WEBROOT®

an opentext™ company

エンドポイントプロテクション管理者ガイド

著作権

ウェブルートエンドポイントプロテクション管理者ガイド

目次

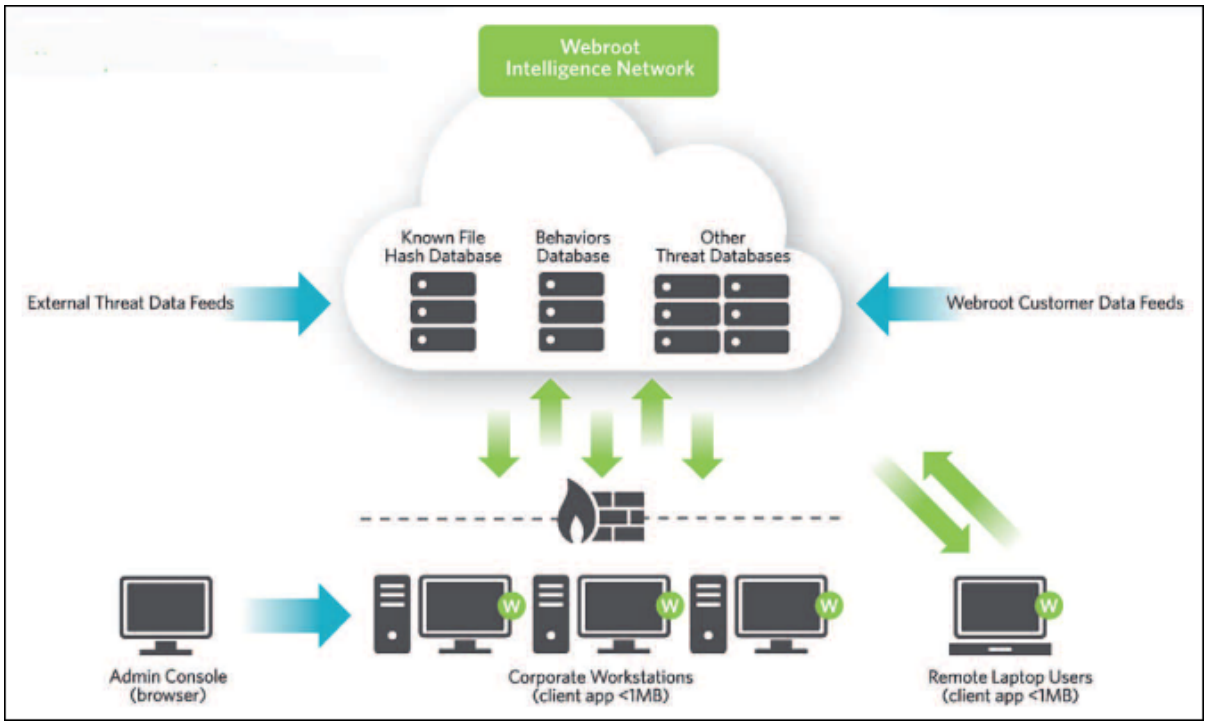
第 1 章: WSA Business エンドポイントプロテクション管理者ガイド

エンドポイントプロテクションの基本情報については、以下のトピックを参照してください。

WSA Business - エンドポイントプロテクション管理者ガイドの概要

Webroot SecureAnywhere™ Endpoint Protection は、ウェブルートによる動作の認識技術とクラウドコンピューティングを組み合わせて、マルウェアなどの脅威から企業を守ります。エンドポイントプロテクションには、エンドポイントの表示と管理に使用する一元的な Web サイトである管理ポータル (管理コンソールとも呼ばれます) があります。

PC、ノートパソコン、サーバー、仮想サーバーなど、Windows のあらゆる企業向けワークステーションをエンドポイントとして使用できます。これらのエンドポイントへの SecureAnywhere ソフトウェアの配備はわずか数秒で完了でき、ユーザーの保護を即座に開始できます。SecureAnywhere はエンドポイントのスキャンを実行し、管理ポータルにエンドポイントの状態を報告します。



このオンラインヘルプでは、管理者による SecureAnywhere の配備方法と、管理ポータルを使用した脅威に対する警告やデータのグラフ、エンドポイントのアクティビティに関するその他の情報の表示方法を説明します。実行できるタスクは、与えられているアクセス権限と、エンドポイントの設定時に選択した管理モードによって異なります。このガイドは、完全なアクセス権限を与えられた状態でエンドポイントプロテクションを使用する管理者を対象としています。

第 2 章: エンドポイントプロテクションの基本情報

エンドポイントプロテクションの基本情報については、以下のトピックを参照してください。

システム要件

システム要件については、Business エンド ポイント プロテクション Web ページのシステム要件のセクションを参照してください。

セットアップの準備

このセクションの設定手順を読み、環境がシステム要件を満たしていることを事前に確認してください。

注意: 以下の設定手順は、完全なアクセス権限を与えられたエンドポイントプロテクション管理者を対象としています。

設定手順

1. キーコードを使用してアカウントを作成します。

   キーコードは事前にウェブルートから電子メールで送信されています。詳細については、「*アカウントの作成 ページ11*」を参照してください。

2. 管理ポータルにログインし、セットアップウィザードを開きます。

   ウィザードでは、エンドポイントへの SecureAnywhere のインストールにデフォルトのポリシーを選択する必要があります。

   - ポリシーは、プログラムが脅威をスキャンする方法や検出されたアイテムを管理する方法など、SecureAnywhere の設定を定義するものです。
   - PC、ノートパソコン、サーバー、仮想サーバーなど、Windows のあらゆる企業向けワークステーションをエンドポイントとして使用できます。

   ポリシーを選択すると [ようこそ] ウィンドウが表示され、SecureAnywhere のエンドポイントへの配備方法に関する情報が提示されます。詳細については、「*ログインとセットアップウィザードの使用 ページ24*」を参照してください。

3. 連絡先の電話番号や所在地のタイムゾーンなど、管理ポータルのアカウント設定を編集します。詳細については、「*自分のアカウント設定の編集 ページ55*」を参照してください。

   また、他の管理者が管理ポータルにアクセスできるよう、ログインを作成することもできます。詳細については、「*ポータルユーザーの管理 ページ68*」を参照してください。

   注意: この手順は任意です。

4. SecureAnywhere ソフトウェアをエンドポイントに配備します。詳細については、「*エンドポイントへの SecureAnywhere の配備 ページ112*」を参照してください。
5. デフォルトのポリシーがビジネス要件を満たしているかを判断します。ウェブルートのデフォルトのポリシーは変更できません。

   必要に応じて、設定の異なる新しいポリシーを追加してください。詳細については、「*ポリシーの導入 ページ222*」を参照してください。また、正当なアプリケーションと思われるファイルに対して、オーバーライドを作成する必要がある場合があります。詳細については、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。

6. 管理目的に応じて、複数のエンドポイントのグループを作成する必要があるかを判断します。

   SecureAnywhere をエンドポイントに配備する際、エンドポイントプロテクションはすべてを 1 つのデフォルトグループに配備します。必要に応じて、新しいグループを作成し、それらを新しいポリシーに割り当てることができます。詳細については、「*エンドポイントをグループに整理 ページ330*」を参照してください。

7. エンドポイントが感染を報告した際、または新しいエンドポイントに SecureAnywhere がインストールされた際に、レポート配信先リストに送信される警告メッセージをカスタマイズします。詳細については、「*警告の導入 ページ405*」を参照してください。

   注意: この手順は任意です。

ファイアウォールを介した通信

ファイアウォールがある場合、以下の表に記載されたウェブルートのパスマスクを許可してください。

パス	ポート	詳細
***.webrootcloudav.com**	ポート 443 (https)	エージェントの通信とアップデート。 **注意:** 一部のファイアウォールでは、単一のワイルドカードマスクを使用したダブルドットを含むサブドメイン名 (例: 「g1.p4.webrootcloudav.com」を「*.webrootcloudav.com」で表示) をサポートしていません。このため、一部の環境では「*.p4.webrootcloudav.com」または「*.*.webrootcloudav.com」のいずれかにしなければならないことがあります。
***.webroot.com**	ポート 443 (https)	エージェントのメッセージ送受信。
https://wrskynet.s3.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードとアップロード。
https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードとアップロード。
https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*	ポート 443 (https)	エージェントのファイルのダウンロードとアップロード。

パス	ポート	詳細
WSAWebFilteringPortal.elasticbeanstalk.com	ポート 80 (http) & 443 (https)	エージェントの Web フィルタリングに必要。elasticbeanstalk は Amazon の AWS ドメイン。
***.webrootanywhere.com**	ポート 80 (http) & 443 (https)	管理ポータルとサポートチケットログのアップロード。

Webroot SecureAnywhere Business - Endpoint Protection でプロキシ設定を使用する際は、ご使用の製品がウェブルートのクラウドサーバーと通信できるようにする方法が他にもあります。詳細については、以下を参照してください。

プロキシバイパスの入力

注意: ウェブルート推奨の方法です。

プロキシバイパスを入力するには

1. g*.p4.webrootcloudav.com のプロキシバイパスを入力します。

   注意: このオプションを選択する場合、ワイルドカードマスク (*) がサポートされていることを確認してください。サポートされていない場合、g1、g2、g3、... g99、g100 のように 100 個の URL を個別に追加しなければなりません。

インストーラー内でのプロキシ情報の入力

これはウェブルートが推奨する別の方法です。

インストーラー内でプロキシ情報を入力するには

1. SecureAnywhere MSI インストーラーをネットワーク共有にダウンロードします。

   http://anywhere.webrootcloudav.com/zerol/wsasme.msi

2. msi エディタを使用します。
3. プロパティの表で、以下のコマンドを使用して GUILIC プロパティに定期購入契約のキーコードを、CMDLINE プロパティにプロキシの資格情報をそれぞれ入力します。

   ```
   -proxyhost=X -proxyport=X -proxyuser=X -proxypass=X -proxyauth=#
   ```

4. すべてのパラメータを使用し、不要なパラメータについては値を入力せずに二重引用符のみを入力してください。以下のように入力します。

   ```
   proxypass=""

   proxyauth # being: 0 = Any authentication 1 = Basic 2 = Digest 3 = Negotiate 4 = NTLM
   ```

5. これらの引数は実行可能なインストールで適用することも可能です。以下のように入力します。

   ```
   C:\wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn.nn -proxyauth=n -
   proxyuser="proxyuser" -proxypass="password" -proxyport=port_number
   ```

配備後の各エンドポイントでのプロキシ情報の入力

この方法は、プロキシバイパスを入力できない場合や、インストーラー内でプロキシ情報を入力できない場合にのみお勧めします。

1. SecureAnywhere エンドポイントプロテクションの [グループの管理] タブを開き、グループを開いて、エンドポイントを選択します。
2. 選択したエンドポイントの [ポリシー] カラムでポリシー名をダブルクリックし、使用可能なポリシーの一覧を表示します。
3. 非管理ポリシーを選択して適用します。新しいポリシー名に赤いフラグが付き、変更されたことを示します。
4. [**変更を保存**] をクリックします。
5. ポリシーが適用されたら、各エンドポイントのワークステーションで以下の手順に従います。
6. システムトレイアイコンから SecureAnywhere エンドポイントプロテクションを開きます。
7. [**設定**] をクリックします。
8. [設定] ウィンドウで [**プロキシ**] タブをクリックします。

9. プロキシ情報を入力します。
10. [**すべて保存**] をクリックして変更を保存します。
11. プロキシ情報を入力した後、マシンを元のポリシーに戻すことができます。

> **注意:** プロキシ設定の最適なテスト方法は、デフォルトのゲートウェイ経由でのインターネットアクセスが存在しないことを確認することです。デフォルトのゲートウェイや DNS サーバーを追加しなくても、エンドポイントのネットワークカードの IP アドレスおよびサブネットマスクをハードコード化することができます。プロキシサーバーが同じサブネット上にある限り、プロキシサーバー経由以外のインターネットアクセスが存在しないことを確信できます。.

アカウントの作成

エンドポイントプロテクションにログインする前に、ライセンスキーコードを使用してアカウントを作成する必要があります。キーコードは、アクティブ化と設定の手順に関する電子メールに記載されています。

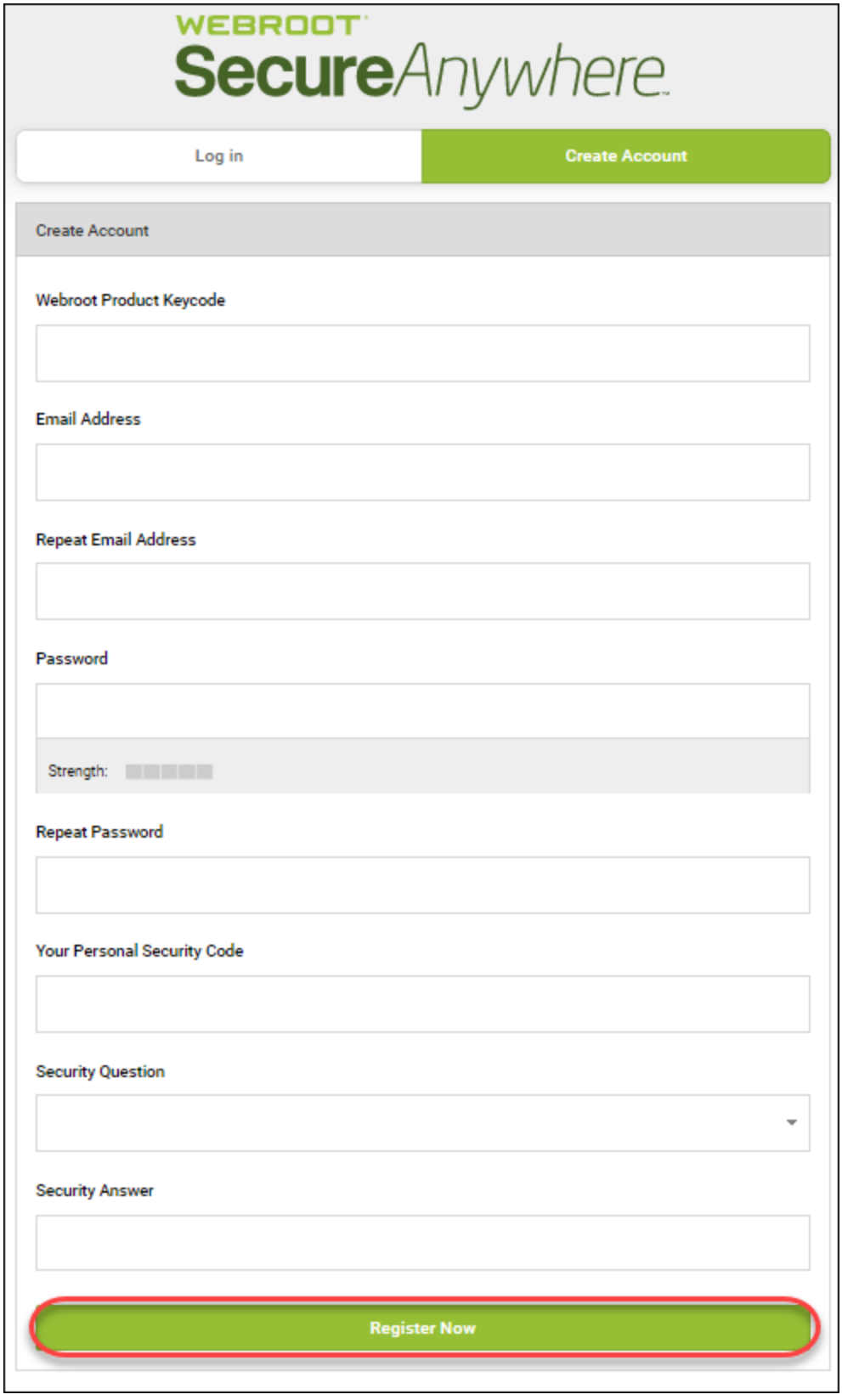
アカウントを作成するには

1. 管理コンソールに移動し、[**アカウントの作成**] ボタンをクリックします。
2. 製品キーコードと管理者の電子メールアドレスを入力します。また、パスワードと個人用セキュリティコードを作成します。詳細については、以下の表の情報を参照してください。

