照**をクリックしてWebコンソールからエクスポートされた [.derファイル \(公開鍵\)](#)を選択します。これはカスタム証明書が署名される公開鍵です。
9. **[次へ]**をクリックして修復を完了します。
10. ESET Managementエージェントはカスタム.pfx証明書を使用します。



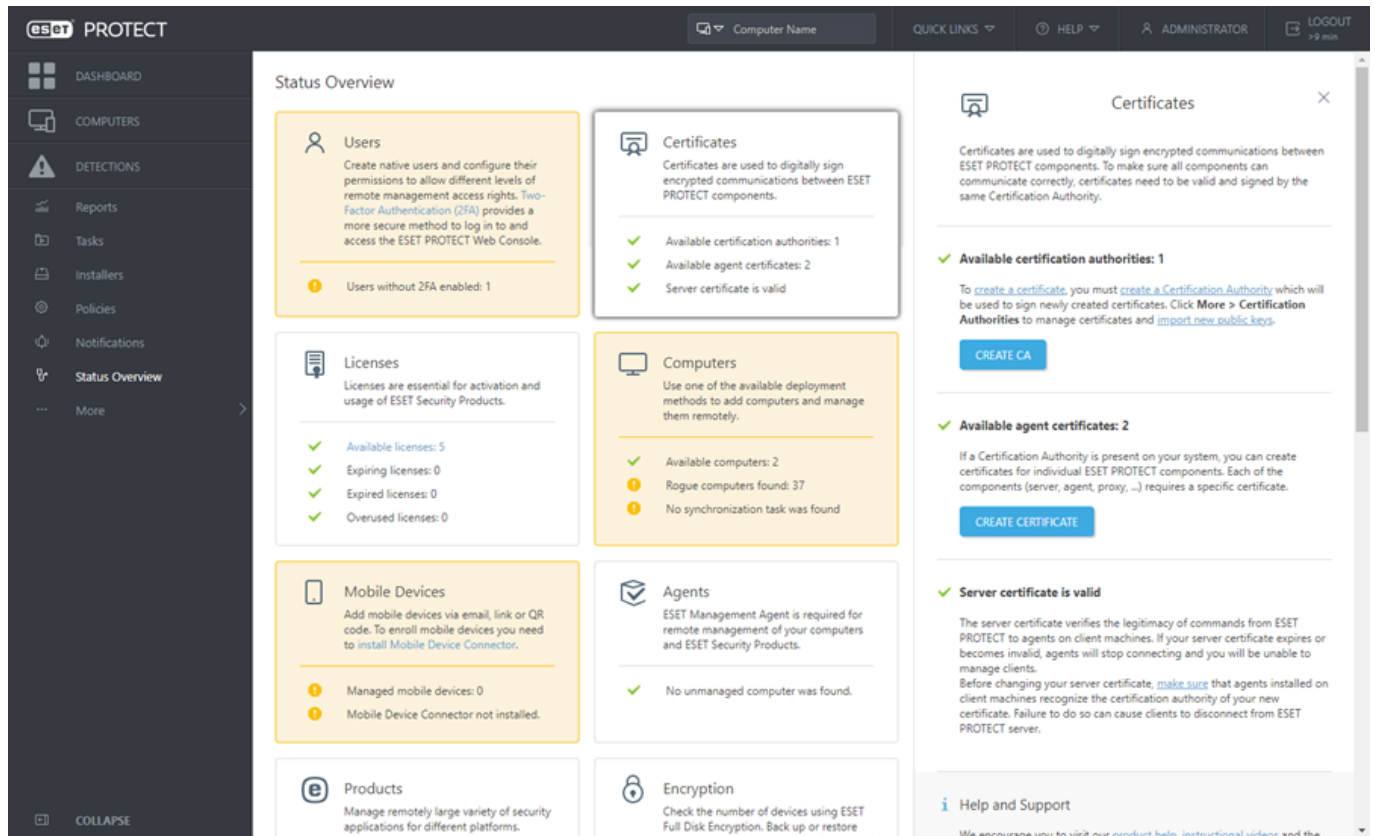
期限切れの証明書 – 報告と置換

ESET PROTECTはまもなく期限切れの証明書または認証局を通知できます。[\[通知\]](#)タブにはESET PROTECT証明書とESET PROTECT認証局の定義済み通知があります。

この機能を有効にするには、[通知を編集](#)し、[\[配信\]](#)セクションでメールアドレスやSNMPトラップなどの詳細情報を指定します。各ユーザーは、ホームグループの証明書の通知のみを表示できます(証明書の読み取り権限がある場合)。

i 最初にサーバー設定で[SMTP接続設定](#)を構成していることを確認してください。完了したら、[通知を編集](#)し、配信メールアドレスを追加します。

まもなく期限切れの証明書がコンピューターにある場合は、ステータス情報が自動的に変更されます。ステータスは[ダッシュボード](#) [コンピューターリスト](#) [ステータス概要](#)、および[証明書](#)タブに報告されます。



期限切れの認証局または証明書を置換するには、次の手順に従います。

- 1.新しい有効期間で(古いものが期限切れになる場合)[新しい認証局を作成](#)し、ただちに有効になるようにします。
- 2.新しい認証局の有効期限内にESET PROTECTサーバーと他のコンポーネント(エージェント/MDM)の新しい[ピア証明書](#)を作成します。
- 3.ポリシーを作成し、新しいピア証明書を設定します。ESET PROTECTコンポーネント、MDMおよびネットワークのすべてのクライアントコンピューターのESET Managementエージェントにポリシーを適用します。
- 4.新しい認証局とピア証明書が適用され、クライアントがレプリケーションされるまで待ちます。

i 24時間待機するか、すべてのESETPROTECTコンポーネント(エージェント)が2回以上レプリケーションされるかどうかを確認することをお勧めします。









- 5.[ESET PROTECTサーバー設定のサーバー証明書](#)を置換し、クライアントが新しいピア証明書を使用して認証できるようにします。
- 6.上記のすべての手順が完了したら、すべてのクライアントがESET PROTECTに接続し、すべてが想定通りに動作しています。古いピア証明書を[取り消し](#)、古い認証局を削除します。

認証局

認証局は、**[認証局]**セクションに一覧表示され、管理されます。複数の認証局がある場合は、フィルターを適用して、並べ替えることができます。

i 認証局と証明書は、証明書機能と同じ権限でアクセスされます。証明書と認証機関はインストール中に作成され、管理者が後から作成した証明書と認証機関は、すべて静的グループに含まれます。アクセス権の詳細については、[権限の一覧](#)を参照してください。

アクションをクリックして、選択した認証局を管理します。

-  **新規** - [新しい認証局を作成します](#)
-  **タグ**: [タグ](#)を編集します(割り当て、割り当て解除、作成、削除)。
-  **編集** - 認証局の説明を編集します。
-  **監査ログ** - 選択した項目の[監査ログ](#)を表示します。
-  **削除** - 選択した認証局を削除します。
-  [公開鍵のインポート](#)
-  [公開鍵のエクスポート](#) - このオプションを使用して、認証局をバックアップします。
-  **アクセスグループ** - 認証局を別のグループに移動し、このグループに対する十分な権限があるユーザーが使用できるようにすることができます。

フィルターとレイアウトのカスタマイズ

現在のWebコンソール画面ビューをカスタマイズできます。

- [サイドパネルとメインテーブルを管理](#)します。
- [フィルター](#)とフィルタープリセットを追加します。 [タグ](#)を使用して、表示される項目をフィルタリングできます。

証明書と権限へのアクセスを分割する方法

管理者がユーザーJohnがESET PROTECT認証局にアクセスすることを許可せず、彼が[証明書](#)を操作できるようにする必要がある場合は、管理者は次の手順に従う必要があります。


1. [新しい](#)静的グループ証明書を作成します。

2. 新しい[権限設定](#)を作成します。

a. この権限設定の名前を証明書の権限にします。

b. グループ証明書を **静的グループ** セクションで追加します。


c. **[機能]** セクションで、**証明書の書き込み**を選択します。


d. **[ユーザー]** セクションで、 **[ネイティブユーザー]** をクリックし、**John**を選択します。

e. **[完了]** をクリックして権限設定を保存します。

3. **すべて**グループから新しく作成された**証明書**グループに証明書を移動します。

a. **[詳細]** > **[ピア証明書]**に移動します。

b. 移動する証明書の横のチェックボックスをオンにします。

c. **[アクション]** >  **[アクセスグループ]** をクリックし、**[証明書]**グループを選択し、**[OK]**をクリックします。

Johnは移動された証明書を修正および使用できます。ただし、認証局はこのユーザーが届かないところに安全に保存されます。Johnは、証明書を署名するために既存の認証局(**すべてグループ**)を使用することもできません。

新しい認証局を作成する

新しい認証局を作成するには、**詳細** > **認証局**に移動し、**アクション** > ページの下の**新規**をクリックします。

認証機関

認証機関の説明を入力し、パスフレーズを選択します。このパスフレーズは12文字以上で指定します。

属性(件名)

1. 認証機関の**共通名**(名前)を入力します。複数の認証機関を識別する一意の名前を選択します。任意で、認証機関に関するわかりやすい情報を入力できます。
2. 有効開始と有効終了値を入力して、証明書が有効であることを保証します。

ESET PROTECTコンポーネントのインストール中に作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の2日前に設定されます。

i ESET PROTECT Webコンソールで作成されたすべての証明書と認証局の場合、有効期間の開始値は証明書作成の1日前に設定されます。この理由は、影響を受けるシステム間のすべての考えられる時間の不一致に対応するためです。

たとえば、インストール中の2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値が2017年1月10日00:00:00です。ESET PROTECT Webコンソールで2017年1月12日に作成された認証局と証明書の場合、定義済みの有効期間開始値は2017年1月11日00:00:00です。

3. **[保存]**をクリックして、新しい認証機関を保存します。**[詳細]**>**[認証局]**の下に認証機関が一覧表示され、使用できます。認証局は、作成したユーザーのホームグループで作成されます。

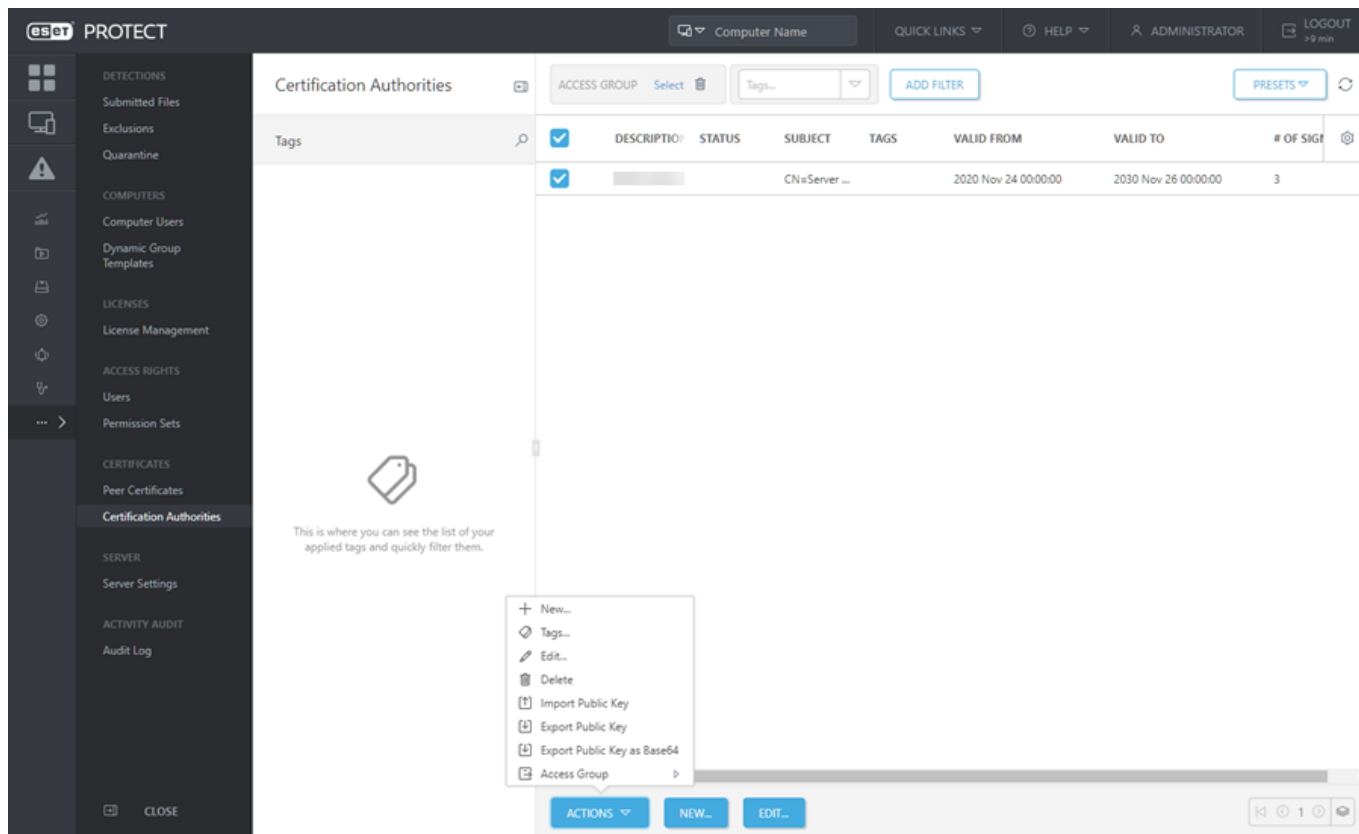
認証機関を管理するには、リストの認証機関の横にある**チェックボックス**を選択し、コンテキストメニュー(認証機関をクリック)またはページの下**[アクション]**ボタンを使用します。使用可能なオプションは、[公開鍵のインポート](#)と[公開鍵のエクスポート](#)または認証局の**編集**です。

公開鍵のエクスポート

認証局をエクスポートするには、[詳細]>認証局をクリックします。

i 証明書をエクスポートするには、証明書の使用権限が必要です。詳細については、[アクセス権の一覧](#)を参照してください。

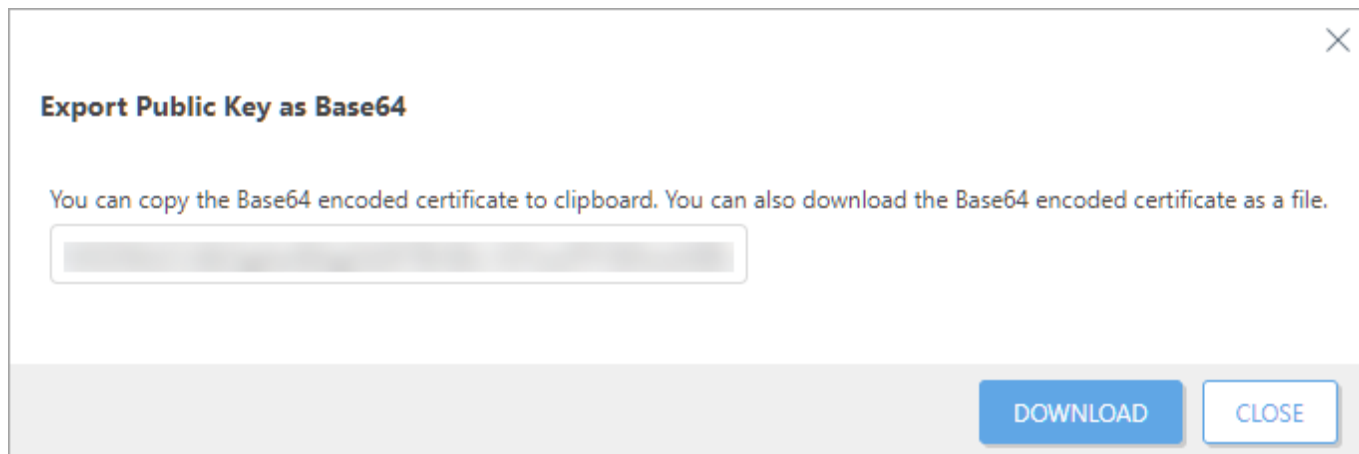
1. リストから使用する認証機関を選択し、横のチェックボックスをオンにします。



2. エクスポートオプションのいずれかを選択します。

a. **アクション** > **公開鍵のエクスポート**を選択します。[公開鍵を別のESET PROTECTインストール\(サーバー間の移行\)](#)にインポートする場合は、このオプションを選択します。公開鍵の名前を入力し、[保存]をクリックします。公開鍵は.derファイルとしてエクスポートされます。

b. **アクション** > **Base64として公開鍵のエクスポート**を選択します。Base64でエンコードされた証明書文字列をコピーするか、**ダウンロード**をクリックして、エンコードされたBase64証明書をファイルとしてダウンロードできます。



既定のESET PROTECT認証機関を削除し、新しいものを作成しても、動作しません。CAを交換するには、新しいCAで署名されたピア証明書を作成および配布する必要があります。また、[サーバー設定](#)でサーバー証明書を変更しESET PROTECTサーバーサービスを再起動する必要があります。

公開鍵のインポート

サードパーティの認証局をインポートするには、[\[詳細\]> 認証局](#)をクリックします。

1. [\[アクション\]](#) ボタンをクリックし、[\[公開鍵のインポート\]](#) を選択します。
2. **アップロードするファイルを選択:** [\[参照\]](#) をクリックして、インポートする設定ファイルがある場所に移動します。インポートできるのは `.der` ファイルのみです。
3. 証明書の **説明** を入力し、[\[インポート\]](#) をクリックします。認証機関が正常にインポートされました。

サーバーの設定

このセクションではESET PROTECTサーバー自体の特定の設定を構成することができます。これらの設定はポリシーに似ていますがESET PROTECTサーバーで直接適用されます。

接続


サーバーポート（再起動が必要） - これはESET PROTECTサーバーとエージェント間の接続ポートです。このオプションを変更するには、変更が有効になる前に、ESET PROTECTサーバーサービスを再起動する必要があります。ポートを変更すると、ファイアウォール設定の変更が必要になる場合があります。

Webコンソールポート（再起動が必要です） - ESET PROTECT WebコンソールおよびESET PROTECTサーバー間の接続用のポートです。ポートを変更すると、ファイアウォール設定の変更が必要になる場合があります。

高度なセキュリティ（再起動が必要） - この設定ではESET PROTECTコンポーネントのネットワーク通信の[高度なセキュリティ](#)が有効になります。

証明書（再起動が必要） - ここでESET PROTECTサーバー証明書を管理することができます。[証明書の変更](#)をクリックし、ESET PROTECTサーバーで使用するESET PROTECTサーバー証明書を選択します。詳細につ

いては、「[ピア証明書](#)」を参照してください。

 これらの変更にはESET PROTECT Serverサービスの再起動が必要です。手順については、[ナレッジ記事](#)を参照してください

更新

アップデート間隔 - アップデートを受信する間隔。定期的な間隔を選択して、設定を構成するか、または[CRON式を使用することができます](#)。

アップデートサーバ - ESET PROTECTサーバがESET製品バージョンおよびESET PROTECTコンポーネントのアップデートを受信するアップデートサーバ。ミラー([ミラーツール](#))からESET PROTECT 9.0をアップデートするにはHTTPサーバのルートの場所に応じて)era6アップデートフォルダーの完全なアドレスを設定します。例:

http://your_server_address/mirror/eset_upd/era6

アップデートの種類 - 受信するESET PROTECT サーバモジュールアップデートの種類を選択します。ヘルプ>[バージョン情報](#)で、インストールされたESET PROTECTサーバモジュールの現在のバージョンを確認できます。

通常アップデート	ESET PROTECTサーバモジュールアップデートは、最小のネットワークトラフィックでESETサーバから自動的にダウンロードされます。既定の設定。
テストモード	これらのアップデートは内部テストが行われ、まもなく公開されますESET PROTECTサーバモジュールの最新のアップデートにアクセスして、リリース前アップデートを有効にする利点があります。リリース前アップデートは、一部の場合に、ESETPROTECTサーバの問題を解決できます。ただし、リリース前アップデートは常に十分安定していない可能性があり、最大限の可用性と安定性が要求される本番サーバでは使用しないでください。テストモードは、 アップデートサーバパラメーター でAUTOSELECTが設定されている場合にのみ使用できます。

詳細設定

HTTPプロキシ - プロキシサーバを使用し、ネットワーク上のクライアントのインターネットトラフィックを容易にできます。オールインワンインストーラーを使用してESET PROTECT をインストールする場合、既定ではHTTPプロキシが有効ですHTTPプロキシ設定は、Secure Authenticationサーバ([2FA](#))との通信には適用されません。

ウェイクアップコール - ESET PROTECTサーバは、[EPNS](#)経由でクライアントコンピューターでESET Managementエージェントとの即時複製を実行します。これはESET ManagementエージェントがESET PROTECTサーバに接続するときに、定期間隔を待機しない場合に便利です。たとえば、クライアントでただちに[タスク](#)を実行する場合や、[ポリシー](#)をただちに適用する場合に便利です。

Wake On Lan - 1つ以上のIPアドレスにWake on LANコールを送信する場合は、マルチキャストアドレスを設定します。

SMTPサーバ - [SMTPサーバ](#)を使用してESET PROTECTサーバに電子メールメッセージを送信させることができます(メール通知またはレポートなど)SMTPサーバの詳細を指定します。

Active Directory - AD設定をあらかじめ設定できますESET PROTECTは、Active Directory同期タスクで、既定で資格情報を使用します([ユーザー同期](#)[静的グループ同期](#))。関連するフィールドがタスク構成で空白のときにはESET PROTECTは設定済みの資格情報を使用します。読み取り専用のADユーザーを使用し

まずESET PROTECTはAD構造を変更しません。


Linux (または仮想アプライアンス)でESET PROTECTサーバーを実行している場合は、*Kerberos*設定ファイルを正しく設定する必要があります。複数のドメインと同期するように、*Kerberos*を設定できます。

ドメインに接続されたWindowsコンピューターでESET PROTECTサーバーを実行している場合は、**ホストフィールド**のみが必要です。ドメインが信頼を確立している場合は、その他のドメイン間での同期が可能です。

- **ホスト:** ドメインコントローラのサーバー名またはIPアドレスを入力します。
- **ユーザー名:** 次の形式でドメインコントローラーのユーザー名を入力します。

ODOMAIN\username (Windowsで実行中のESET PROTECT Server)

ouusername@FULL.DOMAIN.NAMEまたはusername (Linuxで実行中のESET PROTECT Server)

 ドメイン名は必ず大文字で入力してください。クエリを正常にActive Directoryサーバーで認証するには、この形式が必要です。


- **パスワード** - ドメインコントローラにログインするためのパスワードを入力します。
- **ルートコンテナー-ADコンテナーの完全識別子**を入力します。例: CN=John,CN=Users,DC=Corp。設定済みの**識別名**として機能します。サーバータスクからこの値をコピーして貼り付け、正しい値を確認することをお勧めします(選択したら、**識別名**フィールドから値をコピーします)。

既定ではWindowsのESET PROTECTサーバー9.0は、すべてのActive Directory (AD)接続で、暗号化されたLDAPS (SSLを使用したLDAP)プロトコルを使用します。 [ESET PROTECT仮想アプライアンスでLDAPSを設定](#)することもできます。

Windowsコンピューターでバージョン7.0-7.1からESET PROTECT 9.0にアップグレードし、Active Directory同期を使用していた場合は、ESET PROTECT 9.0で同期タスクが失敗します。LDAPSでAD接続を正常に実行するために、次の項目を設定します。

1. ドメインコントローラーには、コンピューター証明書をインストールしている必要があります。ドメインコントローラーの証明書を発行するには、次の手順を実行します。

a)サーバーマネージャーを開き、**管理>役割と機能の追加**をクリックして、**Active Directory証明書サービス>認証局**をインストールします。新しい認証局が**信頼できるルート認証局**に作成されます。

 b)スタートからcertmgr.mscと入力し、**Enter**を押して、**証明書Microsoft管理コンソールスナップイン**を実行 > **証明書 - ローカルコンピューター>個人**に移動して、空のウィンドウを右クリックし、**すべてのタスク>新しい証明書の要求>ドメインコントローラーの登録ロール**をクリックします。

c)FQDNのドメインコントローラーが発行された証明書に含まれていることを確認します。

d)ESMCサーバーで、生成したCAを証明書ストアにインポート(certmgr.mscツールを使用)し、**信頼できるCAフォルダー**にインポートします。

2. ADサーバーに接続設定を入力するときには、**サーバー**または**ホストフィールド**に、ドメインコントローラーのFQDNを(ドメインコントローラー証明書の記載のとおり)に入力しますLDAPSではIPアドレスは十分な情報ではありません。

LDAPプロトコルへのフォールバックを有効にする場合は、[静的グループ同期](#)または[ユーザー同期](#)タスクで、**Active Directoryの代わりにLDAPを使用する**の横のチェックボックスを選択します。

Syslogサーバーを使用してESET PROTECTは通知とイベントメッセージを[Syslogサーバー](#)に送信できます。また、クライアントコンピューターのESET製品から[ログをエクスポート](#)し、Syslogサーバーに送信できます。

静的グループ - [検出されたコンピューターと静的グループのコンピューターとの自動組み合わせ](#)を有効にします。組み合わせはESET Managementエージェントで報告されたホスト名で動作し、信頼できない場合は無効にしてください。組み合わせに失敗すると、コンピューターはLOST+FOUNDグループに入ります。

リポジトリ - すべてのインストールファイルが格納されているリポジトリの場所です。

- 既定のESETリポジトリは**AUTOSELECT**です (<http://repository.eset.com/v1>を参照します) ESET PROTECTサーバーの地理的ロケーション(IPアドレス)に基づいて、最適な接続を使用して、リポジトリサーバーを自動的に決定します(CDN - [Content Delivery Network](#)を使用)。このため、リポジトリ設定を変更する必要はありません。
- 任意で、ESETサーバーのみを使用するリポジトリを設定できます:
<http://repositorynocdn.eset.com/v1>
- ESETリポジトリにアクセスするためにIPアドレスを使用しないでください
- [オフラインリポジトリ](#)を作成および使用できます。

製品改善プログラムに参加 - 顧客経験の向上のため、匿名のクラッシュレポート統計をESETに送信することを有効または無効にします。

ロギング > 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。

ESET PROTECTサーバーの最新のログファイルは次の場所にあります。

- Windows: `C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs`
- Linux: `/var/log/eset/RemoteAdministrator/Server/`

ここで[Syslogへのログのエクスポート](#)を設定できます。


データベースのクリーンアップ - データベースの過負荷を防止するために、このオプションを使用して定期的にログをクリーンアップすることができます。データベースクリーンアップには次のタイプのログを削除します SysInspector ログ、診断ログ、収集されなくなったログ (削除されたデバイスからのログ、削除されたレポートテンプレートからのログ)。データベースクリーンアップ処理は、既定では夜間に毎日実行されます。この設定の変更は次のクリーンアップの後に有効になります。次のタイプのログにはそれぞれクリーンアップ期間を設定できます。

ログタイプ	ログタイプの例	
インシデントログ	<div>高重要度の検出ログ。</div> <div>ログのリストを参照してください。</div> <div><div>インシデントログ</div><div>ActiveThreats</div><div>BlockedFiles</div><div>EESEvent_</div><div>EnterpriseInspectorAlert</div><div>Firewall_</div><div>FirewallAgregated</div><div>Functionality_Computer</div><div>Functionality_ProblemsDetails</div><div>Functionality_Product</div><div>Functionality_Products</div><div>Hips_</div><div>Quarantine_UploadedFile</div><div>Scan</div><div>Spam_</div><div>SubmittedFiles</div><div>SysInspector_SysInspector</div><div>Threat</div><div>ThreatsFlag</div><div>ThreatsMute</div><div>ThreatsMute2</div><div>WebControl_Link</div></div>	
管理ログ	<div>サービスの品質データ。</div> <div>ログのリストを参照してください。</div>	管理ログ
監査ログ	<div>監査ログレポート。</div> <div>ログのリストを参照してください。</div>	監査ログ
監視ログ	<div>低重要度のWebコンソールログ、デバイスコントロールログ、HIPSログ。</div> <div>ログのリストを参照してください。</div>	監視ログ

診断ログは毎日クリーンアップされます。ユーザーは駆除間隔を変更できません。[ログのリストを参照してください。](#)

診断ログ
Diagnostics_DeviceControl_Device
Diagnostics_DiagnosticZip
Diagnostics_Firewall
Diagnostics_Hips
Diagnostics_Spam

診断ログ
Diagnostics_WebControl_Link
Performance_DiskIO
Performance_Machine
Performance_Memory
Performance_NetworkIO
Performance_Processor
Performance_User

 データベースクリーンアップ中に、駆除されたインシデントログに対応する[検出](#)の項目も(検出ステータスには関係なく)削除されます。既定では、インシデントログ(および検出)のクリーンアップ期間は6か月に設定されています。この期間は、[サーバー設定](#)で変更できます。




■ カスタマイズ

UIのカスタマイズ - カスタムロゴをESET PROTECT Webコンソールと、[サーバータスク](#)で生成されたレポートに追加できます。

- なし - 基本デザイン、カスタムロゴなし
- 共同ブランディング - Webコンソールとレポートのフッターにカスタムロゴを追加できます。
- ホワイトラベリング(MSPライセンスが必要) - Webコンソールとレポートのフッターまたはヘッダーにカスタムロゴを追加できます。


会社ロゴ

- 暗い背景ロゴ(Webコンソールヘッダー) - このロゴはWebコンソールの左上端に表示されます。
- 明るい背景ロゴ - このロゴは、ヘッダー(MSPライセンス所有者)または[サーバータスク](#)で生成されたレポートのフッター(コブランディング設定)に表示されます。

 をクリックしてロゴを選択します。 をクリックして現在のロゴをダウンロードします。 をクリックして現在のロゴを削除します。

レポートと通知

- レポートのカスタマイズ - このオプションを有効にすると、レポートで選択したロゴを使用したり、フッターテキストを追加したりすることができます。
- レポートフッターテキスト - PDF形式で生成された[レポート](#)の右下端に追加されるテキストを入力します。

 カスタムロゴは、カスタムフッターテキストとともに使用できません。ロゴはフッターテキストと同じ位置です。ロゴとフッターが同時に使用される場合、ロゴのみが表示されます。ホワイトラベリング設定を使用するときには、カスタムロゴはレポートの左上端に表示されます。より小さいpowered by ESETロゴがフッターテキストの代わりに右下端に表示されます。

高度なセキュリティ

高度なセキュリティにはESET PROTECTコンポーネント間の安全なネットワーク通信があります。

- [証明書](#)と認証局はSHA-256 (SHA-1ではない)を使用します。
- ESET PROTECTサーバーは、TLS 1.2をエージェントとの通信で使用します。
- 高度なセキュリティはSyslogおよびSMTP通信でTLS 1.2の使用を強制します。
- MDMユーザーESET PROTECTサーバーは、TLS 1.2をMDMサーバーとの通信で使用します。MDMサーバーとモバイルデバイス間の通信には影響しません。

高度なセキュリティは、すべてのサポートされているオペレーティングシステムで動作します。

- [Windows](#)
- [Linux](#) - 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。最新のOpenSSLバージョン(1.1.1)を使用することをお勧めします。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`
- [macOS](#)



ESET PROTECT 8.1以降のすべての新規インストールでは、既定で高度なセキュリティが有効です。高度なセキュリティが無効な状態でESMCまたはESET PROTECT 8.0を使用し、ESET PROTECT 8.1以降にアップグレードする場合、高度なセキュリティは無効のままです。次の手順に従い、有効にすることをお勧めします。

ネットワークで高度なセキュリティを有効にして適用する方法



- 高度なセキュリティを有効にするときにはESET PROTECTサーバーを再起動し、この機能の使用を開始する必要があります。
- 高度なセキュリティは既存の認証局(CA)と証明書に影響しません。高度なセキュリティには、高度なセキュリティが有効になった後に作成された新しいCAと証明書のみが含まれます。現在のESET PROTECTインフラストラクチャで高度なセキュリティを適用するには、既存の証明書を[置換](#)する必要があります。
- [高度なセキュリティ](#)を使用する場合MSPアカウントをインポートする前に、設定することをお勧めします。

1. 詳細 > サーバー設定 > 接続に移動し、高度なセキュリティの横のスライダーをクリックします(再起動が必要)。
2. 保存をクリックして設定を適用します。
3. コンソールを閉じ、ESET PROTECT Serverサービスを再起動します。
4. サービスの開始後に数分待機し、Webコンソールにログインします。
5. すべてのコンピューターが接続し、他の問題がないことを確認します。
6. [詳細] > [認証] > [新規]に移動し、[新しいCAを作成](#)します。新しい証明書は、次のエージェントとサーバーの通信中に、すべてのクライアントに自動的に送信されます。

7.この新しいCAで署名された[新しいピア証明書を作成](#)します。エージェントとサーバーの証明書を作成します(ウィザードの**製品**ドロップダウンメニューで選択できます)。

8.現在のESET PROTECTサーバー証明書を新しいものと[交換](#)します。

9.新しいESET Managementエージェントポリシーを[作成](#)し、新しいエージェント証明書を使用するエージェントを設定します。

a.**接続**セクションで、**証明書>証明書リストを開く**をクリックし、新しいピア証明書を選択します。

b.高度なセキュリティを使用するコンピューターにポリシーを割り当てます。

c.**[完了]**をクリックします。

10. すべてのデバイスが新しい証明書で接続しているときには、[古いCAを削除](#)し、[古い証明書を取り消す](#)ことができます。



接続されたクライアントコンピューターの一部(すべてではない)でのみ高度なセキュリティを使用した場合は、古いCAを削除したり、古い証明書を取り消したりしないでください。

高度なセキュリティを (Mobile Device Management) MDMコンポーネントに適用するには、新しいCAによって署名された新しいMDMとプロキシ証明書を作成し、次のようにポリシー経由でMDMサーバーに割り当てます。

- ESET Mobile Device Connectorポリシー > **一般**>HTTPS証明書ををクリックします。新しいMDM証明書をインポートします。
- ESETモバイルデバイスコネクタポリシー > **エージェント**>**証明書** = プロキシ証明書。

SMTPサーバー

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>サーバー設定>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、ポップアップ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。

Gmailアカウントがある場合は、SMTPサーバーとしてGmailを使用できます。以下の設定を使用します。

設定	値
SMTPサーバーを使用	真
ホスト	smtp.gmail.com
ポート	465 (TLS) または 587 (STARTTLS)
ユーザー名	Gmailアドレス
パスワード	Gmailパスワード
接続セキュリティタイプ	TLS または STARTTLS
認証タイプ	Automatic
送信元アドレス	Gmailアドレス

電子メールの送信に失敗した場合は、Gmailアカウントで[安全性の低いアプリを許可](#)するかGmailアカウントの[ロックを解除](#)する必要があります。

検出されたコンピューターを自動的に組み合わせる

ESET PROTECTで同じコンピューターの複数のインスタンスが発生した場合(ESET Managementエージェントが既に管理されているクライアントコンピューターに再インストールされた場合など)、**検出されたコンピューターを自動的に組み合わせる**機能によって、これらを実行し、これらのインスタンスを1つに組み合わせます。これにより、手動検証と検出されたコンピューターのソートの必要がなくなります。


組み合わせはESET Managementエージェントで報告されたホスト名で動作します。信頼できない場合は、**検出されたコンピューターを自動的に組み合わせる**機能を無効にすることをお勧めします。組み合わせに失敗すると、コンピューターは**LOST+FOUNDグループ**に入りますESET Managementエージェントが既に管理されているコンピューターに再インストールされるたびに、自動的に組み合わせられるため、介入なしでESET PROTECTに正しく配置されます。また、新しいESET Managementエージェントはそのポリシーとタスクをただちに取得します。

- **無効にすると**、**LOST+FOUNDグループ**のコンピューターはESET PROTECTツリーのどこかにある最初に検出された管理対象外のコンピューター(プレースホルダー、円アイコン)と組み合わせられます。同じ名前のプレースホルダーがない場合は、コンピューターは**LOST+FOUND**に配置されます。
- **有効にする(既定)**と、**LOST+FOUND**のコンピューターはESET PROTECTツリーのどこかにある最初に検出された管理対象外のコンピューター(プレースホルダー、円アイコン)と組み合わせられます。同じ名前のプレースホルダーがない場合、コンピューターはESET PROTECTツリーのどこかにある最初に検出された管理対象のコンピューターと組み合わせられます(アラートまたは確認アイコン)。この組み合わせも失敗した場合、コンピューターは**LOST+FOUND**に配置されます。


i 自動組み合わせが不要だと考えられる場合は、無効にしてください。常に検証し、コンピューターを手動でソートできます。

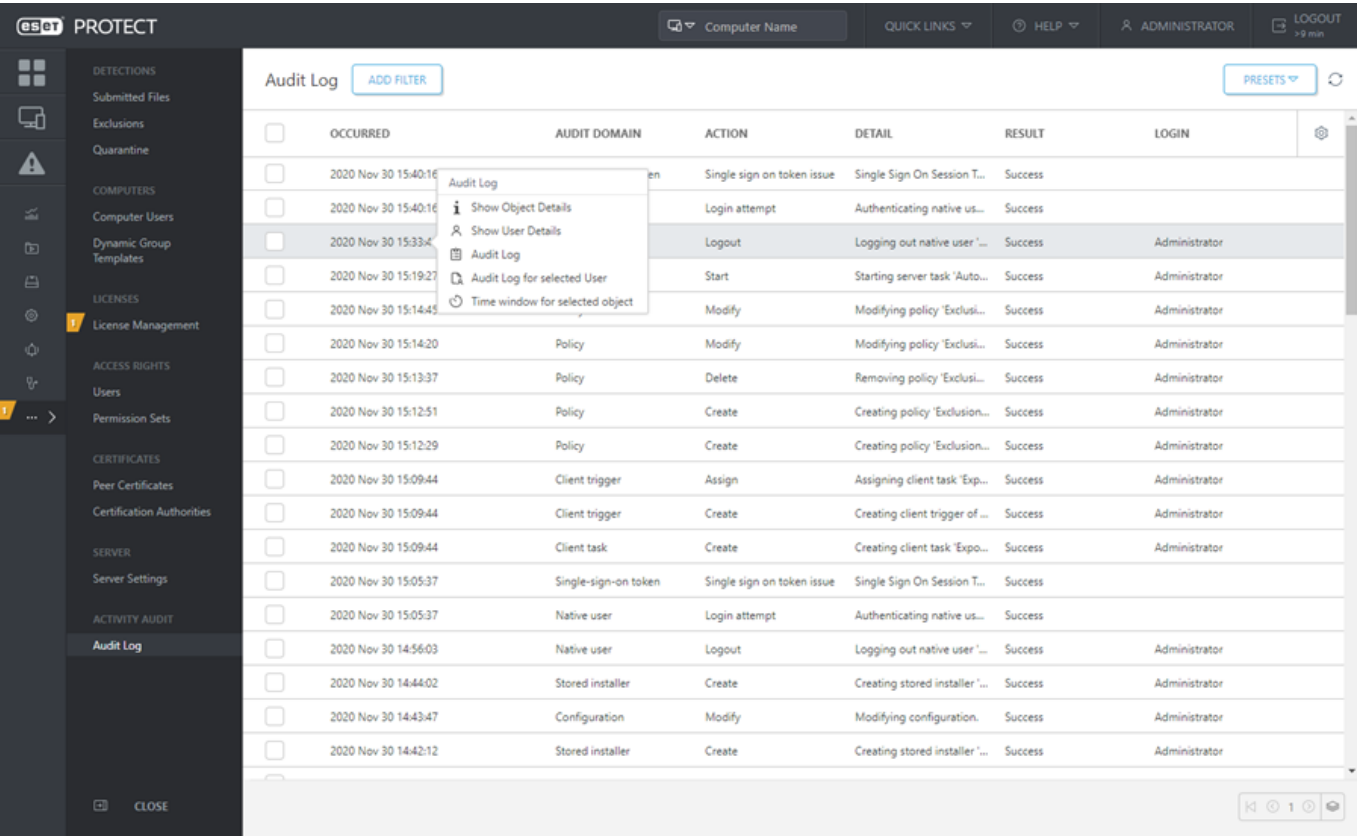
監査ログ

ユーザーがESET PROTECT Web コンソールでアクションを実行すると、アクションがログに記録されます。監査ログは、ESET PROTECT Web コンソールオブジェクト(コンピューター、ポリシー、検出など)が作成または変更された場合に作成されます。