フィールド	説明
ウェブルート製品のキーコード	エンドポイントプロテクションの購入時に受け取ったライセンスキーコードを入力します。
電子メールアドレス	エンドポイントプロテクションを管理する管理者の電子メールアドレスを入力します。 アカウントをアクティブ化するための確認のメッセージがこの電子メールアドレスに送信されます。このメールアドレスは、管理ポータルにログインする際のユーザー名にもなります。
パスワード	9 文字以上を入力してください。パスワードは、少なくともアルファベット 6 文字と数字 3 文字を含む必要があります。パスワードは最小文字数の 9 文字を超えても問題ありません。山括弧 (< >) 以外の特殊文字は使用可能です。パスワードの大文字と小文字は区別されます。 入力を始めると、強度メーターがパスワードの安全性を示します。最適なセキュリティを確保するために、パスワードはできるだけ強力なものにすることをお勧めします。

フィールド	説明
個人用セキュリティコード	文字または数字を入力してください。ログインする際に、パスワードを入力した後の追加のセキュリティ対策として使用されます。6 文字以上で、覚えやすいコードを使用してください。 管理ポータルへのログイン時には毎回、このコードからランダムな 2 文字を入力するように求められます。たとえば、コードが *123456* で、4 番目と 6 番目の文字を入力するよう求められた場合、「4」と「6」を入力します。この個人用セキュリティコードでは大文字と小文字が区別されます。
セキュリティの質問	ドロップダウンリストから質問を選択します。 ログインの詳細情報を忘れた場合に、この質問に答えることで情報を取得できます。
セキュリティの回答	セキュリティの質問に対する回答を入力します。セキュリティの回答では大文字と小文字が区別されます。

3. アカウントの詳細を入力したら、[**今すぐ登録**] ボタンをクリックします。


WEBROOT
SecureAnywhere
Log in
Create Account
Create Account
Webroot Product Keycode
Email Address
Repeat Email Address
Password
Strength:
Repeat Password
Your Personal Security Code
Security Question
Security Answer
Register Now

SecureAnywhere により確認メッセージが表示され、指定した管理者の電子メールアドレスに確認のメールが送信されます。これには数分かかることがあります。

4. 電子メールのアプリケーションを開き、確認の電子メールメッセージに記載されたリンクをクリックします。

   SecureAnywhere の登録確認ページが開いたら、アカウント作成の際に指定したセキュリティコードからランダムに選択された 2 文字を入力します。

5. [**今すぐ登録確認する**] をクリックします。

   セキュリティコードを入力すると、2 要素認証 (2FA) の設定に関するオプションが表示されます。このトピックの詳細については、「*2 要素認証 (2FA) の有効化 ページ16*」を参照してください。

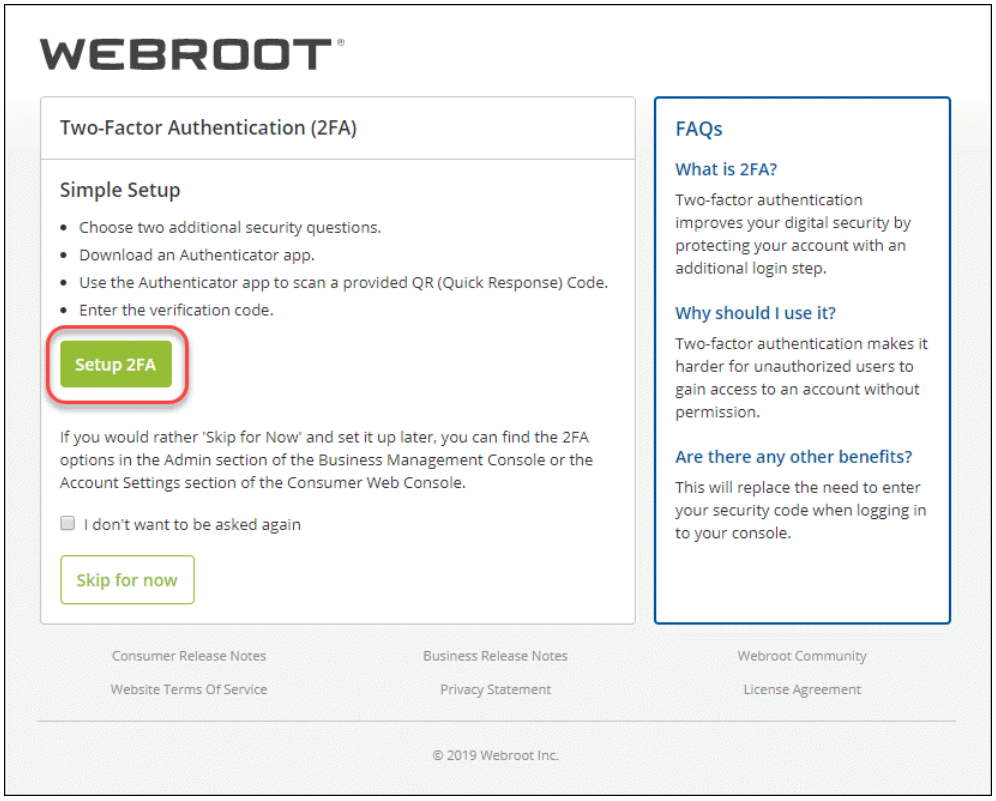
---

2 要素認証 (2FA) の有効化

Webroot SecureAnywhere では、2 要素認証 (2FA) を有効化することで、承認されていないユーザーによるアカウントへの無許可のアクセスを防止できます。

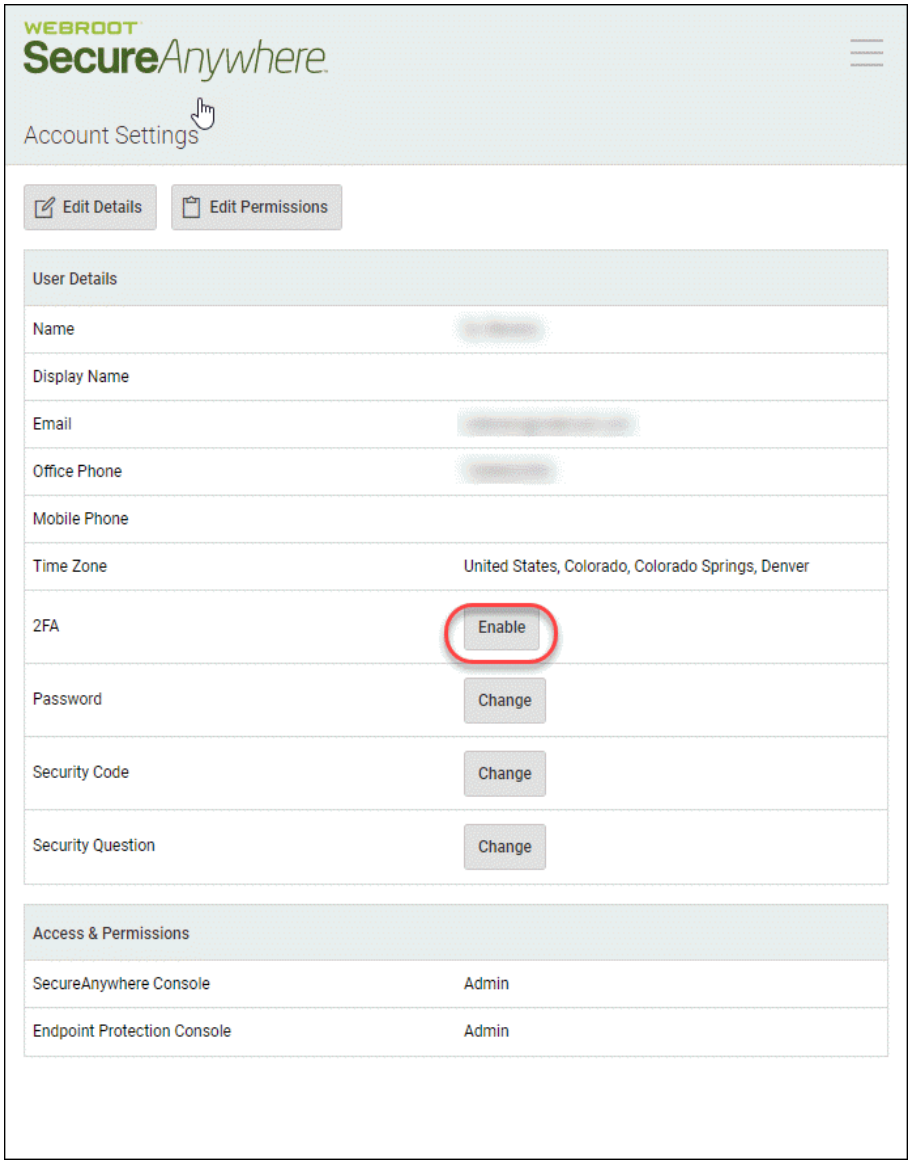
2FA を有効にするには

1. まず、ウェブルートの管理コンソールに移動し、ビジネス管理者アカウントの資格情報を使用してログインします。
2. 2FA の設定画面が表示されます。管理コンソールへのログインが初めての場合は、[**2FA を設定する**] をクリックしてプロセスを開始することも、[今はスキップする] をクリックしてコンソールを開くこともできます。

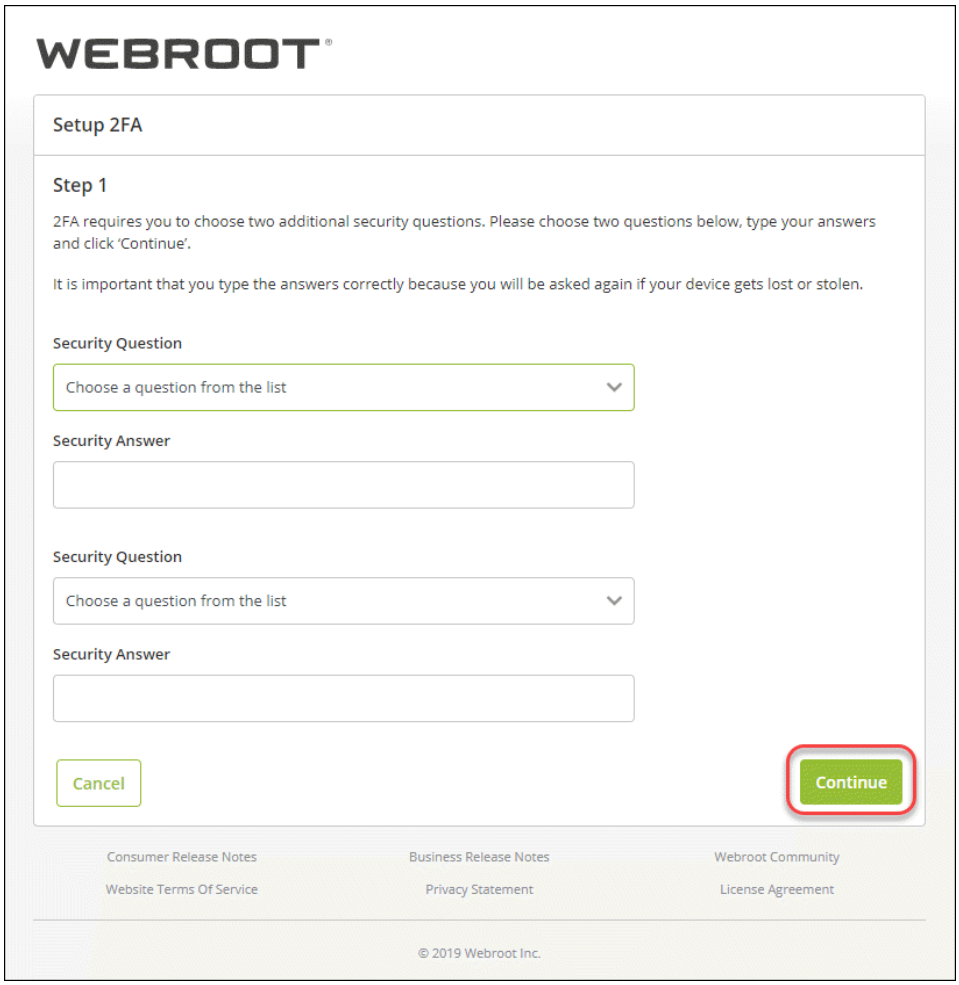


以前に管理コンソールにログインし、2FA を設定するプロセスのスキップを選択している場合は、こちらをクリックして最初に 2FA の設定をスキップした後に 2FA を有効化する手順を確認してください。

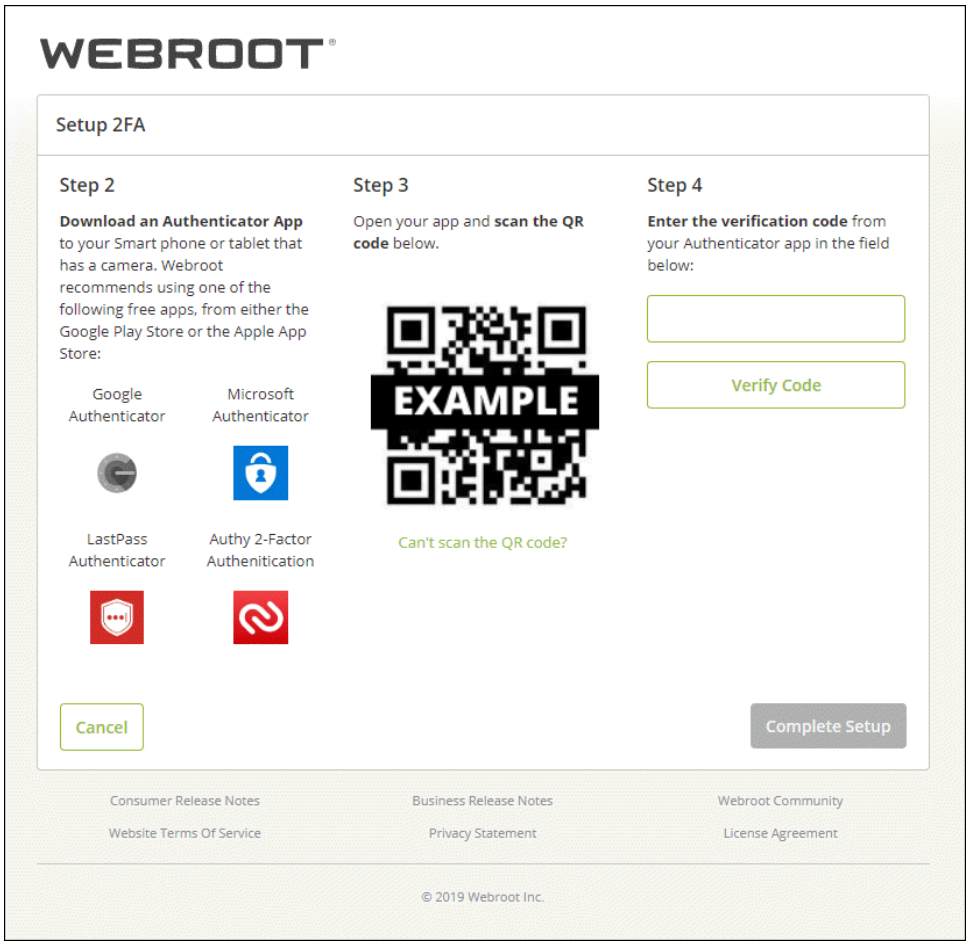
2FA の設定プロセスは、エンドポイントコンソールの右上隅にある [**アカウント設定**] から開始することもできます。ユーザーの詳細情報が表示される [アカウント設定] ページで [**有効化**] をクリックします。



3. 次に表示される [**2FA を設定する**] 画面で、セキュリティの質問を 2 つ選択して回答を入力するよう求められます。設定が完了したら、[**続行**] をクリックします。


WEBROOT
Setup 2FA
Step 1
2FA requires you to choose two additional security questions. Please choose two questions below, type your answers and click 'Continue'.
It is important that you type the answers correctly because you will be asked again if your device gets lost or stolen.
Security Question
Choose a question from the list
Security Answer
Security Question
Choose a question from the list
Security Answer
Cancel
Continue
Consumer Release Notes
Business Release Notes
Webroot Community
Website Terms Of Service
Privacy Statement
License Agreement
© 2019 Webroot Inc.