監査ログは、ESET PROTECTで提供されている新しい画面です。監査ログには[監査ログレポート](#)と同じ情報が含まれますが、表示されたデータを簡単にフィルタリングできます。Web コンソールオブジェクトをクリックして、 **監査ログ**を選択すると、さまざまなWeb コンソールのフィルタリングされた監査ログを直接表示することもできます。

監査ログを使用すると、管理者は、特にWeb コンソールのユーザーが多い場合に、ESET PROTECT Web コンソールで実行されたアクティビティを検査できます。

 監査ログを表示するにはWeb コンソールユーザーに[監査ログ機能](#)を含む権限セットが必要です。



監査ログの行をクリックすると、次のアクションを実行できます。

 オブジェクトの詳細を表示	監査されたオブジェクトの詳細を表示します。
 ユーザー詳細を表示	オブジェクトでアクションを実行したユーザーの詳細を表示します。
 監査ログ	選択したオブジェクトの監査ログを表示します。
 選択したユーザーの監査ログ	選択したユーザーの監査ログを表示します。
 選択したオブジェクトの時間枠	選択したオブジェクトの監査ログを発生時刻の有効なフィルターで表示します。

フィルターの追加をクリックし、さまざまな条件でテーブルビューをフィルタリングします。

- **<** = 発生-アクションが発生する前の日時を設定します。
- **>** = 発生-アクションが発生した後の日時を設定します。
- **アクション** - 実行されたアクションを選択します。
- **監査ドメイン** - 変更されたWebコンソールオブジェクトを選択します。
- **監査ユーザー** - アクションを実行したWebコンソールユーザーを選択します。
- **結果** - アクション結果を選択します。

ログをSyslogにエクスポートする

ESET PROTECTは特定のログ/イベントをエクスポートし、[Syslogサーバー](#)に送信できます。次のログカテゴリからのイベントは、Syslogサーバーにエクスポートされます。検出、ファイアウォール、HIPS、監査、Enterprise Inspector イベントは、ESET製品(ESET Endpoint securityなど)を実行する管理対象のクライアントコンピュータで生成されます。これらのイベントは、Syslogサーバーからのイベントのインポート機能を備えた任意のESET Endpoint securityソリューションで処理できます。イベントはESET PROTECTによってSyslogサーバーに書き込まれます。

1. [Syslogサーバー](#)を有効にするには、**詳細 > サーバー設定 > 詳細設定 > Syslogサーバー > Syslogサーバーを使用**をクリックします。
2. エクスポートを有効にするには、**詳細 > サーバー設定 > 詳細設定 > ロギング > ログをSyslogサーバーにエクスポート**をクリックします。
3. イベントメッセージに次の形式のいずれかを選択します。

a. [JSON \(JavaScript Object Notation\)](#)

b. [LEEF](#) (Log Event Extended Format)- IBMアプリケーションQRadarで使用される形式。

Syslogに送信されたイベントログをフィルタリングするには、定義されたフィルターで[ログカテゴリ通知](#)を作成します。

Syslogサーバー

ネットワークでSyslogサーバーが実行されている場合は、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。また、[ログをSyslogにエクスポート](#)を有効にし、たとえばESET Endpoint Securityを実行するクライアントコンピュータから特定のイベント(検出イベント、ファイアウォール集約イベント、HIPS集約イベントなど)を受信できます。

Syslogサーバーを有効にするには

1. **[詳細] > [サーバー設定] > [詳細設定]**に移動します > **Syslogサーバー**に移動し、**Syslogサーバーを使用する**の横のスライダーバーをクリックします。
2. 次の必須設定を指定します。
 - a. **ホスト** (Syslogメッセージの宛先のIPアドレスまたはホスト名)

b.ポート番号(既定値は514)。

c.ログの形式:BSD (仕様)⇄Syslog (仕様)

d.Syslog (UDP⇄TCP⇄TLS) へのメッセージ送信用のトランスポートプロトコル

変更した後、[保存]をクリックします。

i

標準アプリケーションログファイルに常に書き込まれます⇄Syslogは、通知やさまざまなクライアントコンピューターのイベントなどの特定の非同期イベントをエクスポートするための媒体としてのみ機能します。

LEEF形式にエクスポートされたイベント

Syslogに送信されたイベントログをフィルタリングするには、定義されたフィルターで[ログカテゴリ通知](#)を作成します。

LEEF形式は IBM® Security QRadar®のカスタムイベント形式です。イベントには標準およびカスタム属性があります：

- ESET PROTECTは[公式IBMドキュメント](#)で説明された標準属性の一部を使用します。
- [カスタム属性](#)はJSON形式と同じです。

イベントカテゴリ：

- 検出
- ファイアウォール

- フィルタリングされたWebサイト
- HIPS
- 監査
- Enterprise Inspectorアラート
- ブロックされたファイル

i Log Event Extended Format (LEEF)の詳細については、[公式IBM Webサイト](#)を参照してください。

JSON形式にエクスポートされたイベント

JSONはデータ交換用の軽量形式です。名前/値のペアのコレクションと値の順序付けされたリストで作成されます。

エクスポートされたイベント

このセクションでは、すべてのエクスポートされたイベントの属性の形式と意味について説明します。イベントメッセージはJSONオブジェクトの形式で、必須キーと任意のキーがあります。各エクスポートされたイベントには次のキーがあります。

event_type	string		エクスポートされたイベントのタイプ: <ul style="list-style-type: none"> • Threat Event • FirewallAggregated Event • HipsAggregated Event • Audit Event • FilteredWebsites Event • EnterpriseInspectorAlert Event • BlockedFiles Event
ipv4	string	任意	イベントを生成するコンピューターのIPv4アドレス。
ipv6	string	任意	イベントを生成するコンピューターのIPv6アドレス。
source_uuid	string		イベントを生成するコンピューターのUUID ^②
occurred	string		イベントの発生時刻(UTC) ^② 形式は%d-%b-%Y %H:%M:%Sです。
severity	string		イベントの重大度。値(重要度の低い順):情報 通知 警告 エラー 重大

i 次の一覧のすべての重要度レベルのすべてのイベントタイプがSyslogサーバーに報告されます^②
Syslogに送信されたイベントログをフィルタリングするには、定義されたフィルターで[ログカテゴリ通知](#)を作成します。

event_typeに基づくカスタムキー:

Threat_Event

管理されたエンドポイントによって生成されたすべての検出イベントがSyslogに転送されます。検出イベント固有のキー:

threat_type	string	任意	検出のタイプ
threat_name	string	任意	検出名
threat_flags	string	任意	検出関連フラグ
scanner_id	string	任意	スキャナID
scan_id	string	任意	検査ID
engine_version	string	任意	検査エンジンのバージョン
object_type	string	任意	このイベントに関連するオブジェクトのタイプ
object_uri	string	任意	オブジェクトURI
action_taken	string	任意	エンドポイントによって実行されたアクション
action_error	string	任意	アクションが失敗した場合のエラーメッセージ
threat_handled	bool	任意	検出が処理されたかどうかを示します
need_restart	bool	任意	再起動が必要かどうか
username	string	任意	イベントに関連付けられたユーザーアカウントの名前
processname	string	任意	イベントに関連付けられたプロセスの名前
circumstances	string	任意	イベントの原因の簡単な説明
hash	string	任意	(検出)データストリームのSHA1ハッシュ。
firstseen	string	任意	そのコンピューターで初めて検出された日時。ESET PROTECTは、ログ出力形式(firstseenまたはJSON)に応じて、LEEF属性のさまざまな日時形式を使用します。 <ul style="list-style-type: none"> JSON 形式: "%d-%b-%Y %H:%M:%S" LEEF 形式: "%b %d %Y %H:%M:%S"

[Threat Eventログの例:](#)

```
Jun 21 11: 46: 40 030 - MG ERAServer[5648]: {
  "event_type": "Threat_Event",
  "ipv4": "192.168.30.30",
  "hostname": "030-mg",
  "source_uuid": "1361a9f6-1d45-4561-b33a-b5d6c62c71e0",
  "occured": "21-Jun-2021 09:46:15",
  "severity": "Warning",
  "threat_type": "Virus",
  "threat_name": "XF/Gydhex.A",
  "scanner_id": "Real-time file system protection",
  "scan_id": "virlog.dat",
  "engine_version": "23497 (20210621)",
  "object_type": "file",
```

```

"object_uri": "file:///C:/Users/Administrator/Downloads/xls/YICT080714.xls",
"action_taken": "Deleted",
"threat_handled": true,
"need_restart": false,
"username": "030-MG\\Administrator",
"processname": "C:\\Program Files\\WinRAR\\WinRAR.exe",
"circumstances": "Event occurred on a newly created file.",
"firstseen": "21-Jun-2021 09:46:14",
"hash": "5B97884A45C6C05F93B22C4059F3D9189E88E8B7"
}

```

FirewallAggregated_Event

ESET Firewallによって生成されたイベントログは、管理しているESET Managementエージェントによって集約され、ESET Managementエージェント/ESET PROTECTサーバーレプリケーション中に帯域幅を浪費することがなくなります。ファイアウォールイベント固有のキー:

event	string	任意	イベント名
source_address	string	任意	イベントソースのアドレス
source_address_type	string	任意	イベントソースのアドレスのタイプ
source_port	number	任意	イベントソースのポート
target_address	string	任意	イベント宛先のアドレス
target_address_type	string	任意	イベント宛先のアドレスのタイプ
target_port	number	任意	イベント宛先のポート
protocol	string	任意	プロトコル
account	string	任意	イベントに関連付けられたユーザーアカウントの名前
process_name	string	任意	イベントに関連付けられたプロセスの名前
rule_name	string	任意	ルール名
rule_id	string	任意	ルールID
inbound	bool	任意	接続が受信かどうか
threat_name	string	任意	検出名
aggregate_count	number	任意	ESET PROTECTサーバーと管理するESET Managementエージェント間で、2つの連続するレプリケーションの間に、エンドポイントによって生成されたまったく同じメッセージの数
action	string	任意	実行されたアクション
handled	string	任意	検出が処理されたかどうかを示します

 [FirewallAggregated_Eventログの例:](#)

```
Jun 21 3: 54: 07 030 - MG ERAServer[5648]: {
```

```

"event_type": "FirewallAggregated_Event",
"ipv4": "192.168.30.30",
"hostname": "w16test",
"source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
"occured": "21-Jun-2021 13:10:04",
"severity": "Warning",
"event": "Security vulnerability exploitation attempt",
"source_address": "127.0.0.1",
"source_address_type": "IPv4",
"source_port": 54568,
"target_address": "127.0.0.1",
"target_address_type": "IPv4",
"target_port": 80,
"protocol": "TCP",
"account": "NT AUTHORITY\\NETWORK SERVICE",
"process_name": "C:\\Program Files\\Apache Software Foundation\\apache-
tomcat-9.0.41\\bin\\tomcat9.exe",
"inbound": true,
"threat_name": "CVE-2017-5638.Struts2",
"aggregate_count": 1
}

```

HIPSAggregated_Event

HIPSのイベントは、Syslogメッセージとして送信される前に、**重要度**でフィルタリングされます。**重要度**レベルが**Error**、**Critical**、**Fatal**のイベントのみがSyslogに送信されます。HIPS固有の属性は次のとおりです。

application	string	任意	アプリケーション名
operation	string	任意	処理
target	string	任意	対象
action	string	任意	実行されたアクション
action_taken	string	任意	エンドポイントによって実行されたアクション
rule_name	string	任意	ルール名
rule_id	string	任意	ルールID

application	string	任意	アプリケーション名
aggregate_count	number	任意	ESET PROTECTサーバーと管理するESET Managementエージェント間で、2つの連続するレプリケーションの間に、エンドポイントによって生成されたまったく同じメッセージの数
handled	string	任意	検出が処理されたかどうかを示します

[HipsAggregated Eventログの例:](#)

```
Jun 21 13: 54: 07 030 - MG ERAServer[5648]: {
  "event_type": "HipsAggregated_Event",
  "ipv4": "192.168.30.181",
  "hostname": "test-w10-uefi",
  "source_uuid": "5dbe31ae-4ca7-4e8c-972f-15c197d12474",
  "occured": "21-Jun-2021 11:53:21",
  "severity": "Critical",
  "application": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\java.exe",
  "operation": "Attempt to run a suspicious object",
  "target": "C:\\Users\\Administrator\\Desktop\\es_pack_to_test\\test\\trojan.exe",
  ,
  "action": "blocked",
  "handled": true,
  "rule_id": "Suspicious attempt to launch an application",
  "aggregate_count": 2
}
```

Audit_Event

ESET PROTECTはサーバーの内部監査ログメッセージをSyslogに転送します。固有の属性は次のとおりです。

domain	string	任意	監査ログドメイン
action	string	任意	実行中のアクション
target	string	任意	ターゲットアクションが動作しています
detail	string	任意	アクションの詳細説明
user	string	任意	関係するセキュリティユーザー
result	string	任意	アクションの結果

[Audit Eventログの例:](#)

```
Jun 21 11: 42: 00 030 - MG ERAServer[5648]: {  
  "event_type": "Audit_Event",  
  "ipv4": "192.168.30.30",  
  "hostname": "030-MG",  
  "source_uuid": "72cdf05f-f9c8-49cc-863d-c6b3059a9e8e",  
  "occured": "21-Jun-2021 09:42:00",  
  "severity": "Information",  
  "domain": "Native user",  
  "action": "Login attempt",  
  "target": "Administrator",  
  "detail": "Authenticating native user 'Administrator'.",  
  "user": "",  
  "result": "Success"  
}
```

FilteredWebsites_Event

ESET PROTECTはフィルタリングされたWebサイト(**Web 保護**検出)をSyslogに転送します。固有の属性は次のとおりです。

hostname	string	任意	イベントのあるコンピューターのホスト名
processname	string	任意	イベントに関連付けられたプロセスの名前
username	string	任意	イベントに関連付けられたユーザーアカウントの名前
hash	string	任意	フィルタリングされたオブジェクトのSHA1ハッシュ
event	string	任意	イベントタイプ
rule_id	string	任意	ルールID
action_taken	string	任意	実行されたアクション
scanner_id	string	任意	スキャナID
object_uri	string	任意	オブジェクトURI
target_address	string	任意	イベント宛先のアドレス
target_address_type	string	任意	イベント宛先のアドレスのタイプ (25769803777 = IPv4; 25769803778 = IPv6)
handled	string	任意	検出が処理されたかどうかを示します

[FilteredWebsites Eventログの例:](#)

```

Jun 21 3: 56: 03 020 - MG ERAServer[5648]: {
  "event_type": "FilteredWebsites_Event",
  "ipv4": "192.168.30.30",
  "hostname": "win-test",
  "source_uuid": "d9477661-8fa4-4144-b8d4-e37b983bcd69",
  "occured": "21-Jun-2021 03:56:20",
  "severity": "Warning",
  "event": "An attempt to connect to URL",
  "target_address": "192.255.255.255",
  "target_address_type": "IPv4",
  "scanner_id": "HTTP filter",
  "action_taken": "blocked",          "object_uri": "https://test.com",
  "hash": "ABCDAA625E6961037B8904E113FD0C232A7D0EDC",
  "username": "WIN-TEST\\Administrator",
  "processname": "C:\\Program Files\\Web browser\\browser.exe",
  "rule_id": v"Blocked by PUA blacklist"
}

```

EnterpriseInspectorAlert_Event

ESET PROTECTはESET Enterprise InspectorアラームをSyslogに転送します。固有の属性は次のとおりです。

processname	string	任意	このアラームを発生させるプロセスの名前
username	string	任意	プロセスの所有者
rulename	string	任意	このアラームをトリガーするルールの名前
count	number	任意	前回のアラーム以降に生成されたこのタイプのアラート数
hash	string	任意	アラームのSHA1ハッシュ
eiconsolelink	string	任意	ESET Enterprise Inspectorコンソールのアラームへのリンク
eialarmid	string	任意	アラームリンクのID部分(^http.*/alarm/([0-9]+)\$)の\$1
computer_severity_score	number	任意	コンピューター重要度スコア
severity_score	number	任意	ルール重要度スコア

 [EnterpriseInspectorAlert_Eventログの例:](#)

```

Jun 16 16:19:00 Win2016Std ERAServer[2772]: {
  "event_type": "EnterpriseInspectorAlert_Event",

```



```

"ipv4": "192.168.30.30",
"hostname": "shdsolec.vddjc",
"source_uuid": "csd77ad2-2453-42f4-80a4-d86dfa9d0543",
"occured": "13-Jun-2021 07:45:00",
"severity": "Warning",
"processname": "ProcessName",
"username": "UserName",
"rulename": "RuleName2",
"count": 158,
"eiconsolelink": "http://eiserver.tmp/linkToConsole",
"computer_severity_score": "1",
"severity_score": "1"
}

```

BlockedFiles_Event

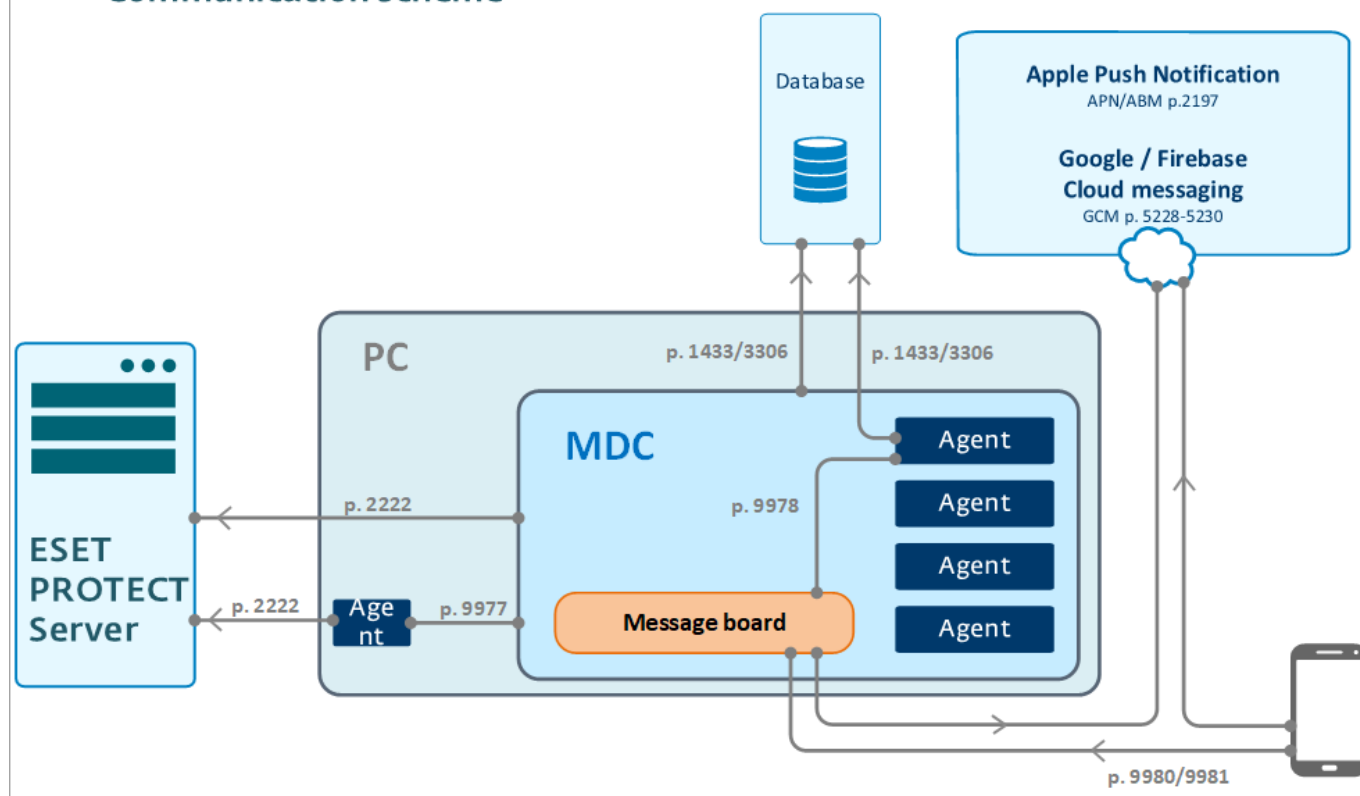
ESET PROTECTはESET Enterprise InspectorブロックされたファイルをSyslogに転送します。固有の属性は次のとおりです。

hostname	string	任意	イベントのあるコンピューターのホスト名
processname	string	任意	イベントに関連付けられたプロセスの名前
username	string	任意	イベントに関連付けられたユーザーアカウントの名前
hash	string	任意	ブロックされたファイルのSHA1ハッシュ
object_uri	string	任意	オブジェクトURI
action	string	任意	実行されたアクション
firstseen	string	任意	そのコンピューターで初めて検出が特定された日時(日時形式) ²
cause	string	任意	
description	string	任意	ブロックされたファイルの説明
handled	string	任意	検出が処理されたかどうかを示します

モバイルデバイス管理

次の図は、ESET PROTECTコンポーネントとモバイルデバイス間の通信を示します。

ESET PROTECT – MDC – Device Communication scheme



[ここをクリックすると、大きい画像を表示します](#)



MDMのセキュリティ推奨事項:MDMホストデバイスにはインターネット接続が必要です。MDMホストデバイスはファイアウォールの後ろにし、MDMに必要なポートのみを開くことをお勧めします。またIDS/IPSを展開し、ネットワークの特異性を監視できます。

Mobile Device Connector (MDC) はESET PROTECTコンポーネントであり、ESET PROTECTによるモバイルデバイス管理を可能にします。またAndroidおよびiOSモバイルデバイスの管理と、モバイルセキュリティの管理を許可します。

MDCは、モバイルデバイスでエージェントが直接実行されないエージェントレスソリューションを提供します(バッテリーとモバイルデバイスのパフォーマンスを節約)。MDCはこれらの仮想エージェントのホストとして機能します。MDCは専用SQLデータベースにモバイルデバイスのデータを保存します。

モバイルデバイスとMDC間の通信を認証するにはHTTPS証明書が必要です。ESET PROTECTサーバーとMDC間の通信を認証するには、プロキシ証明書が使用されます。

Appleデバイスの管理には、いくつかの追加要件があります。ESET PROTECT MDCを使用してiOSデバイスを管理するには、Appleプッシュ通知サービス証明書が必要です。APNサービスによりESET MDCが安全にAppleモバイルデバイスと通信できます。この証明書は、(Appleプッシュ証明書ポータルを使用して)Appleによって直接署名され、ポリシー経由でMDCに配信される必要があります。その後、iOSデバイスをESET PROTECT MDCで登録できます。

一部の国ではApple Business Manager (ABM)が利用可能です。ABMは、企業iOSデバイスを登録するための、新しい強力な方法です。ABMでは、デバイスに直接接続せず、最低限のユーザー操作で自動的にデバイスをMDCに登録できます。ABMはiOS MDMの機能を大幅に拡張し、デバイスセットアップの完全なカス

タマイズが可能です。

モバイルデバイスコネクタの[インストールとセットアップ](#)が完了した後、モバイルデバイスを[登録](#)できます。登録が成功した後、モバイルデバイスはESET PROTECT Webコンソールから管理できます。

MDM設定

ESET PROTECTでモバイルデバイス管理コンポーネントを活用するには、モバイルデバイスを登録および管理するにはMDMのインストール後に次の手順を実行します。

1. モバイルデバイスコネクタ (MDC) を、[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ラー ([Windows](#) または [Linux](#) 用) を使用してインストールします。[仮想アプライアンスとしてMDMを展開](#)することもできます。インストールの前に、前提条件を満たしていることを確認してください。

[オールインワンインストーラー](#)を使用してMDCをインストールする場合は、ESET PROTECT CAが署名したHTTPS証明書がインストール処理中に自動的に生成されます。この証明書はパスワードで保護され (ランダムに生成されたパスワードを使用) ます。この証明書は[詳細 > ピア証明書](#)に表示されません。

i オールインワンインストーラーでESET PROTECTをインストールし、第三者のHTTPS証明書を使用する場合は、まずESET PROTECTをインストールしてから、[ポリシーを使用してHTTPS証明書を変更します](#) ([モバイルデバイスコネクタポリシー] > [一般] > [証明書の変更] > [カスタム証明書])^⑧ MDCコンポーネントのみをインストールしている場合は、次のものを使用できます。

- a) [ESET PROTECT CAが署名した証明書](#) (基本 > 製品: モバイルデバイスコネクタ: ホスト: MDCのホスト名/IPアドレス; 署名 > 署名方法: 認証局; 認証局: ESET PROTECT 認証機関)
- b) Appleが信頼するCAが署名した第三者のHTTPS証明書チェーン ([Appleが信頼するCAの一覧](#))^⑧

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ESET PROTECT MDCをアクティベーションします。手順は、クライアントコンピューターでESETセキュリティ製品をアクティベーションする場合と同じです (ライセンス単位は使用されません)。

3. [ユーザー同期](#)サーバータスクを実行します (推奨)。これにより、[コンピューターユーザー](#)の目的で、ユーザーがActive DirectoryまたはLDAPと自動的に同期されます。

i Androidデバイスのみを管理する予定の場合 (iOSデバイスは管理されません)、手順7に進みます。

4. [APN/ABM証明書](#)を作成します。この証明書はiOSデバイス登録のESET PROTECT MDMで使用されます。登録プロファイルに追加される証明書は、ABMプロファイルにも追加される必要があります。

5. APNSを有効にするには、新しい[ESETモバイルデバイスコネクタのポリシー](#)を作成します。

i Apple Business Manager (ABM) でiOSデバイス登録を実行している場合は、[ここ](#)で続行します。

6. [デバイス登録](#)タスクを使用してモバイルデバイスを登録します。タスクを構成し、AndroidまたはiOSのデバイスを登録します。また、これをコンピューターまたはグループタブから実行するには、**静的グループ**を選択した状態で、[新規追加 > モバイルデバイス](#)をクリックします (新規追加は動的グループで使用できません)。

7. デバイス登録中にライセンスを指定しない場合は、[製品アクティベーションクライアントタスク](#)を使用してモバイルデバイスをアクティベーションします^⑧ESET Endpoint Securityライセンスを選択します。各モバイルデバイスでライセンス単位が使用されます。

製品のアクティベーションタスクは、[オフラインライセンス](#)を使用して、モバイル製品ESET Endpoint For Androidをアクティベーションできます。



アクティベーションタスクでは、オフラインライセンスを使用して、バージョン4および5のESET製品をアクティベーションすることはできません。製品を手動でアクティベーションするか、サポートされている製品バージョンを使用する必要があります(最新バージョンを使用することをお勧めします)。

8. デバイス登録中にユーザーを割り当てていない場合は、[ユーザーを編集](#)して、カスタム属性を設定し、モバイルデバイスを割り当てることができます。

9. ポリシーを適用して、モバイルデバイスを管理できます。たとえば、[iOS MDMのポリシー - Exchange ActiveSyncアカウント](#)を作成し、iOSデバイスのメールアカウント、連絡先、カレンダーを自動的に構成できます。またiOSデバイスで[制限を適用](#)し、[Wi-Fi接続を追加](#)できます。

トラブルシューティング

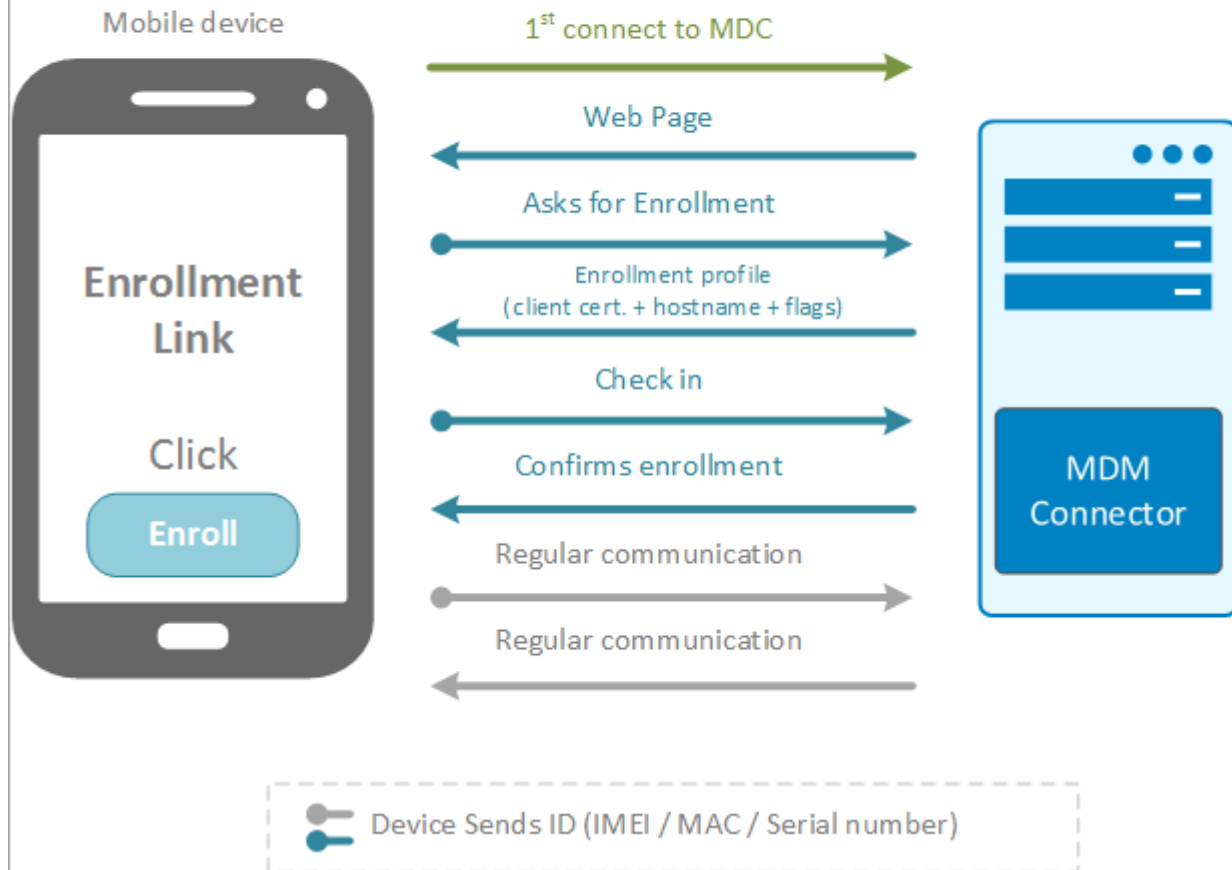
- 破損またはワイプされたモバイルデバイスでは**再登録**を使用できます。再登録リンクは電子メールで送信されます。
- [管理の停止\(ESET Management エージェントのアンインストール\)](#)タスクは、モバイルデバイスのMDM登録をキャンセルし、ESET PROTECTから削除します。
- MDCをアップグレードするには、[ESET PROTECTコンポーネントアップグレードタスク](#)を使用します。
- [MDMトラブルシューティング](#)も参照してください。

デバイス登録

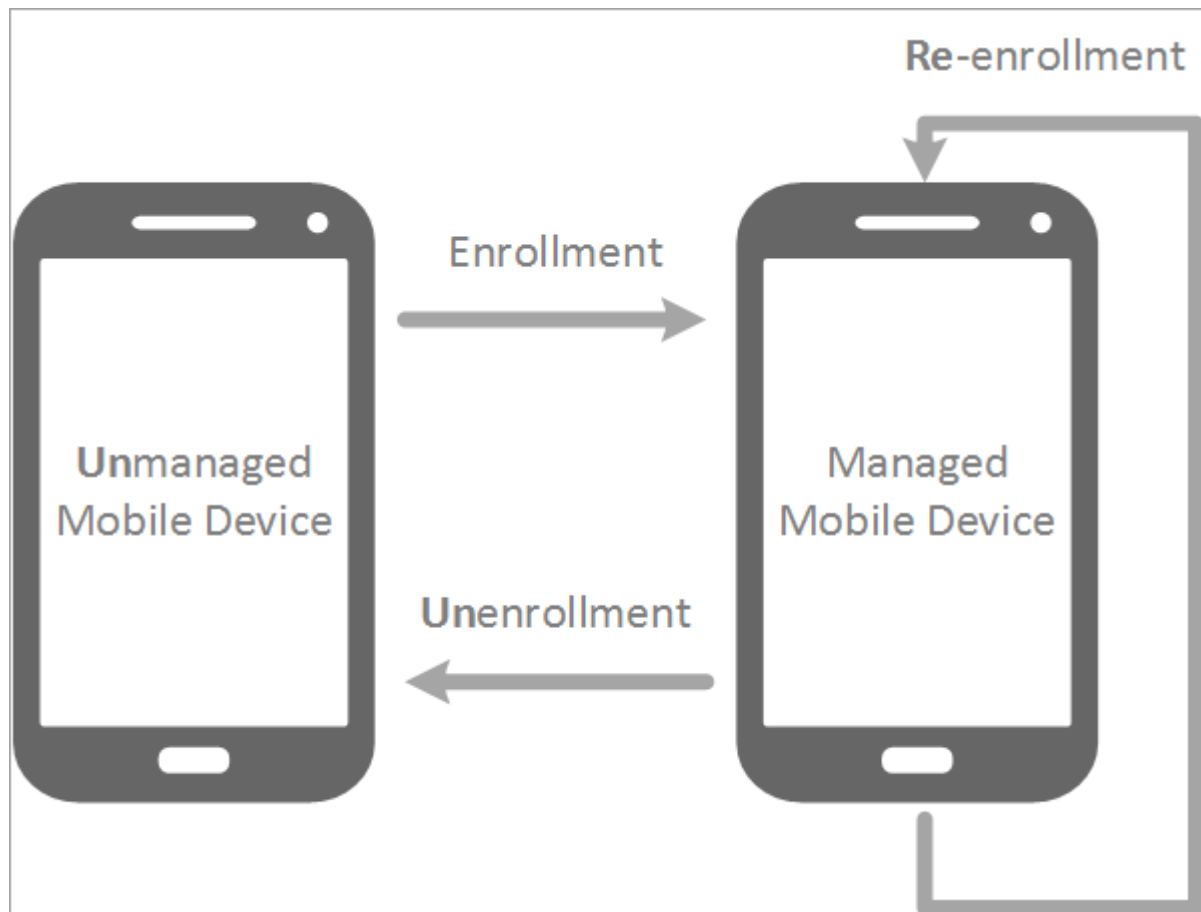
モバイルデバイスはESET PROTECTおよびモバイルデバイスで実行中のESETセキュリティ製品で管理できます。モバイルデバイスの管理を開始するにはESET PROTECTに登録する必要があります(モバイルデバイスにIMEIまたはその他の識別番号を入力する必要はなくなりました)。

以下の図は、登録処理中にモバイルデバイスがモバイルデバイスコネクターと通信する方法を示します。

Device Enrollment



この図は、登録、再登録、登録解除が使用されるとき、および管理対象および管理対象外のデバイスの違いについて説明します。



- **登録:**登録は、デバイスがMDMで管理されていないときにのみ使用できます。この場合、デバイスは**コンピューターセクション**に存在しません。Webコンソールからデバイスを削除しても管理対象外にはなりません。レプリケーションが成功した後にデバイスはWebコンソールに表示されます。登録解除処理でのみ、管理されたステータスからデバイスを削除できます。各登録トークンは一意であり、1回のみ使用できます。トークンが使用されると、再利用できません。

- **再登録:**再登録はデバイスが管理されている場合にのみ使用できます。再登録トークンは必ず登録トークンとは異なり、1度のみ使用できます。
デバイスを再登録するには、**コンピューターセクション**を開き、再登録するモバイルデバイスを選択します。**アクションメニュー**を開き、**モバイル > 再登録**を選択します。

- **登録解除:**登録解除はデバイスの管理を停止するための正しい方法です。[クライアントタスクの管理の停止](#)を使用して、登録解除が実行されます。デバイスが応答していない場合、デバイスが実際に削除されるまで最大3日かかる可能性があります。デバイスを削除して再登録する場合は、代わりに再登録を使用してください。

i Apple Business Manager (ABM)でiOSデバイス登録を実行している場合は、[ここ](#)で続行します。

コンピューターセクションまたは**詳細 > グループ**でモバイルデバイスを登録できます。モバイルデバイスを追加する**静的グループ**を選択し、**新規追加 > モバイルデバイス**をクリックしてから、次の登録方法のいずれかを選択します。

- **[電子メールで登録](#)** – 電子メールでのモバイルデバイスの一括登録。多数のモバイルデバイスを登録する必要がある場合、または物理的にアクセスできない既存のモバイルデバイスがある場合に、このオプションが最適です。このオプションを使用するには、モバイルデバイスのユーザー/所有者からのアクティブな参加が必要です。

- **[リンクまたはQRコードでの個別登録](#)** – 1回のモバイルデバイス登録。1度に1つのモバイルデバイス

を登録でき、各デバイスで同じ手順を繰り返す必要があります。少ない数のモバイルデバイスを登録するときのみ、このオプションを使用することをお勧めします。ユーザー/モバイルデバイスの所有者に何もさせずに、自分で登録全部を実行させる場合には、このオプションが最適です。また、デバイスがすべて設定された後にユーザーに渡される新しいモバイルデバイスの場合に、このオプションを使用できます。

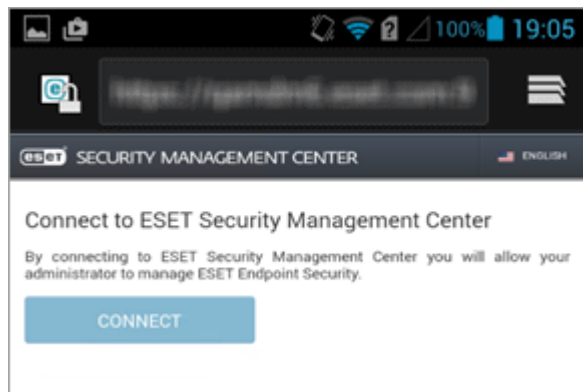
- [デバイス所有者として個別に登録\(Android 7以上のみ\)](#) - Androidデバイス専用の1台のモバイルデバイス登録。1度に1つのモバイルデバイスを登録でき、各モバイルデバイスで同じ手順を繰り返す必要があります。この登録処理は、購入直後の新しいモバイルデバイスまたはワイプ/初期設定リセット後のモバイルデバイスでのみ実行できます。この登録処理は、モバイルデバイスの管理権限よりも上の、昇格された管理権限を管理者に付与します。

Androidデバイス登録

ESET Endpoint Security for Android (EESA)がモバイルデバイスでアクティベートされる時には、2つの登録シナリオがあります。製品アクティベーションタスクを使用してモバイルデバイスでEESAをアクティベートします(推奨)。もう1つのシナリオは、ESET Endpoint Security for Androidアプリが既にアクティベートされているモバイルデバイス用です。

EESAは既にアクティベートされています - 次の手順に従って、デバイスを登録します。

1. 電子メールで受信した登録リンクURLをタップするかブラウザに手入力します。ポート番号も含まれます(<https://eramdm:9980/<token>>など)SSL証明書を許可するように指示される場合があります。同意する場合は[同意]をクリックし、[接続]をクリックします。



- ! モバイルデバイスにESET Endpoint Securityがインストールされていない場合は、自動的にGoogle Playストアに移動します。ここでアプリをダウンロードできます。

- i このリンクを開くアプリが見つかりませんでした」という通知を受信した場合は、既定のAndroid Webブラウザで登録リンクを開いてください。

2. 接続詳細情報(モバイルデバイスコネクターサーバーアドレスとポート)が表示された場合は確認し、[接続]をクリックします。

Remote administrator

To connect a device to Remote Administrator:

- In Remote Administrator add a new mobile device to the "Computers" list.
- Enter Mobile Device Connector (MDC) server address.

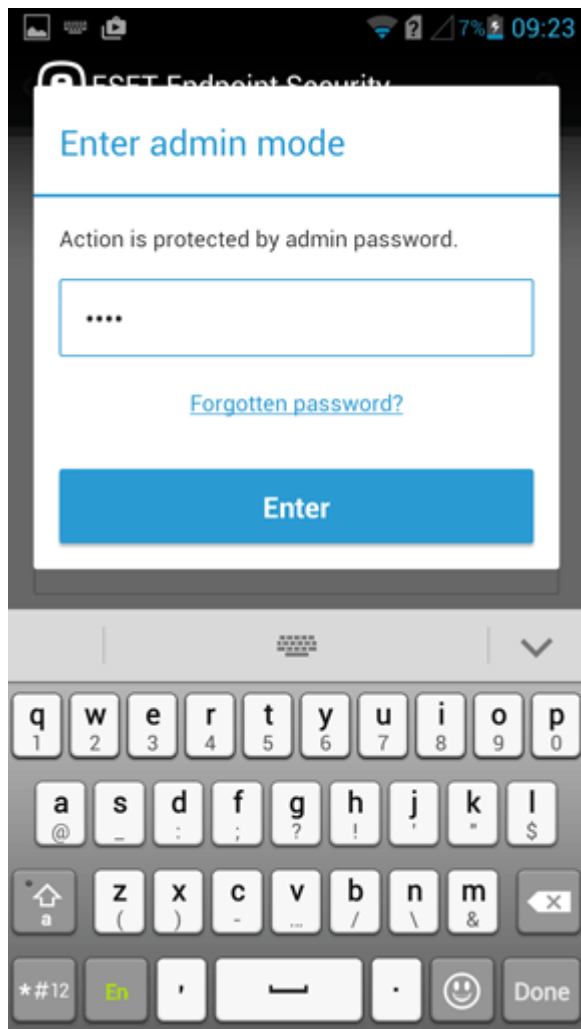
MDC SERVER ADDRESS

https:// [REDACTED]

Requirements: Remote Administrator 6 or newer with Mobile Device Connector.

Connect

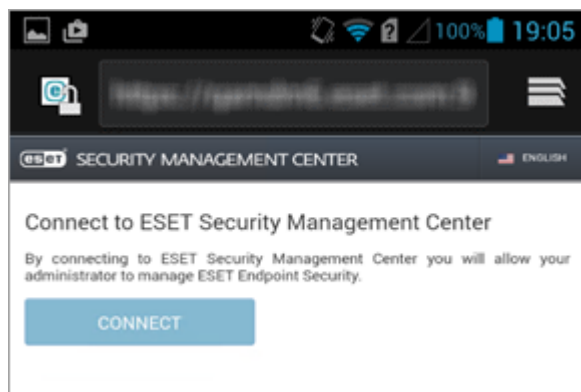
3. ESET Endpoint Security管理者モードパスワードを空のフィールドに入力し、[入力]をタップします。



4. このモバイルデバイスはESET PROTECTで管理されています。[完了]をタップします。

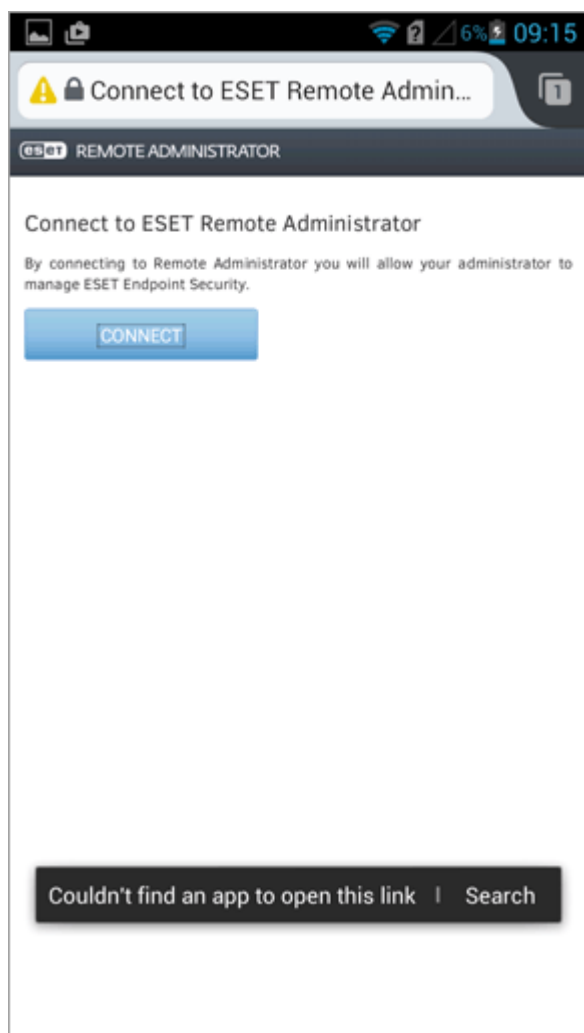
EESAがまだアクティベートされていません – 次の手順に従い、製品をアクティベートし、デバイスを登録します。

1. 登録リンクURL (ポート番号を含む)をタップし、手動でブラウザーに入力します(たとえば、<https://esmcmdm:9980/<token>>)。あるいは、提供された**QRコード**を使用できます。SSL証明書を許可するように指示される場合があります。同意する場合は[同意]をクリックし、[接続]をクリックします。

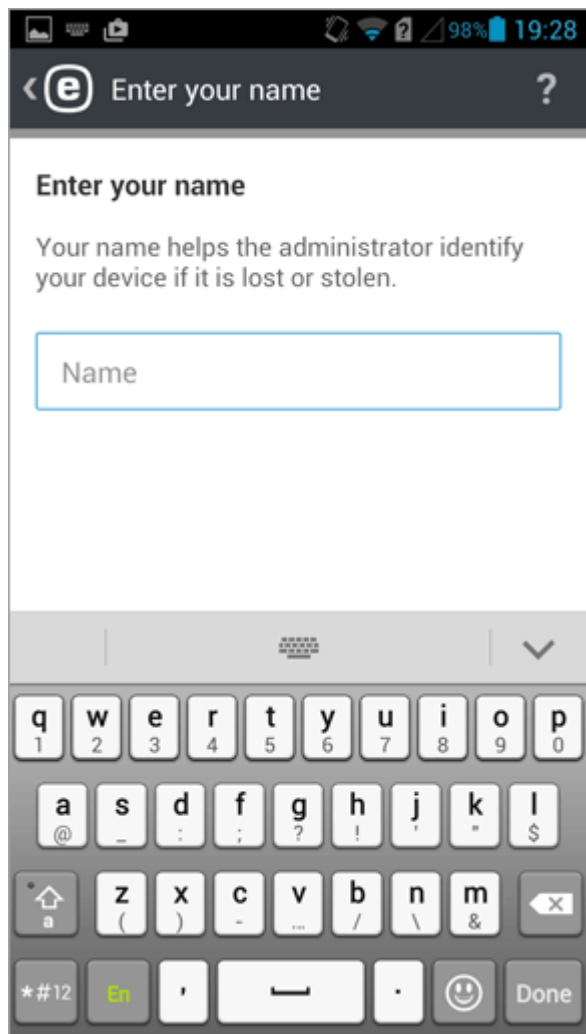


モバイルデバイスにESET Endpoint Securityがインストールされていない場合は、自動的にGoogle Playストアに移動します。ここでアプリをダウンロードできます。

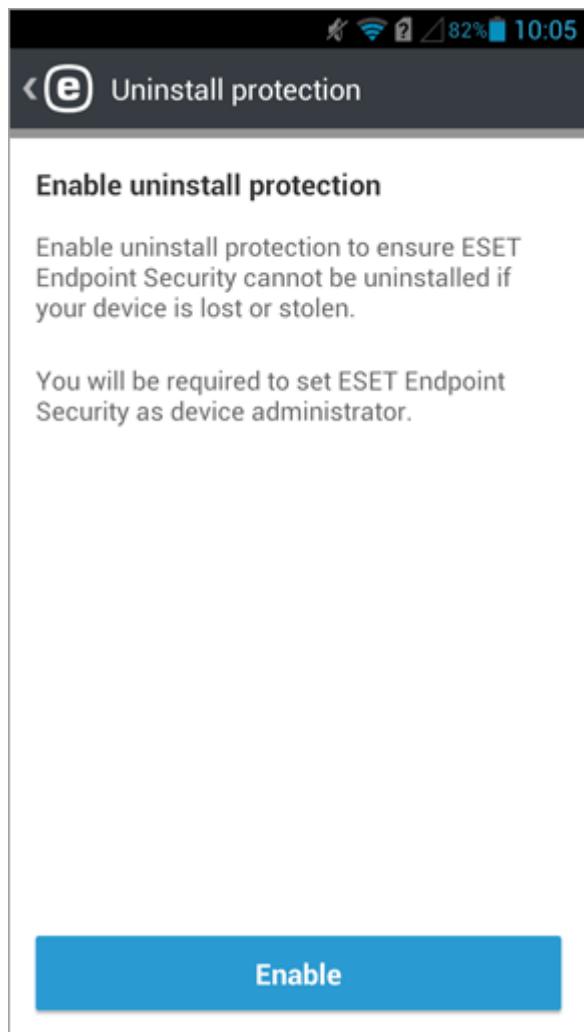
i このリンクを開くアプリが見つかりませんでした」という通知を受信した場合は、既定のAndroid Webブラウザで登録リンクを開いてください。



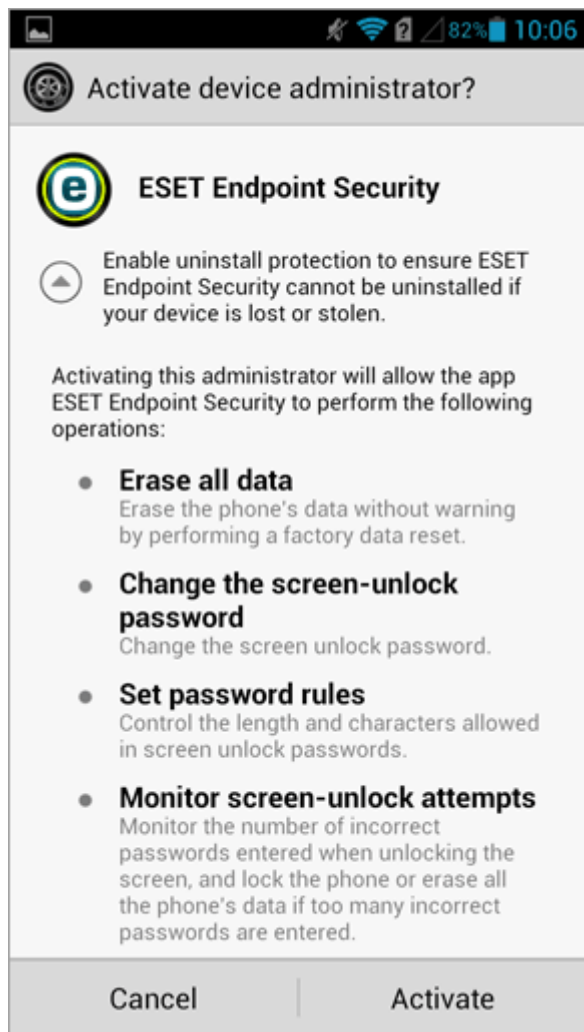
2. モバイルデバイスの名前を入力します。(この名前はESET PROTECTに表示されできません。アンチセフトおよび診断ログ目的にのみ関連します。)



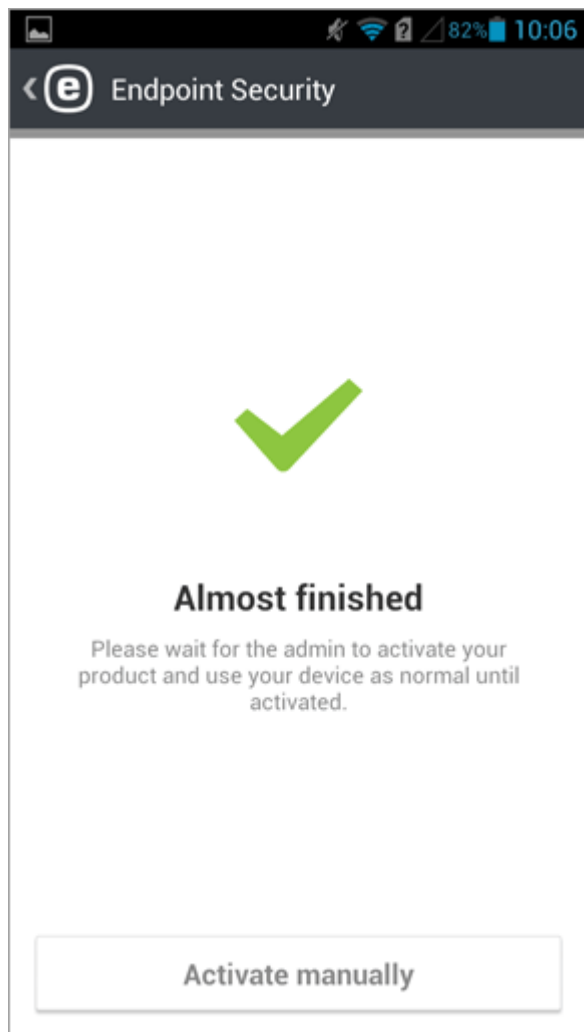
3. [有効にする]をタップして、アンインストール保護を有効にします。



4. [アクティベート]をタップして、デバイス管理者を有効にします。

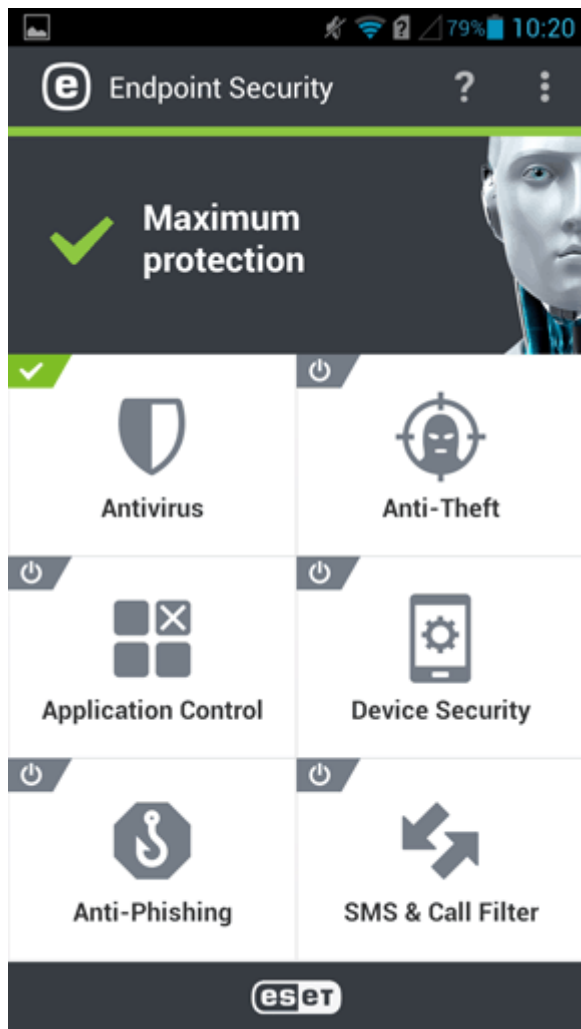


5. この時点で、モバイルデバイスのESET Endpoint Security for Androidアプリを終了し、ESET PROTECT Webコンソールを開くことができます。



6. ESET PROTECT Webコンソールで、[クライアントタスク]>[モバイル]>[\[製品アクティベーション\]](#)に移動し、[新規]をクリックします。

製品アクティベーションクライアントタスクがモバイルデバイスで実行するには、時間がかかる場合があります。タスクが正常に実行されたらESET Endpoint Security for Androidアプリがアクティベートされ、モバイルデバイスをESET PROTECTで管理できます。ユーザーはESET Endpoint Security for Androidアプリを使用できますESET Endpoint Security for Androidアプリが開くと、メインメニューが表示されます。

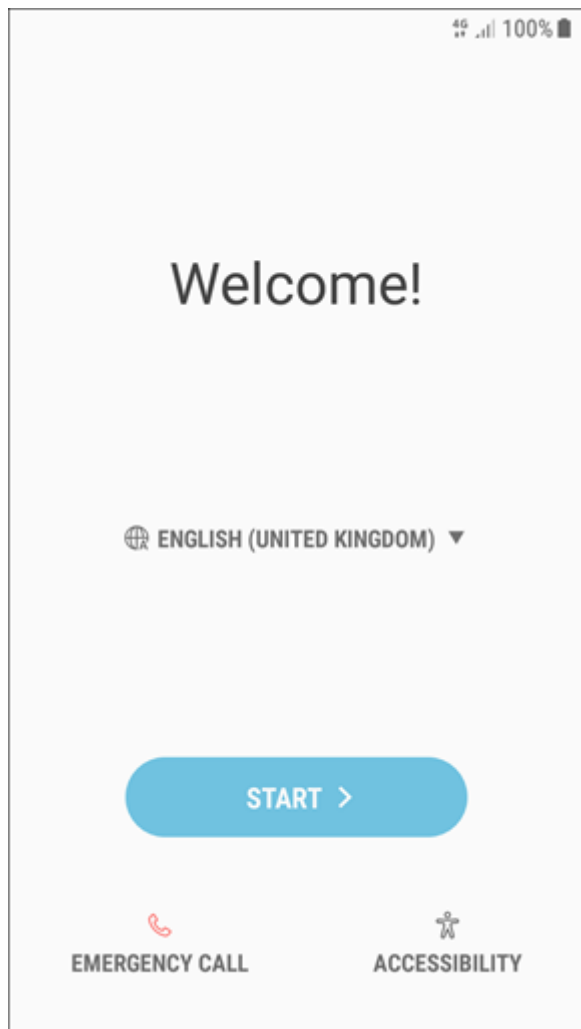


デバイス所有者としてのAndroidデバイス登録

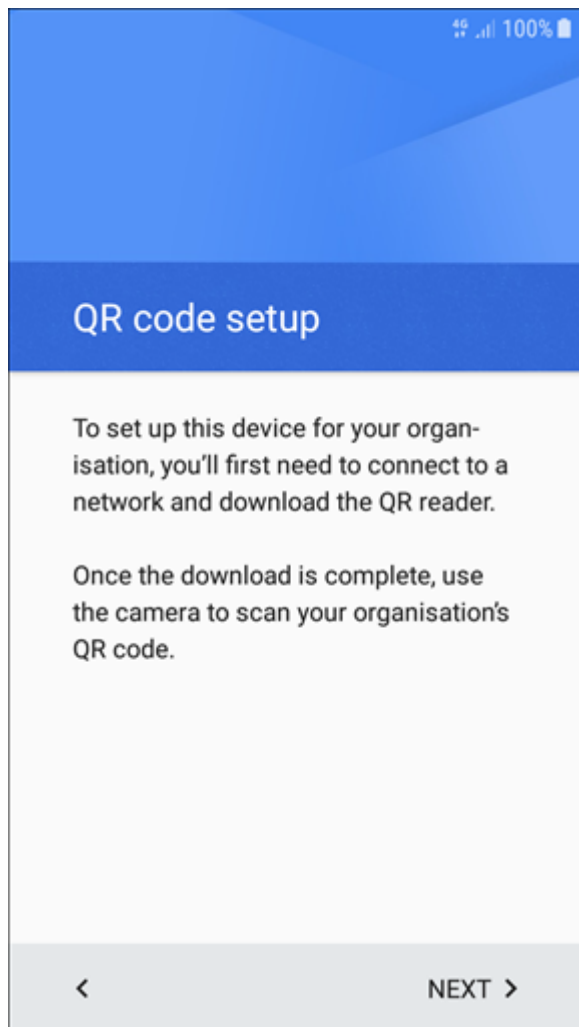
このタイプの登録は、Android v7以上のAndroidデバイスでのみ使用できます。

i 次の登録ステップを実行するにはAndroidデバイスがワイプ/初期設定リセット後であるか、新品である必要があります。

1. モバイルデバイスの電源を入れます。
2. SIMカードPINの入力画面が表示された場合は入力します。
3. [ようこそ]画面で、優先言語を選択して、[ようこそ]テキストの周りの画面を6回タップしてQR設定を開始します。

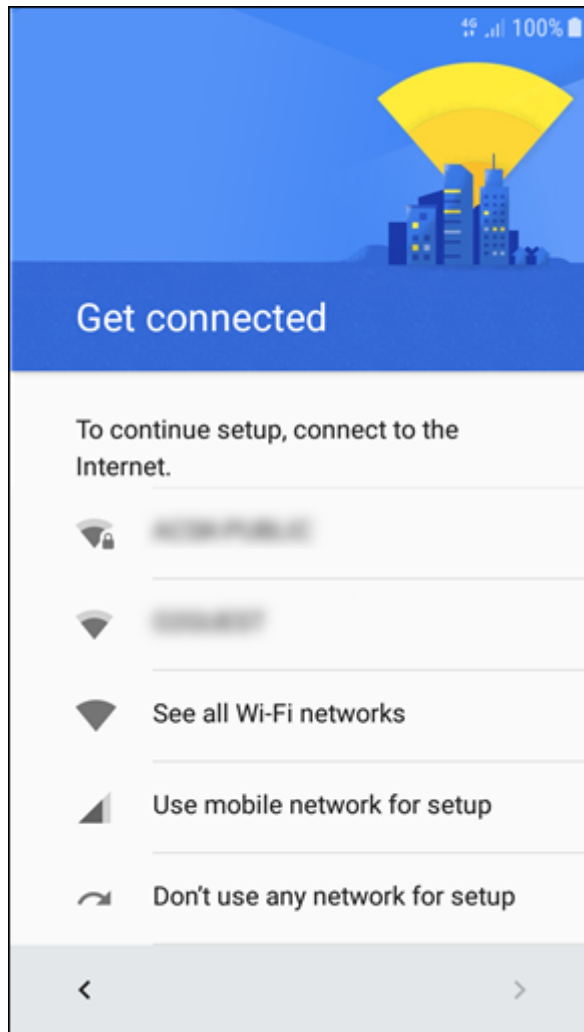


4. 前のステップを正しく実行した場合、**QRコード設定**画面が表示されます。**次へ**をタップして続行します。



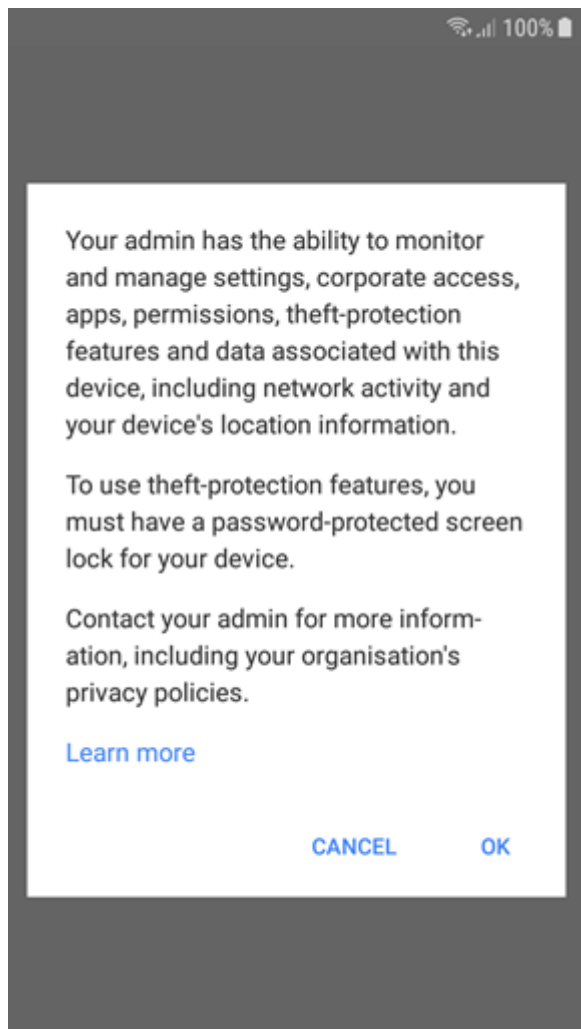
i 一部のデバイスでは、デバイスのストレージを暗号化する必要があります(充電器に接続する必要がある場合もあります)。任意の暗号化タイプを選択し、画面の手順に従って進めます。

5. インターネット接続を選択します。これは、次のステップに必要なQRコードリーダーをダウンロードするために使用されます。

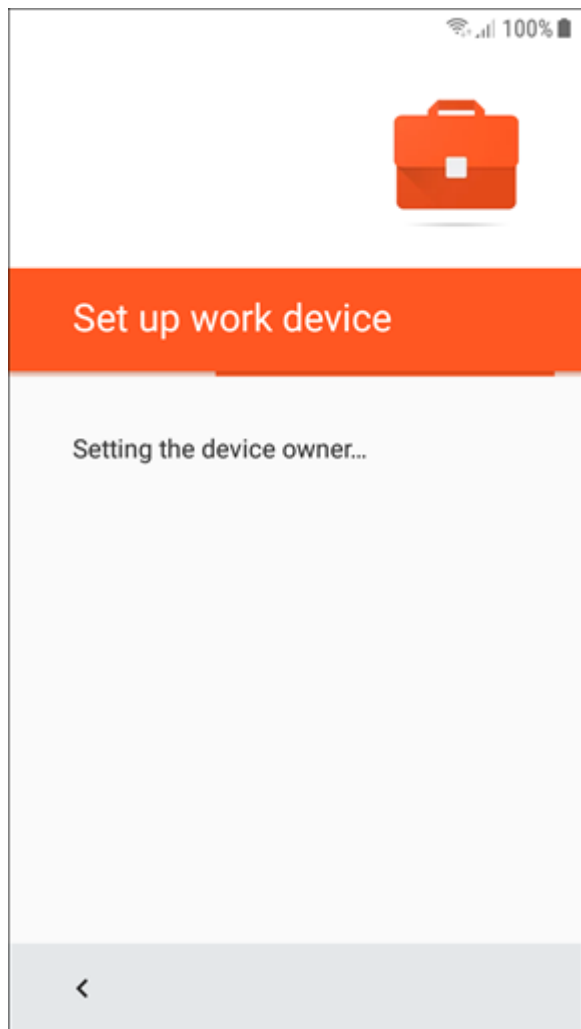


6. QRコードリーダーがインストールされます。インストールが完了した後、ESET PROTECT Webコンソールで[生成](#)されたQRコードをスキャンします。

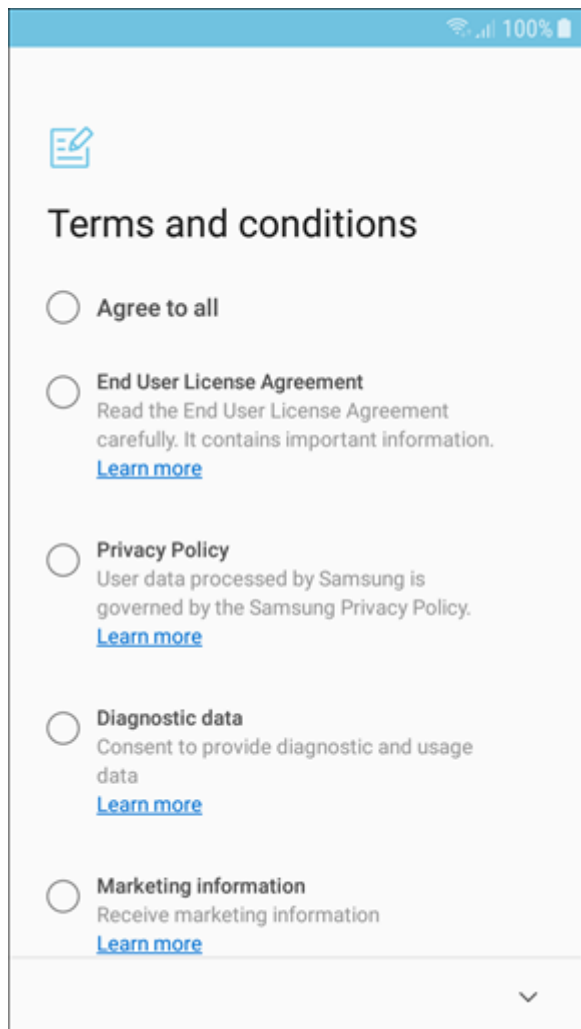
7. 昇格されたデバイス所有者権限を管理者に付与することを理解していることを確認するように要求されます。**OK**をタップして続行します。



8. ESET Endpoint Security for Androidがインストールされ、必要な権限が適用されます。



9. **すべてに同意**をタップしEULA[®]プライバシーポリシー、診断およびマーケティングデータ送信を許可します。

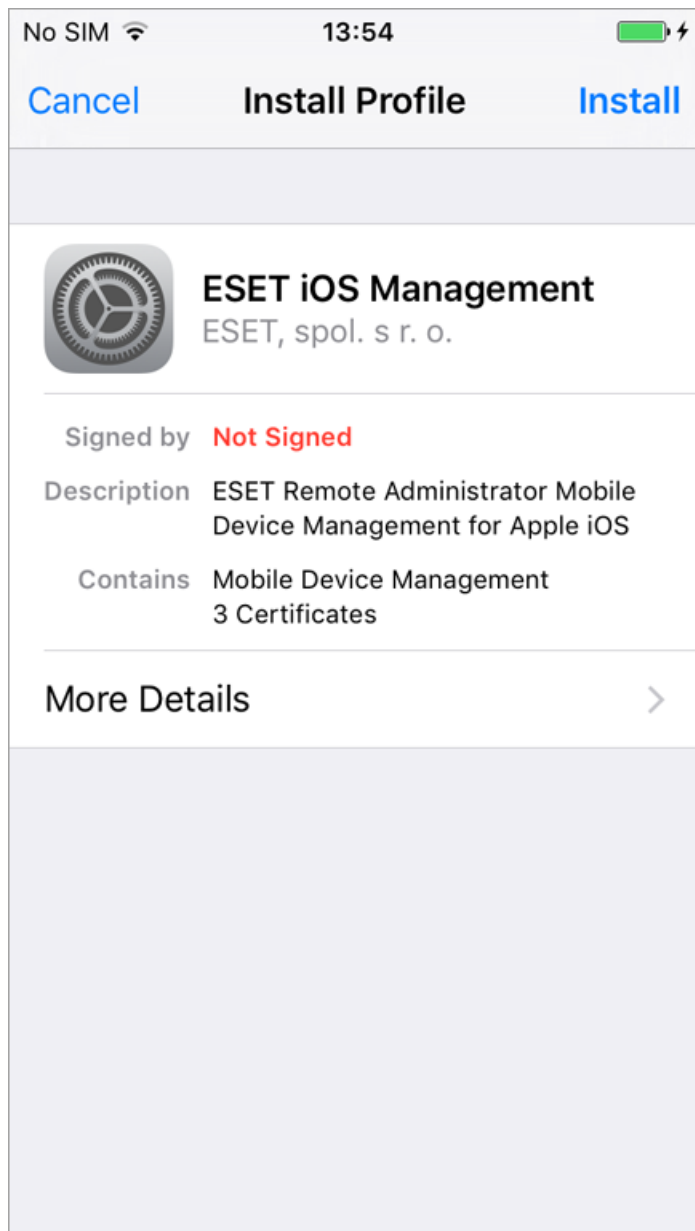


10. デバイスはデバイス所有者モードで登録されます。

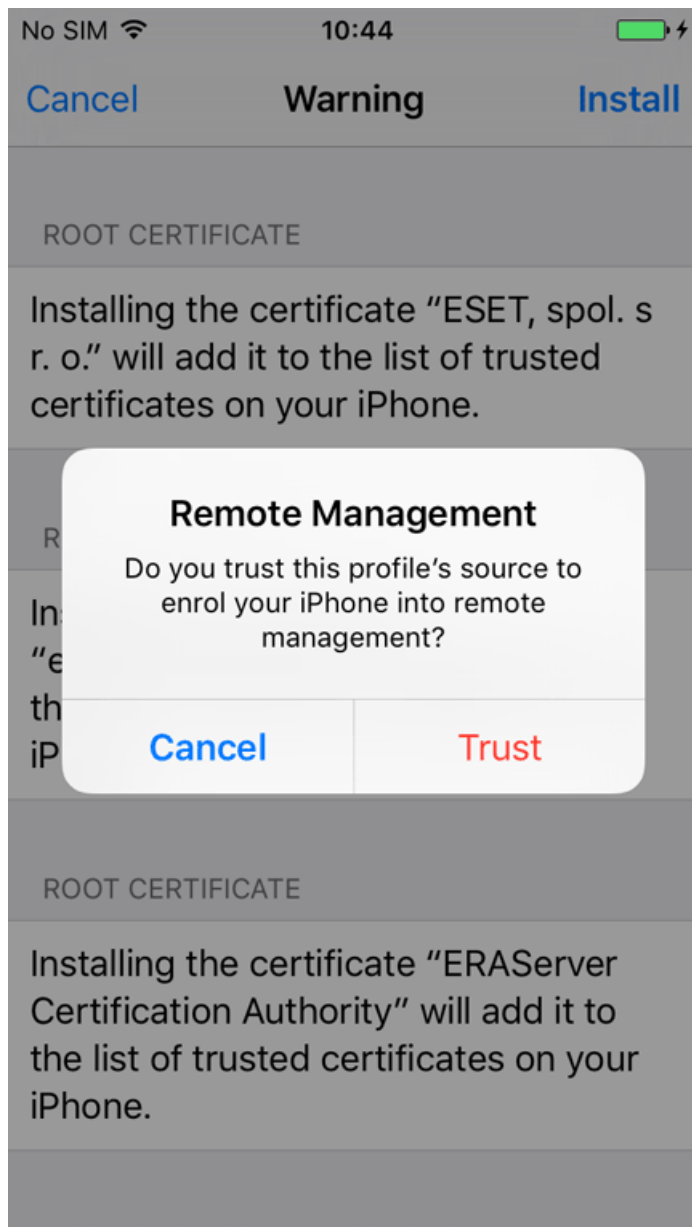
iOSデバイス登録

i Apple Business Manager (ABM)でiOSデバイス登録を実行している場合は、[ここ](#)で続行します。

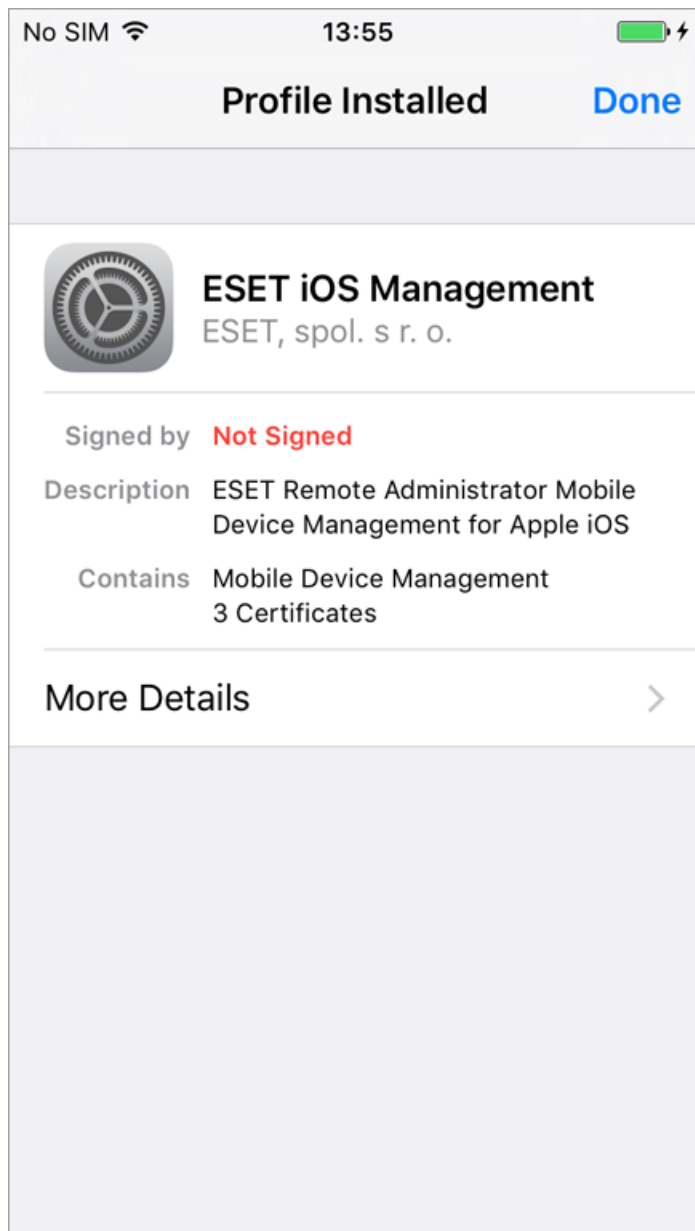
1. 登録リンクURL (ポート番号を含む) をタップし、手動でブラウザーに入力します (たとえば、`https://eramdm:9980/<token>`)。あるいは、提供された**QRコード**を使用できます。
2. [インストール] をタップし、MDM登録の[プロフィールのインストール]画面で続行します。