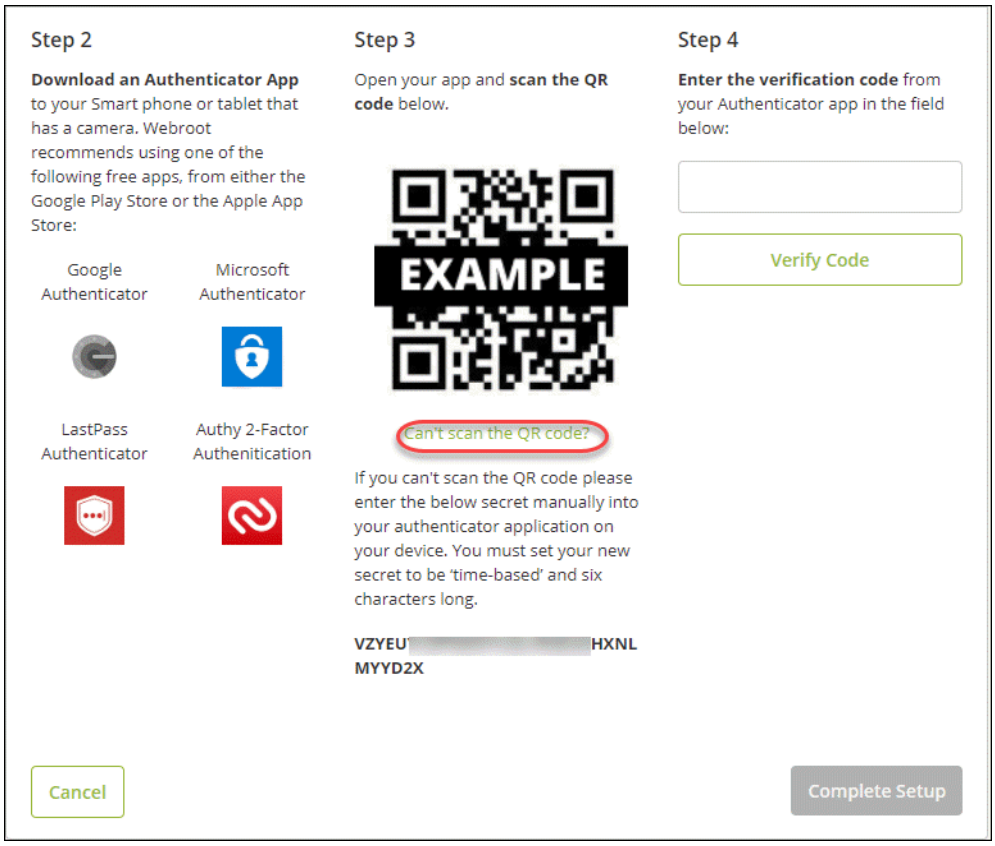
4. スマートフォンまたはカメラ付きタブレットに、Google Play ストアまたは Apple App Store から認証用アプリをダウンロードしてインストールする必要があります。



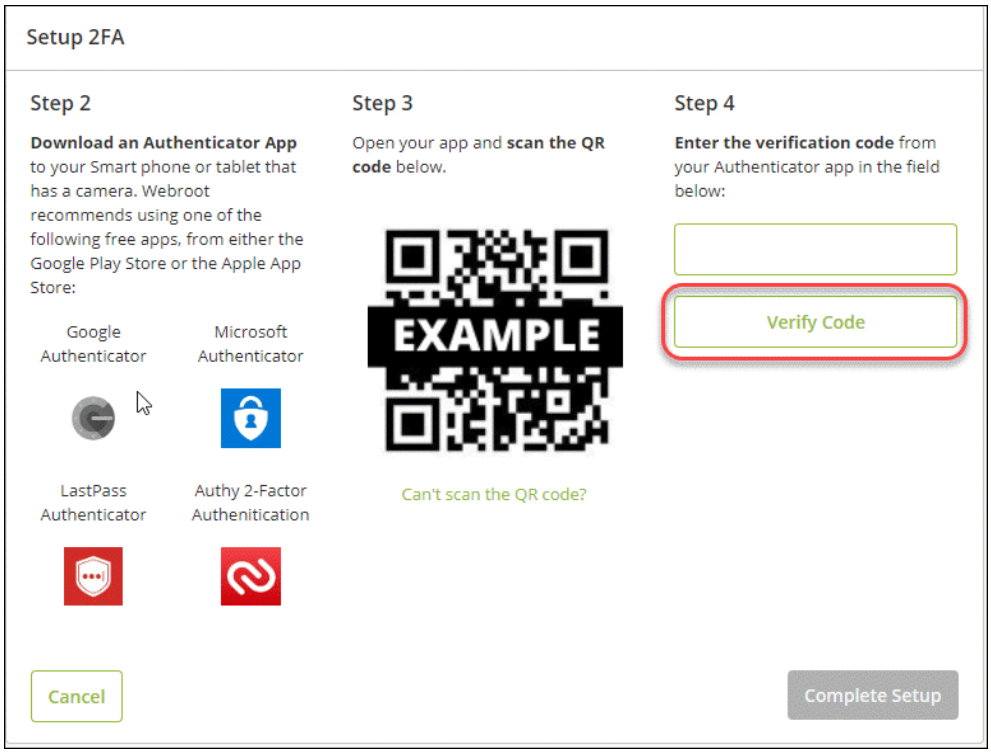
モバイル認証用アプリの例は以下のとおりです。

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy の 2 要素認証

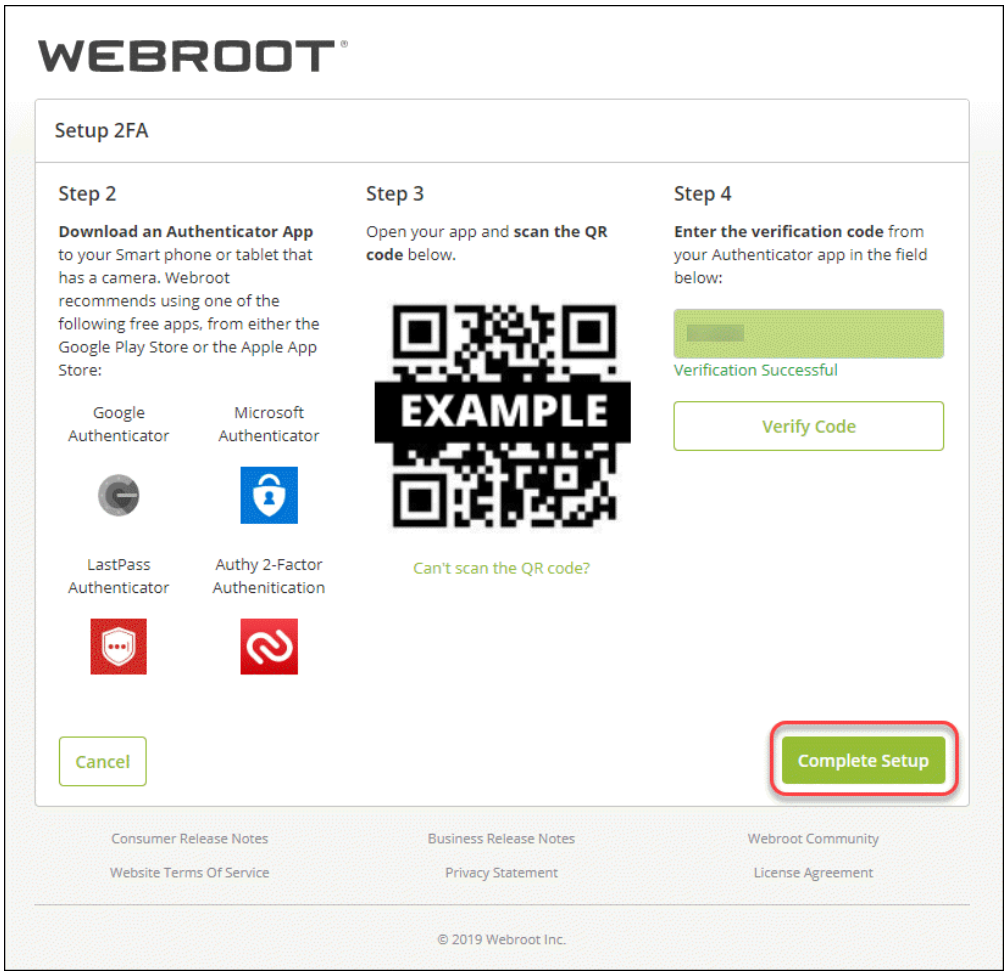
5. 認証用アプリをダウンロードしたら、アプリを開き、画面の指示に従ってアプリがスマートフォンのカメラにアクセスできるようにします。これにより、管理コンソールに表示される QR コードをスキャンできるようになります。QR コードをスキャンできない場合は、ディスプレイの明るさを調整するか、[**QR コードをスキャンできない場合**] をクリックして、表示されたコードをデバイスの認証アプリに入力します。コードの大文字と小文字は区別されます。



6. 認証アプリから取得した認証コードを [**ステップ 4**] のボックスに入力し、[**認証コードを確認する**] をクリックします。


Setup 2FA
Step 2
Download an Authenticator App to your Smart phone or tablet that has a camera. Webroot recommends using one of the following free apps, from either the Google Play Store or the Apple App Store:
Google Authenticator
Microsoft Authenticator
LastPass Authenticator
Authy 2-Factor Authenitication
Step 3
Open your app and scan the QR code below.
EXAMPLE
Can't scan the QR code?
Step 4
Enter the verification code from your Authenticator app in the field below:
Verify Code
Cancel
Complete Setup

7. コードの確認が行われ、"認証が成功しました というメッセージが画面に表示されます。[**設定を完了する**] をクリックして 2FA の設定を完了します。

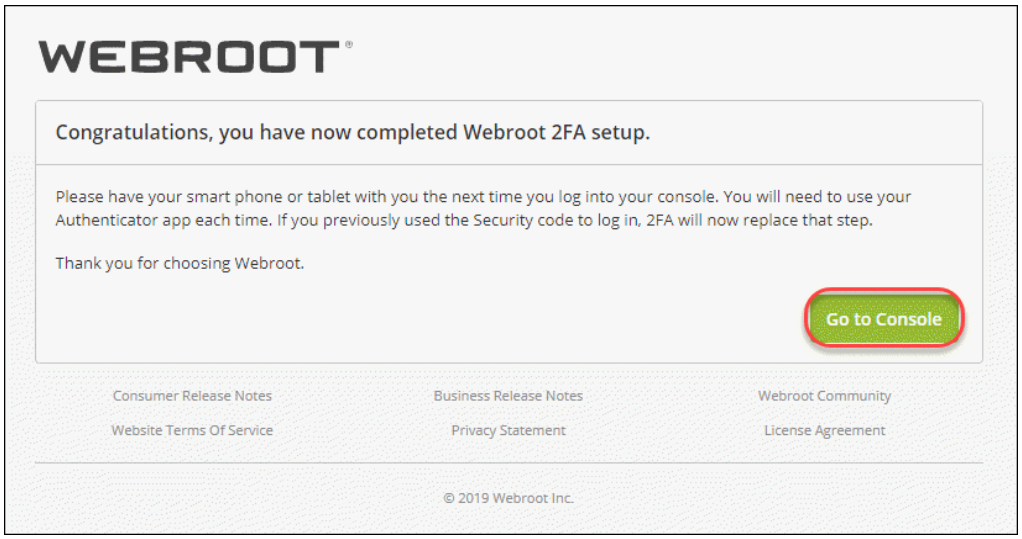


注意: コードは 30 秒で有効期限が切れるため、コードの入力時に "認証に失敗しました" というメッセージが表示された場合は、認証アプリから新しいコードを取得して入力し、[**認証コードを確認する**] をクリックする必要があります。

8. 2FA が有効になり、"おめでとうございます!" という画面が表示されます。[**コンソールに進む**] をクリックし、2FA を使用してエンドポイントプロテクションのコンソールにログインします。

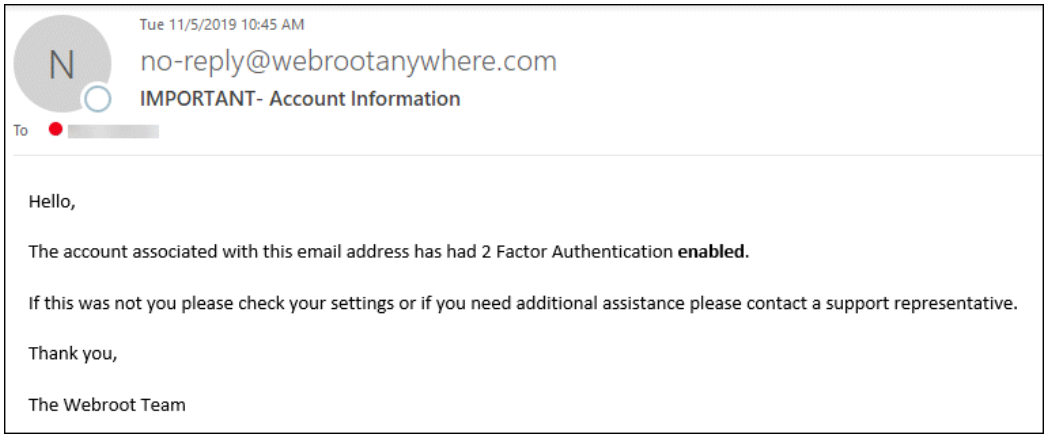
   ログイン時に入力する認証用コードは認証用アプリから提供されます。このコードがセキュリティコードの