3. [信頼]をタップし、新しいプロファイルのインストールを許可します。



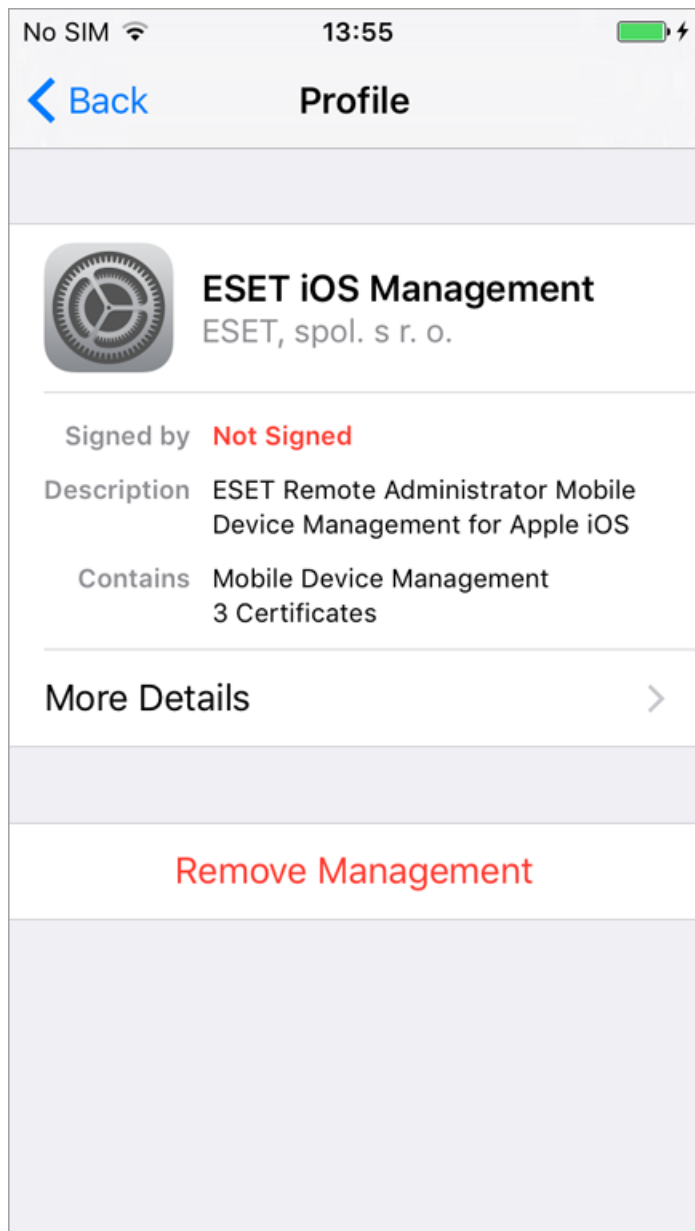
4. 新しいプロファイルをインストールした後に、[署名]フィールドにプロファイルが**未署名**であることが表示されます。これはiOSが証明書を認識していないためです。署名された登録プロファイルを使用するには、[Appleが信頼するCA](#)によって証明されたHTTPS証明書を使用します。あるいは、独自のHTTPS登録証明書を使用し、登録に[署名](#)できます。



5. この登録プロファイルでは、デバイスを構成し、ユーザーまたはグループのセキュリティポリシーを設定できます。



この登録プロファイルを削除すると、すべての企業設定(メール、カレンダー、連絡先など)が削除され、iOSモバイルデバイスは管理されません。ユーザーが登録プロファイルを削除するとESET PROTECTはこれを認識せず、デバイスのステータスが⚠️に変わり、デバイスが接続していないため、14日後に🚨に変わります。登録プロファイルが削除されたというその他の表示はありません。



ABMを使用したiOSデバイス登録

Apple Business Manager (ABM)はAppleの新しい企業iOSデバイス登録方法です。ABMでは、デバイスに直接接続せず、最低限のユーザー操作でiOSデバイスを登録できます。Apple ABM登録により、管理者は完全なデバイスセットアップ処理をカスタマイズできます。また、ユーザーがデバイスからMDMプロファイルを削除できないようにすることができます。既存のiOSデバイス(iOSデバイスがABM要件を満たす場合)と、将来購入するすべてのiOSデバイスを登録できます。Apple ABMの詳細については、[Apple ABM ガイド](#)と[Apple ABMドキュメントを参照してください](#)。

ESET PROTECT MDMをApple ABMサーバーと同期する：

1.すべてのApple ABM要件(アカウント要件とデバイス要件)が満たされていることを確認します。

- ABMアカウント：

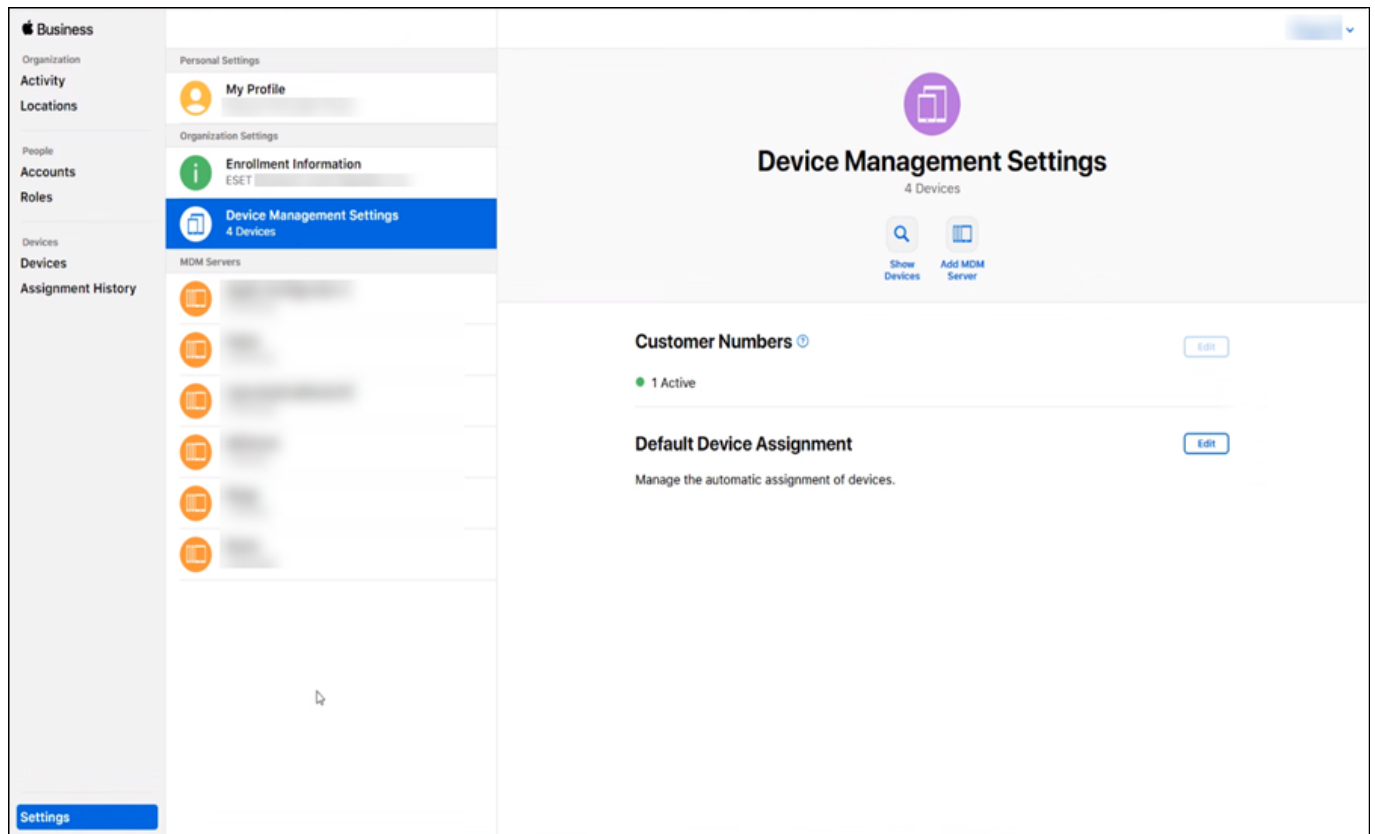
oこのプログラムは特定の国でのみ提供されています。[Apple ABM Webページ](#)にアクセスし、国でABMが提供されているかどうかを確認してください。

oApple ABMアカウント要件は次のWebサイトをご覧ください。[Apple展開プログラム要件](#)および[Apple Device Enrollment要件](#)。

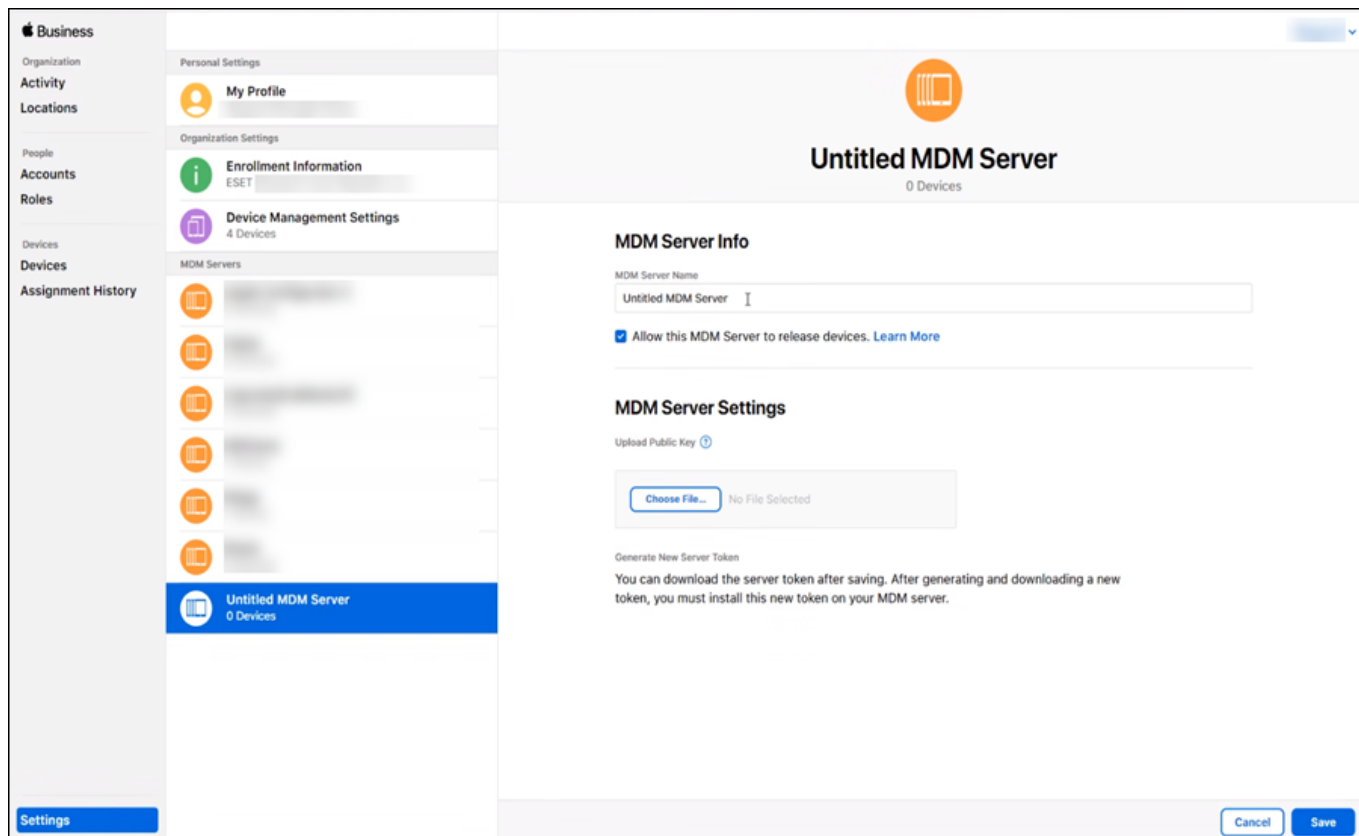
oABMデバイス要件の詳細については、[ここ](#)を参照してください。

2.Apple ABMアカウントにログインします(Apple ABMアカウントがない場合は、[ここ](#)で作成できます)。

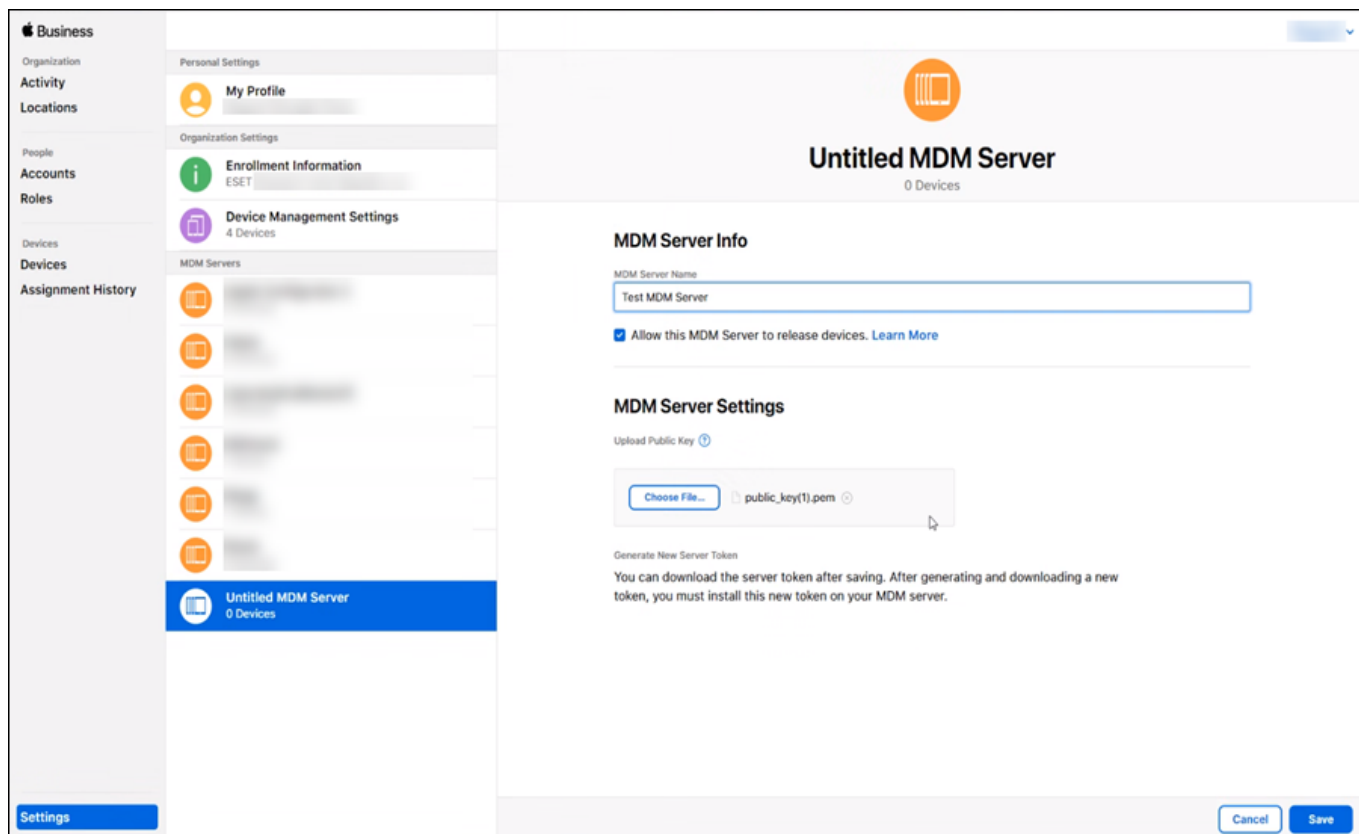
3.デバイス管理設定セクションで、**MDMサーバーの追加**を選択します。



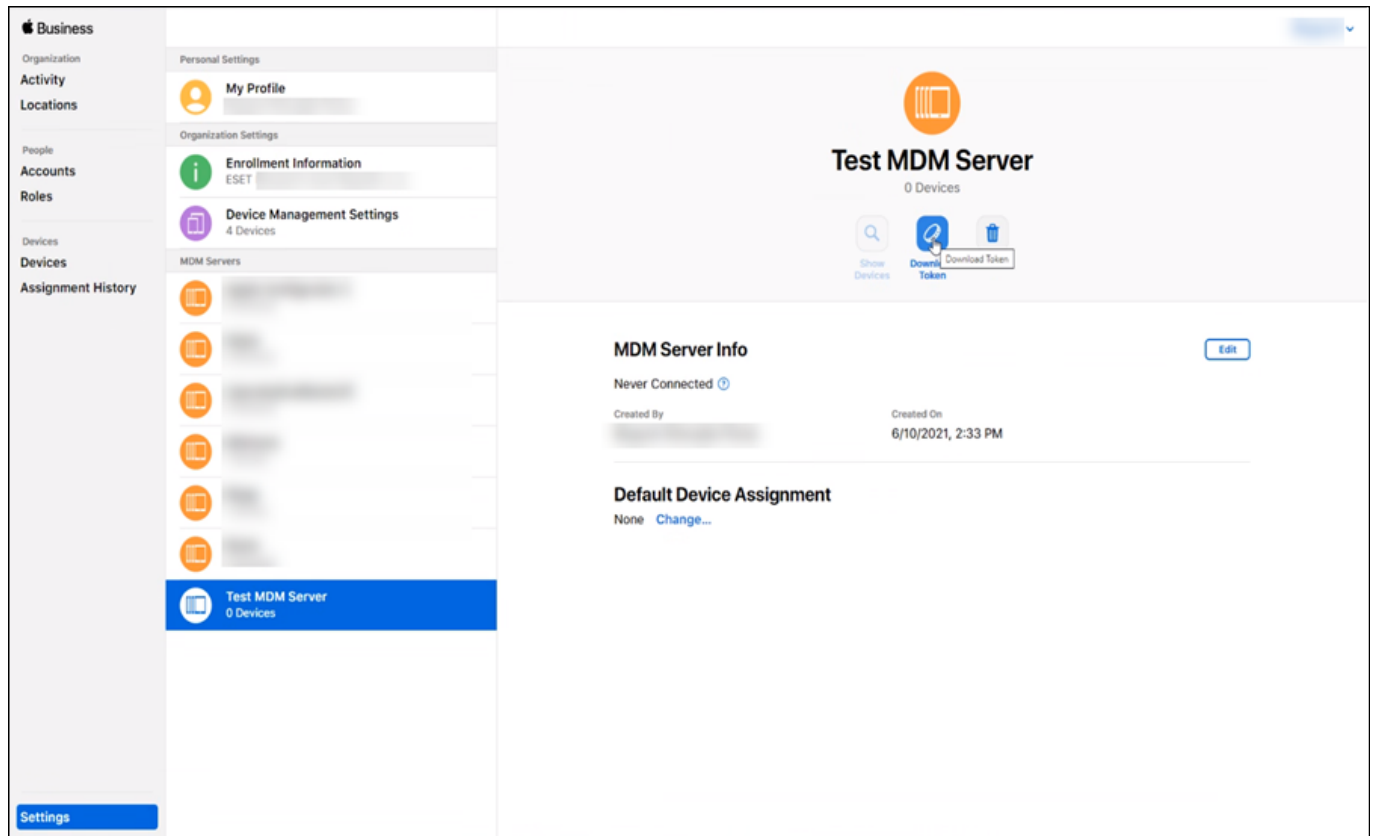
4.無題のMDMサーバー画面で**MDMサーバー名**を入力します。例:"MDM_Server,"



5.公開鍵をABMポータルにアップロードします。[ファイルの選択]をクリックし、公開鍵ファイル(Apple Push CertificateポータルからダウンロードしたAPNS証明書)を選択して、[保存]をクリックします。



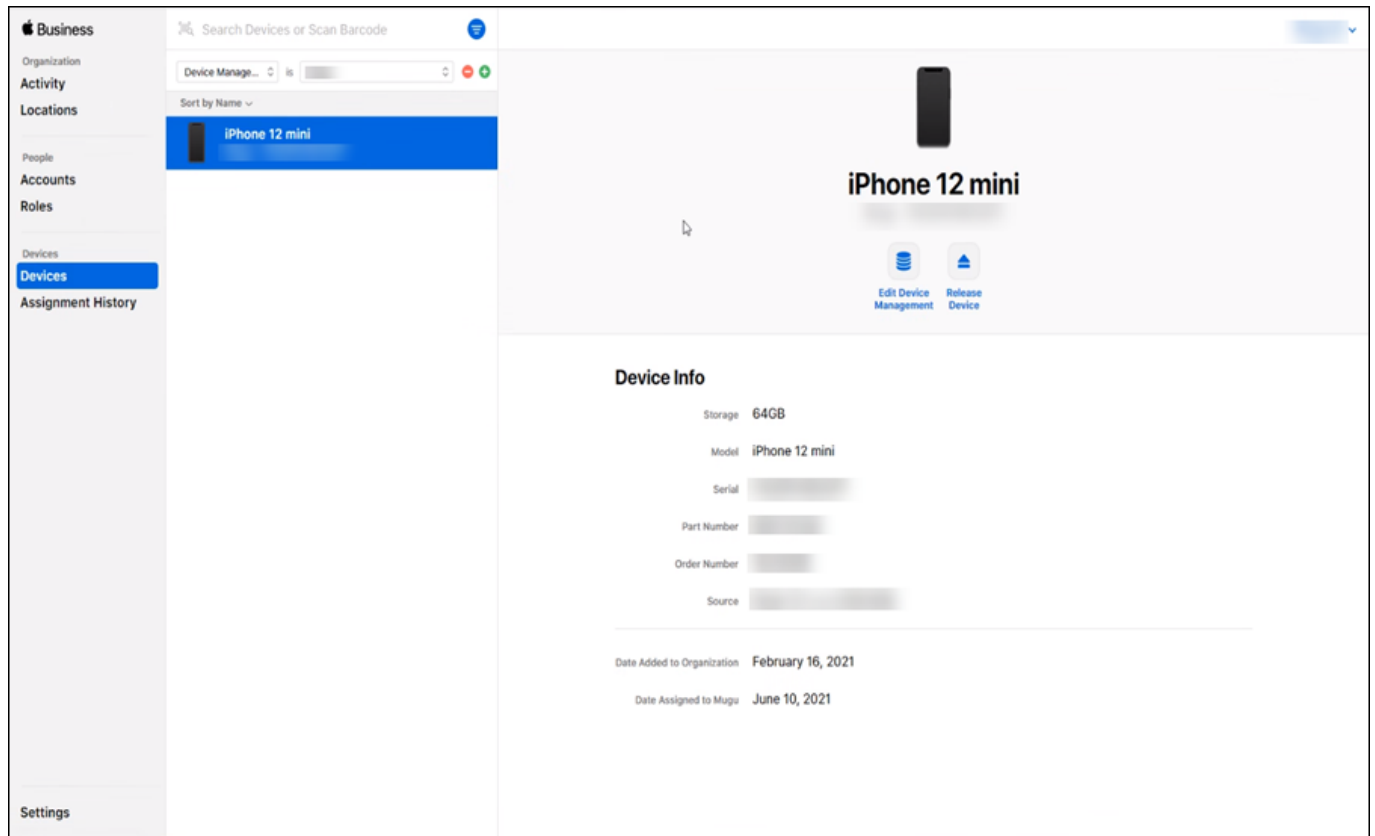
6.トークンのダウンロードをクリックし、Apple ABMトークンをダウンロードします。 **Apple Business Manager (ABM) -> 認証トークンのアップロードで、このファイルがESET PROTECT MDCポ**
リシーにアップロードされます。



iOSデバイスをApple ABMに追加する：

次に、iOSデバイスをApple ABMポータル内の仮想MDMサーバーに割り当てます。シリアル番号、注文番号でiOSデバイスを割り当てるかCSV形式で対象デバイスのシリアル番号リストをアップロードします。いずれにしてもiOSデバイスを仮想MDMサーバーに割り当てる必要があります(前の手順で作成)。

1. ABMポータルの**デバイス**セクションに移動し、割り当てるデバイスを選択して、**デバイス管理の編集**をクリックします。



2. リストからMDMサーバーを選択した後、選択内容を確認すると、モバイルデバイスがMDMサーバーに割り当てられます。

! デバイスがABMポータルから削除されると、完全に削除され、もう一度追加できません。

その後、Apple ABMポータルを離れESET PROTECT Webコンソールで続けることができます。

! 現在使用中(かつデバイス要件を満たす)のiOSデバイスを登録している場合、新しいポリシー設定が、対象デバイスの初期設定リセット後に適用されます。

登録処理を完了するには、[APNS証明書](#)を、MDMサーバーに割り当てられた[MDCポリシー](#)にアップロードする必要があります。(このMDCポリシーはMDMサーバー設定のロールを実行します)。

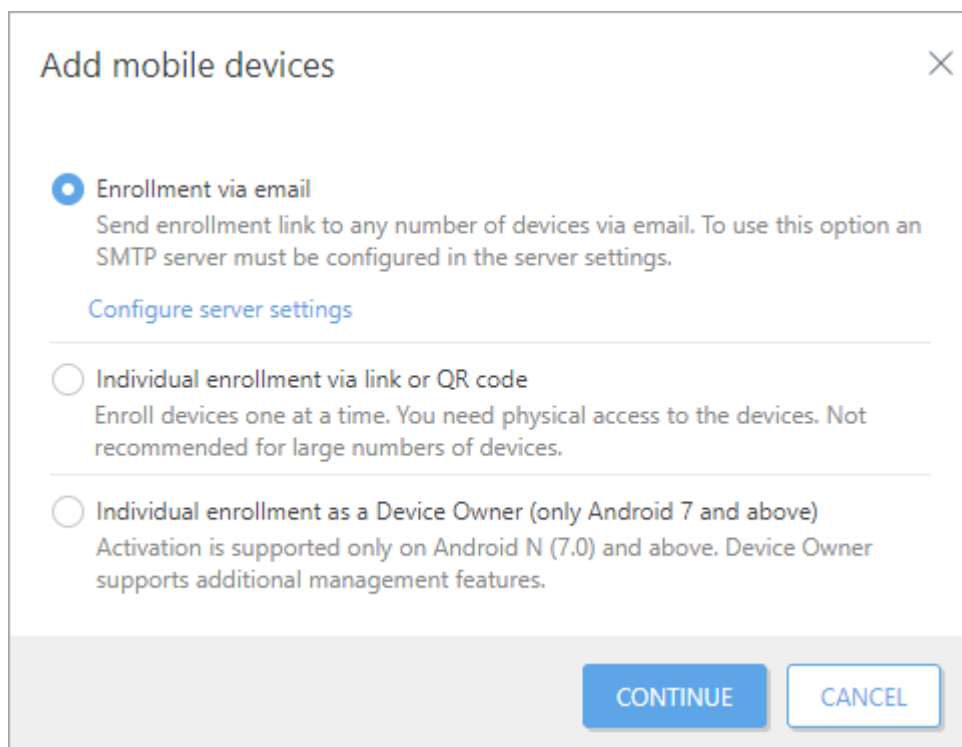
i iOSデバイスで、登録中にESETからプロファイルをダウンロードできないというメッセージが表示される場合は、ABM内のMDMサーバーが正しく設定され(正しい証明書がある)、正しいiOSデバイスをApple ABM内で選択したESET PROTECT MDMサーバーに割り当てたことを確認します。

電子メールで登録

この方法はモバイルデバイスの一括登録に最適です。登録リンクを任意の数のデバイスにメールで送信できます。各モバイルデバイスは電子メールアドレスに基づいて一意のワンタイムトークンを受信します。

! 電子メールでの一括登録用にSMTPサーバーを設定する必要があります。[サーバー設定](#)に移動し、[詳細設定](#)を展開して、[SMTPサーバー詳細](#)を指定します。

1.新しいモバイルデバイスを追加するには、**コンピューターセクション**または**詳細>グループ**に移動します。モバイルデバイスを追加する**静的グループ**を選択し、**新規追加>モバイルデバイス>電子メールで登録**をクリックします。



Add mobile devices [X]

☒ **Enrollment via email**
Send enrollment link to any number of devices via email. To use this option an SMTP server must be configured in the server settings.
[Configure server settings](#)

☐ **Individual enrollment via link or QR code**
Enroll devices one at a time. You need physical access to the devices. Not recommended for large numbers of devices.

☐ **Individual enrollment as a Device Owner (only Android 7 and above)**
Activation is supported only on Android N (7.0) and above. Device Owner supports additional management features.

CONTINUE **CANCEL**

2.**Mobile Device Connector**が自動的に選択されます。複数のMDCがある場合は、使用するMDCのFQDNを選択します。モバイルデバイスコネクタがまだインストールされていない場合は、インストール手順について、本ガイドの「[モバイルデバイスコネクタインストール - Windows](#)」または「[Linux](#)」の章を参照してください。

3.**ライセンス (任意) - 選択**をクリックして、アクティベーションで使用するライセンスを選択します。製品のアクティベーションクライアントタスクがモバイルデバイス用に作成されます。ライセンス単位が取得されます(各モバイルデバイスに1つ)。

4.**親グループ** - モバイルデバイスの特定の静的グループがない場合は、**新しい静的グループ**(モバイルデバイスなど)を作成することをお勧めします。既存のグループがある場合は、**すべて**をクリックすると、ポップアップウィンドウが開き、静的グループを選択できます。

5.**デバイスの一覧** - 登録するモバイルデバイスを指定します。次の機能を使用して、モバイルデバイスを追加できます。

- **デバイスの追加** - 1つのエントリ。登録メールが送信されるモバイルデバイスの電子メールアドレスを手動で入力する必要があります。また、ユーザーをモバイルデバイスに割り当てるには、**ペア**をクリックしてユーザーを選択します。**詳細>コンピューターユーザー**画面内で指定された電子メールで電子メールアドレスが上書きされます。別のモバイルデバイスを追加する場合は、**デバイスの追加**をもう一度クリックして、必須情報を送信します。

- **ユーザーの追加** - デバイスを追加するには、**詳細>コンピューターユーザー**のリストで該当するユーザーチェックボックスをオンにします。登録するモバイルデバイスのリストを修正する場合は、**ペアの解除**をクリックします。割り当てられたユーザーのペアを解除すると、ペア未設定になります。**[ペア]**をクリックし、ペアリングされていないデバイスの任意のユーザーを選択します。**ごみ箱**アイコンをクリックしてエントリを削除します。

- **CSVのインポート** - 大量のモバイルデバイスを簡単に追加する方法。**追加するデバイスのリ**

ストが含まれた.csvファイルをアップロードします。詳細については、[CSVのインポート](#)を参照してください。

- **コピーと貼り付け** – カスタム区切り文字で区切られたアドレスのカスタムリストをインポートします(この機能はCSVインポートでも動作します)。

1つ以上のユーザーをモバイルデバイスに割り当てることをお勧めします。[iOSでパーソナリ化されたポリシー](#)を使用する場合は、ユーザーをデバイスに割り当てる必要があります。

CSVのインポートを使用するときには、各エントリで**デバイス名**を指定することをお勧めします。これは**コンピューター**セクションに表示されるデバイス名です。**デバイス名**フィールドを空にする場合は、電子メールアドレスが使用され、**コンピューター**と**グループ**にデバイス名として表示されます。これは、特に、同じ電子メールアドレスで複数のデバイスを登録する場合に、混乱を招くおそれがあります。この電子メールアドレスが何度も表示され、デバイスを識別できなくなります。

6. [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。詳細については、[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](#)を参照してください。

7. **登録電子メールメッセージ**– 定義済みのメッセージテンプレートには、通常は十分な詳細が含まれていますが、ユーザーの詳細を追加して、**件名**および**コンテンツ**をカスタマイズできます。**手順**部分は登録メールの**コンテンツ**の下に表示され、**デバイス名** (または電子メールアドレス)と登録リンク(URL)が含まれます。1つの電子メールアドレスを使用して複数のモバイルデバイスを登録する場合は、デバイスのリストが表示され、それぞれに固有の登録リンク(URL)が割り当てられます。また、モバイルデバイス(iOSおよびAndroid)ユーザーが登録を完了するために実行する必要があります。

8. **登録**をクリックすると、各電子メールアドレスに該当する登録リンクと手順が記載された電子メールが送信されます。

9. モバイルデバイス登録を完了するには、これらの手順に従うか、モバイルデバイスのユーザー/所有者に手順を実行させます。

- [Androidデバイス登録](#)

- [iOSデバイス登録](#)

リンクまたはQRコードで個別に登録

登録リンクまたはQRコードを使用してモバイルデバイスを登録する場合は、デバイスへの物理的なアクセスが必要です。またQRコードを使用するにはQRコードリーダー/スキャナーアプリケーションがモバイルデバイスにインストールされている必要があります。

i 多数のモバイルデバイスの場合、[電子メールでの登録](#)をお勧めします。

1. 新しいモバイルデバイスを追加するには、**コンピューター**セクションまたは**詳細 > グループ**に移動します。モバイルデバイスを追加する**静的グループ**を選択し、**新規追加 > モバイルデバイス > リンクまたはQRコードで個別に登録**をクリックします。

Add mobile devices

☐ Enrollment via email

Send enrollment link to any number of devices via email. To use this option an SMTP server must be configured in the server settings.

[Configure server settings](#)

☒ Individual enrollment via link or QR code

Enroll devices one at a time. You need physical access to the devices. Not recommended for large numbers of devices.

☐ Individual enrollment as a Device Owner (only Android 7 and above)

Activation is supported only on Android N (7.0) and above. Device Owner supports additional management features.

CONTINUE

CANCEL

2. **デバイス名** – モバイルデバイスの**名前**(この名前は [コンピューター](#) のリストに表示されます)と**説明**(任意)を入力します。

3. **ユーザー(任意)** – ユーザーにモバイルデバイスを割り当てることをお勧めします。これはiOSデバイスでは必須ですがAndroidでは任意です。

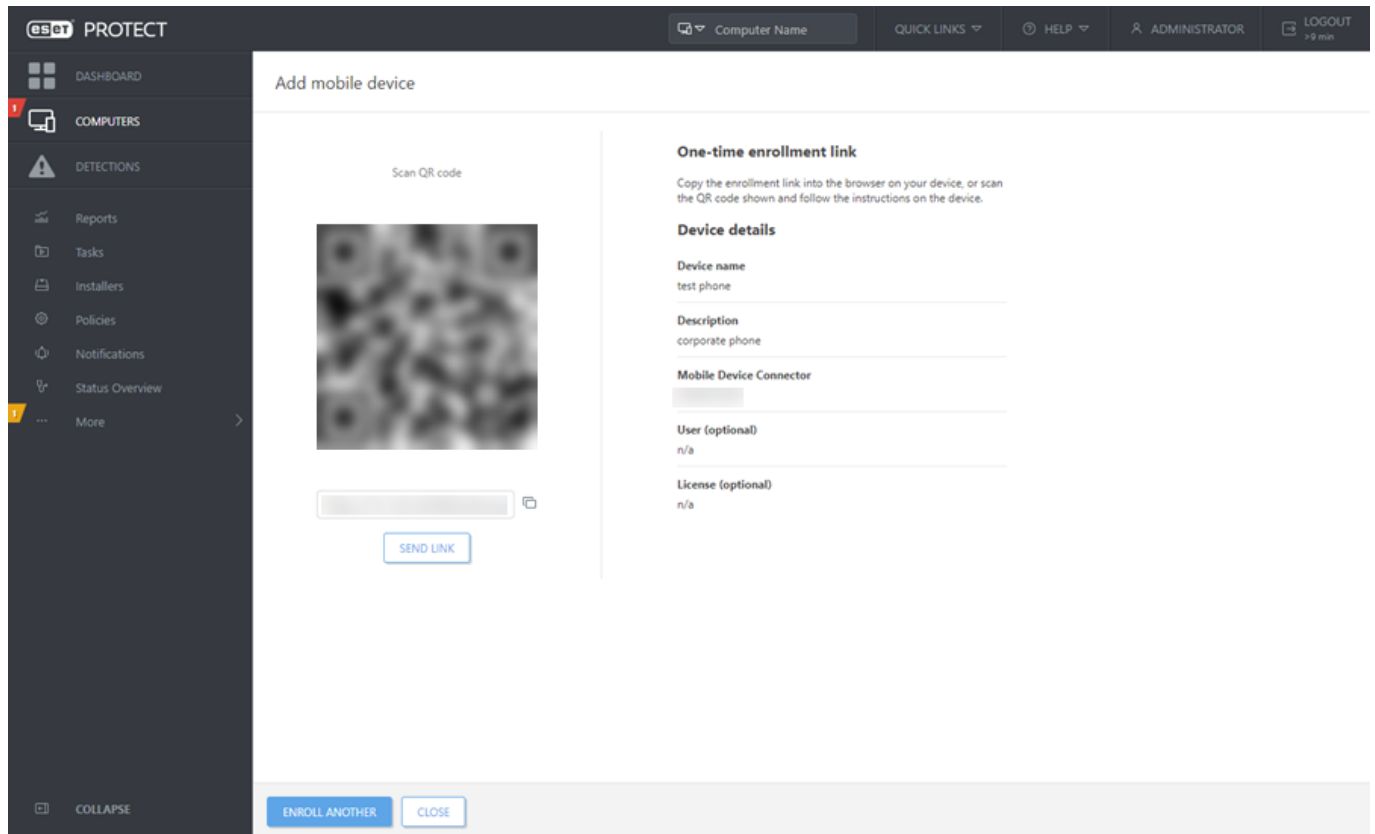
4. **モバイルデバイスコネクタ** – 自動的に選択されます。複数のMDCがある場合は、FQDNをクリックしてリストから選択します。モバイルデバイスコネクタがまだインストールされていない場合は、インストール手順について、本ガイドの「[モバイルデバイスコネクタインストール-Windows](#)」または「[Linux](#)」の章を参照してください。

5. **ライセンス(任意)** - **選択**をクリックして、アクティベーションで使用するライセンスを選択します。製品のアクティベーションクライアントタスクがモバイルデバイス用に作成されます。ライセンス単位が取得されます(各モバイルデバイスに1つ)。

6. **親グループ** – モバイルデバイスの特定の静的グループがない場合は、**新しい静的グループ**(モバイルデバイスなど)を作成することをお勧めします。既存のグループがある場合は、**/すべて**をクリックすると、ポップアップウィンドウが開き、静的グループを選択できます。

7. **[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。詳細については、[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](#)を参照してください。

8. **次へ**をクリックすると、**登録リンク(URL)**と**QRコード**が表示されます。URL全体をモバイルデバイスのWebブラウザに手動で入力(たとえば <https://eramdm:9980/token>。トークンは各モバイルデバイスで異なります)するか、このURLを他の手段でモバイルデバイスに送信します。あるいは、提供された**QRコード**を使用できます。これはURLを入力するよりも便利ですがQRコードリーダー/スキャナーがモバイルデバイスに必要です。



9.別のモバイルデバイスを追加するには、**別のデバイスの登録**をクリックします。[モバイルデバイスの新規追加]ページが開き、[一般]セクションの前の選択が記憶されています。デバイス名を入力し、ユーザーを割り当ててから、**次へ**をクリックして、手順7に従います。登録URLとQRコードの生成が完了したら、**閉じる**をクリックし、前のウィンドウに戻ります。

10. モバイルデバイスの実際の登録を実行するには、次の段階的な手順に従います。

o [Androidデバイス登録](#)

o [iOSデバイス登録](#)

デバイス所有者としての個別の登録

登録QRコードを使用してモバイルデバイスを登録する場合は、Androidデバイスへの物理的なアクセスが必要です。また、この登録は、ワイプ/初期状態リセット後のデバイスまたは新しいすぐに使える状態のデバイスでのみ可能です。

i デバイス所有者としてのAndroidデバイスの一括登録では、[電子メールでの登録](#)を使用できません。

1.新しいモバイルデバイスを追加するには、**コンピューター**セクションまたは**詳細 > グループ**に移動します。モバイルデバイスを追加する**静的グループ**を選択し、**新規追加 > モバイルデバイス > デバイス所有者として個別に登録(Android 7以上のみ)**をクリックします。

Add mobile devices

☐ Enrollment via email

Send enrollment link to any number of devices via email. To use this option an SMTP server must be configured in the server settings.

[Configure server settings](#)

☐ Individual enrollment via link or QR code

Enroll devices one at a time. You need physical access to the devices. Not recommended for large numbers of devices.

☒ Individual enrollment as a Device Owner (only Android 7 and above)

Activation is supported only on Android N (7.0) and above. Device Owner supports additional management features.

CONTINUE

CANCEL

2. **デバイス名** – モバイルデバイスの**名前**(この名前は [コンピューター](#) のリストに表示されます)を入力します。

3. **ユーザー(任意)** – ユーザーにモバイルデバイスを割り当てることをお勧めします。これはiOSデバイスでは必須ですがAndroidでは任意です。

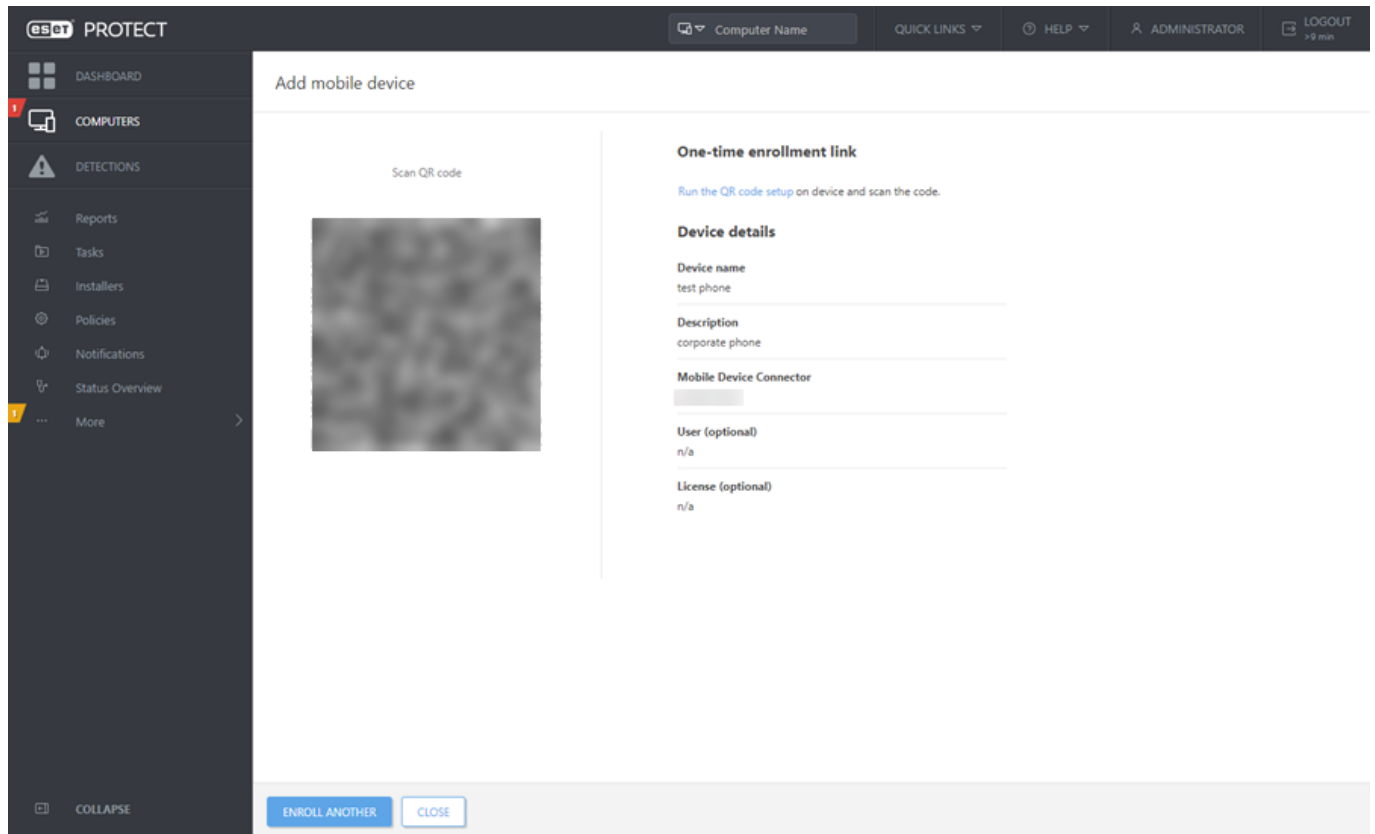
4. **モバイルデバイスコネクタ** – 自動的に選択されます。複数のMDCがある場合は、FQDNをクリックしてリストから選択します。モバイルデバイスコネクタがまだインストールされていない場合は、インストール手順について、本ガイドの「[モバイルデバイスコネクタインストール - Windows](#)」または「[Linux](#)」の章を参照してください。

5. **ライセンス(任意)** - **選択**をクリックして、アクティベーションで使用するライセンスを選択します。製品のアクティベーションクライアントタスクがモバイルデバイス用に作成されます。ライセンス単位が取得されます(各モバイルデバイスに1つ)。

6. **親グループ** – モバイルデバイスの特定の静的グループがない場合は、**新しい静的グループ**(モバイルデバイスなど)を作成することをお勧めします。既存のグループがある場合は、**/すべて**をクリックすると、ポップアップウィンドウが開き、静的グループを選択できます。

7. **[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。詳細については、[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](#)を参照してください。

8. **次へ**をクリックすると、**登録QRコード**が表示されます。



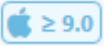
9. Androidデバイスで [これらの](#) 手順に従い、登録処理を実行します。


10. 別のモバイルデバイスを追加するには、**別のデバイスの登録**をクリックします。[モバイルデバイスの新規追加]ページが開き、[一般]セクションの前の選択が含まれています。デバイス名を入力し、ユーザーを割り当ててから、**次へ**をクリックして、手順7に従います。登録QRコードの生成が完了したら、**閉じる**をクリックし、前のウィンドウに戻ります。

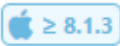
iOS MDMのポリシーの作成 - Exchange ActiveSyncアカウント

このポリシーはiOSデバイスのすべての設定を統制します。これらの設定は、ABMおよび非ABM iOSデバイスの両方に適用されます。

- ABMのみの設定はABMアイコン  で示されます。これらの設定はApple ABMポータルで登録されたiOSデバイスにのみ適用されます。非ABM iOSデバイスのポリシーを作成するときには、これらのABM専用設定をカスタマイズしないことをお勧めします。
- 一部の設定は特定のバージョンのiOSのiOSデバイスでのみ適用できます。これらの設定はiOSバージョンを表すアイコンで示されます。

o iOSバージョン9.0以上 

o iOSバージョン9.3以上 

o iOSバージョン8.1.3以上 

iOSバージョン11.0以上



- 両方のアイコン(ABMアイコンとiOSバージョンアイコン)は特定の設定の横に表示されます。デバイスは両方の要件を満たす必要があります。そうでないと、設定の管理が失敗します。

Microsoft Exchange Mailアカウントを設定するときには、iOS MDMポリシーを使用する方法を説明する以下のサンプルシナリオを参照してください。

このポリシーを使用して、ユーザーのiOSモバイルデバイスのMicrosoft Exchange メールアカウント、連絡先、カレンダーを構成できます。このようなポリシーを使用する利点は、各デバイスのポリシーを個別に設定せずに、複数のiOSモバイルデバイスに適用できるポリシーを1つ作成すればよいという点です。これはActive Directoryユーザー属性を使用して実現されます。`${exchange_login/exchange}`などの変数を指定する必要があります。これは、特定のユーザーのADの値に置換されます。

Microsoft ExchangeまたはExchange ActiveSyncを使用していない場合は、各サービス(メールアカウント、連絡先アカウント、LDAPアカウント、カレンダーアカウント、登録されたカレンダーアカウント)を手動で構成できます。

次に、新しいポリシーを作成して適用し、Exchange ActiveSync (EAS)プロトコルを使用してiOSモバイルデバイスで各ユーザーのメール、連絡先、カレンダーを自動的に設定し、これらのサービスを同期する方法の例を示します。

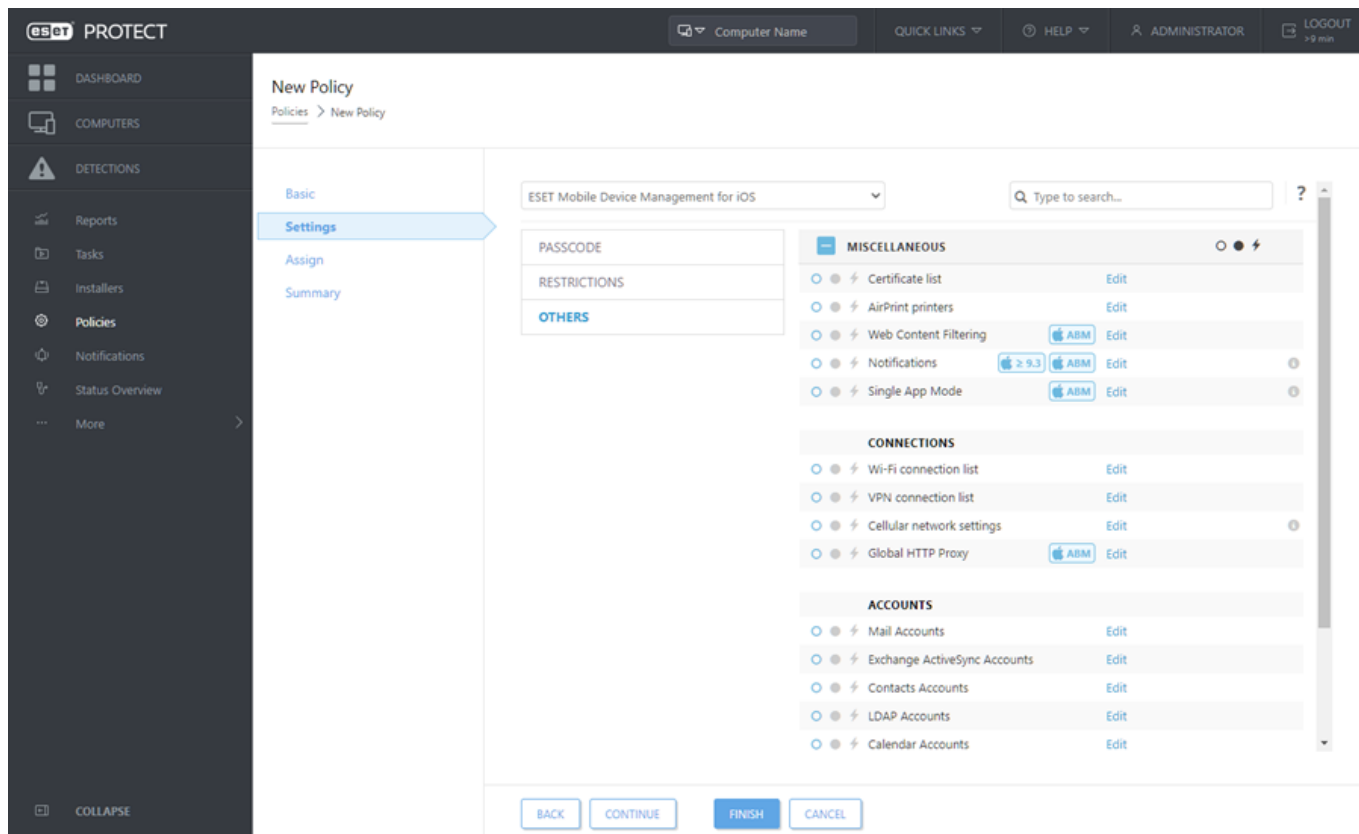
i これらのポリシーを設定する前に、[モバイルデバイス管理](#)で説明されている手順を実行してください。

基本

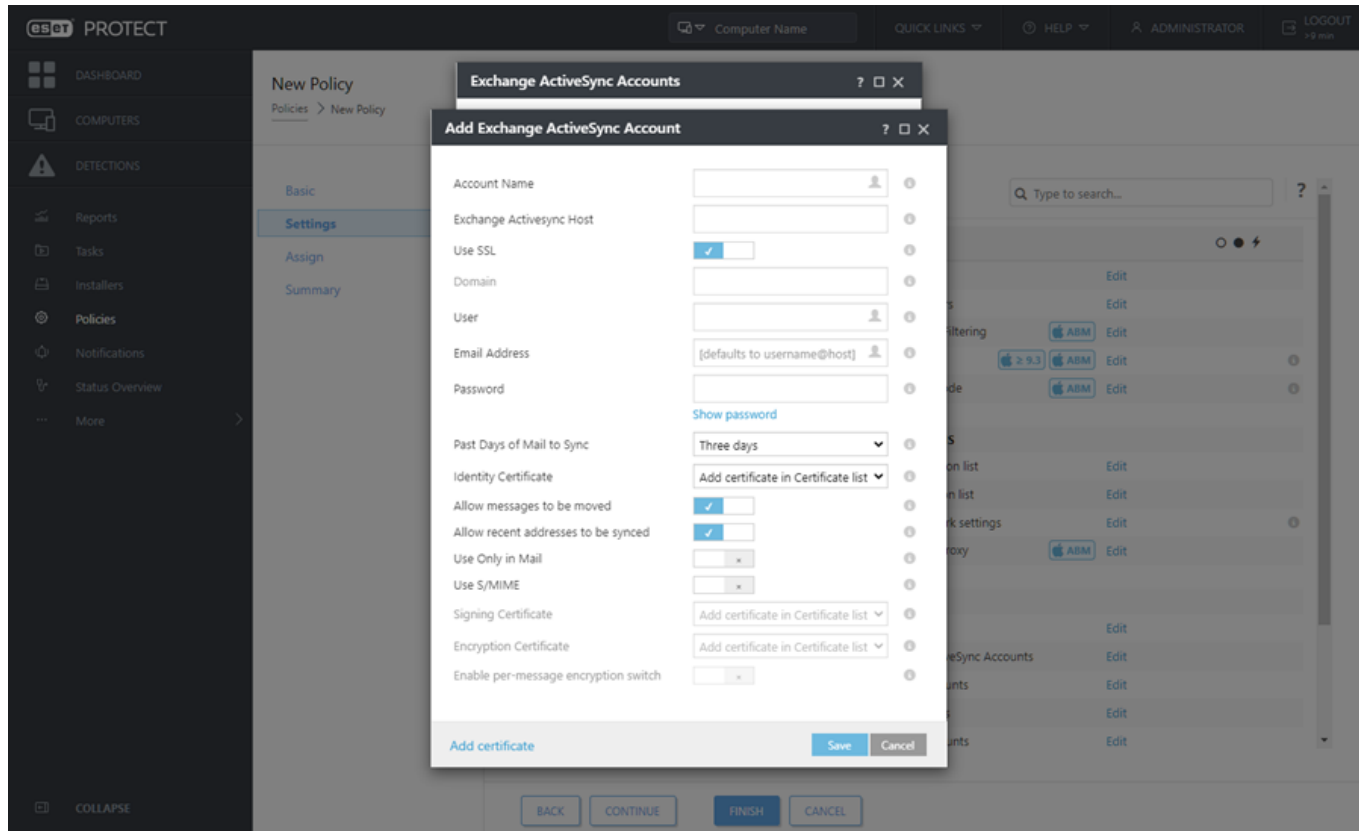
このポリシーの**名前**を入力します。[説明]フィールドは任意です。

設定

ドロップダウンメニューから**ESET MDM for iOS/iPadOS**を選択し、**その他**をクリックしてカテゴリを展開し、**Exchange ActiveSync アカウントの横にある編集**をクリックします。



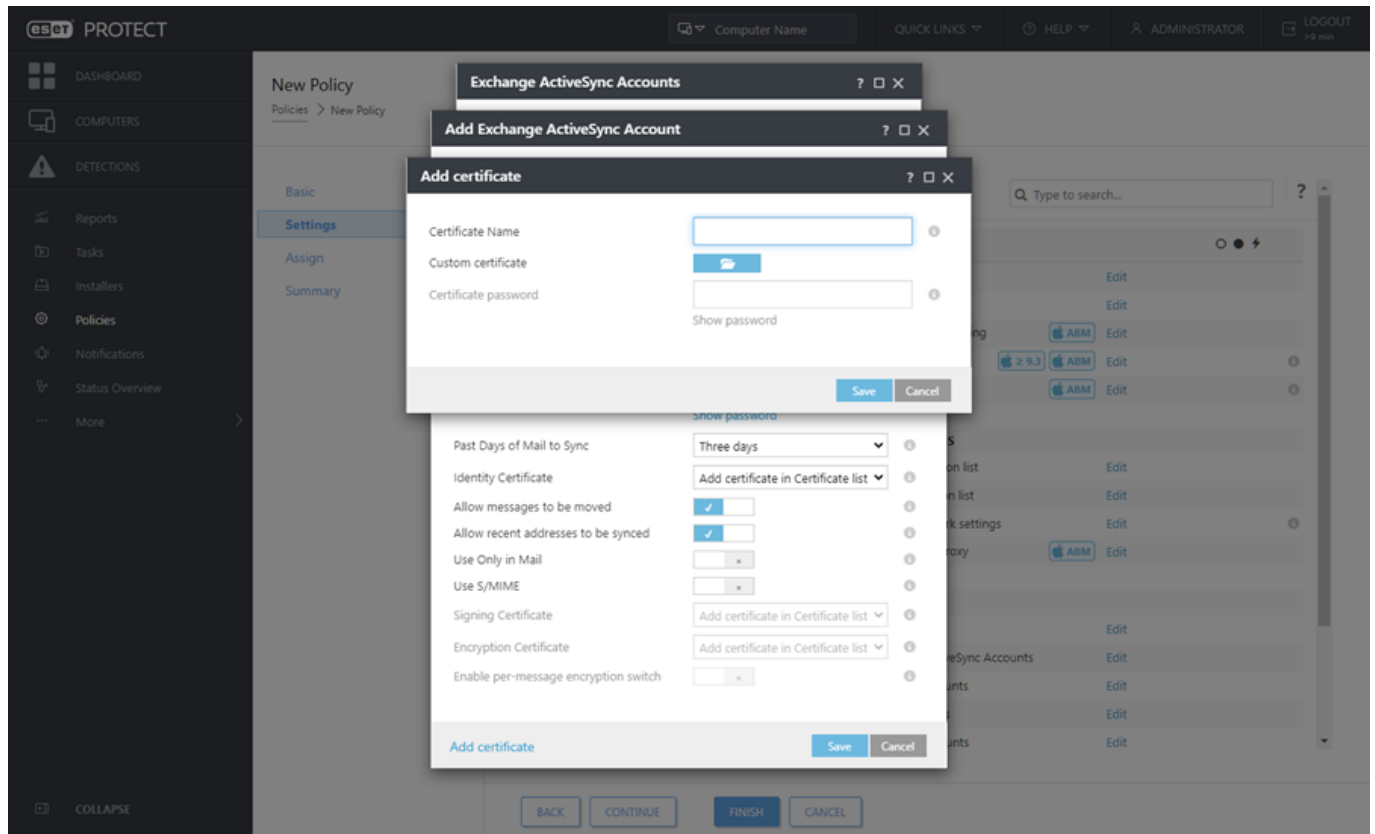
[追加]をクリックしてExchange ActiveSyncアカウントの詳細を指定します。ユーザーやメールアドレスなど、特定のフィールドで変数を使用できます(ドロップダウンリストから選択)。これらの変数は、ポリシーが適用されるときに、コンピューターユーザーの実際の値で置換されます。



- **アカウント名** - Exchangeアカウントの名前を入力します。
- **Exchange ActiveSyncホスト** - Exchangeサーバーのホスト名またはIPアドレスを指定します。

- **SSLを使用** – このオプションは、既定では有効になっています。Exchangeサーバーが認証でSecure Sockets Layer (SSL)を使用するかどうかを指定します。
- **ドメイン** – このフィールドは任意です。このアカウントが属するドメインを入力できます。
- **ユーザー** - Exchangeログイン名。ドロップダウンリストから該当する変数を選択し、各ユーザーのActive Directoryから属性を使用します。
- **電子メールアドレス** – ドロップダウンリストから該当する変数を選択し、各ユーザーのActive Directoryから属性を使用します。
- **パスワード** – 任意。このフィールドを空欄にすることをお勧めします。空欄にする場合、ユーザーが独自のパスワードを作成する必要があります。
- **メールを同期する過去の日数** – ドロップダウンリストからメールを同期する過去の日数を選択します。
- **ID証明書**- ActiveSyncに接続するための認証情報。
- **メッセージの移動を許可** – 有効な場合、アカウント間でメッセージを移動できます。
- **最近のアドレスの同期を許可** – このオプションが有効な場合、ユーザーは最近使用したアドレスをデバイス間で同期できます。
- **メールでのみ使用** – メールアプリのみがこのアカウントから電子メールメッセージを送信することを許可する場合は、このオプションを有効にします。
- **S/MIMEを使用** – 送信メールメッセージでS/MIME暗号化を使用する場合は、このオプションを有効にします。
- **署名証明書** - MIMEデータを署名するための認証資格情報。
- **暗号化証明書** - MIMEデータを暗号化するための認証資格情報。
- **メッセージ単位の暗号化切り替えを有効にする** – ユーザーは各メッセージを暗号化するかどうかを選択できます。

i 値を指定せずフィールドを空欄にする場合、モバイルデバイスユーザーがこの値を入力する必要があります。たとえば、**Password**です。

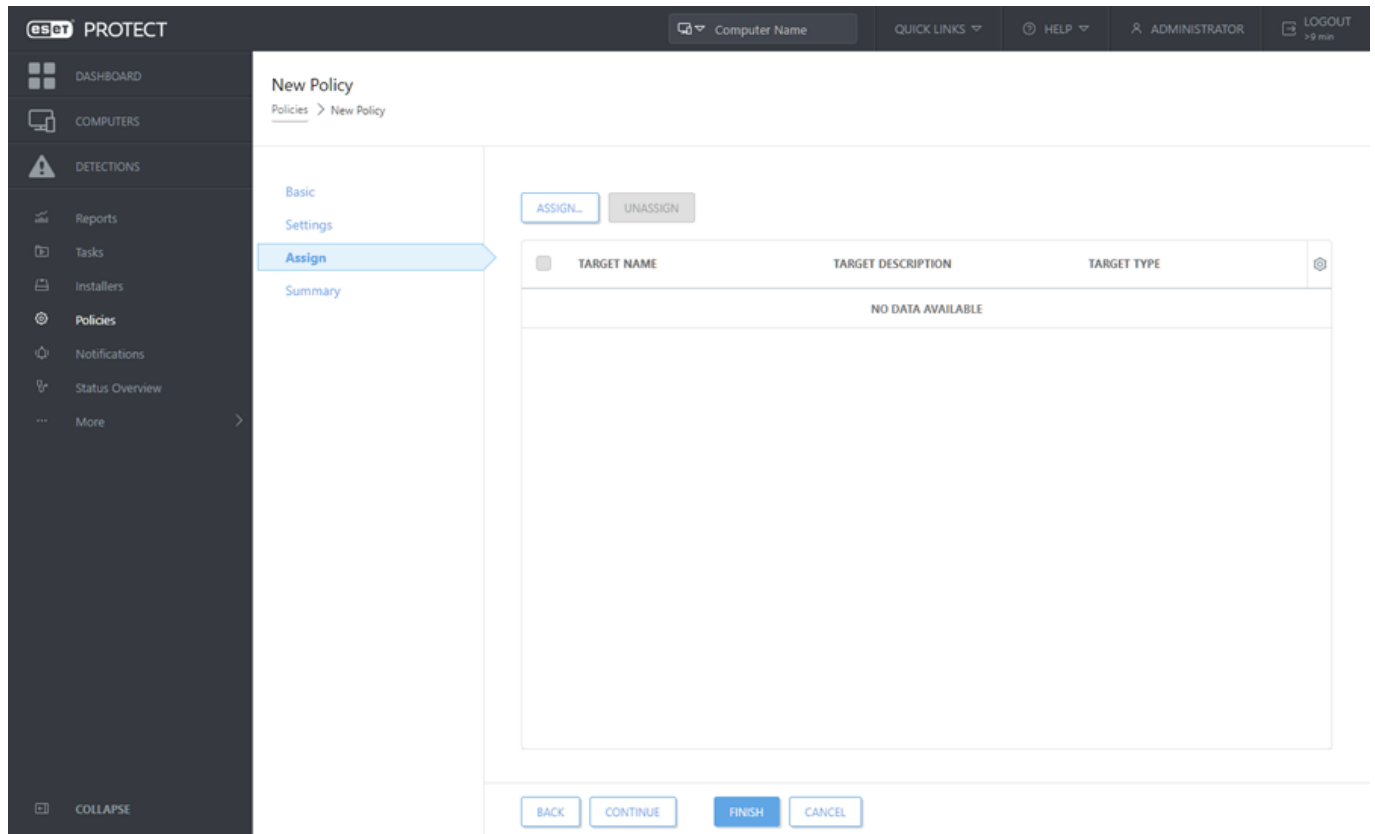


- 証明書の追加 – 必要に応じて、特定のExchange証明書(ユーザIDデジタル署名、暗号化証明書)を追加できます。

i 必要に応じて、上記の手順を使用し、複数のExchange ActiveSyncアカウントを追加できます。このように、1台のモバイルデバイスで複数のアカウントが構成されます。また、必要に応じて、既存のアカウントを編集できます。

割り当て

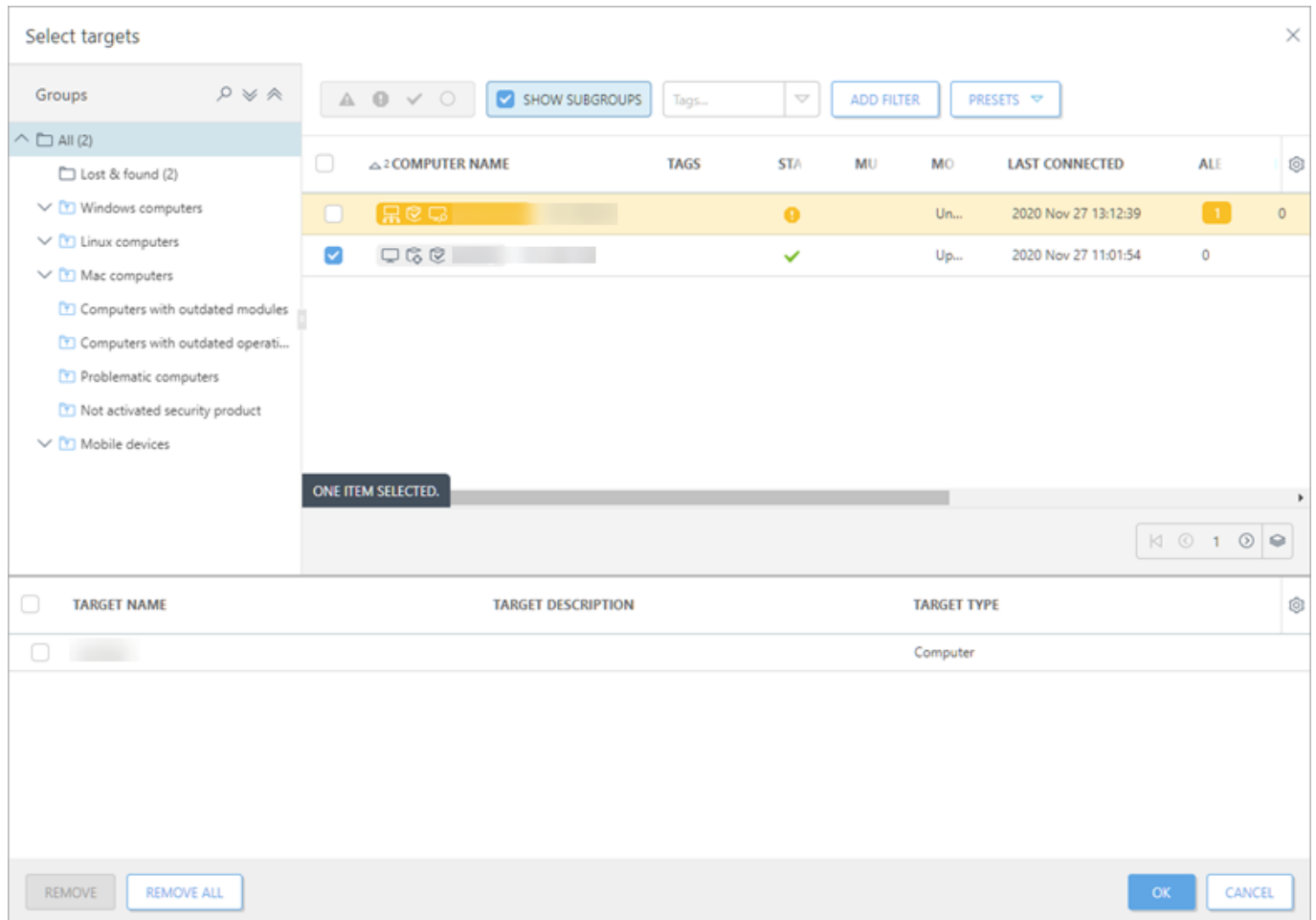
このポリシーを受信するクライアント(個別のコンピューター/モバイルデバイスまたはグループ全体)を指定できます。



[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。任意のコンピューターまたはグループを選択し、**OK**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、**Web**コンソールの速度低下を防止します。
多数のコンピューターを選択すると**Web**コンソールに警告が表示されます。



概要

このポリシーの設定を確認し、[完了]をクリックします。ポリシーは、次回ESET PROTECTサーバーに接続した後にターゲットに適用されます(エージェント接続間隔によって異なります)。

MDCのポリシーを作成してiOS登録でAPN/ABMを有効にする

MDCのポリシーで使用されるHTTPS証明書を変更するときには、以下の手順に従い、MDMからモバイルデバイスが切断されないようにします。

1. 新しいHTTPS証明書を使用する新しいポリシーを作成して適用します。
2. デバイスがMDMサーバーにチェックインし、新しいポリシーを受信できるようにします。
3. デバイスが新しいHTTPS証明書を使用していることを確認します(HTTP証明書交換が完了します)。
4. デバイスが新しいポリシーを受信するには、72時間以上かかります。すべてのデバイスが新しいポリシーを受信した後(MDMコアアラート「HTTPS証明書変更を実行中です。古い証明書がまだ使用中です」がアラートタブに表示されなくなります)、古いポリシーを削除できます。

次に、ESETモバイルデバイスコネクタでAPNS (Apple Push Notification Services)およびiOSデバイス登録プログラム機能を有効にするための新しいポリシーを作成する方法の例を示します。これは[iOSデバイス登録](#)が必要です。このポリシーを構成する前に、[新しいAPN証明書を作成](#)し、Apple Push Certificates PortalでApple社からの署名を受け、署名証明書またはAPNS証明書とする必要があります。段階的な手順については、「[APN 証明書](#)」セクションを参照してください。

基本

このポリシーの**名前**を入力します。[説明]フィールドは任意です。

設定

ドロップダウンリストから**[ESETモバイルデバイスコネクタ]**を選択します。

オールインワンインストーラーを使用して(スタンドアロンやコンポーネントとしてではなく)MDMサーバーをインストールした場合、HTTPS証明書はインストール中に自動的に生成されます。他のすべての場合、カスタムHTTPS証明書を適用する必要があります。[モバイルデバイス管理トピック](#)の手順1に従い、注釈の情報を参照してください。

ESET PROTECT証明書(ESET PROTECT CAが署名)またはカスタム証明書を使用できます。また、**強制証明書変更**の日付を指定できます。詳細については、この設定の横のツールチップをクリックしてください。

i Organization文字列に実際の組織名を入力します。これは、プロファイルにこの情報を含めるために、登録プロファイル生成機能によって使用されます。

HTTPS certificate

Peer certificate

☒ ESET management certificate
☐ Custom certificate

ESET management certificate Open certificate list

Custom certificate

Certificate password

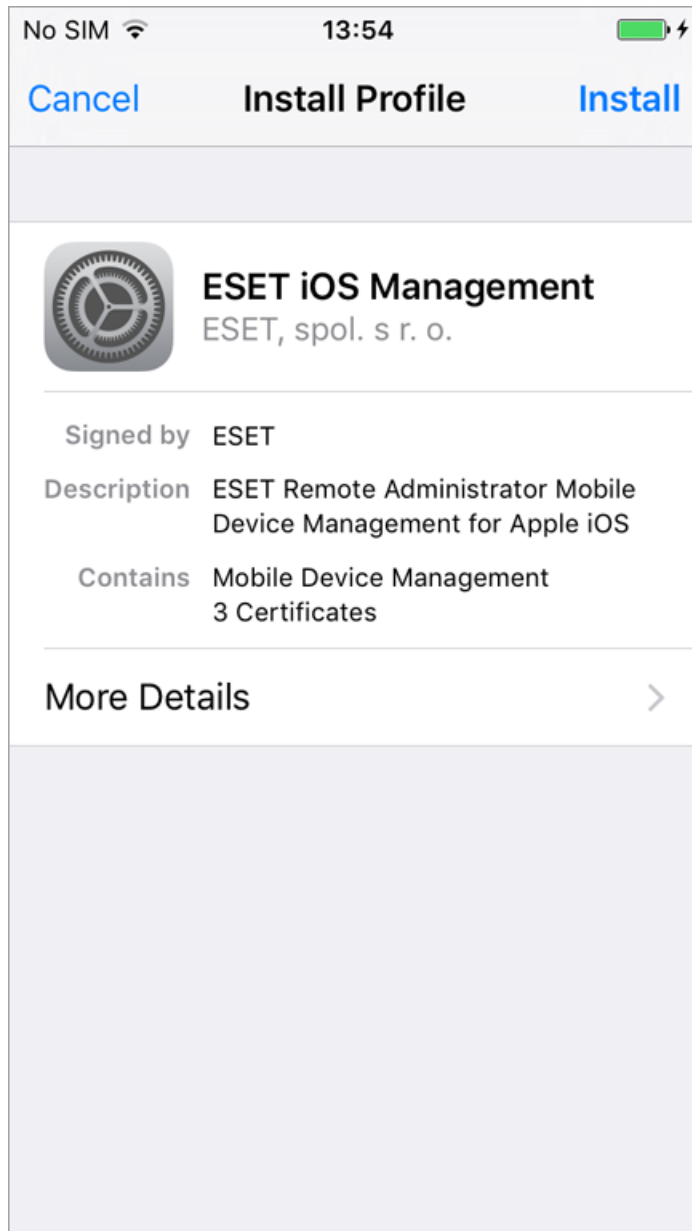
Show password

Force certificate change on

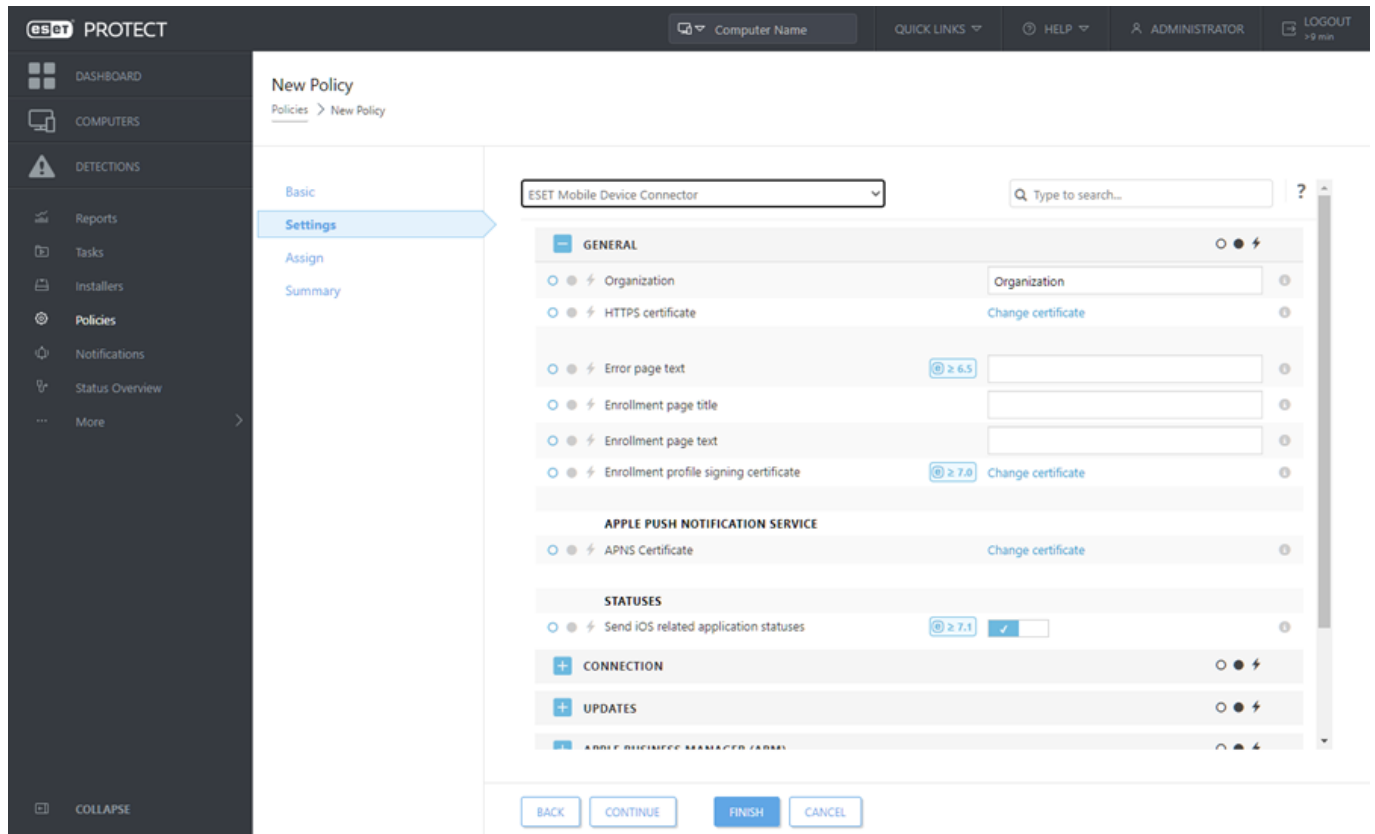
Warning! All devices that do not connect by this date will need to be re-enrolled manually! Changing the certificate in MDC version 6.4 will cause all devices to de-enroll.