代わりになります。



注意: セキュリティコードはアカウントに保存され、2FA が無効になった場合に使用されます。

9. アカウントで 2FA が有効になったことを知らせる電子メールが no-reply@webrootanywhere.com から届きます。



これでエンドポイントプロテクションのコンソールにログインして、設定を開始できます。詳細については、「*ログインとセットアップウィザードの使用 ページ24*」を参照してください。

ログインとセットアップウィザードの使用

アカウントを作成すると、管理ポータルにログインできるようになります。初回のログイン時にセットアップウィザードが開き、設定を開始することができます。

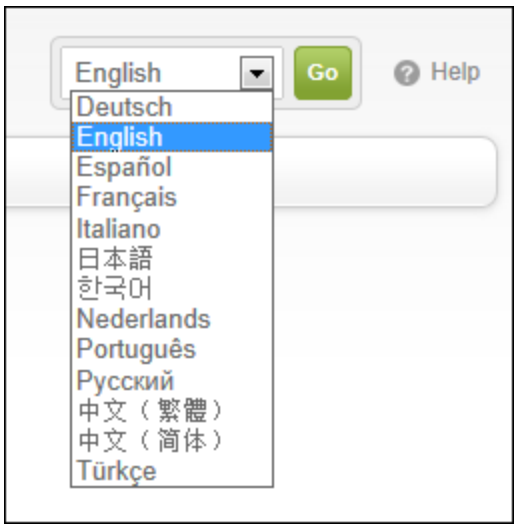
このトピックでは、次の手順について説明します。

- ログイン
- 設定中のデフォルトのポリシーの選択
- 配備方法の選択とテストインストールの実行

詳細については、「*アカウントの作成 ページ11*」を参照してください。

初回のログイン

1. SecureAnywhere Web サイトに移動します。
2. 英語以外の言語で表示するには、ページ下部のドロップダウン矢印をクリックし、目的の言語を選択します。

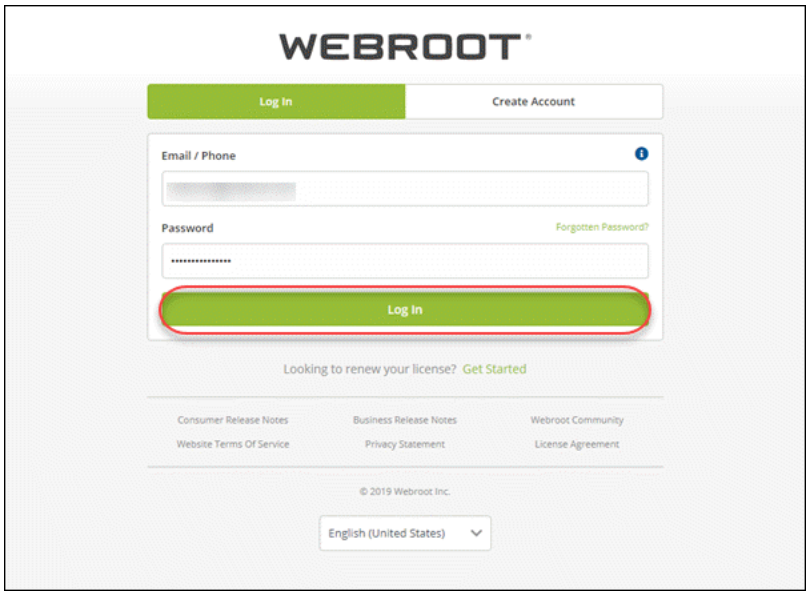


注意： ダブルバイト文字セットを使用する言語を有効にするには、適切な言語パックがコンピュータにインストールされている必要があります。computer.

3. [ログイン] 画面で、アカウント作成時に指定した電子メールアドレスとパスワードを入力します。

> **注意:** 光通信のユーザーは、[電話番号] タブをクリックすると、電話番号とパスワードを使ってログインできます。[電話番号] タブはすべてのユーザーに表示されますが、光通信ユーザー以外は電子メールアドレスとパスワードでログインしてください。

4. [**ログイン**] ボタンをクリックします。



</bpt>1ログインに 3 回失敗すると、パスワードまたはセキュリティコードをリセットするリンクを記載した電子メールが送信されます。

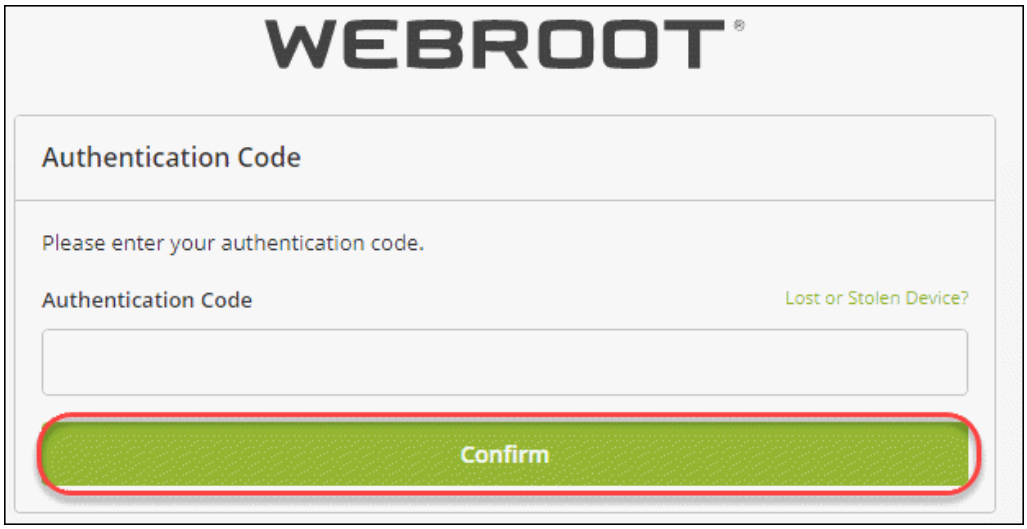
Iさらに、次のメッセージが表示されます。

"残念ながら、このコンソールへのアクセス試行の最大限度回数を超えました。15 分後にコンソールへのアクセスを試みることができます。アカウント情報を忘れた場合は、https://my.webrootanywhere.comにアクセスし [**パスワードをお忘れですか。**] リンクをクリックしてください。"

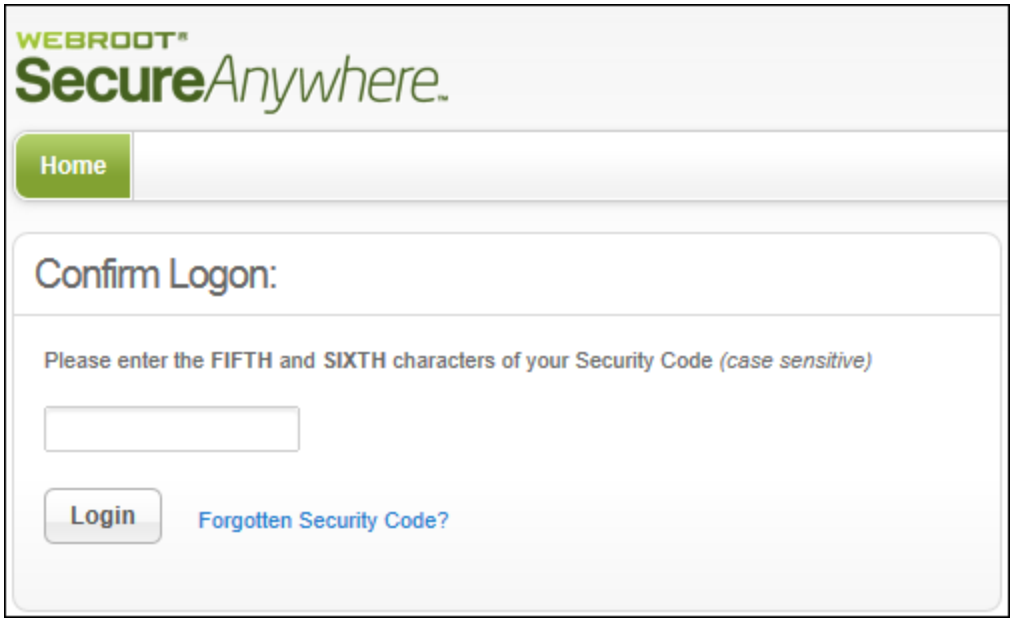
パスワードまたはセキュリティコード忘れた場合は、[**パスワードをお忘れですか。**] リンクをクリックして、[**パスワードを忘れました**] または [**セキュリティコードをお忘れの場合**] をクリックします。

システムから電子メールアドレスを入力するよう求められ、パスワードまたはセキュリティコードをリセットするリンクを記載した電子メールが送信されます。

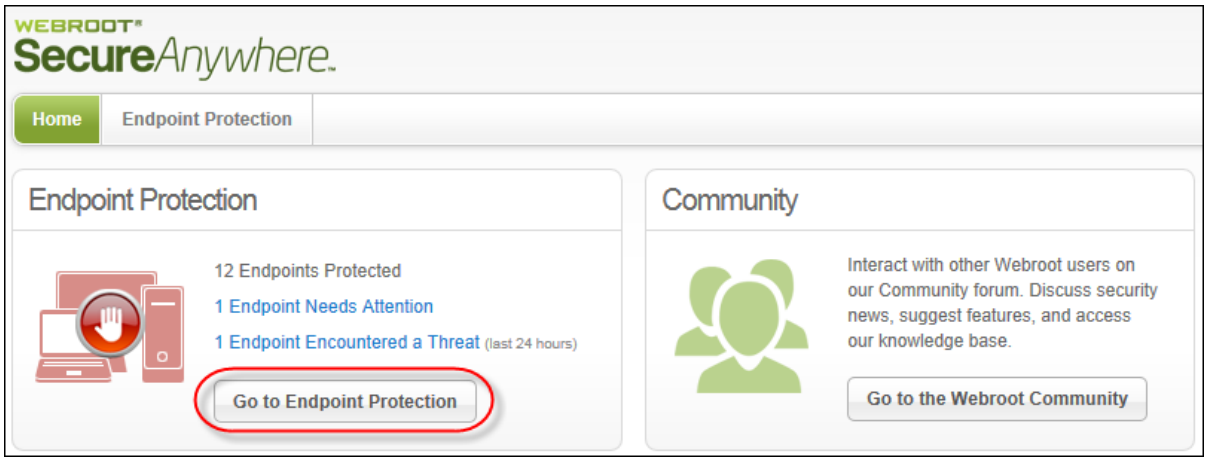
5. 2FA を有効にしている場合は、モバイル認証用アプリに表示されたコードを [ログオン確認] ウィンドウに入力し、[**確認**] ボタンをクリックします。



2FA を有効にしていない場合は、[ログオン確認] ウィンドウでウェブルートアカウントの登録時に作成したセキュリティコードを入力します。エンドポイントプロテクションは、ログイン時に毎回この追加のセキュリティ手順を要求します。このコードからランダムな 2 文字を入力するよう求められます。たとえば、コードが 123456 で、4 番目と 6 番目の文字を入力するよう求められた場合は、「4」と「6」を入力します。.



6. SecureAnywhere Web サイトにアクセスできたら、[**エンドポイントプロテクションに進む**] ボタンをクリックします。

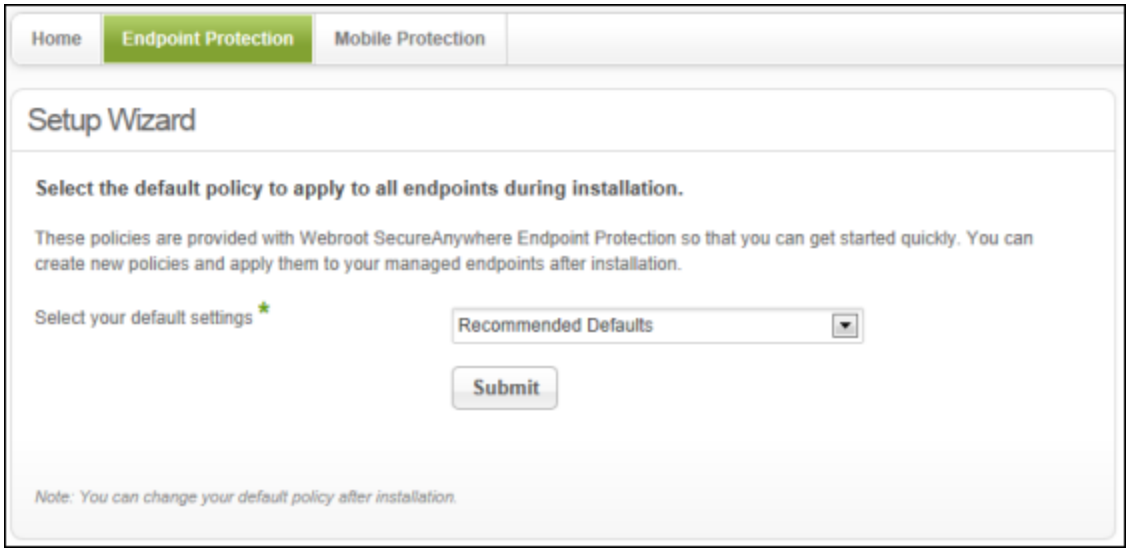


注意: モバイルプロテクションも購入した場合は、モバイルプロテクションのポータルにもアクセスできます。購入していない場合は [モバイルプロテクション] パネルは表示されません。詳細については、WSA Business - モバイルプロテクション管理者ガイドを参照してください。

初めてログインするときに、セットアップウィザードが表示されます。「設定中のデフォルトのポリシーの選択」に進んでください。

設定中のデフォルトのポリシーの選択

セットアップウィザードで、Windows エンドポイントでの新規の SecureAnywhere のインストールに適用するデフォルトのポリシーを選択するよう求められます。ポリシーは、プログラムが脅威をスキャンする方法や検出されたアイテムを管理する方法など、SecureAnywhere の設定を定義するものです。



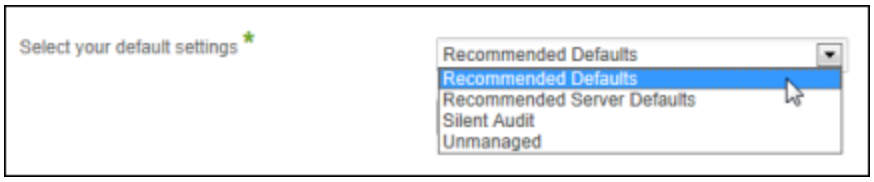
セットアップウィザードは次のようなデフォルトのポリシーを提供します。

- **推奨デフォルト設定** - 脅威に対する自動削除と隔離機能を備えた推奨セキュリティ設定です。
- **推奨サーバーデフォルト設定** - 脅威に対する自動削除と隔離機能を備えたサーバー向けの推奨セキュリティ設定です。サーバーが最適なパフォーマンスで実行されるようにします。
- **サイレント監査** - ユーザーの操作なしで脅威をスキャンします。検出されたアイテムのブロックまたは隔離は行いません。このポリシーでは、SecureAnywhere が検出した脅威をユーザーが最初に確認できるため、ユーザーは検出されたアイテムを確認し、すべての正当なアプリケーションファイルにオーバーライドを追加することができます。このポリシーは、誤検出に対する懸念がある場合や、SecureAnywhere を重要なサーバーに適用する際に使用します。検出されたアイテムを自動修正する厳格なポリシーを適用する前に、オーバーライドをあらかじめ設定する際に便利です。オーバーライドの詳細については、「*[オーバーライド]タブからのオーバーライドの適用 ページ439*」を参照してください。
- **管理対象外** - 推奨されるセキュリティを設定します。ユーザーは SecureAnywhere 設定をエンドポイントで変更できます。管理対象外のエンドポイントは引き続き管理ポータルへの報告を行い、スキャン結果が表示されます。管理者はコマンドを送信できますが、ポリシーの設定を変更することはできません。