OK Cancel

一般の下で、登録用のHTTPS証明書を**登録プロファイル署名証明書**に任意でアップロードできます(これは非ABM登録にのみ影響します)。これにより、登録処理中にアクセスするiOSデバイスの登録ページに署名し、証明書に基づくファイルで署名に表示されます。

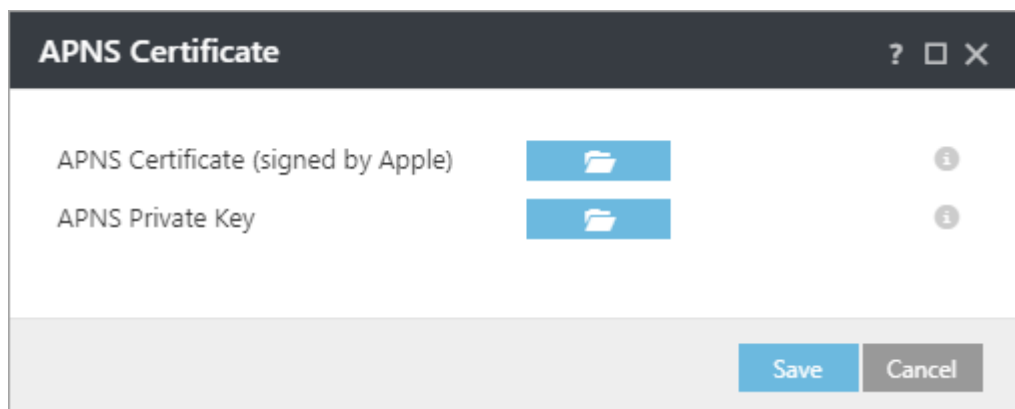


IOS登録のApple証明書をアップロード - [APPLEプッシュ通知サービス]に移動し、APNS証明書とAPNS秘密鍵をアップロードします。



APNS証明書(Apple社が署名) – フォルダーアイコンをクリックし、APNS証明書を参照してアップロードします。このAPNS証明書はApple Push Certificatesポータルからダウンロードされるファイルです。


APNS秘密鍵 – フォルダーアイコンをクリックし、APNS秘密鍵を参照してアップロードします。APNS秘密鍵は[APN/ABM証明書](#)作成中にダウンロードしたファイルです。



製品改善プログラム – クラッシュレポートおよび匿名のテレメトリデータのESETへの送信を有効または無効にできます。

ロギング>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。

Apple ABMでiOS登録用にこのポリシーを作成している場合は、**Apple Business Manager (ABM)**に移動します。

Apple Business Manager (ABM) – これらの設定はABM専用です。 



初期設定の後、これらの設定のいずれかが変更される場合、初期状態にリセットし、影響を受けるすべてのiOSデバイスを再登録して変更を適用する必要があります。

認証トークンのアップロード – フォルダーアイコンをクリックし、ABMサーバートークンを参照します。ABMサーバートークンは、Apple ABMポータルで仮想MDMサーバーを作成したときにダウンロードしたファイルです。

必須インストール – ユーザーはMDMプロファイルをインストールせずにデバイスを使用できません。

ユーザーがMDMプロファイルを削除することを許可する – ユーザーがMDMプロファイルを削除することを禁止するには、デバイスが監視モードである必要があります。

ドメインログインが必要 – ユーザーはデバイスセットアップウィザードで有効なドメイン資格情報を入力する必要があります。

セットアップ項目のスキップ – この設定により、初期iOSセットアップ中にスキップされる初期セットアップステップを選択できます。各ステップの詳細については、[Appleナレッジベース記事](#)を参照してください。

割り当て

ポリシーの対象となるMDMサーバーをホストするデバイスを選択します。

[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。ポリシーを適用するモバイルデバイスコネクタインスタンスを選択し、[OK]をクリックします。

概要

このポリシーの設定を確認し、[完了]をクリックします。

iOSおよびWi-Fi接続で制限を適用するポリシーの作成

iOSモバイルデバイスのポリシーを作成し、特定の制限を適用できます。また、複数のWi-Fi接続を定義し、たとえばユーザーが自動的に別のオフィスロケーションの企業Wi-Fiネットワークに接続させることができます。同じことが[VPN接続](#)に当てはまります。

iOSモバイルデバイスに適用できる制限はカテゴリに一覧表示されます。たとえばFaceTimeとカメラの使用を無効にしたり、特定のiCloud機能を無効にしたり、セキュリティとプライバシーオプションを微調整したり、選択したアプリケーションを無効にできます。

i 適用できる制限とできない制限は、クライアントデバイスによって使用されるiOSのバージョンによって異なります。iOS 8.x以降がサポートされます。

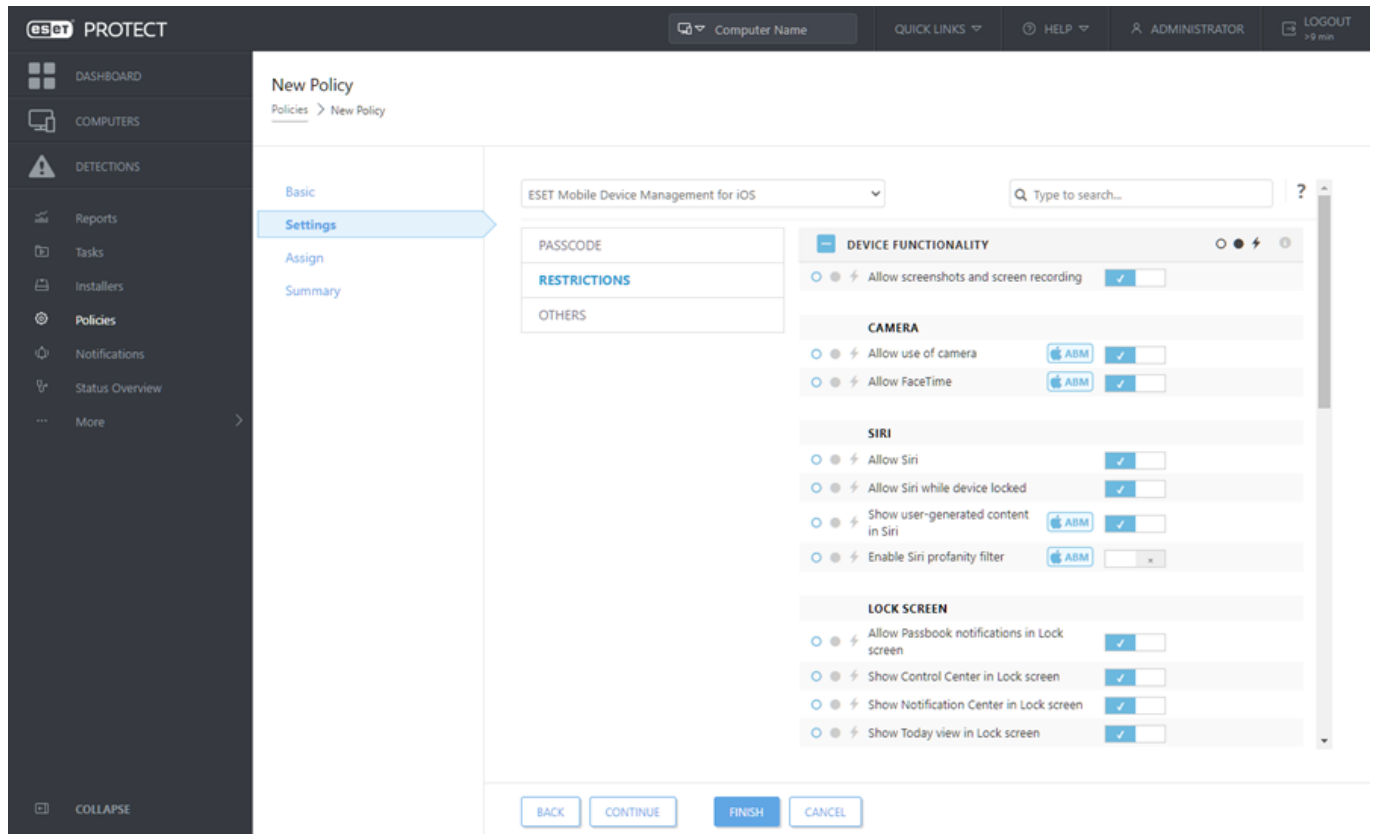
次に、カメラとFaceTimeアプリを無効にしWi-Fi接続詳細を一覧に追加して、ネットワークが検出されるたびにiOSモバイルデバイスをWi-Fiネットワークに接続させる方法の例を示します。自動参加オプションを使用する場合は、iOSモバイルデバイスが既定でネットワークに接続します。ポリシー設定は、ユーザーが手動で選択したWi-Fiネットワークを上書きします。

基本

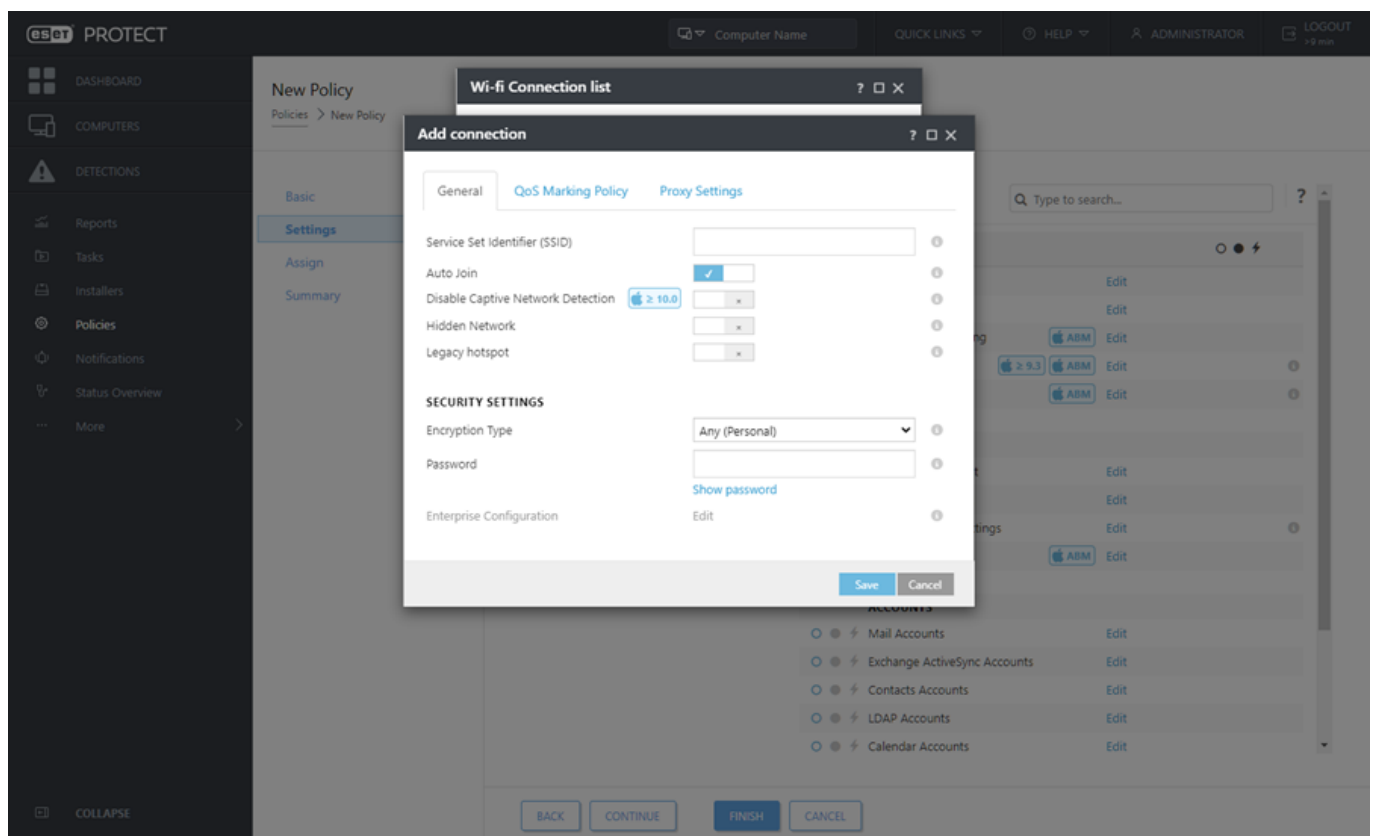
このポリシーの**名前**を入力します。[説明]フィールドは任意です。

設定

[ESET MDM for iOS & iPadOS]を選択し、[制限]をクリックしてカテゴリを表示します。[カメラの使用を許可]の横のスイッチを使用して無効にします。カメラが無効になるためFaceTimeも自動的に無効になります。FaceTimeのみを無効にする場合は、カメラを有効にし、[FaceTimeを許可]の横のスイッチを使用して無効にします。



制限を構成した後に、[その他]をクリックしてから、**Wi-Fi接続リスト**の横の[編集]をクリックします。Wi-Fi接続のリストがあるウィンドウが開きます。[追加]をクリックして、追加するWi-Fiネットワークの接続詳細情報を指定します。[保存]をクリックします。



- **Service Set Identifier (SSID)** – 使用されるWi-FiネットワークのSSID
- **自動参加** – 任意(既定では有効)。デバイスが自動的にこのネットワークに参加します。

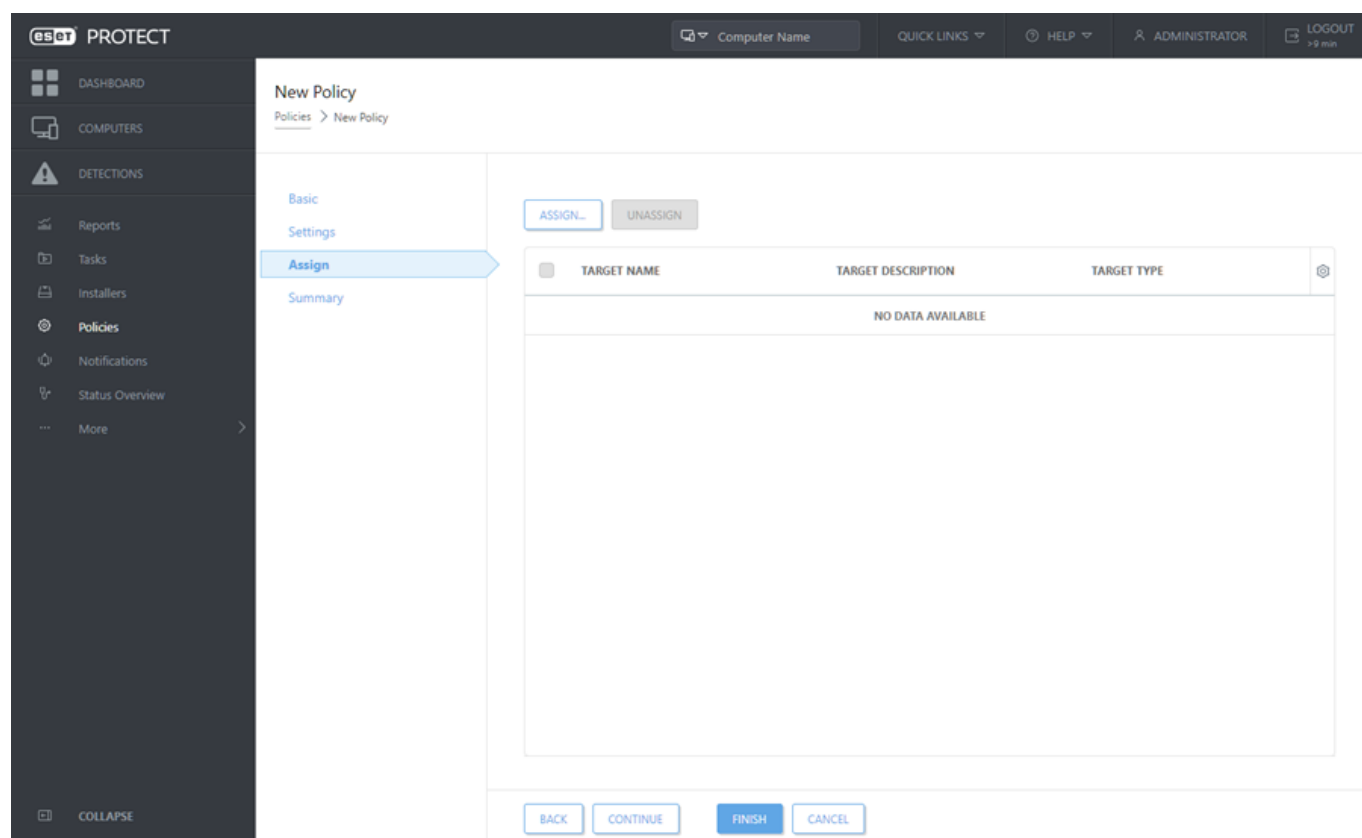
セキュリティ設定:

- **暗号化タイプ** - ドロップダウンリストから該当する暗号化を選択し、この値がWi-Fiネットワークの機能と正確に一致することを確認します。
- **パスワード** - Wi-Fi ネットワークに接続するときに認証で使用するパスワードを入力します。

プロキシ設定 - 任意。ネットワークがプロキシを使用する場合は、値を指定します。

割り当て

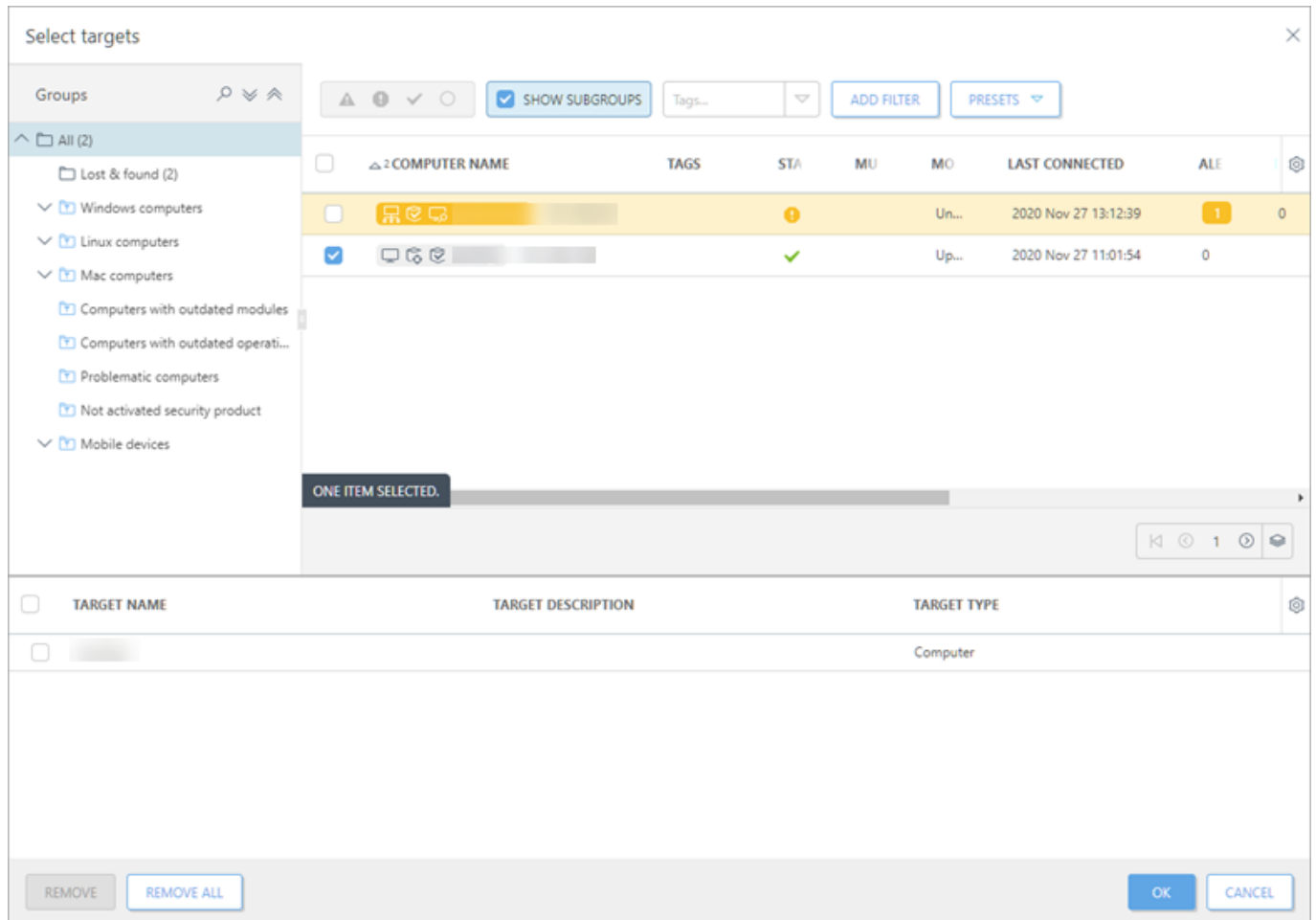
このポリシーを受信するクライアント(個別のコンピューター/モバイルデバイスまたはグループ全体)を指定できます。



[割り当て]をクリックすると、すべての静的および動的グループと、そのメンバーが表示されます。任意のコンピューターまたはグループを選択し、**OK**をクリックします。



グループのすべてのコンピューターを割り当てるには、個別のコンピューターではなくグループを割り当て、Webコンソールの速度低下を防止します。
多数のコンピューターを選択するとWebコンソールに警告が表示されます。



概要

このポリシーの設定を確認し、[完了]をクリックします。ポリシーは、次回ESET PROTECTサーバーに接続した後にターゲットに適用されます(エージェント接続間隔によって異なります)。

MDM構成プロファイル

プロファイルを構成し、管理されたモバイルデバイスでポリシーと制限を適用できます。

プロファイル名	簡単な説明
パスコード	アイドル状態から復帰するたびに、エンドユーザーはパスコードでデバイスを保護する必要があります。これにより、管理されたデバイスの機密企業情報が確実に保護されます。複数のプロファイルが1つのデバイスでパスコードを適用する場合は、最も厳しいポリシーが適用されます。
制限	制限プロファイルは、デバイス機能、アプリケーション@iCloud@セキュリティ、およびプライバシーに関連付けられた特定の権限の使用を制限し、管理されたデバイスのユーザーが使用できる機能を制限します。
Wi-Fi接続リスト	Wi-Fiプロファイル は企業Wi-Fi設定を管理されたデバイスに直接プッシュし、すぐにアクセスできるようにします。

プロファイル名	簡単な説明
VPN接続リスト	VPNプロファイルは企業の仮想プライベートネットワーク設定を企業デバイスにプッシュし、ユーザーはリモートロケーションから安全に企業インフラストラクチャにアクセスできます。 接続名 – デバイスに表示される接続名を表示します。 接続タイプ – このプロファイルで有効にされる接続のタイプを選択します。各接続タイプにより異なる機能が有効になります。 サーバー – 接続中のサーバーのホスト名またはIPアドレスを入力します。
メールアカウント	管理者はIMAP/POP3電子メールアカウントを構成できます。
Exchange ActiveSyncアカウント	Exchange ActiveSync プロファイルにより、エンドユーザーは企業のプッシュベースの電子メールインフラストラクチャにアクセスできます。あらかじめ入力されたルックアップ値フィールドとオプションがあり、iOS 5以上にのみ適用されます。
CalDAV - カレンダーアカウント	CalDAVには構成オプションがあり、エンドユーザーはエンタープライズCalDAVサーバーとワイヤレスで同期できます。
CardDAV - 連絡先アカウント	このセクションでは、CardDAVサービスの固有の構成ができます。
登録されたカレンダーアカウント	登録されたカレンダーはカレンダー構成を提供します。

OSアップデート管理

ESET Endpoint Security for Androidを使用すると、管理者は管理対象のAndroidデバイスでAndroid OSのアップデートを管理できます。

i この機能では、ESET Endpoint Security for Androidバージョン3.0が必要です。また、Androidデバイスをデバイス所有者モードで登録する必要があります。

管理されたデバイスでOSアップデートを管理するには、新しいポリシーを作成します。

1. [管理] > [ポリシー] > [新規ポリシー]をクリックします。
2. 設定で、**ESET Endpoint Security for Android (2+)**を選択します。
3. デバイスセキュリティで、デバイスセキュリティを選択し、デバイスセキュリティを有効にする設定を有効にします。
4. OS管理機能を有効にするには、システムアップデート管理に移動し、システムアップデートの管理を有効にします。

このセクションでは、管理されたAndroidデバイスで更新されたAndroid OSの異なるルールを設定できます。

• システムアップデートポリシー:

- o **自動:**Android OSアップデートは遅延なく実行されます。
- o **時間帯設定:**Android OSアップデートは、毎日のメンテナンスウィンドウ設定で指定されたメンテナンス期間にのみ実行されます。
- o **30日間延期されました:**Android OSアップデートはリリース日の30日後に実行されます。

- **毎日のメンテナンスウィンドウ:**管理されたAndroidデバイスでOSアップデートが実行される特定の時間を設定します。
- **フリーズ期間:**デバイスをアップデートできない複数の期間を指定します。

MDMトラブルシューティング

MDMCore設定とログファイル

[他のESET PROTECTコンポーネントのログファイル](#)も参照してください。

ロケーション	ファイルの詳細
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Configuration Linux: /etc/opt/eset/RemoteAdministrator/MDMCore	<ul style="list-style-type: none"> • startupconfiguration.ini (Windows)startupconfiguration.ini (Linux) - データベース接続情報。 • loggerLevel.cfg - ロギングの上書きログレベルを指定する1行。このファイルはどのポリシーの設定よりも優先されます(ポリシーを配信できない場合に使用できます)。認識されると、行「Setting log level from loggerLevel.cfg override file to XYZ」がトレースログに出力されます(情報レベル)。認識される値: alltracedebuginformationwarningerrorcriticalfatalallに設定すると、電話のすべての通信もログに記録されます。 • shouldLogPhoneComm.cfg - 電話との通信を別のログファイルに記録するかどうかを指定する1行。認識された値: 1truelog • skipPnsCertCheck.cfg - PNSサービス証明書を検証するかどうかを指定する1行。
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Data\MultiAgent Linux: /var/opt/eset/RemoteAdministrator/MDMCore/MultiAgent	エージェント単位のサブフォルダーの個別のエージェントのトレースログ。
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Dumps Linux: /var/opt/eset/RemoteAdministrator/MDMCore/Dumps	ESET CrashReportingサービスにまだ送信されていないクラッシュダンプ。
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs Linux: /var/log/eset/RemoteAdministrator/MDMCore	<ul style="list-style-type: none"> • trace.logtrace.log.<N>.gz - MDMCoreのトレースログ。番号付きのgzip圧縮されたファイルはログの内容よりも古くなります。
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Logs\Proxy Linux: /var/log/eset/RemoteAdministrator/MDMCore/Proxy	<ul style="list-style-type: none"> • trace.logtrace.log.<N>.gz - MDMCoreのMultiProxyコンポーネントのトレースログ。番号付きのgzip圧縮されたファイルはログの内容よりも古くなります。
Windows: %ProgramData%\ESET\RemoteAdministrator\MDMCore\Modules Linux: /var/opt/eset/RemoteAdministrator/MDMCore/Modules	<ul style="list-style-type: none"> • em*.dat - 設定エンジンおよびローダーモジュール。
Windows: %ProgramFiles%\ESET\RemoteAdministrator\MDMCore Linux: /opt/eset/RemoteAdministrator/MDMCore	MDMCoreで必要なすべての実行ファイル。

MDMエラーメッセージ

- 1.エラーメッセージが表示される場合はどうすればよいのですか?「登録トークンは既に使用中であるか、無効です。」

古い登録トークンで再登録しようとしている可能性がありますWebコンソールで新しい登録トークンを作成し、それを使用してください。また、最初の再登録の直後に2番目の再登録を試みている可能性があります。再登録トークンが最初のトークンとは異なることを確認してください。そうでない場合は、数分間待機してから、新しい再登録トークンを再生成してください。

2. 「サービス証明書の検証が失敗しました」というエラーメッセージが表示される場合はどうすればよいですか。

このエラーメッセージは、APNSまたはFCMサービス証明書に問題があることを示します。これはMDMコアアラートの下の次の警告のいずれかとしてESET PROTECT Web コンソールに表示されます。

- FCMサービス証明書確認が失敗しました (0x00000000100001002)
- APNSサービス証明書確認が失敗しました (0x00000000100001000)
- APNSフィードバックサービス証明書確認が失敗しました (0x00000000100001004)

システムで正しい認証局があることを確認します：

- APNS認証局: **Entrust** 認証局は、gateway.push.apple.com:2195から証明書を検証する必要があります。
- APNSフィードバック認証局: **Entrust** 認証局は、feedback.push.apple.com:2196から証明書を検証する必要があります。
- FCM認証局: **GeoTrust Global CA**は、android.googleapis.com:443から証明書を検証する必要があります。

目的の認証局は、MDMホストコンピューターの証明書ストアに含まれる必要があります。Windowsシステムでは、「信頼できるルート証明書の管理」を検索できます。Linuxシステムでは、証明書の場所を使用しているディストリビューションによって異なります。証明書ストアの宛先の例：

- Debian/CentOS: `/usr/lib/ssl/cert.pem` `/usr/lib/ssl/certs`
- Red Hat: `/usr/share/ssl/cert.pem`, `/usr/share/ssl/certs`
- 通常、`openssl version -d` コマンドは任意のパスを返します。

目的の認証局がMDMコアが実行されているシステムにインストールされていない場合は、インストールします。インストールの後、ESET PROTECT MDCサービスを再起動します。



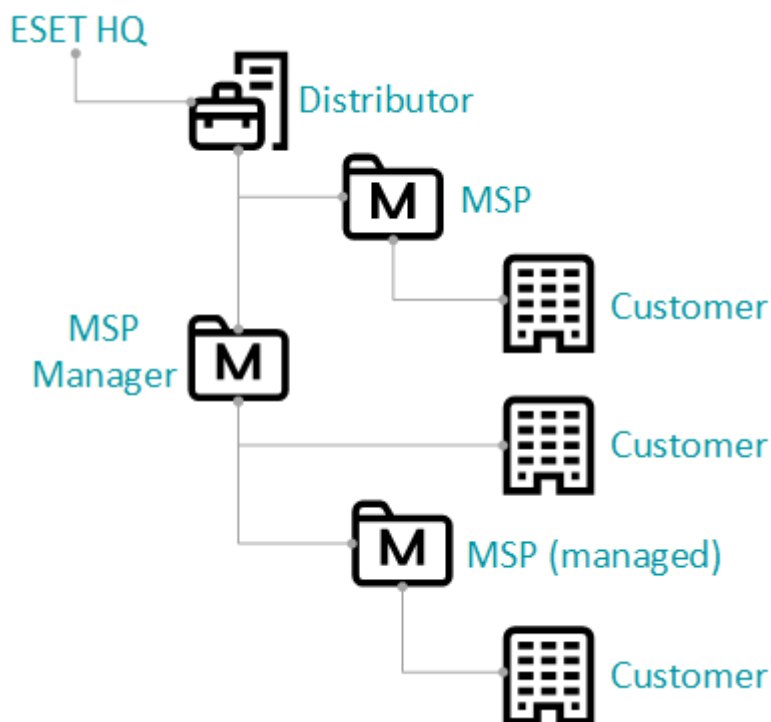
注意してください。証明書の検証は安全な機能であるためWebコンソールで警告が発生する場合は、セキュリティ脅威を示している可能性があります。

マネージドサービスプロバイダー向けESET PROTECT

MSPについて

略語のMSPとは、「マネージドサービスプロバイダー」のことです。通常MSPユーザーは、セキュリティ製品 (例: ESET Endpoint Antivirus) の管理など、顧客に対してITサービスを提供します。MSPユーザーには、エンタープライズユーザーやSMB (中小企業) ユーザーとは異なる要件がありESET PROTECTの使用方法も異なります。推奨される[MSP向け展開シナリオ](#)を参照してください。ESET MSPプログラムの詳細については、各地域のESETパートナーにお問い合わせになるか、[ESETマネージドサービスプロバイダープログラム](#) ページをご覧ください。

MSPの事業体の構造



- **販売店** - 販売店はESETパートナーおよびMSPまたはMSPマネージャーパートナーです。
- **MSPマネージャー** - 複数のMSP企業を管理します。MSPマネージャーには直接の顧客がいる場合もあります。
- **MSP** - 本ガイドの対象読者。MSPは顧客にサービスを提供します。たとえば、MSPは、リモートで顧客のコンピューターを管理し、ESET製品のインストールや管理を行います。
- **マネージドMSP** - MSPに似ていますが、マネージドMSPはMSPマネージャーによって管理されます。
- **顧客** - ESET製品ライセンスのエンドユーザー。顧客はESET製品を操作しません。

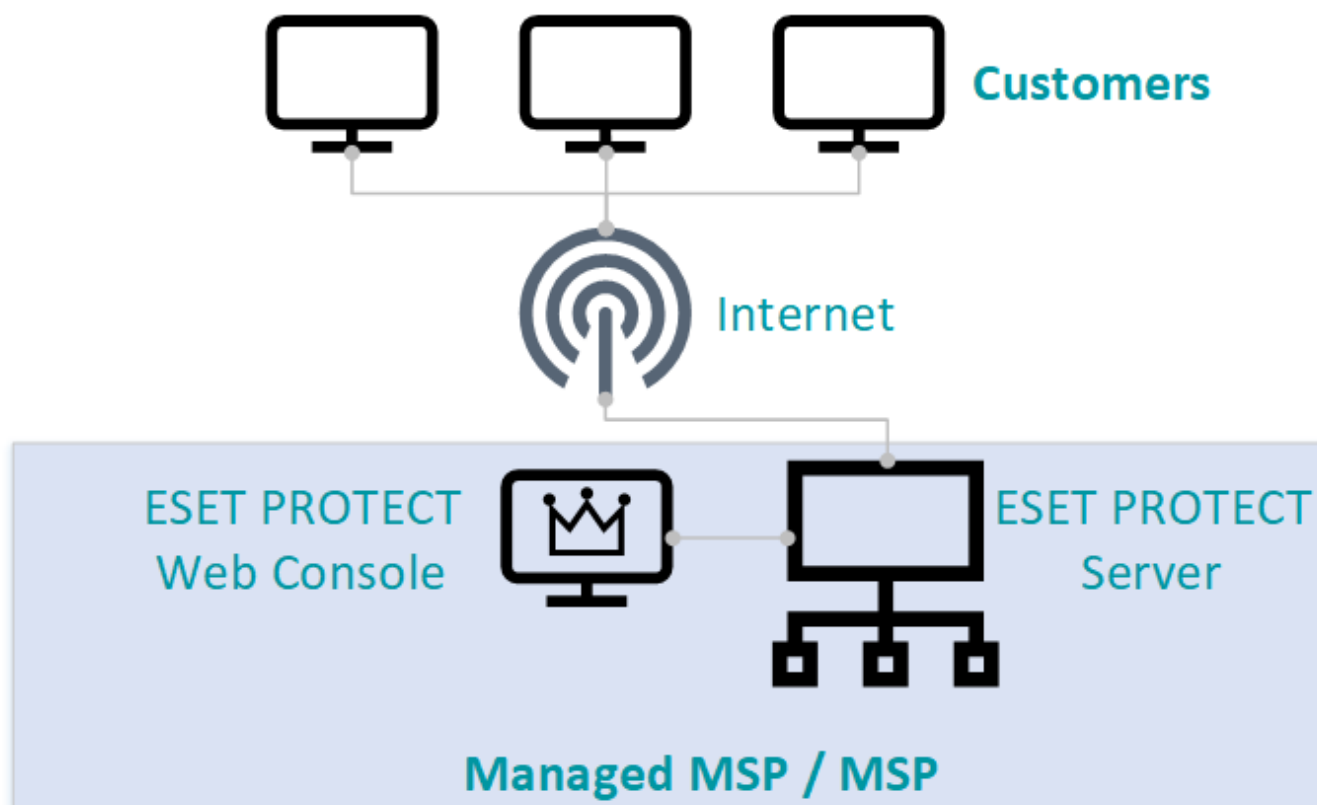
MSP環境の仕様

MSPビジネスモデルは、エンタープライズまたはSMBとは異なるインフラストラクチャ設定を使用します。MSP環境では、一般的に、顧客はMSP企業ネットワーク外にあります。多くの場合、ESET PROTECTサーバー自体も、MSP企業外でホストされています。ESET Managementエージェントは、公開インターネット上で、直接ESET PROTECTサーバーに接続する必要があります。MSP向けのESMCサーバーの推奨設定:

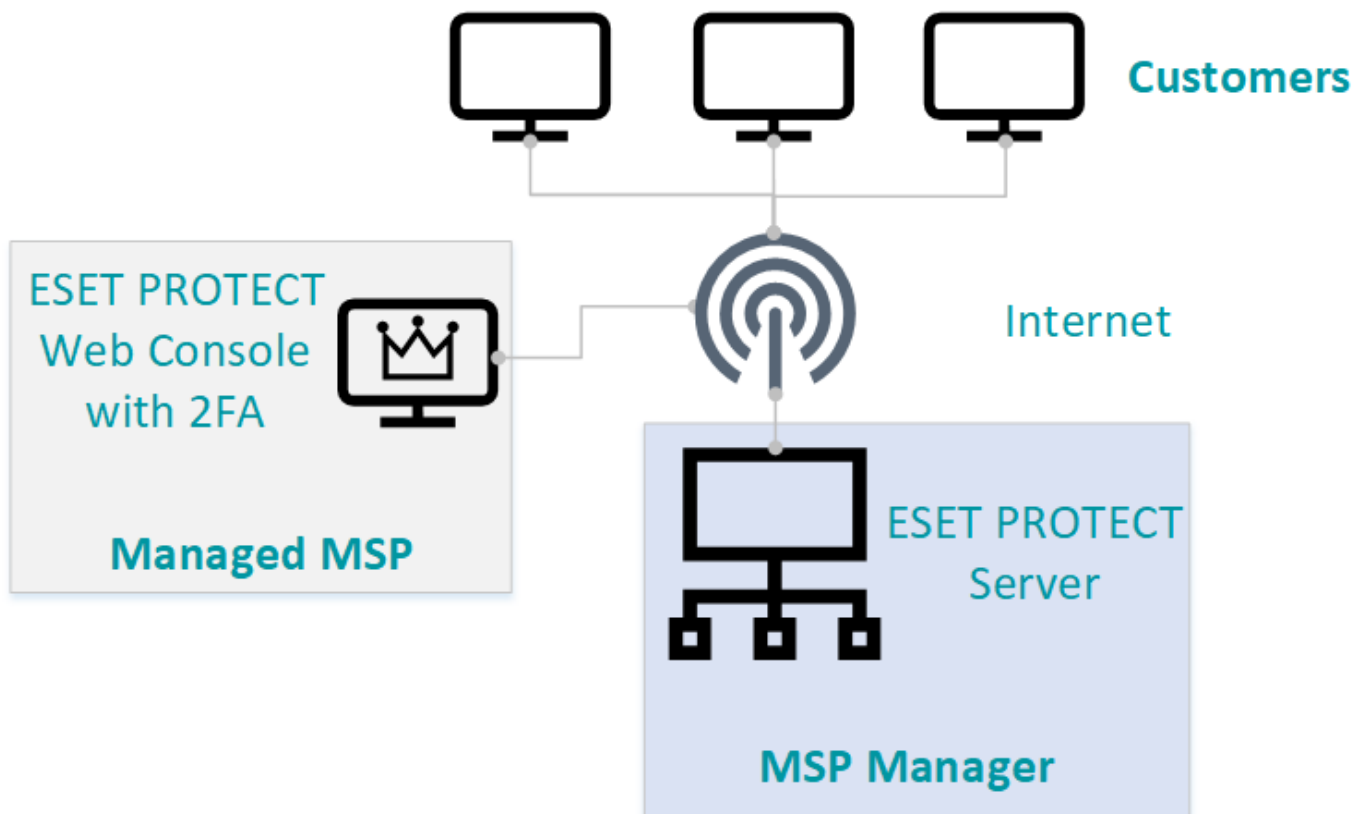
- パブリッククラウドでホストされている。
- MSPのプライベートクラウドでホストされている。(多くの場合、[特定のポート](#)を開き、インターネットからESET PROTECTが表示されるようにする必要があります)
- MSPプライベートネットワークでホストされている。(サーバーが直接表示できない場合、HTTPプロキシを使用して、インターネットから接続を転送します。)