注意: どのポリシーを選択すべきかわからない場合は、エンドポイントの保護をただちに開始する [推奨デフォルト設定] ポリシーを選択することをお勧めします。「*新しいデフォルトのポリシーの選択 ページ227*」で説明するように、デフォルトのポリシーは後で簡単に変更できます。「*ポリシーの作成 ページ233*」で説明するように、独自のポリシーを作成してエンドポイントのグループに割り当てることもできます。

デフォルトのポリシーを選択するには

1. [デフォルトの設定を選択してください] ドロップダウンメニューで、適用するポリシーを選択します。



2. [**送信**] ボタンをクリックします。

   エンドポイントプロテクションの [状態] ページが開き、[ようこそ] パネルが上に、配備オプションが下に、サポートリソースが右側に、それぞれ表示されます。次のセクションに進み、配備方法を選択します。

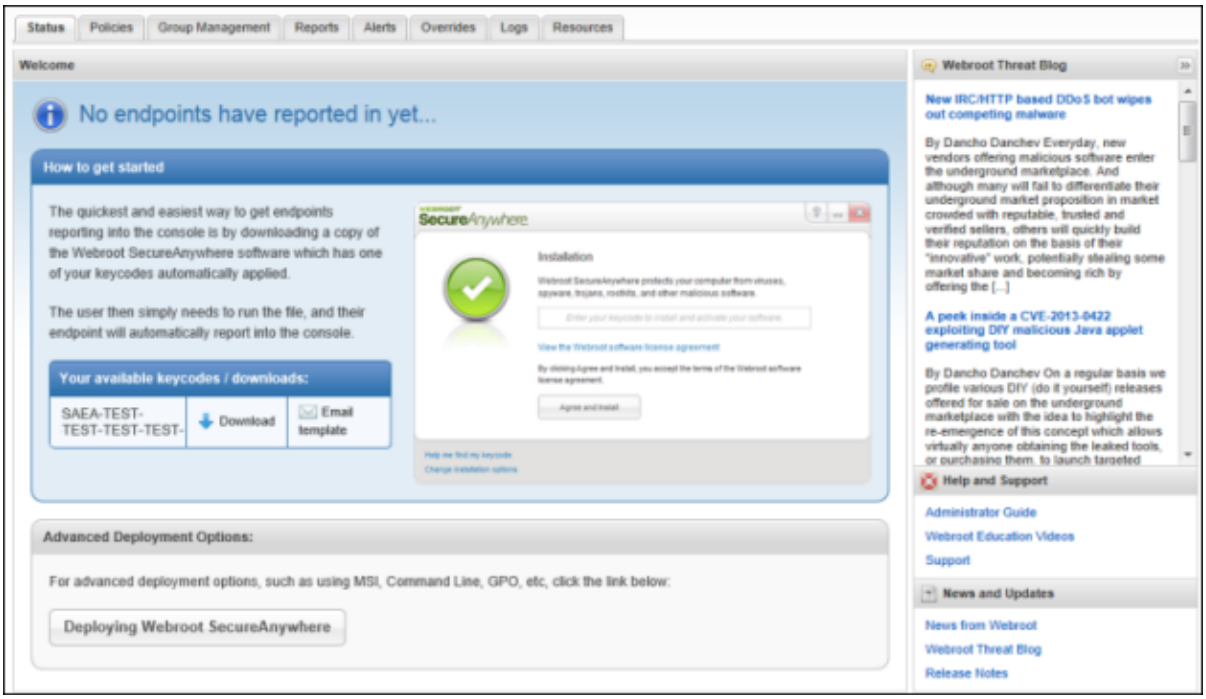
配備方法の選択とテストインストールの実行

[ようこそ] パネルで、SecureAnywhere プログラムをエンドポイントに配備する方法を確認できます。

注意: これらの配備方法は、Windows コンピュータのみを対象としています。Mac コンピュータにインストールする必要がある場合は、「*エンドポイントへの SecureAnywhere の配備 ページ112*」の説明に従って SecureAnywhere Mac インストーラーを使用してください。

- エンドポイントの数が 100 未満の小規模ネットワークでは、[使用を開始するには] パネルで説明されている簡単な方法を使用することをお勧めします。表示される手順に従ってください。
- 大規模なネットワークで Active Directory を使用している場合は、下部にある [Webroot SecureAnywhere の配備] をクリックし、高度な配備オプションの詳細を確認することをお勧めします。詳細については、「エン

ドポイントへの SecureAnywhere の配備 ページ112」を参照してください。



注意: [ようこそ] パネルを閉じた場合は、[リソース] タブをクリックすると、キーコードおよび配備に関する情報を確認できます。

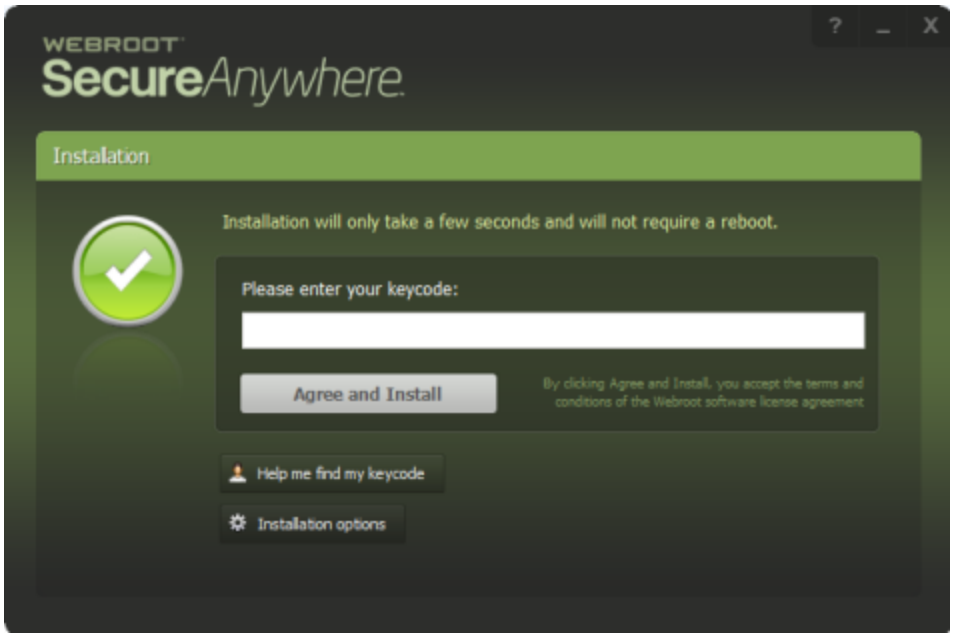
最初は、管理ポータルで状態を確認できるよう、少なくとも 1 つのテストエンドポイントに SecureAnywhere を配備することをお勧めします。

テストエンドポイントに SecureAnywhere を配備するには

1. [使用を開始するには] パネルでキーコードを探します。このキーコードは、エンドポイントプロテクションのライセンスを識別するものです。

2. [**ダウンロード**] リンクをクリックして SecureAnywhere インストーラーファイルをダウンロードします。

3. エンドポイントからインストーラーファイルを実行します。
4. 次のような [インストール] パネルが表示されたら、エンドポイントプロテクションのキーコードを入力して [**同意してインストール**] ボタンをクリックします。



または、SecureAnywhere をインストールするエンドユーザーにテスト電子メールを送信する方法もあります。この場合は、[ようこそ] パネルまたは [リソース] タブで [**電子メールテンプレート**] リンクをクリックし、テキストをカット & ペーストして電子メールメッセージに入力します。正しいキーコードがリンクにより自動的に追加されます。次に、ユーザーがリンクをクリックしてインストールを開始します。プログラムは、入力

済みの正しいキーコードを使用してバックグラウンドでインストールを実行します (サイレントモード)。終了すると、ウェブルートのアイコンがエンドポイントのシステムトレイに表示されます。

5. SecureAnywhere が最初のスキャンを完了するまで待ちます。スキャンは数分で済みます。

   スキャンが完了すると、SecureAnywhere は管理ポータルへの報告を行います。

6. エンドポイントのスキャンが完了したら、SecureAnywhere Web サイトに再度ログインし、その状態を確認します。[**エンドポイントプロテクションに進む**] をクリックすると、管理ポータルが開きます。セットアップウィザードは再表示されません。

詳細については、「*管理コンソールの使用 ページ33*」を参照してください。

管理コンソールの使用

管理コンソールは、管理者がネットワークの状態を一元的に表示、管理できる Web サイトです。管理者はまずウェブルートアカウントを作成します。このアカウントを使用して、ポータルのすべての機能にアクセスできます。詳細については、「*アカウントの作成 ページ11*」を参照してください。

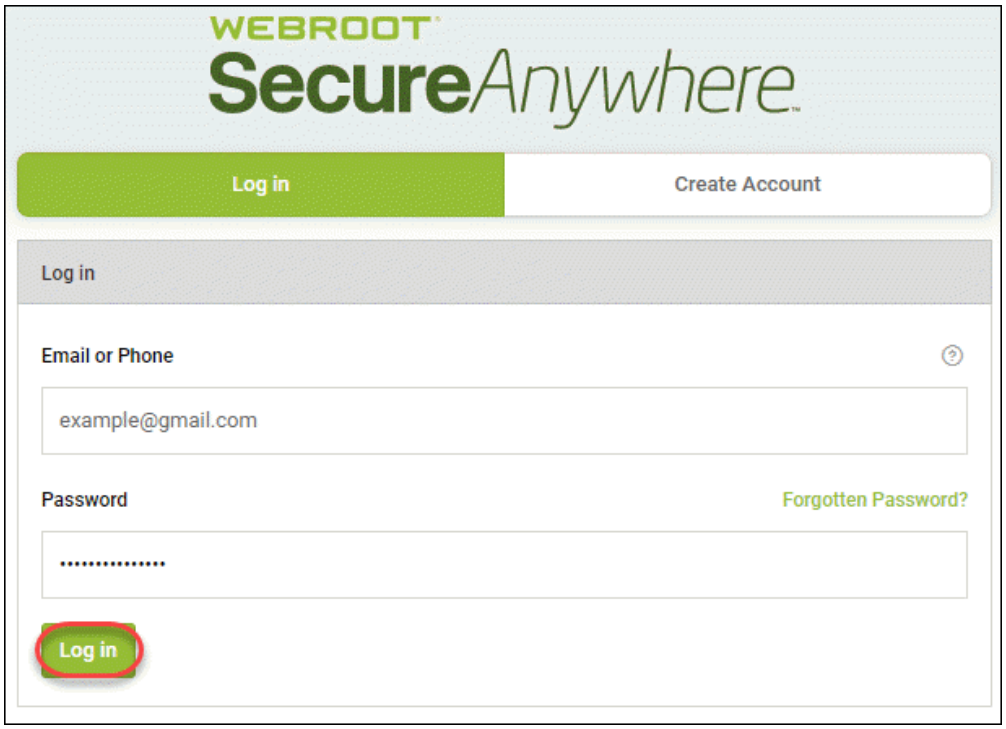
必要に応じて、管理者は完全なアクセス権または制限されたアクセス権をもつ追加のユーザーを作成できます。詳細については、「*ポータルユーザーの管理 ページ68*」を参照してください。

このトピックでは、次の手順と情報を紹介します。

- 管理コンソールの使用
- エンドポイントプロテクションの主要なタブ
- エンドポイントプロテクションのメインメニューを開く
- パネルの展開と折りたたみ
- スプレッドシートへのデータのエクスポート
- ビデオチュートリアルを開く
- ヘルプファイルを開く

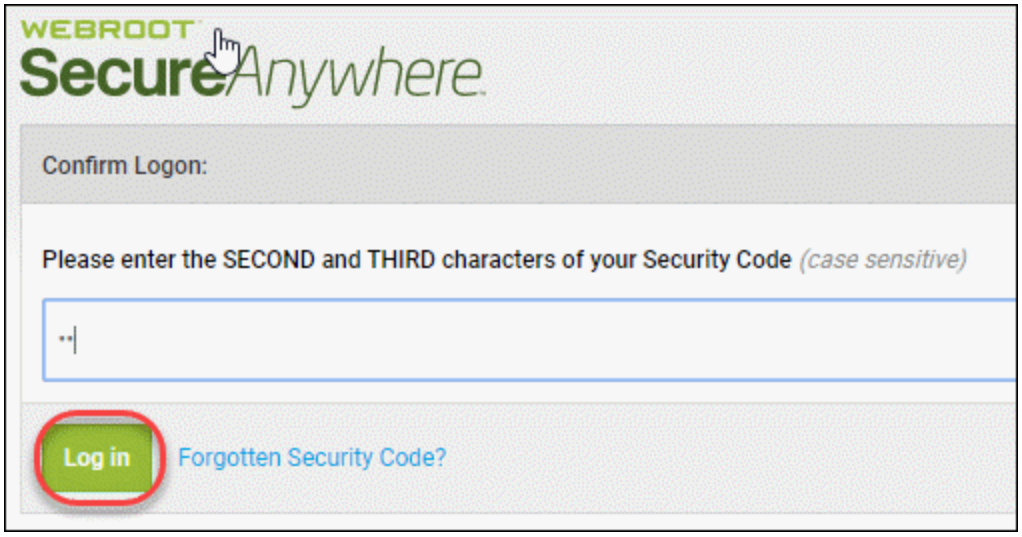
管理コンソールを使用するには

1. SecureAnywhere 管理コンソールにログインします。
2. [ログイン] パネルで、アカウント作成時に指定した電子メールアドレスとパスワードを入力し、[**ログイン**] ボタンをクリックします。



注意： 光通信のユーザーは、[電話番号] タブをクリックすると、電話番号とパスワードを使ってログインできます。[電話番号] タブはすべてのユーザーに表示されますが、光通信ユーザー以外は電子メールアドレスとパスワードでログインしてください。