基本設定

- **集中管理設定** - 顧客はインターネット経由でESET PROTECTサーバーにアクセスします。ESET PROTECT Webコンソールは、MSP企業ネットワークからのみアクセスできます。



- **分散設定** - 顧客は、インターネット経由でESET PROTECTサーバーにアクセスします。ESET PROTECT Webコンソールは、インターネット経由でMSPにアクセスできます。インターネットからWebコンソールにアクセスできるようにする場合は、必ず[二要素認証を有効](#)にしてください。



ESMC 7.xからの移行

EMA 2アカウントをインポートしたユーザーで、

- ESMC 7.0からアップグレードしている場合、MSPツリーはESET PROTECTをアップグレードした後に同期されます。すべての静的および動的グループは変更されず、新しいMSPツリーが設定されます。新しいMSPツリーを使用する必要はありません。ただし、デバイスとグループを新しいMSPツリーに移行(移動)することをお勧めします。
- ESMC 7.1または7.2からアップグレードしている場合、MSPツリーとグループ構造は影響を受けません。

MSPユーザー向けESET PROTECTの新機能

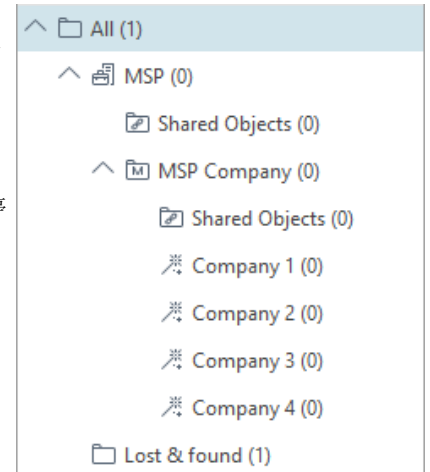
ESET PROTECTはMSPユーザー向けの機能群を備えています。すべてのMSP関連機能は、[EMA 2アカウント](#)をESET PROTECTに[インポート](#)した後に有効にされます。

顧客セットアップウィザード

ESET PROTECTの鍵となるMSP機能は、[MSP顧客設定](#)です。この機能では、顧客の[ユーザー](#)とカスタマイズされたESET Managementエージェント[インストーラー](#)を作成できます。

MSP ツリー

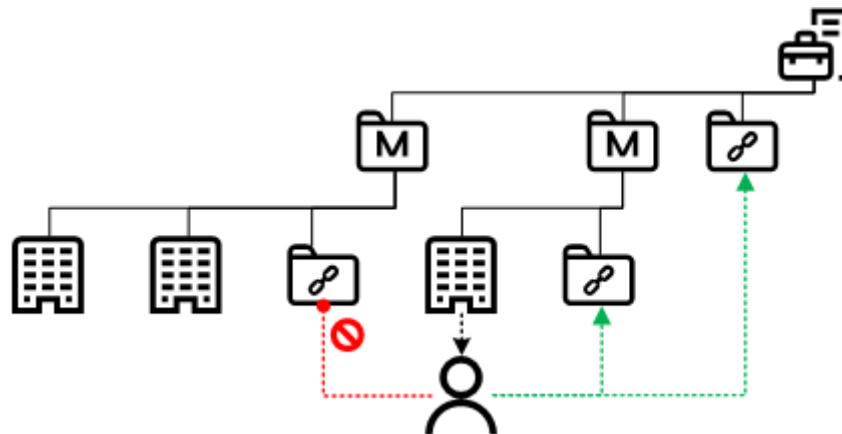
EMA 2 アカウントをインポートした後、ESET PROTECTは [ESET MSP ポータル \(EMA 2\)](#) と同期し、MSP ツリーを作成します。MSP ツリーは [コンピューター](#) メニューの構造であり、EMA 2 アカウントの会社の構造を表します。MSP ツリーの項目は、標準の ESET PROTECT デバイスおよびグループとは異なるアイコンです。Web コンソールでは MSP ツリー構造を修正できません。ライセンス管理から [EMA 2 アカウントを削除](#) した後にのみ、ツリーで顧客を編集したり削除したりすることができます。EMA 2 で会社を一時停止しても ESET PROTECT の MSP ツリーからは削除されません。



共有オブジェクトグループ

MSP アカウントの同期後 ESET PROTECT は MSP ツリーを作成します。各 MSP と MSP マネージャーには、1 つの **共有オブジェクト** の静的グループがあります。MSP は、**共有オブジェクトグループ** 経由で、ポリシーやタスクなどのオブジェクトを共有できます。

[会社セットアップウィザード](#) を使用して作成された MSP ユーザーは、そのユーザーの上のすべての **共有オブジェクト** への読み取りおよび使用アクセス権があります。ユーザーに割り当てられた [権限セット](#) を確認し、アクセスグループのリストを表示できます。ユーザーは、並列の MSP マネージャーのグループではなく、上位の共有オブジェクトグループにのみアクセスできます。



ESET PROTECT 証明書と MSP

ESET PROTECT で [EMA 2 アカウントをインポート](#) すると ESET PROTECT サーバーが新しい MSP [認証局 \(CA\)](#) を作成します。MSP CA は、MSP ルートグループの下に **共有オブジェクト** の静的グループに保存されます。複数のアカウントをインポートしても MSP CA は 1 つだけです。MSP CA を削除すると ESET PROTECT は、次のライセンスサーバーとの同期の後に、新しい MSP CA を作成します。同期は自動的に 1 日に 1 回実行されます。

ESET PROTECT は、[顧客セットアップウィザード](#) を使用して会社を設定した後、新しい [ピアエージェント証明書](#) を作成します。MSP CA はこれらのピア証明書を署名します。各証明書は、会社名で [タグ付け](#) されます。各会社個別の証明書を作成すると、全体的なセキュリティが改善されます。

! [高度なセキュリティ](#) を使用する場合 MSP アカウントをインポートする **前** に、設定することを強くお勧めします。

CA を削除すると CA で署名された証明書を使用しているすべてのコンピューターは、ESET PROTECT サー

バーに接続できなくなります。ESET Management エージェントの手動再展開が必要です。

ステータス概要のMSP

EMA 2 アカウントをインポートした後に、[ステータス概要](#)で新しいMSPタイルにアクセスできます。MSP タイルには、アカウントに関する基本情報が表示されます。

MSPの展開処理

ESET PROTECTがインストールされていない場合は、次の推奨事項を考慮しながらWindows オールインワンインストーラーを使用して、[インストールガイド](#)に従うことをお勧めします。

- **Apache HTTP Proxy**をインストールするオプションは選択しないでください。顧客は、(ダウンロード、アクティベーション、アップデートのため)直接ESETサーバーに接続します。大規模な顧客は、独自のローカル[HTTPプロキシ](#)ソリューションを所有している場合があります。HTTPプロキシは後から設定できます。
- ESET PROTECTサーバーは、(EMA 2との同期、アップデートのダウンロードなどのため)ESETサーバーにも接続する必要があります。

ESET PROTECTサーバーをインストールした後は、次の手順に従います。

- 1.有効な[EMA 2 アカウント](#)が所有していることを確認します。
- 2.1つ以上の[ライセンス](#)を持った顧客を準備します。既存の顧客を使用することもできます。
- 3.EMA 2 アカウントをESET PROTECTに[インポート](#)します。
- 4.[MSP顧客設定](#)を完了します。確認メッセージが表示されたら、**エージェントのみのインストーラー**を選択します。
- 5.ESET Management エージェントインストーラーを[ローカル](#)または[リモート](#)で配布およびインストールします。
- 6.[ESETセキュリティ製品をインストールして、ポリシーを設定します](#)

以下の体系は、MSP顧客登録プロセスの概要説明です。

エージェントのローカル展開

エージェントのみのインストーラーのローカル展開

エージェントのみのインストーラーは、クライアントコンピューターがESET Managementエージェントをダウンロードしてインストールするために必要なすべての情報を含むスクリプトです(Windowsは.bat、LinuxおよびmacOSは.sh)。Linuxコンピューターでインストールしている場合は、コンピューターが[前提条件](#)を満たしていることを確認してください。

また、インストーラーをローカルで実行するか、リムーバブルメディア(USBフラッシュドライブなど)から実行することもできます。

⚠ エージェントインストールパッケージをダウンロードし、ESET PROTECTサーバーに接続するには、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必要があります。

手動で[スクリプトを編集](#)し、必要に応じて特定の設定を調整できます。 上級ユーザーにのみ推奨されます。

オールインワンインストーラーのローカル展開

[オールインワン](#)インストーラーには、任意のESETセキュリティ製品と設定済みのESET Managementエージェントインストーラーが含まれます。

詳細については、[インストールマニュアル](#)を参照してください。

エージェントのリモート展開

エージェントのみのインストーラーのリモート展開

エージェントのみのインストーラーは、クライアントコンピューターがESET Managementエージェントをダウンロードしてインストールするために必要なすべての情報を含むスクリプトです(Windowsは.bat、LinuxおよびmacOSは.sh)。Linuxコンピューターでインストールしている場合は、コンピューターが[前提条件](#)を満たしていることを確認してください。電子メールでインストールを配布し、ユーザーに展開させることができます。 使用可能な場合は、カードパーティの管理ツールを使用してスクリプトを配布して実行します。

⚠ エージェントインストールパッケージをダウンロードし、ESET PROTECTサーバーに接続するには、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必要があります。

オールインワンインストーラーのリモート展開

[オールインワン](#)インストーラーは、ESET Remote Deployment Toolを使用して、リモートで、ローカルネットワーク内にインストールできます。詳細な手順については、[ESET Remote Deployment Tool](#)文書を参照してください。

MSPライセンス

有効なアカウント

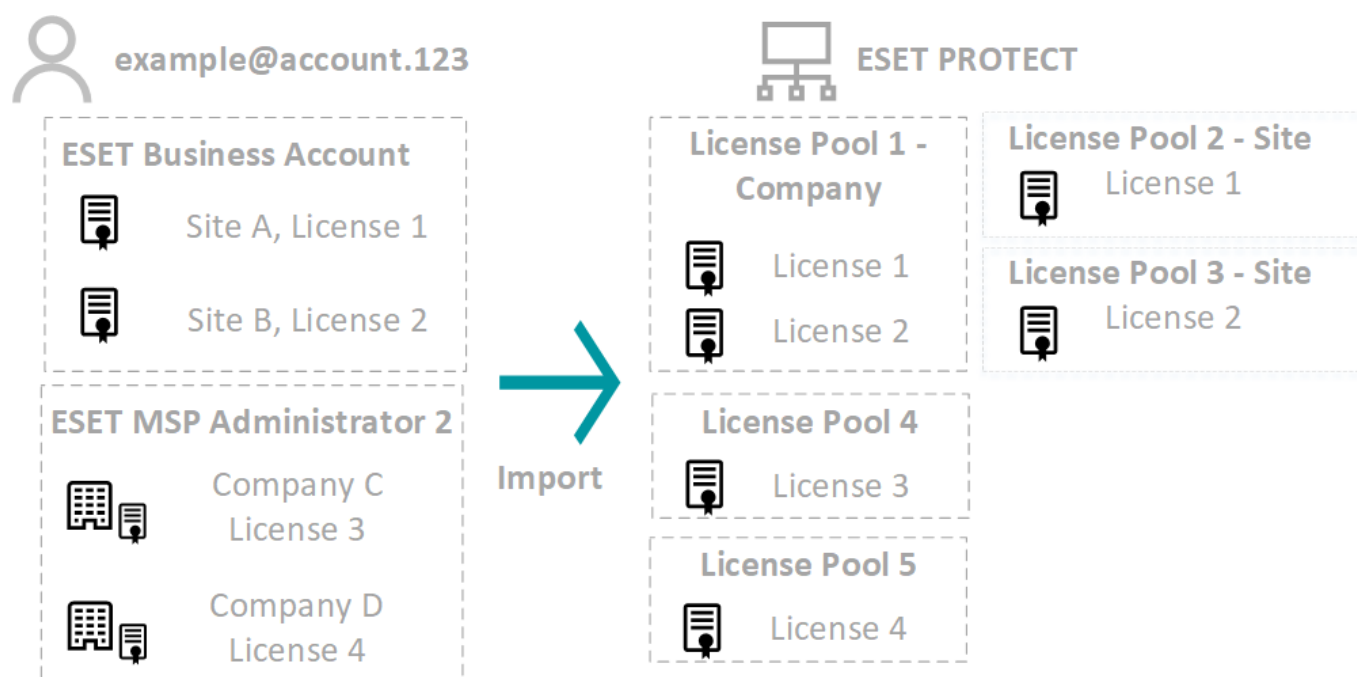
ESET PROTECT 9.0でMSP機能を有効にするにはESET PROTECTのライセンス管理で[MSPアカウントをインポート](#)する必要があります。次のタイプのEMA2アカウントをインポートできますMSPマネージドMSPおよびMSPマネージャー。すべてのアカウントには、少なくとも1つの会社（親会社または1つの顧客）に対する読み取り許可が必要です。親会社へのアクセスは必要ありません。販売店アカウントはインポートできません。

ライセンスと会社に関する情報

- MSPアカウントからインポートされたライセンスは、会社名で[タグ付け](#)されます。後から会社名を変更する場合、タグ名が自動的に変更されます。手動で編集することはできます。
- すべてのライセンスは、ESET PROTECT [セキュリティモデル](#)に対応する方法でインポートされます。[MSP顧客設定](#)を使用して作成された各ユーザーは、そのライセンスのみを表示および使用することができます。
- 同期時点までに、ライセンスがないMSP構造の会社がある場合、その会社はコンピュータMSPツリーとのみ同期され、[ライセンス管理](#)内のMSPツリーには同期されません。
- ESET MSP Administrator 2で新しい会社を追加した場合、次のライセンス同期後に、ESET PROTECTが会社をMSPツリーに追加します。
- MSPアカウントをインポートするときには、すべてのライセンスが1つのライセンスプールに保存されます。プールからライセンスを移動することはできません。ライセンスプール全体は移動できます。プールを移動するには、プール > [アクション](#) > [アクセスグループ](#) > [移動](#)を選択し、新しいアクセスグループを選択します。後からMSPアカウントを同期する場合は、新しいライセンスがプールの実際の場所に表示されます。
- [ライセンス管理](#)のライセンスユーザー列で会社名とサイトを検索できます。[レポート](#)を作成するときには、[ライセンスユーザーデータ](#)を使用できます。
- 同じ認証情報でESET Business AccountとESET MSP Administrator 2の両方にライセンスがある場合ESET PROTECTは両方のアカウントからすべてのライセンスを同期します。すべてのESET Business Accountライセンスは複数のライセンスプールに保存されますESET MSP Administrator 2のライセンスは、会社ごとに、1つの[プール](#)に分割されます。バージョン8.0以降ではESET PROTECTは、ライセンスを分割するための[ESET Business Accountサイト](#)をサポートしています。

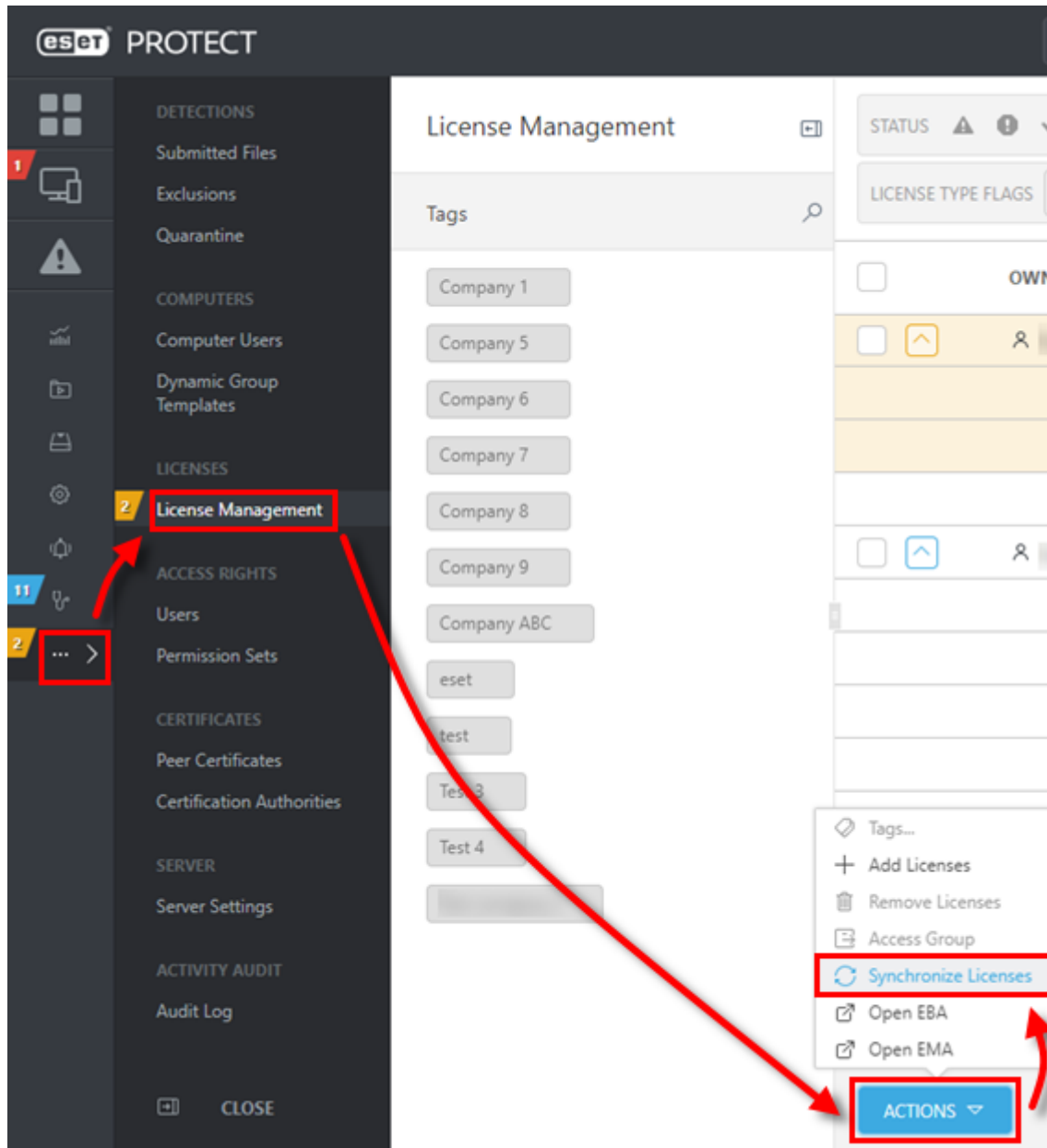
同期されたESMC 2アカウントを使用してESET MSP Administrator 7.0からアップグレードすると、ライセンスプールが元のアクセスグループに残ります。[インストーラーを作成](#)する前には、個別のライセンスプールをMSP顧客グループに移動する必要があります。ライセンスプールを移動するには、**ライセンス管理**に移動し、ライセンスプールを選択して、**アクセスグループ>移動**を選択します。ライセンスを別の静的グループに移動すると、既存のインストーラーとユーザーセキュリティに影響することに注意してください。

- ライセンスプールを削除するときには、同じアカウントに関連付けられた他のすべてのライセンスプールを自動的に削除します。[会社を削除](#)する方法の詳細についてお読みください。



オンデマンド同期

ESET PROTECTサーバーは、1日1回、ライセンスサーバーと同期します。MSPアカウントで変更を行い、ライセンス画面とMSPツリーを更新する場合、**ライセンス管理>アクション**に移動し、**ライセンスの同期**に移動します。



MSPアカウントのインポート

! 高度なセキュリティを使用する場合、MSPアカウントをインポートする前に、設定することを強くお勧めします。

1. Webコンソールにログインし、**詳細 > ライセンス管理**に移動します。
2. **アクション > ライセンスの追加**をクリックします。
3. **ESET Business Account**または**ESET MSP Administrator**オプションを選択します。MSP認証情報(EMA 2ログイン)を以下のログインおよびパスワードフィールドに入力します。

Add License

×

You can add your license using one of the following options:

☒ ESET Business Account or ESET MSP Administrator

☐ License Key

☐ Offline License File

ESET Business Account or ESET MSP Administrator Login

Password

.....

Show password


Note: You can use ESET License Administrator Security Admin account credentials as well, however we do recommend to migrate your licenses to the new [ESET Business Account](#).

ADD LICENSES

CANCEL

4. ライセンスの追加をクリックして確認します。

×



Licenses have been successfully added using ESET account credentials (login:).

There may be some delay before the list is updated.

OK

5. ESET PROTECTは、MSPポータルからWebコンソールの[コンピューター](#)メニューに構造を同期します。同期された構造は、*MSPツリー*といいます。

i 多数の顧客(数千)を含むMSPアカウントをインポートすると、時間がかかる場合があります(数時間かかることもあります)。

MSP顧客設定の開始

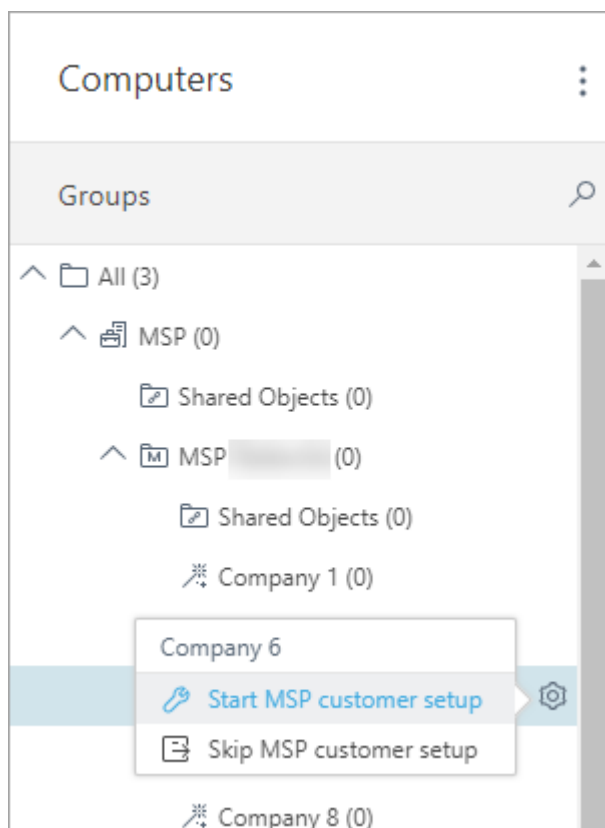
MSPアカウントを[インポート](#)し、[MSPツリー](#)が同期された後、会社の設定を開始できます。MSP顧客設定により、次の項目が作成されます。

- カスタムESET Managementエージェント、またはバンドルされた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。MSP顧客設定は、ESET Full Disk EncryptionのインストーラーまたはESET Enterprise Inspectorエージェントインストーラーの作成をサポートしません。
- Webコンソールを使用して、会社のコンピューターを管理できる[MSPユーザー](#)。

[MSP顧客設定をスキップ](#)することもできますが、MSP設定を利用することをお勧めします。

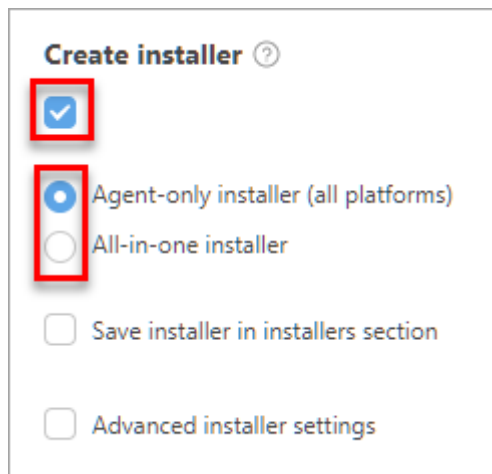
❗ 少なくとも1つ有効な[ライセンスシート](#)がある会社だけが設定できます。

1. コンピューターウィンドウで、設定する会社の横の歯車アイコンをクリックし、**MSP顧客設定の開始**を選択します。



2. この設定を既定の設定として保存する場合は、**設定を記憶する**の下チェックボックスをオンにします。**続行**をクリックします。

3. 設定中にカスタムインストーラーを作成する場合(推奨)は、**インストーラーの作成**の下チェックボックスをオンにします。



4. 次の2つの種類のインストーラーを作成できます。

- エージェントのみのインストーラー(すべてのプラットフォーム) – この [エージェントライブインストーラー](#) を Windows、macOS および Linux コンピューターにインストールできます。
- オールインワンインストーラー – このインストーラーは、ESET Management エージェントと選択した ESET ビジネスセキュリティ製品(Windows)で構成されています。

オールインワンインストーラーオプションが表示されない場合は、ライセンスが会社に [割り当てられている](#)ことを確認してください。

[オールインワンインストーラーを選択しました](#)

製品 - ESET Management エージェントと一緒にインストールする ESET セキュリティ製品を選択します。

言語 - ESET セキュリティ製品インストーラーの言語バージョンを選択します。

[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。詳細については、[ESET 製品のエンドユーザーライセンス契約\(EULA\)と利用規約、およびプライバシーポリシー](#)を参照してください。

インストーラーを後で使用するために [インストーラー](#) に保存するには、インストーラーをインストーラーセクションに保存の横にあるチェックボックスをオンにします。

[詳細インストーラー設定](#) (推奨)

サーバーホスト名は、ESET Management エージェントが ESET PROTECT サーバーに接続するアドレスです。必要に応じて、エージェントとサーバー間の通信に別のポートを選択します。ポートを変更する場合は、すべての接続するエージェントと、[サーバー設定](#)で変更する必要があります。

インストーラーを使用するすべてのクライアントデバイスが **サーバーホスト名** アドレスに到達できることを確認します。[MSP 環境の推奨事項](#)を参照してください。

[HTTP プロキシ設定を有効にする](#)

HTTP プロキシを使用する場合は、**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 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。HTTP プロキシは既定でポート 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。

! 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す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。

HTTP proxy settings [?]

☒ Enable HTTP proxy settings

Host [?]

protect.local

Port [?]

3128

Username

Password

Show password

Fallback [?]

☐ Use direct connection if HTTP proxy is not available

5. **続行**をクリックして、**ユーザー**セクションに移動します。

6. 会社の**新しいユーザー**を作成する場合は、**ネイティブユーザーを作成**チェックボックスをオンにします。ユーザーは**Web**コンソールにログインして、会社のデバイスを管理できます。新しいユーザーの有効なユーザー名(文字, ; "を使用しないこと)とパスワードを入力します。

a. **パスワードの変更が必要** - ユーザーは、最初のログインの後にパスワードを変更する必要があります。

b. **アクセス権** - ユーザーに会社オブジェクト(コンピューター、ポリシー、タスク)への**読み取りおよび使用**または**書き込み**アクセスがあるかどうかを選択します。

Create native user ?

☒

Username

Company 1

Password

.....

Confirm password

.....

Show password

☐ Require password change

Access rights ?

Write

i AD同期は、[MSP会社設定](#)を使用して作成されたユーザーでは使用できません。

ユーザーの作成の問題が発生している場合[必要な権限が割り当てられている必要があります](#)?

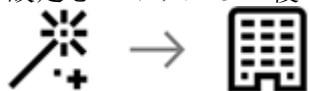
完了をクリックして、インストーラーを準備します。 リンクをクリックして、必要なインストーラーをダウンロードします。 インストーラーの保存を選択した場合は、[インストーラー](#)メニューからインストーラーを再ダウンロードすることもできます。

ESET Management エージェントを[ローカル](#)または[リモート](#)で展開する方法についてお読みください。

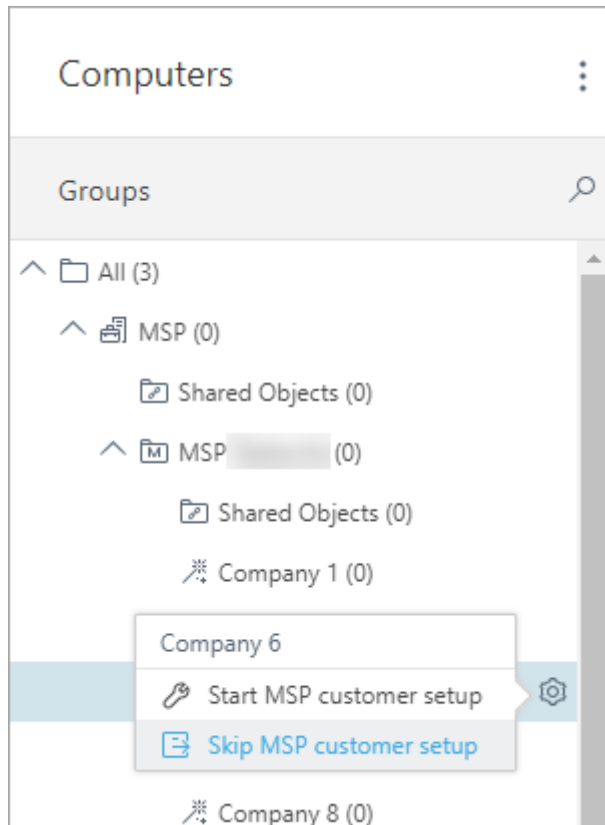
MSP顧客設定のスキップ

設定しない場合は、**MSP顧客設定のスキップ**ができます。 任意で、[インストーラー](#)と[新しいユーザー](#)を後から作成できます。 設定のスキップは推奨されません。


設定をスキップした後は、設定されたかのように、会社のアイコンが変更されます。

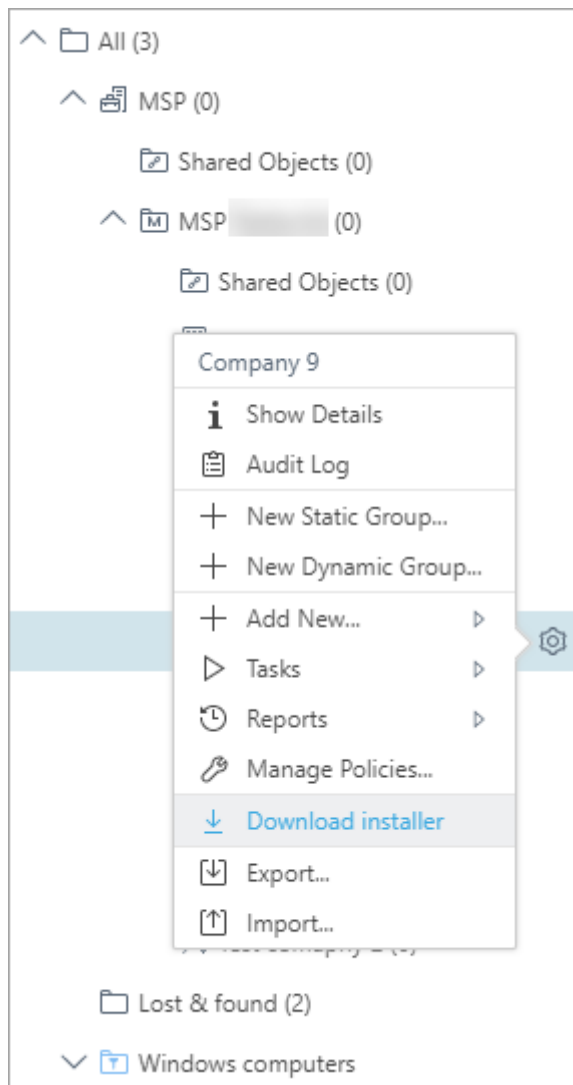


! 設定をスキップする場合は、同じ ESET PROTECT インスタンスで、その会社のサイド [セットアップウィザード](#) をもう一度実行することはできません。



カスタムインストーラーの作成

1. ESMC Webコンソールで、コンピューターメニューに移動します。
2. インストーラーを作成する会社の横の歯車アイコンをクリックし、インストーラーのダウンロードを選択します。



3. 次の2つの種類のインストーラーを作成できます。

- エージェントのみのインストーラー(すべてのプラットフォーム) – この[エージェントライブインストーラー](#)をWindows®/macOS®およびLinuxコンピューターにインストールできます。
- オールインワンインストーラー – このインストーラーは、ESET Managementエージェントと選択したESETビジネスセキュリティ製品(Windows)で構成されています。

オールインワンインストーラーオプションが表示されない場合は、ライセンスが会社に[割り当てられている](#)ことを確認してください。

[オールインワンインストーラーを選択しました](#)

製品 - ESET Managementエージェントと一緒にインストールするESETセキュリティ製品を選択します。

言語 - ESETセキュリティ製品インストーラーの言語バージョンを選択します。

[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。詳細については、[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](#)を参照してください。

インストーラーを後で使用するために[インストーラー](#)に保存するには、インストーラーをインストーラーセクションに**保存**の横にあるチェックボックスをオンにします。

＜詳細インストーラー設定（推奨）

サーバーホスト名は、ESET Management エージェントが ESET PROTECT サーバーに接続するアドレスです。必要に応じて、エージェントとサーバー間の通信に別のポートを選択します。ポートを変更する場合は、すべての接続するエージェントと、[サーバー設定](#) で変更する必要があります。

インストーラーを使用するすべてのクライアントデバイスがサーバーホスト名アドレスに到達できることを確認します。[MSP環境の推奨事項](#) を参照してください。

＜HTTP プロキシ設定を有効にする

HTTP プロキシを使用する場合は、**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 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。HTTP プロキシは既定でポート 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。



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す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。

HTTP proxy settings ?

☒ Enable HTTP proxy settings

Host ?

protect.local

Port ?

3128

Username

Password

[Show password](#)

Fallback ?

☐ Use direct connection if HTTP proxy is not available

MSP installer download

Computers > Company 1

Installer

Download

This installer will deploy the ESET Management Agent and optionally an ESET Security product to the customer's computers.

i The All-in-one Installer is available for Windows and will provide everything needed for protection of the computer. The Agent-only Installer is available for all platforms, but an ESET Security product must be installed and activated afterwards.

Installers can be downloaded at the end of this wizard and can also be saved for later use.