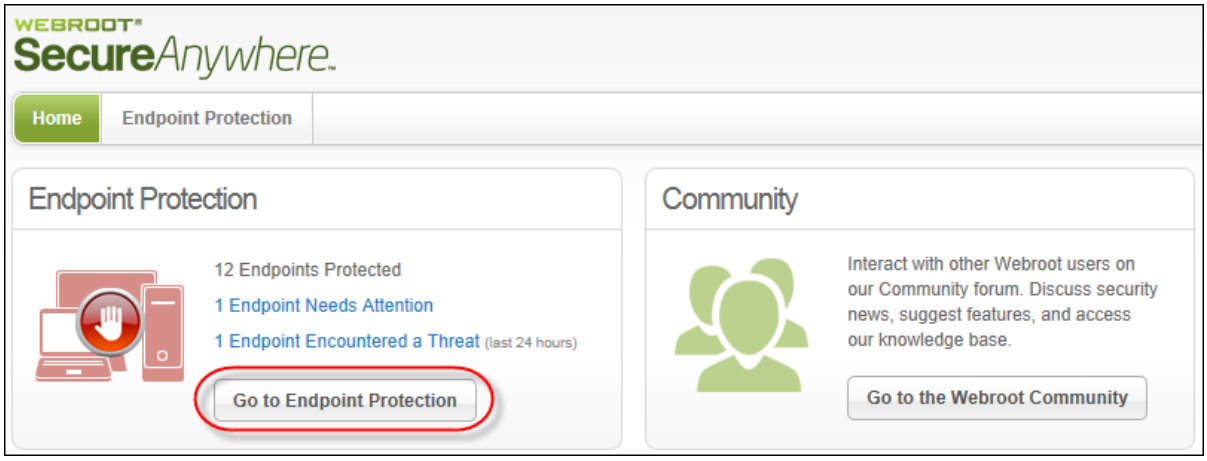
3. [認証コード] ページ (2FA の場合) または [ログオン確認] ページで、要求されたセキュリティコードの文字またはモバイル認証用アプリのコードを入力し、[**ログイン**] をクリックします。



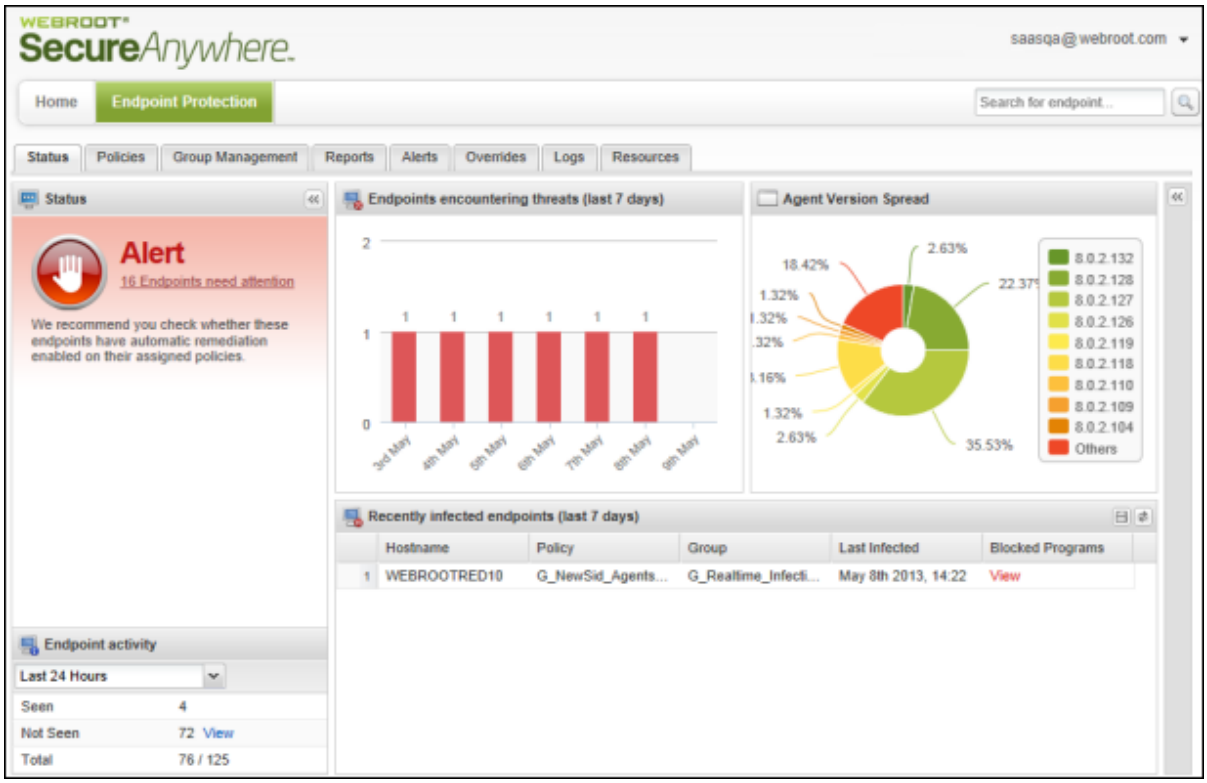
注意: 個人用セキュリティコードは、ウェブルートアカウントの作成時に定義したものです。エンドポイントプロテクションは、ログイン時に毎回この追加のセキュリティ手順を要求し、セキュリティコードのランダムな 2 文字またはモバイル認証用アプリのコードの入力を促します。たとえば、コードが 123456 で、4 番目と 6 番目の文字を入力するよう求められた場合は、「4」と「6」を入力します。

SecureAnywhere Web サイトが開き、ネットワーク内で保護されているエンドポイントの総数、脅威のあるエンドポイント、過去 24 時間以内に脅威が検出されたエンドポイントが表示されます。

4. [エンドポイントプロテクション] パネルで、[**エンドポイントプロテクションに進む**] ボタンをクリックして管理ポータルを開くか、感染したエンドポイントがある場合は感染したエンドポイントのリンクをクリックして管理ポータルを開き、脅威に関する情報のパネルに直接進みます。



管理ポータルが表示されます。[状態] パネルには、脅威に関する警告、エンドポイントのアクティビティ、データのグラフがあります。



5. 上部に表示されるタブをクリックし、設定やその他の操作を行うことができます。

エンドポイントプロテクションの主要なタブ

このセクションでは、タブ、メニュー、パネル、表、検索機能、エクスポート機能など、管理ポータルの各エリアについて説明します。

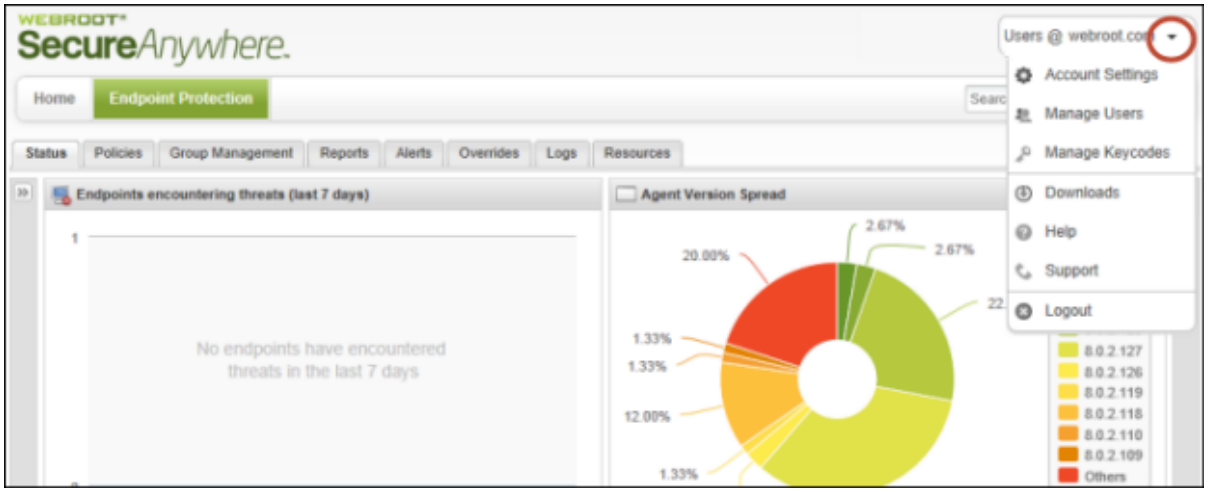
次の表で、エンドポイントプロテクションのタブについて説明します。

タブ	説明
サイトに戻る	管理コンソールに戻ります。詳細については、「*管理コンソールへのアクセス ページ52*」を参照してください。
ホーム	メインのコンソールに戻ります。コンソールでは、セキュリティ意識向上のためのトレーニング、カスタマーサポート、ウェブルートコミュニティなどのその他の機能を選択できます。
状態	次の情報が表示されるダッシュボードです。 • エンドポイントで注意が必要な場合に警告を通知するパネル。脅威にさらされたエンドポイントの一覧を確認するには、通知をクリックします。 • 過去 7 日以内に脅威にさらされたエンドポイントの数を示す棒グラフ。 • エンドポイントにインストールされている SecureAnywhere のバージョンを示す円グラフ。 • 選択した期間に基づき、管理ポータルに報告しているエンドポイントの数を示す、エンドポイントアクティビティパネル。最近状態を報告していないエンドポイントがある場合は、[未確認] の横にある [表示] リンクをクリックして、どのエンドポイントが状態を報告していないかを確認できます。 • 最新の脅威が存在するエンドポイントを示すパネル。行をクリックすると詳細情報が表示され、必要に応じてオーバーライドを追加できます。 • ウェブルートの脅威ブログ、ガイド、ビデオ、リリースノート、その他ニュースへのリンクをまとめたパネル。前述の例には示されていません。詳細については、「*製品情報へのアクセス ページ 43*」を参照してください。
ポリシー	ポリシーはエンドポイントにおける SecureAnywhere の動作を定義します。たとえば、スキャンを実行するタイミングや、潜在的脅威のブロック方法などです。

タブ	説明
グループの管理	グループを使用すると、エンドポイントを整理して管理を簡略化できます。グループやグループ内の各エンドポイントを表示できます。また、個々のエンドポイントを選択して、スキャン履歴を表示することもできます。
レポート	レポートには、エンドポイントに存在する脅威と未判定のソフトウェアと、実行中の SecureAnywhere のバージョンが表示されます。
警告	管理者の配信先リストに送信する、警告や状態に関するメッセージをカスタマイズできます。
オーバーライド	環境内で実行中のファイルを管理できます。ファイルをオーバーライドして、ファイルをブロックしないか、常に隔離するかを設定できます。
ログ	変更とコマンドの使用履歴を確認できます。
リソース	DWP クライアントのダウンロード、テンプレートとして使用する構成ファイル、オンラインヘルプなどの文書へのリンクを利用できます。

エンドポイント プロテクションのメニューを開く

ログイン ID の横にある下向き矢印をクリックすると、エンドポイントプロテクションのメニューが表示されます。メニューに表示されるオプションは、アクセス権限によって異なります。



次の表で、エンドポイントプロテクションのメニューのオプションについて説明します。

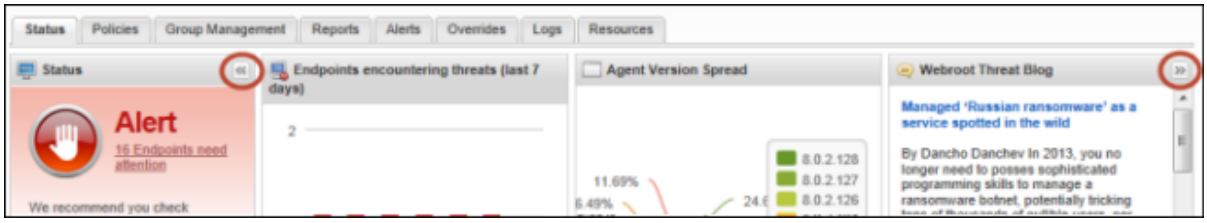
オプション	説明
アカウント設定	パスワードなどの情報を含む、アカウント設定を編集できます。 詳細については、「*自分のアカウント設定の編集 ページ55*」を参照してください。
ユーザーの管理	他のユーザーに管理ポータルへのアクセス権を付与できます。 詳細については、「*ポータルユーザーの管理 ページ68*」を参照してください。
キーコードの管理	現在のエンドポイントプロテクションのライセンスキーコードを表示し、追加のキーコードを購入した場合はポータルに追加することができます。 詳細については、「*アカウントへのキーコードの追加 ページ81*」を参照してください。

オプション	説明
ダウンロード	SecureAnywhere のインストーラーファイルをダウンロードし、配備オプションに関する詳細を確認できます。
ヘルプ	オンラインの WSA Business エンドポイントプロテクションユーザーガイドを開きます。
サポート	対話型のナレッジベースが開き、製品情報を検索できます。
ログアウト	管理ポータルを終了します。

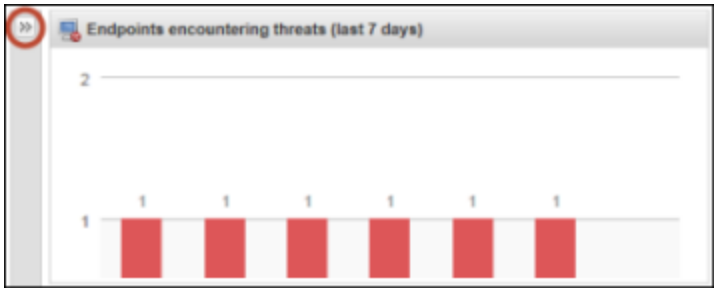
パネルの展開と折りたたみ

データのグラフを大きく表示する場合は、一番左と一番右の **折りたたむ**ボタンをクリックします。

中央のパネルにある棒グラフは固定です。折りたたんだり、表示するグラフのタイプを変更したりできません。

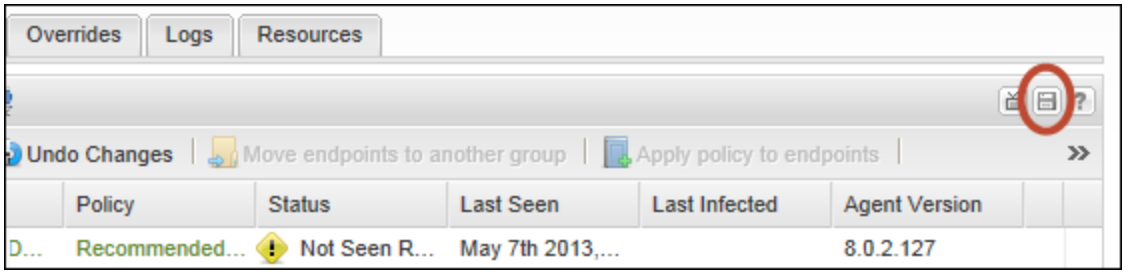


パネルを再び開くには、もう一度 **折りたたむ**ボタンをクリックします。



スプレッドシートへのデータのエクスポート

スプレッドシートのアイコンが表示されている場合は、このアイコンをクリックすると表示されているデータをスプレッドシートにエクスポートできます。

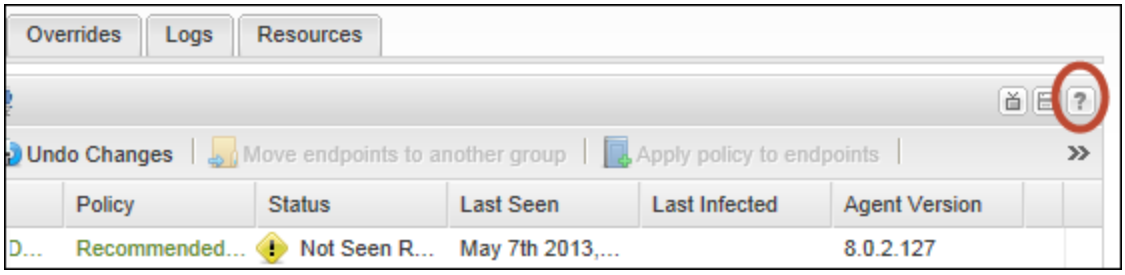


ビデオチュートリアルを開く

テレビのアイコンが表示されている場合は、このアイコンをクリックするとパネルに関連する手順を説明するビデオを見ることができます。

ヘルプファイルを開く

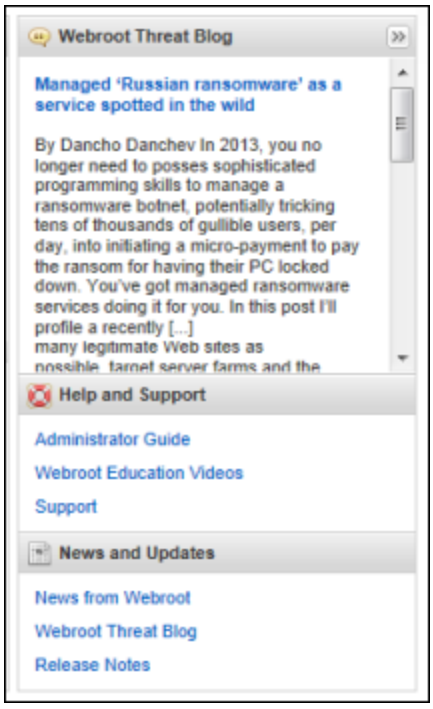
疑問符のアイコンが表示されている場合は、このアイコンをクリックすると現在のパネルに関するヘルプが開きます。