[More information about installer creation.](#)

☒ Agent-only installer (all platforms)

☐ All-in-one installer

☐ Advanced installer settings

4. 作成をクリックすると、インストーラーを作成します。

5. リンクをクリックして、必要なインストーラーをダウンロードします。

MSPユーザー

[MSP顧客設定](#)を使用して会社を設定した場合は、特殊なタイプの[ネイティブユーザー](#)(MSPユーザー)を作成できます。ユーザーを確認および編集するには、[詳細](#)>[アクセス権](#)>[ユーザー](#)メニューに移動します。

MSPまたはリセラーなどの[カスタムMSPユーザーを作成](#)することもできます。

必要な権限

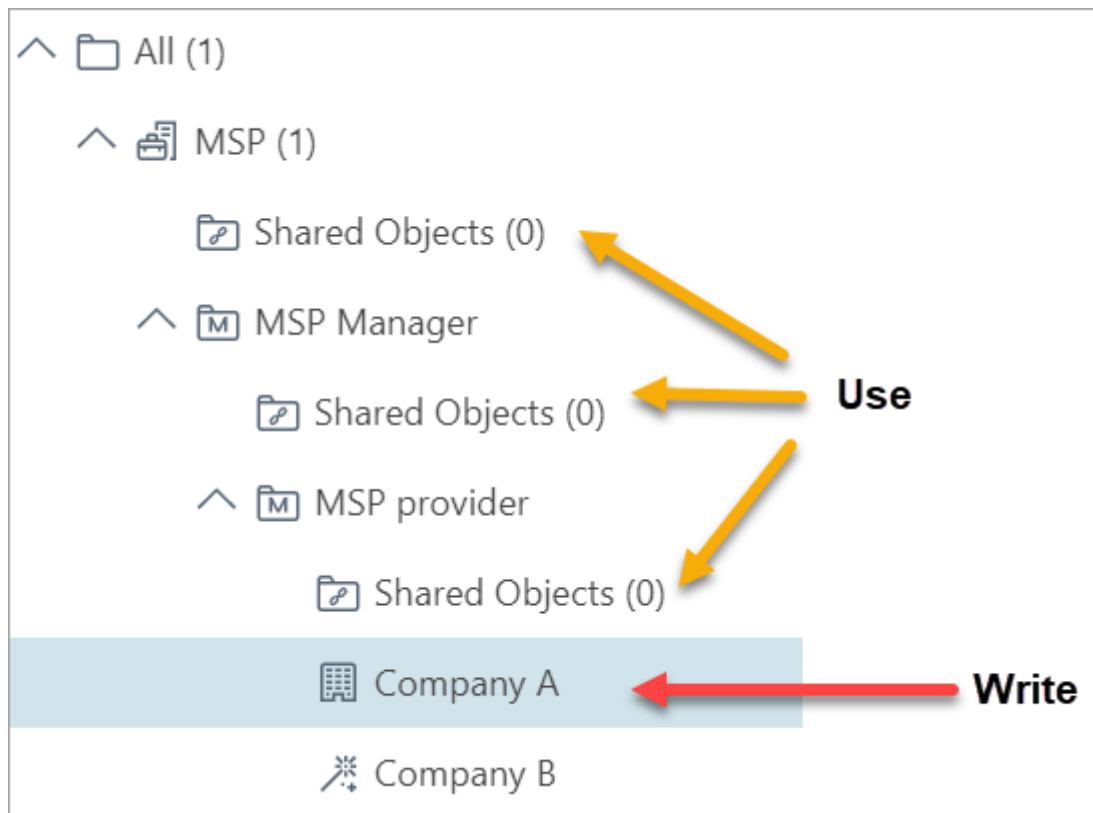
[MSP顧客設定](#)で新しいユーザーを作成するには、設定した会社と共有オブジェクトグループへのアクセス権が必要です。

[^権限体系の詳細](#)

1つの会社を設定する

会社Aの設定中にユーザーを作成するために必要なアクセス権:

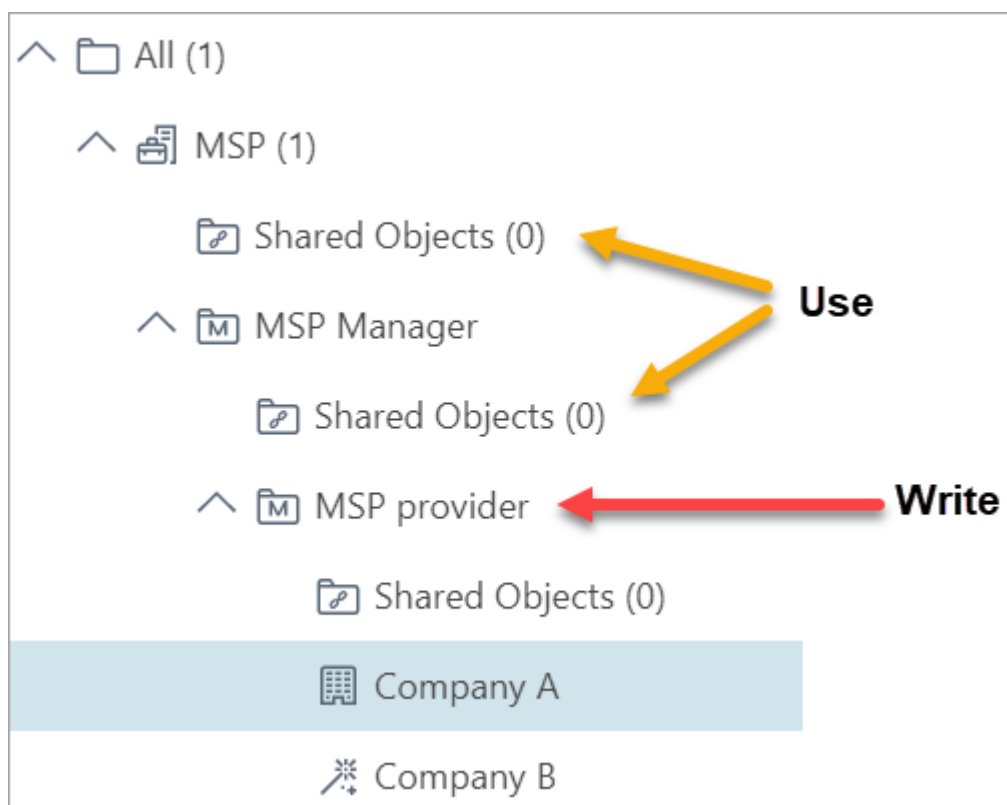
- すべての共有オブジェクトグループの使用アクセス
- MSP顧客のグループの書き込みアクセス。



1つのMSPのすべての会社を設定する

MSPプロバイダーに属するすべての会社のユーザーを作成するために必要なアクセス権:


- すべての共有オブジェクトグループの使用アクセス
- MSPプロバイダのグループの書き込みアクセス。



[アクセス権が割り当てられている](#)と、現在の(有効な)ユーザーには、[権限設定](#)と上記のグループに対するアクセス権が割り当てられています。必要なアクセス権がない場合は、MSP顧客設定がエラーで終了します。


MSPユーザー機能

- ESET PROTECT Web コンソールにログインし、アクセス権があるデバイスおよび他のオブジェクトを管理できます。
- 同じ権限以下の別のネイティブユーザーを作成できます。
- [コンピューターユーザー](#)は作成できません。コンピューターユーザーの作成が必要な場合、管理者はそうにする必要があります。

 AD同期は、[MSP会社設定](#)を使用して作成されたユーザーでは使用できません。

ESET PROTECTには、各新規MSPユーザーの次の設定があります。

- **説明** - MSP顧客セットアップウィザードで作成されたネイティブユーザー
- **タグ** - ユーザーは会社名でタグ付けされます。
- **ホームグループ** - 会社の静的グループ
- **自動ログアウト** - 15分
- アカウントが有効で、パスワード変更は必要ありません。
- **権限設定** - 各MSPユーザーには2つの権限設定があります。1つはホームグループ用、もう1つは共有オブジェクトグループ用です。



Company 1

Company 1

Select tags

Native user created via the MSP customer setup wizard

Permission Sets


2

Home Group

Company 1

Email Address

Phone



Account

Account

Enabled

Autologout (min)

15

Password Changed Last Time

2020 Dec 1 13:11:48


Password expiration (days)

365

Password Change

Not Required

Full Name



Two-factor Authentication

Enabled

No

Locked Access

No

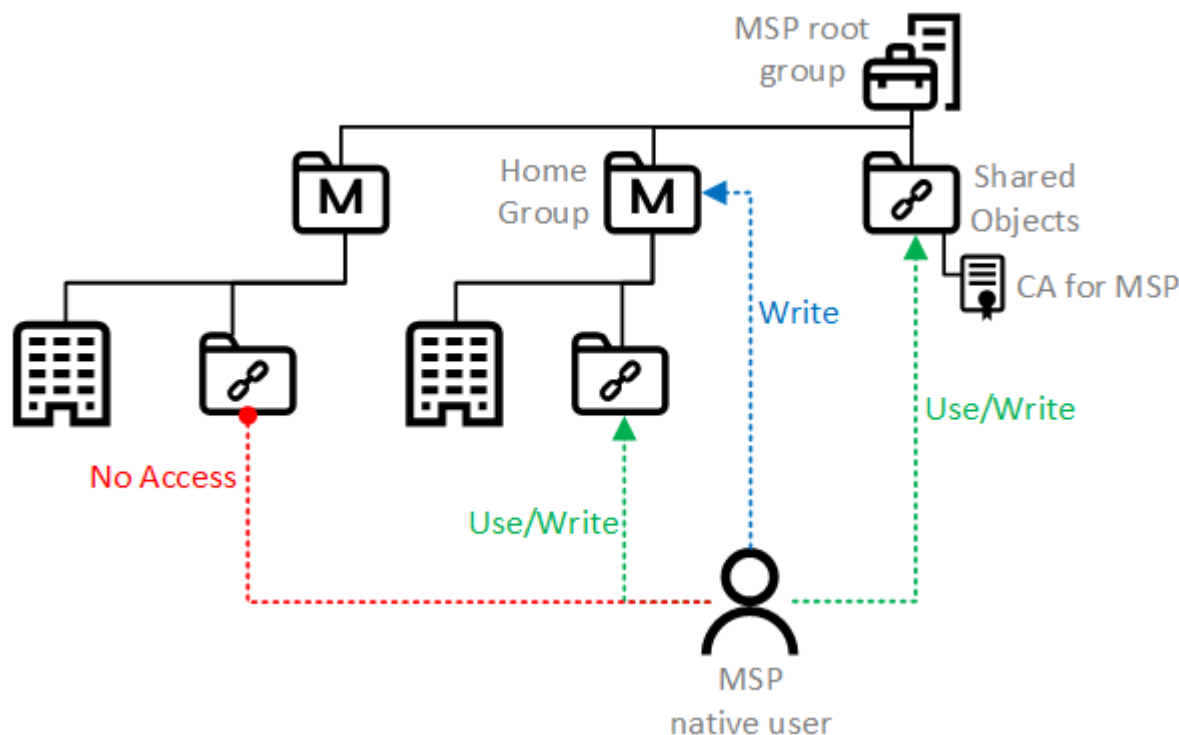
カスタムMSPユーザーの作成

ネイティブWebコンソールユーザーを作成してMSPまたはリセラーなどの顧客を管理できます。

- MSP会社をEMA 2で作成する必要があります。
- MSP会社がMSPツリーで同期されていることを確認します。
- ネイティブユーザーを作成します。カスタムMSPユーザーの重要な設定:
 - ユーザーのホームグループは、対応するMSP静的グループに設定されます。
 - 次の権限セットを作成し、ユーザーに割り当てます:
 - ホームグループの書き込み権限

ii.共有オブジェクトグループの使用または書き込み権限。

i 上位の共有オブジェクトグループには、[MSP CA](#)が含まれています。MSP CAへのアクセスは、ユーザーが[インストーラー](#)を作成するために必要です。



カスタムMSPユーザーアクセススキーム。


これらの手順を使用して作成されたカスタムMSPは、顧客のデバイスを管理し、インストーラーを作成できますが、ユーザーはESET PROTECTサーバーを管理したり、ライセンスをインポートしたりすることができません。

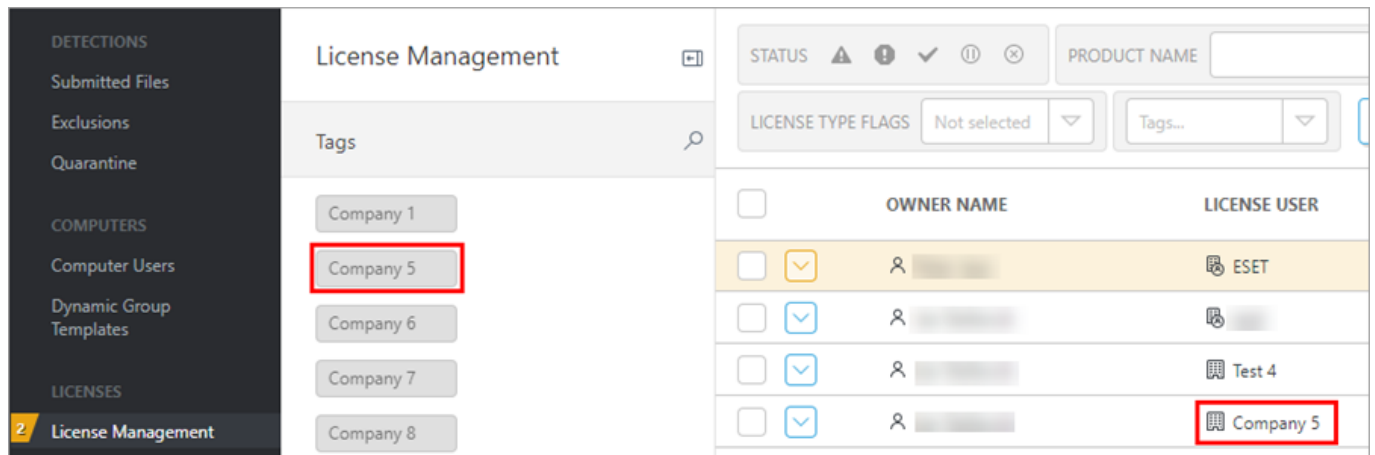
MSPオブジェクトのタグ付け

[有効なMSPアカウントをESET PROTECTにインポート](#)する場合は、MSPオブジェクトの自動タグ付けを有効にします。次のオブジェクトは、自動的にタグ付けされます。

- MSPアカウント経由でインポートされたライセンス
- インストーラー
- [MSP顧客設定](#)を使用して作成された[ユーザー](#)と権限セット

[タグ](#)は、オブジェクトのフィルタリングを改善するために使用されるラベルの形式です。自動タグ名は、[ライセンスユーザー](#)と同じです(ESET PROTECTがタグから破棄する、"文字を除くEMA 2の会社名)。同期の後でEMA 2で顧客名を変更する場合、タグは更新されません。必要に応じて、任意のオブジェクトに別のカスタムタグを追加できます。タグ付けされたオブジェクトに影響を与えずに、タグを削除できます。

 展開アイコンをクリックすると、**タグタブ**が表示されます。



	OWNER NAME	LICENSE USER
<input type="checkbox"/>	Company 1	
<input checked="" type="checkbox"/>	Company 5	ESET
<input type="checkbox"/>	Company 6	
<input type="checkbox"/>	Company 7	Test 4
<input type="checkbox"/>	Company 8	Company 5

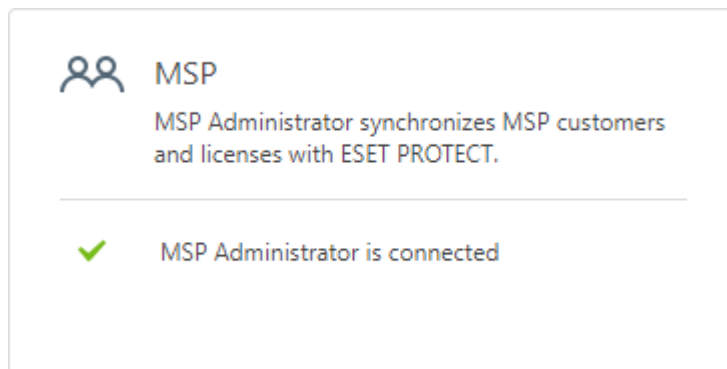
MSPステータス概要


[ステータス概要](#) セクションにはESET PROTECTステータスに関する複雑な情報が表示されます。 [MSPアカウント](#) をインポートする場合は、MSPタイルにMSP関連情報が表示されます。


MSPステータス

アカウントが同期されました

アカウントは同期され、アクションは必要ありません。

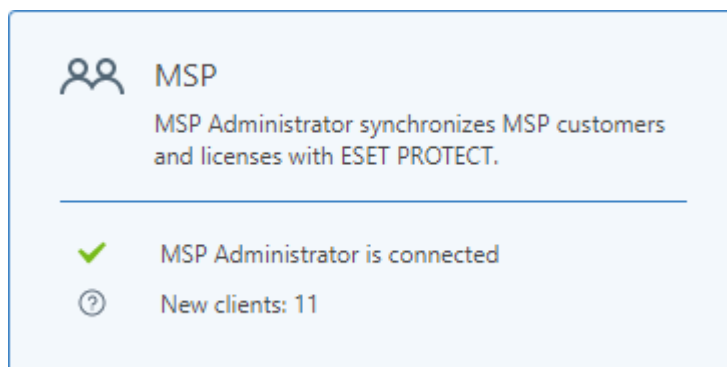



 **MSP**
MSP Administrator synchronizes MSP customers and licenses with ESET PROTECT.


 **MSP Administrator is connected**


実行中の同期

MSPアカウントの同期が実行中の場合は、バックグラウンドで実行されます。大きいアカウントの場合、同期には最大で数時間かかることがあります。同期後に、タイルが白くなります。



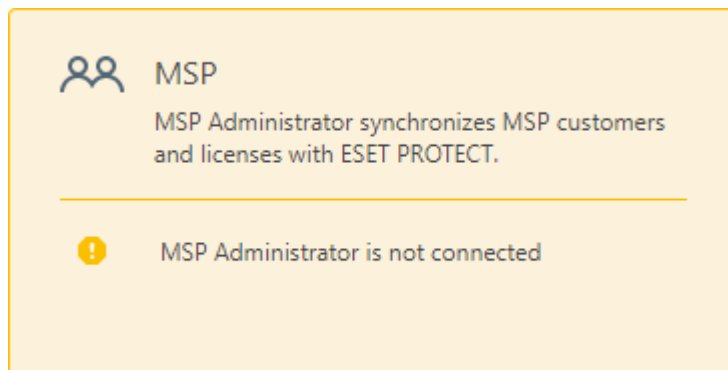
 **MSP**
MSP Administrator synchronizes MSP customers and licenses with ESET PROTECT.

 **MSP Administrator is connected**

 **New clients: 11**

オフラインのアカウント

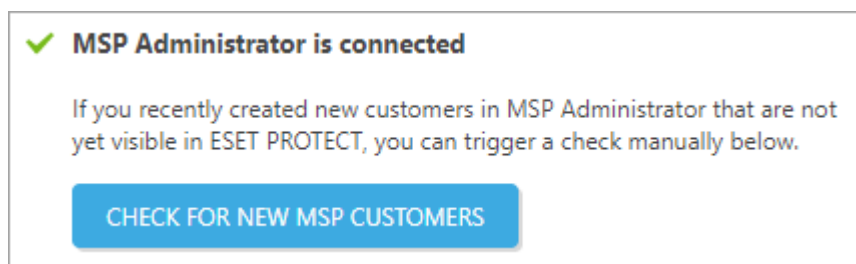
[静的グループ構造](#)にはいくつかのMSPグループ(MSPツリーの一部)がありますが、対応するMSPアカウントはインポートされません。[ライセンス管理](#)からMSPアカウントを削除すると、この現象が発生することがあります。



使用可能なアクション

MSPタイルをクリックすると、詳細が表示されます。

- **新しいMSP顧客の確認** – オンデマンドライセンス同期(MSPツリーのアップデート)を実行します。



- **新しいクライアント** – 会社を設定していない場合は、会社をクリックし、顧客セットアップウィザードに従います。
- **すべての新しいMSP顧客の設定をスキップ** – 設定されていないすべての会社のセットアップウィザードをスキップします。

② New clients: 11

New MSP customers were found in MSP Administrator. They are shown in the group tree and can be easily set up from there.

- ✳ Company 9
- ✳ Company 1
- ✳ Test 3
- ✳ Test
- ✳ Test 4
- ✳ Company 5
- ✳ test
- ✳ Company 7
- ✳ Company ABC
- ✳ Company 8
- ✳ Company 6

SKIP SETUP FOR ALL NEW MSP CUSTOMERS

- **MSP管理者を接続** - MSPアカウントを追加してMSPライセンスおよび構造を[インポート](#)できます。

❗ MSP Administrator is not connected

ESET PROTECT can currently not connect to MSP Administrator. This can have several reasons such as problems with the network, service or account. Visit MSP Administrator to identify possible issues or contact ESET support.

CONNECT MSP ADMINISTRATOR

会社の削除

MSPツリーはMSPアカウントで同期されます。MSPツリーをロック解除するには、ライセンス管理からMSPアカウントを削除する必要があります。アカウントを削除すると、そのアカウントによって管理されているすべての会社がMSPツリーからリンク解除されます。

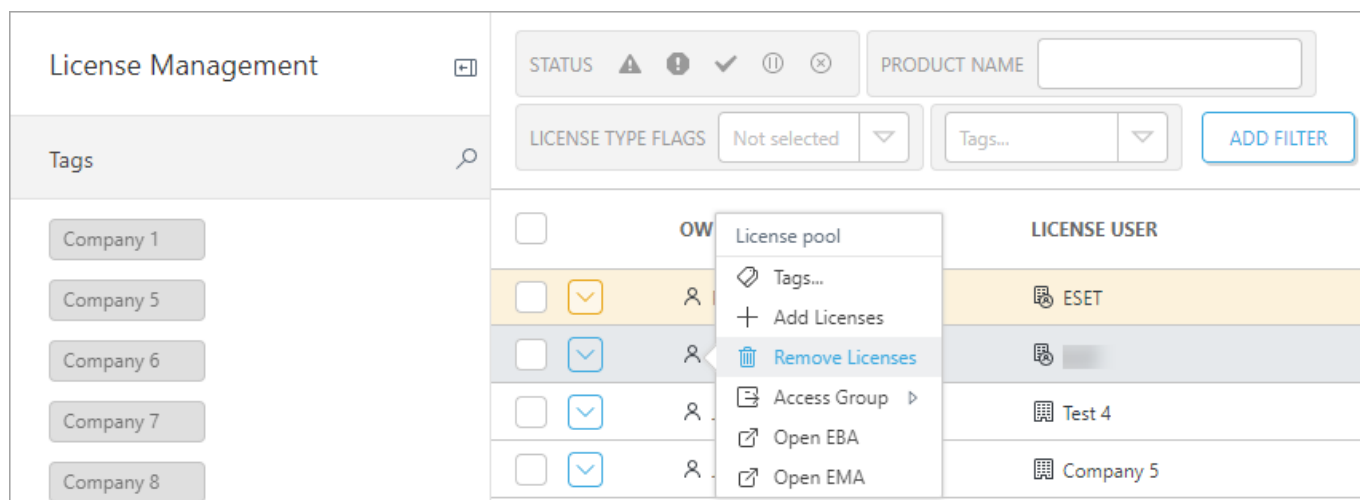
❗ 会社の管理を停止する場合は、その会社のコンピューターからESET Managementエージェントを[削除](#)します。ライセンス管理からMSPアカウント全体を削除しないとMSPツリーから会社を削除することができません。

MSP静的グループは永続的です。MSPライセンスを同期した後は、MSPルートグループを削除できません。削除できるのは、子グループのみです。

MSPツリーからMSPアカウントと会社を削除する

1. ESET PROTECT Webコンソールにログインし、**詳細 > ライセンス管理**に移動します。

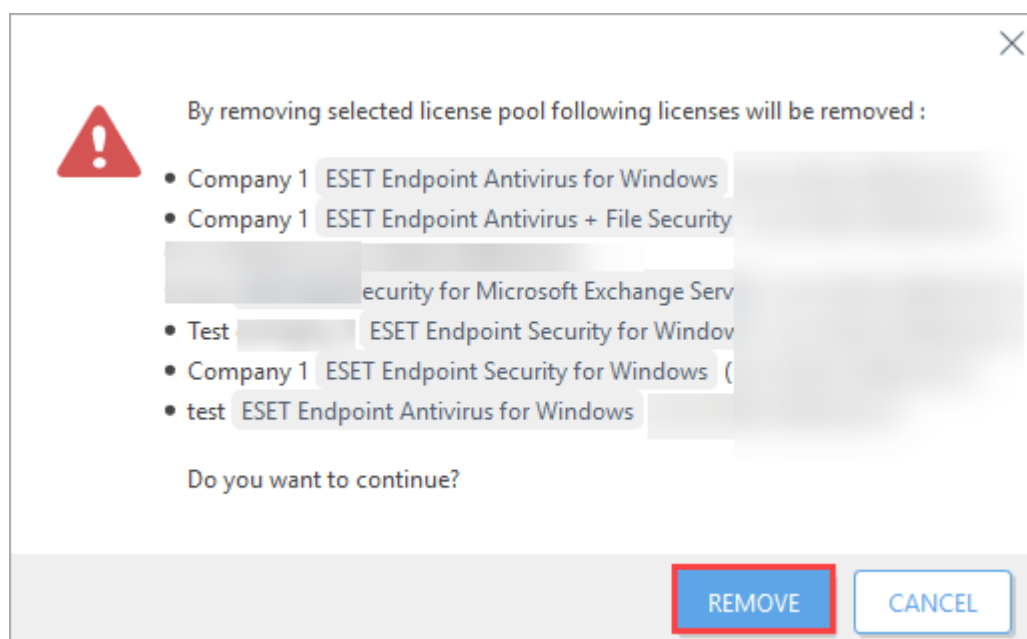
2. 削除するライセンス > **ライセンスの削除**をクリックします。MSPアカウントにリンクされたすべてのライセンスを削除する場合は、アカウントとリンクされたライセンス全体がESET PROTECTから削除されます。



3. 一覧のライセンスをライセンス管理から削除(リンク解除)する選択内容を確認します。

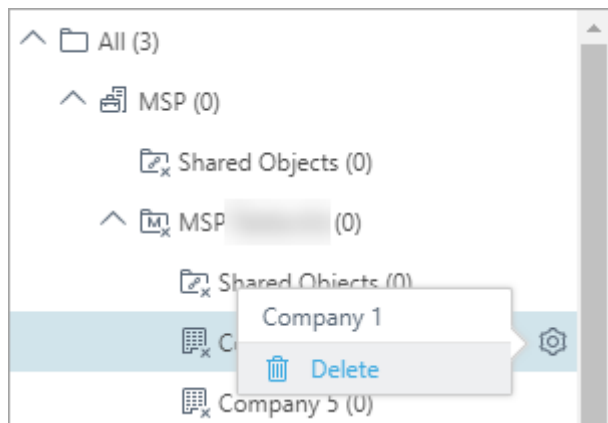
ライセンスプールを削除するときには、同じアカウントに関連付けられた他のすべてのライセンスプールを自動的に削除します。

たとえば、会社Xライセンスは、認証情報joe@test.meを使用してEMA 2からインポートされました。ユーザーが会社Xライセンスを削除する場合、joe@test.me EBAおよびEMA 2アカウントからインポートされたすべてのライセンスはライセンス管理から削除されます。



4. アクションの後少し待機して、**コンピューターメニュー**に移動します。

5. ここで、以前にMSPツリーの一部であったすべての会社をクリックして、**削除**できます。空の場合は、会社のみ(静的グループ)を削除できます。



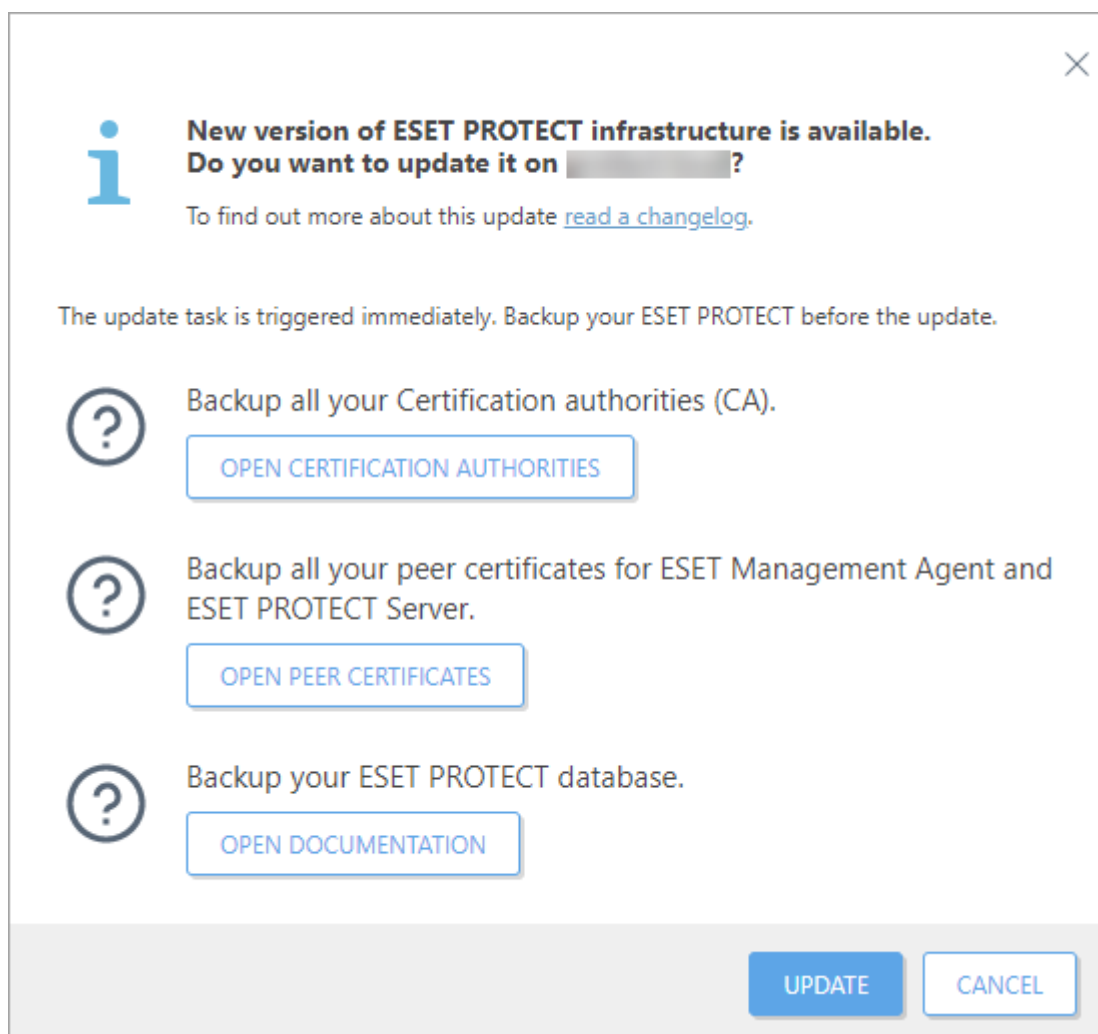
i

ライセンス管理からMSPアカウントを削除した後は、[ステータス概要](#)にMSP管理者が接続されていませんステータスが表示されます。そのステータスをオフにするには、(コンピューターメニューで)以前のMSPツリーからすべてのグループを削除する必要があります。

アップデート ESET PROTECT

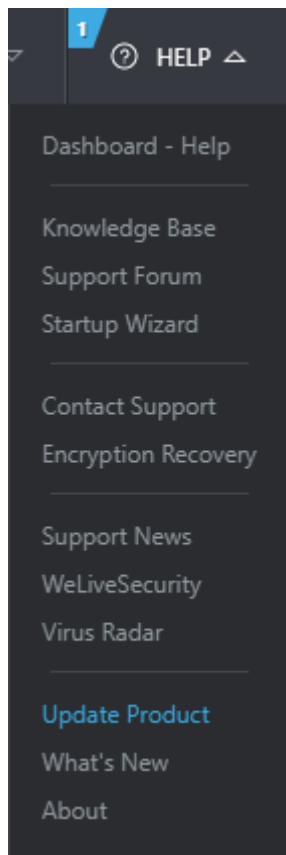
ESET PROTECTサーバーは、ESET PROTECTインフラストラクチャの利用可能なアップデートを定期的に確認します。

アップデートが利用可能なときには、ポップアップウィンドウが表示されます。



利用可能なESET PROTECTアップデートの変更を読むには、**変更ログ**をクリックします。

アップデートを選択しない場合、ヘルプ>**製品のアップデート**をクリックすると、アップデートポップアップウィンドウが表示されます。



i [ESET PROTECTコンポーネントアップグレード](#)クライアントタスクを実行できるユーザーのみが、アップデート通知を確認できます。

1. 認証局を開くボタンをクリックし、[すべてのCAをバックアップ](#)します。
2. ピア証明書を開くボタンをクリックし、[すべての証明書をバックアップ](#)します。
3. 文章を開くボタンをクリックし、[すべてのESET PROTECTデータベースをバックアップ](#)します。
4. アップデートボタンをクリックします。
5. [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。詳細については、[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](#)を参照してください。
6. アップデートボタンをクリックします。ESET PROTECTサーバーのアップデートがスケジュールされます。タスクには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ESET PROTECTコンポーネントをアップグレードする新しいタスクが表示されます。アップグレードが開始するとWebコンソールからログアウトします。アップグレードの完了後にログインできます。

ESET PROTECTサーバーに接続されたデバイスで他のESET PROTECTコンポーネントを最新バージョンにアップデートするには、アップデートポップアップウィンドウから直接[ESET PROTECTコンポーネントアップグレード](#)タスクをトリガーできます。

ESET PROTECT9.0は、管理されたコンピューターでの[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。

FAQ

質問の一覧

1. [「ログインが失敗しました。接続は未接続状態」で失敗しました](#) というエラーの解決方法を教えてください。
2. [LOST+FOUNDグループの目的は何ですか。](#)
3. [デュアルアップデートプロファイルはどのように作成するのですか。](#)
4. [ブラウザウィンドウ全体を更新せずに、ページまたはページのセクションの情報を更新する方法を教えてください。](#)
5. [ESET Management エージェントのサイレントインストールの実行方法を教えてください。](#)
6. [RD Sensor がネットワーク上の一部のコンピューターを検出しません。](#)
7. [検出の駆除後に、ESET PROTECT に表示される未解決の検出数をリセットする方法を教えてください。](#)
8. [ESET Management エージェント接続間隔のCRON式を設定する方法を教えてください。](#)
9. [自動展開用の新しい動的グループを作成する方法を教えてください。](#)
10. [ESET PROTECT 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。](#)
11. [ESET PROTECT の証明書の署名に使用できるのは、どのサードパーティの証明書ですか。](#)
12. [どのようにして Web コンソールの管理者パスワード \(Windows オペレーティングシステム上でセットアップ中に入力したパスワード\) のリセットができるのでしょうか。](#)
13. [どのようにして Web コンソールの管理者パスワード \(Linux でのセットアップ中に入力\) のリセットができるのでしょうか。](#)
14. [RD Sensor が何も検出しない場合のトラブルシューティング方法を教えてください。](#)
15. [動的グループテンプレートウィンドウに項目が表示されません。なぜですか。](#)
16. [ダッシュボードウィンドウに情報が表示されません。なぜですか。](#)
17. [どのようにして ESET セキュリティ製品をアップグレードできますか。](#)
18. [Web コンソールのアドレスでサフィックスを変更する方法](#)

Q: 「ログインが失敗しました。接続は未接続状態」で失敗しました」というエラーの解決方法を教えてく

ださい。

A:ESET PROTECT ServerサービスまたはMS SQL Serverサービスが実行中であるかどうかを確認してください。実行中でない場合は起動します。実行中の場合は、サービスを再起動し、Webコンソールを更新してから、再度ログインしてください。詳細については、「[トラブルシューティングログイン](#)」を参照してください。

Q:「LOST+FOUND」グループの目的は何ですか。

A:ESET PROTECTサーバーに接続し、静的グループのいずれのメンバーでもない各コンピューターは自動的にこのグループに表示されます。他の静的グループ内のコンピューターと同様に、グループとその中のコンピューターを操作できます。グループ名を変更したり、他のグループに移動できますが、削除はできません。

Q:デュアルアップデートプロファイルはどのように作成するのですか。

A: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。

Q:ブラウザウィンドウ全体を更新せずに、ページまたはページのセクションの情報を更新する方法を教えてください。

A:ページセクションの右上にあるコンテキストメニューで、**[更新]**をクリックします。

Q:ESET Managementエージェントのサイレントインストールの実行方法を教えてください。

A:次の方法ではサイレントインストールを実行できます：

- [GPOまたはSCCMスクリプト](#)
- [エージェント展開](#)タスク
- [ESET Remote Deployment Tool](#)

Q:RD Sensorがネットワーク上の一部のコンピューターを検出しません。

A:RD sensorはネットワーク上でパッシブにネットワーク通信をリスニングします。PCが通信していない場合は、RD Sensorでリスニングされません。DNSの設定をチェックし、DNSルックアップの問題が通信を妨げていないことを確認してください。

Q:検出の駆除後に、ESET PROTECTに表示される未解決の検出数をリセットする方法を教えてください。

A:未解決の検出数をリセットするにはESET PROTECTを介してターゲットコンピューターにフルスキャン(詳細検査)を開始する必要があります。手動で検出を駆除した場合は、解決済みにすることができま

す。

Q:ESET Management エージェント接続間隔のCRON式を設定する方法を教えてください。

A: P_REPLICATION_INTERVAL は CRON 式を許可しています。

既定は「R R/20 *** ? *」です。これは、ランダムな20分ごと(3、23、43、または17、37、57など)にランダム秒(R=0-60)で接続することを意味します。ランダム値は時間をロードバランシングして使用する必要があります。このため、すべてのESET Management エージェントは異なるランダム時間で接続しています。「0 * * * * ? *」などの正確なCRONが使用される場合、この設定のすべてのエージェントは同時に接続します(毎分:00秒)。この時間にはサーバー上で負荷のピークが発生します。詳細については、[CRON式の間隔](#)を参照してください。

Q:自動展開用の新しい動的グループを作成する方法を教えてください。

A:段階的な手順については、[ナレッジベース記事](#)を参照してください。

Q:ESET PROTECT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。

A:次の行が含まれたファイルです。

```
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

Q:ESET PROTECTの証明書の署名に使用できるのは、どのサードパーティの証明書ですか。

A:証明書はCA(または中間CA)証明書で、`'keyUsage'`制約の「`'keyCertSign'`」フラグが付いている必要があります。つまり、他の証明書を署名するために使用できます。

Q:どのようにしてWebコンソールの**管理者パスワード(Windowsオペレーティングシステム上でセットアップ中に入力したパスワード)**のリセットができるのでしょうか。

A: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認証を使用しなかった場合は、ESET PROTECTデータベースのパスワードが必要になることがあります。このトピックで、[ナレッジベース記事](#)を参照してください。



- 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、[二要素認証](#)は無効になります。

Q:どのようにしてWebコンソールの**管理者パスワード(Linuxでのセットアップ中に入力)**のリセットがで

きるのでしょうか。

A:十分な権限の別のユーザーがESET PROTECTにある場合、管理者アカウントパスワードをリセットできます。ただし、管理者がシステムの唯一のアカウント(インストール時に作成)の場合、このパスワードはリセットできません。このトピックで、[ナレッジベース記事](#)を参照してください。

Q:RD Sensor が何も検出しない場合のトラブルシューティング方法を教えてください。

A:OSがネットワークデバイスとして検出された場合は、それはコンピューターとしてESET PROTECTに送信されません。ネットワークデバイス(プリンタ、ルータ)は除外されます。RD Sensorは *libpcap version 1.3.0* に準拠しています。システムにこのバージョンがインストールされていることを確認してください。もう1つの要件は、RD Sensorがインストールされている仮想マシンからのブリッジネットワークです。これらの要件が満たされる場合は、OS検出でnmapを実行(<http://nmap.org/book/osdetect-usage.html>)し、コンピューターでOSを検出できるかどうか確認してください。

Q:動的グループテンプレートウィンドウに項目が表示されません。なぜですか。

A:ほとんどの場合、そのユーザーには十分な権限がありません。ユーザーが少なくとも動的グループテンプレートの読み取り権限が割り当てられた静的グループに含まれる場合にのみ、テンプレートが表示されます。

Q:ダッシュボードウィンドウに情報が表示されません。なぜですか。

A:ほとんどの場合、そのユーザーには十分な権限がありません。データを表示するには、ユーザーにコンピューターとダッシュボードに対する権限が必要です。[権限設定の例](#)を参照してください。

Q:どのようにしてESETセキュリティ製品をアップグレードできますか。

A:[ソフトウェアインストール](#)タスクを使用して、アップグレードする製品を選択します。

Q:Webコンソールのアドレスでサフィックスを変更する方法

A:たとえばWebコンソールが10.1.0.5/eraで、サフィックスeraを変更する場合は、フォルダー名自体を変更しないでください。アドレスの変更は推奨されませんが、必要な場合は、別の名前でwebappsフォルダーにリンクを作成します。


たとえばLinuxまたは仮想アプライアンスで、次のコマンドを使用できます。

```
ln -sf /var/lib/tomcat/webapps/era/ /var/lib/tomcat/webapps/esmc
```

ターミナルでコマンドを実行した後、Webコンソールに10.1.0.5/esmcでアクセスすることもできます(独自のIPアドレスを変更)。

ESET PROTECTについて

[バージョン情報]ウィンドウを開くには、[ヘルプ]>[バージョン情報]に移動します。このウィンドウにはESET PROTECTのバージョンに関する詳細が表示されます。ウィンドウの上部には、接続中のクライアントデバイス数とアクティブなライセンス数の情報があります。また、インストールされているプログラムモジュールのリスト、オペレーティングシステム、モジュールアップデートをダウンロードするためにESET PROTECTによって使用されるライセンス(ESET PROTECTをアクティベーションするために使用されるのと同じライセンス)が表示されます。のデータベースに関する情報(名前、バージョン、サイズ、ホスト名、ユーザーなど)がこのウィンドウに表示されます。

 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](#)をご覧ください。

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(ii) 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。メールサーバー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るかぎり、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.エンドユーザーの権利行使。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(ii) 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ー、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