Overrides
Logs
Resources
Undo Changes
Move endpoints to another group
Apply policy to endpoints
Policy
Status
Last Seen
Last Infected
Agent Version
D...
Recommended...
Not Seen R...
May 7th 2013,...
8.0.2.127

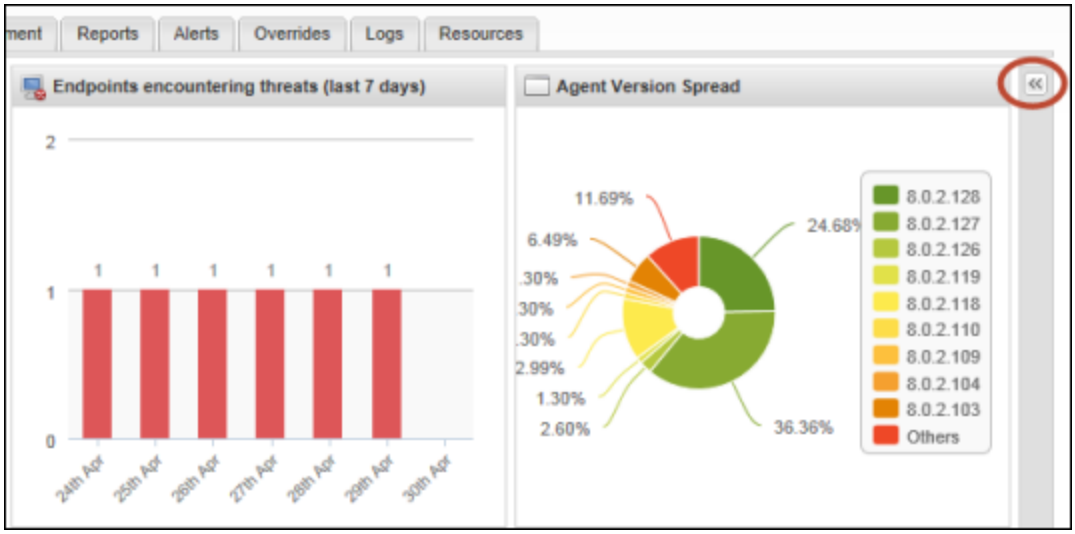
製品情報へのアクセス

ウェブルートの脅威ブログ、ガイド、ビデオ、リリースノート、その他ニュースは、右側のパネルから確認できます。

リソースにアクセスするには、[ヘルプとサポート] または [ニュースおよびアップデート] にあるリンクをクリックしてください。



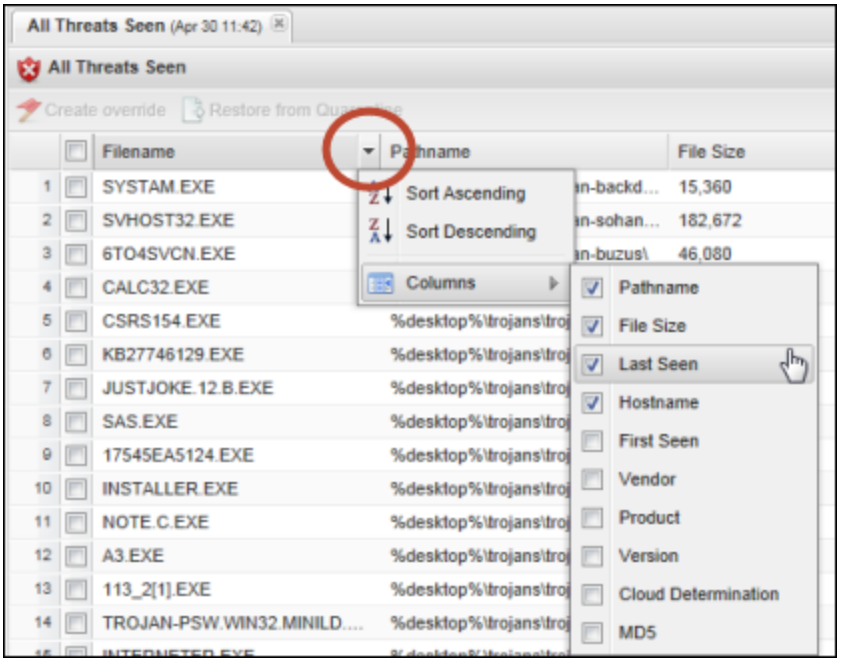
このパネルが開かない場合は、右端にある **折りたたむ** ボタンをクリックしてください。


ment
Reports
Alerts
Overrides
Logs
Resources
Endpoints encountering threats (last 7 days)
Agent Version Spread
2
1
0
1
1
1
1
1
1
24th Apr
25th Apr
26th Apr
27th Apr
28th Apr
29th Apr
30th Apr
11.69%
6.49%
.30%
30%
.30%
2.99%
1.30%
2.60%
24.68%
36.36%
8.0.2.128
8.0.2.127
8.0.2.126
8.0.2.119
8.0.2.118
8.0.2.110
8.0.2.109
8.0.2.104
8.0.2.103
Others

表とレポートのデータの並べ替え

表やレポートでのデータの並べ替え、非表示、表示の操作方法は以下のとおりです。

- **カラムを使用した並べ替え** - カラムの見出しをクリックすると、そのカラムを基準として簡単に並べ替えることができます。たとえば、ポリシー名でデータを並べ替えるには、[**ポリシー**] の見出しをクリックします。
- **昇順または降順の変更** - カラム見出しの右端にあるドロップダウン矢印をクリックすると、ドロップダウンメニューが表示されます。[**昇順に並べ替え**] または [**降順に並べ替え**] を選択すると、カラム内でデータポイントの順番が変更されます。
- **カラムの表示または非表示** - カラム見出しの右端をクリックするとドロップダウン矢印が表示され、この矢印をクリックするとメニューが表示されます。チェックボックスを選択するとカラムが表示されます。チェックボックスの選択を解除するとカラムが非表示になります。



次の表で、エンドポイントプロテクションの表やレポートに表示されるデータ項目について説明します。表示されるデータは、表示されている表やレポートのタイプによって異なります。

オプション	説明
エージェントの言語	SecureAnywhere をインストールした際に選択した言語。 **en** - 英語 **ja** - 日本語 **es** - スペイン語 **fr** - フランス語 **de** - ドイツ語 **it** - イタリア語 **nl** - オランダ語 **ko** - 韓国語 **zh-cn** - 簡体字中国語 **pt** — ポルトガル語 (ブラジル) **ru** - ロシア語 **tr** - トルコ語 **zh-tw** — - 繁体字中国語
エージェントのバージョン	エンドポイントにインストールされている SecureAnywhere ソフトウェアのバージョン。
すべてのエンドポイント	ファイルが検出されブロックされたエンドポイントに関する詳細情報。

オプション	説明
すべてのバージョン	ファイルが検出されブロックされた SecureAnywhere のバージョンに関する詳細情報。
概算のスキャン時間	スキャン時間 (分 / 秒単位)。
エリア	エンドポイントが所在する国のフラグ。
クラウド判定	ウェブルートによるファイルの分類。[正当]、[不正]、[未判定] のいずれか。 分類にカーソルを合わせると、この分類に決定された経緯に関する情報が表示されます。
感染日数	エンドポイントが感染状態にあった日数。
デバイス MID	エンドポイントのハードウェアを識別するマシン ID の値。ウェブルートはアルゴリズムを使用してこの値を決定します。
滞留時間	脅威がデバイス内に存在していた時間。ファイルが最初にアクティブになった時から、ファイルが最後に確認されるまでの期間で計算されます。 詳細については、「*滞留時間について ページ214*」を参照してください。

オプション	説明
影響を受けたエンドポイント	検出されたファイルが存在するエンドポイントの数。
ファイルサイズ	ファイルのサイズ (バイト単位)。
ファイル名	検出された脅威のファイル名。
最初の脅威	脅威が検出された日時。
初回確認日時	このエンドポイントが初めて管理ポータルにチェックインした日時。
グループ	エンドポイントに割り当てられたグループ。
ホスト名	エンドポイントのマシン名。
インスタンス MID	Windows OS の SID (セキュリティ識別子) を識別する値。ウェブルートはアルゴリズムを使用してこの値を決定します。
IP アドレス	エンドポイントの IP アドレス。
キーコード	エンドポイントで SecureAnywhere のインストールに使用されたライセンス。

オプション	説明
最近の感染	エンドポイントで感染が報告された日時。
最新のスキャン時間	このエンドポイントでの最新のスキャンの時刻。
最終確認日時	前回このエンドポイントが管理ポータルにチェックインした日時。
マルウェアグループ	マルウェアの分類。トロイの木馬やシステム監視など。
MD5	ファイルを固有に識別するための指紋のような働きをする、メッセージダイジェストアルゴリズム 5 の値。
OS	エンドポイントの OS。
パス名	ファイルが検出されたディレクトリまたはフォルダ。
ポリシー	エンドポイントに割り当てられたポリシー。
製品	ファイルに関連する製品の名前。SecureAnywhere が情報を特定できる場合のみ。

オプション	説明
スキャンの種類	スキャンの種類: • ディープスキャン • クリーンアップ後のスキャン • カスタム / 右クリックスキャン
状態	エンドポイントの現在の状態: • **保護** - 感染なし。 • **感染** - マルウェアを検出。 • **最近確認されていません** - ポータルへの報告なし。portal. • **期限切れ** - SecureAnywhere ライセンスが期限切れ。 • **感染および期限切れ**
システムパック	OS のサービスパックの番号。
システムの種類	32 ビットまたは 64 ビット。
ベンダー	ファイルに関連するベンダーの名前。SecureAnywhere が情報を特定できる場合のみ。

オプション	説明
バージョン	ファイルに関連する製品のバージョン。SecureAnywhere が情報を特定できる場合のみ。
VM	エンドポイントが仮想マシンにインストールされている場合に [はい]。
Windows フル OS	Windows OS の名前。

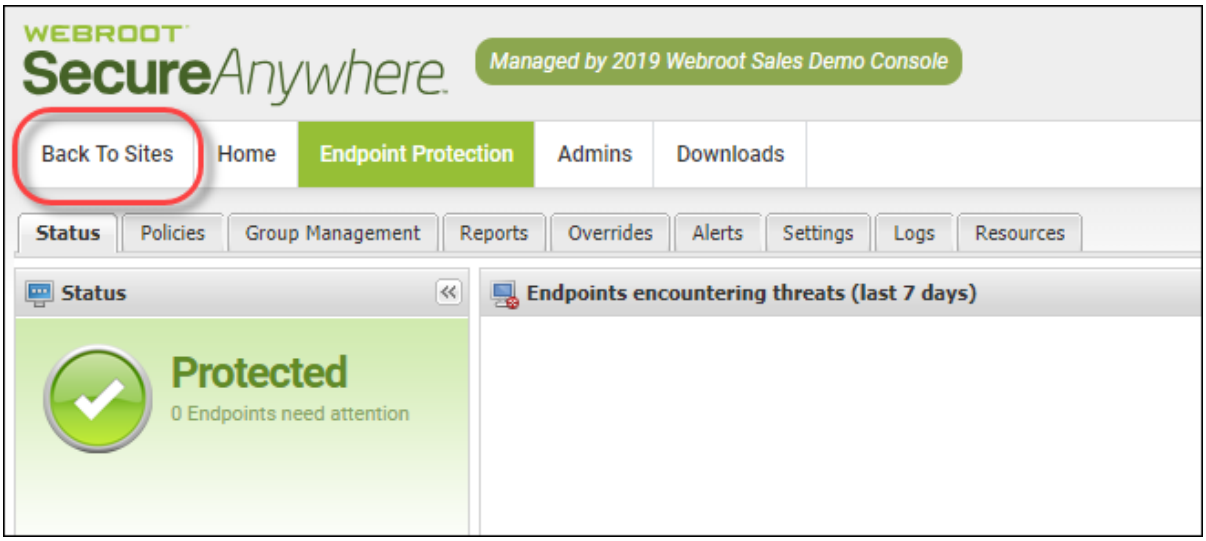
管理コンソールへのアクセス

エンドポイントプロテクションで管理コンソールの [サイト] タブに戻るには、次の手順に従ってください。

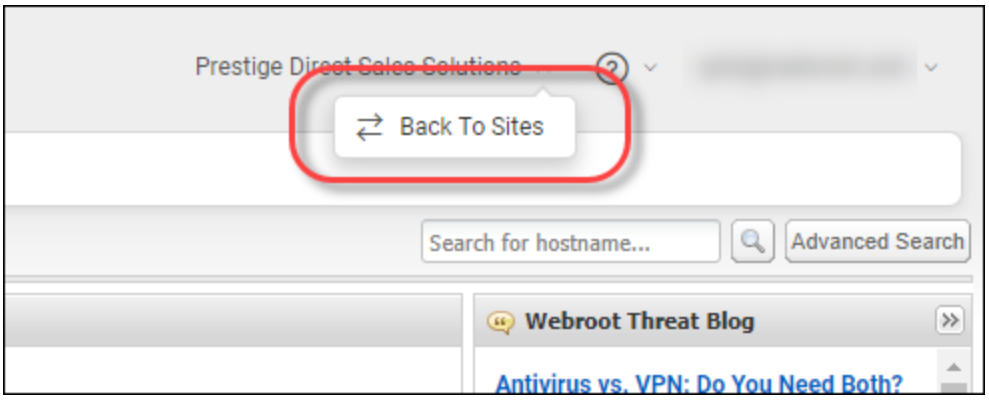
管理コンソールにアクセスするには

1. エンドポイントコンソールで、以下のいずれかを実行します。

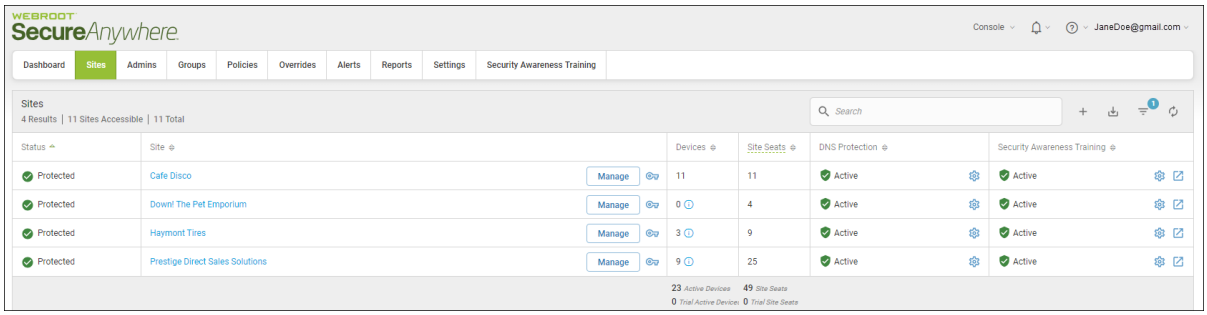
- [**サイトに戻る**] ボタンをクリックします。



- コンソール名のドロップダウンメニューで [**サイトに戻る**] を選択します。



2. [サイト] タブがアクティブになった状態で管理コンソールに戻ります。



第 3 章: ユーザーアカウントの管理

アカウントの管理方法については、以下のトピックを参照してください。

自分のアカウント設定の編集

アカウントでは、ログイン名やパスワードなどユーザーの詳細のほか、アクセス権限を定義します。自分のアカウントについては、ログイン名に指定した電子メールアドレス以外の設定を変更することができます。

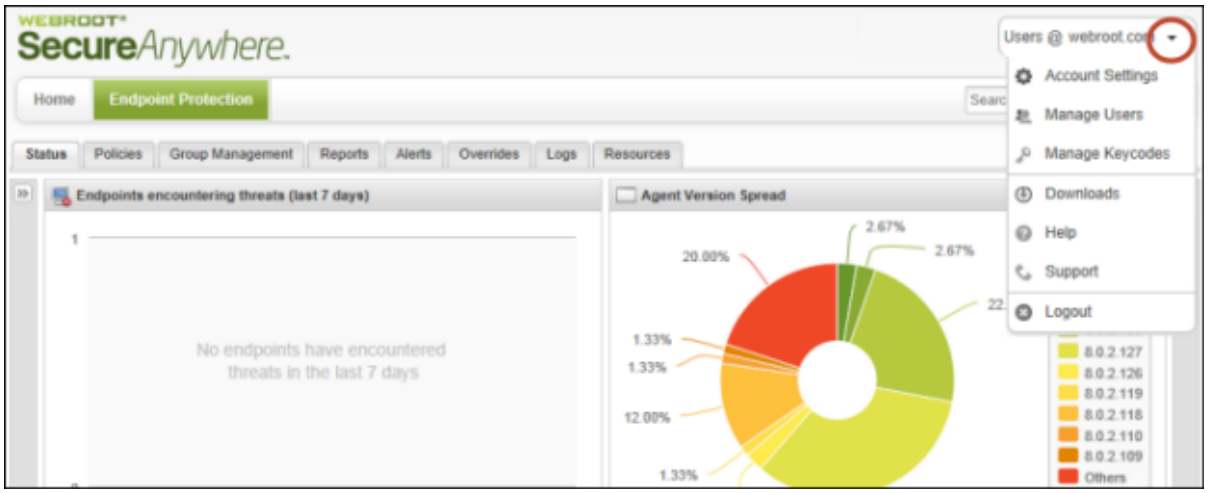
注意: 他のポータルユーザーの設定を編集する場合は、「*ポータルユーザーの管理 ページ68*」を参照してください。

自分のアカウント設定の編集の詳細については、以下の手順を参照してください。

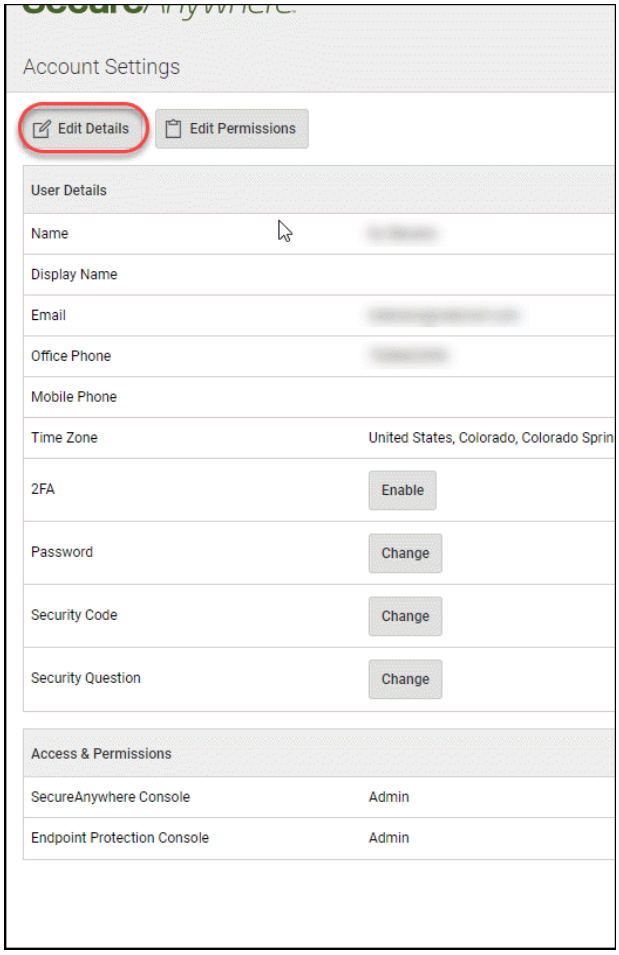
- *管理者の詳細 / 権限の編集 ページ55*
- *2 要素認証の無効化 ページ59*
- *パスワードの変更 ページ61*
- *セキュリティコードの変更 ページ63*
- *セキュリティの質問の変更 ページ65*

管理者の詳細 / 権限の編集

1. ログイン ID の横にある**下向き** 矢印をクリックし、[**アカウント設定**] をクリックします。

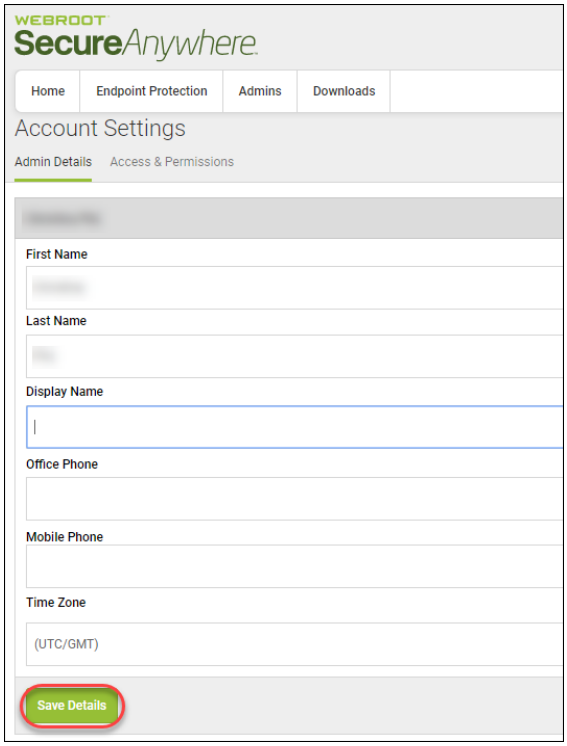


2. [アカウント設定] ページで [**詳細を編集**] をクリックすると、[管理者の詳細] タブが表示されます。このタブで情報を編集できます。

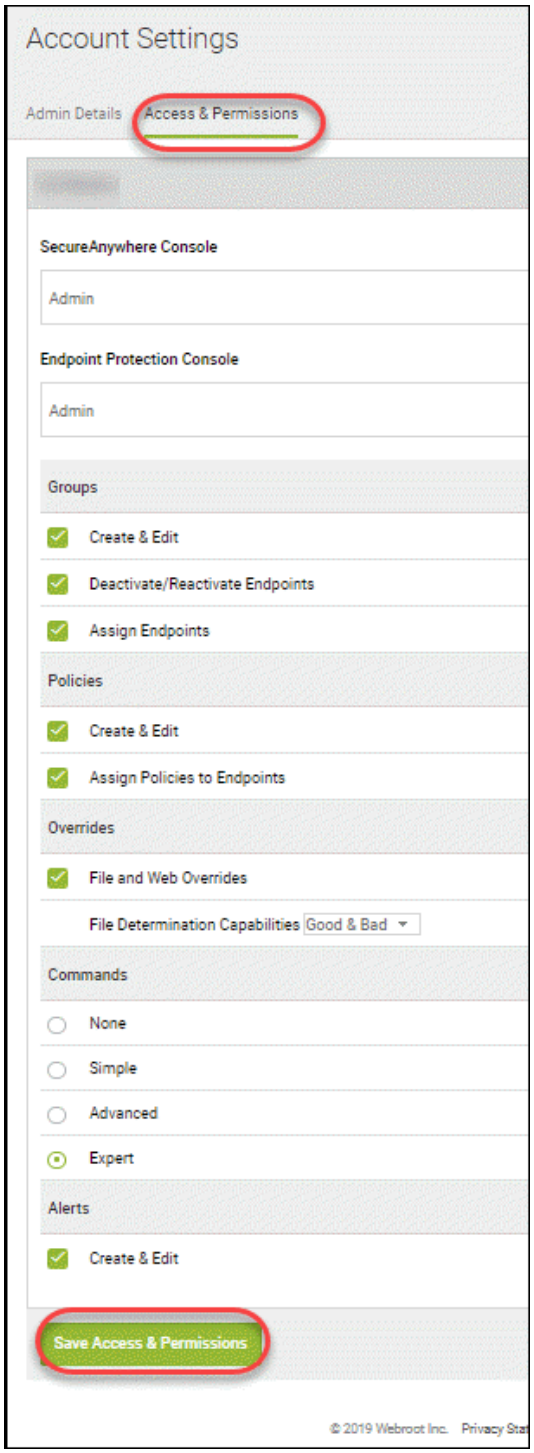


3. [管理者の詳細] パネルで名前、電話番号、タイムゾーンを変更し、[**情報を保存**] をクリックして [アカウント設定] ページに戻ります。

> **注意:** [表示名] は、管理コンソールに表示される名前です。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Admins
Downloads
Account Settings
Admin Details
Access & Permissions
First Name
Last Name
Display Name
Office Phone
Mobile Phone
Time Zone
(UTC/GMT)
Save Details

4. 次に、アクセス権限を確認するために、[**アクセスおよび権限**] タブをクリックします。



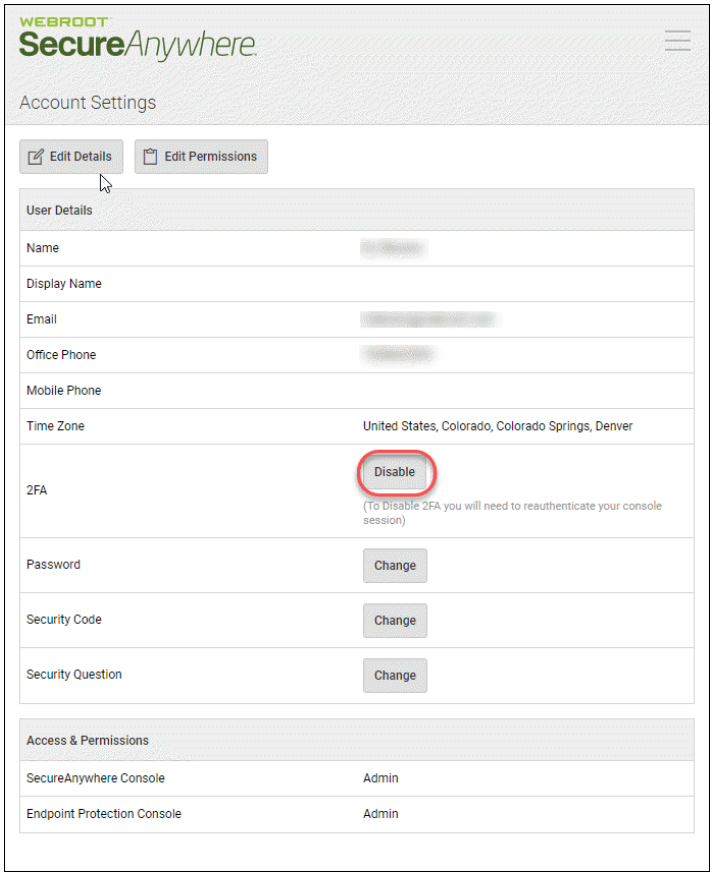
> **注意:** メインのエンドポイントプロテクション管理者の場合は、デフォルトの設定のままにしておくことをお勧めします。

設定の詳細については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

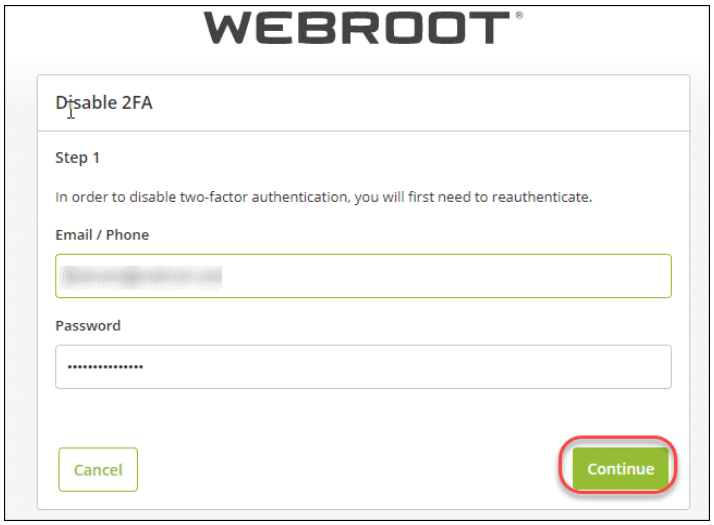
5. 終了したら、[**アクセスおよび権限を保存**] ボタンをクリックして [アカウント設定] ページに戻ります。

2 要素認証の無効化

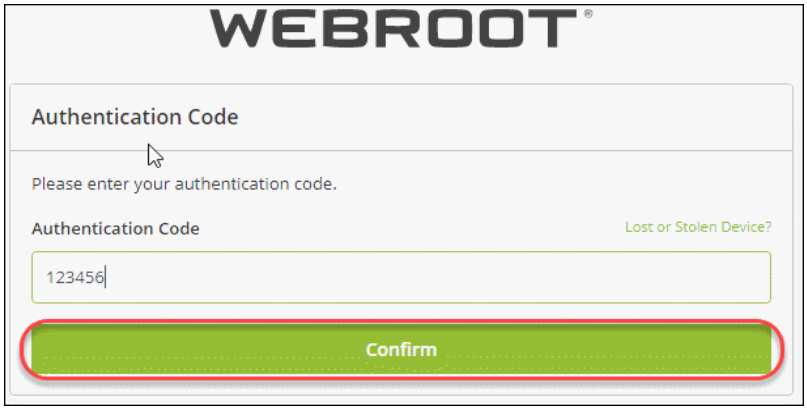
1. エンドポイントコンソールにログインし、画面の右上隅にあるドロップダウンメニューで [**アカウント設定**] タブをクリックしてアカウント設定を表示します。
2. [**2FA**] の横にある [**無効化**] をクリックして [2FA を無効にする] ワークフローを開きます。



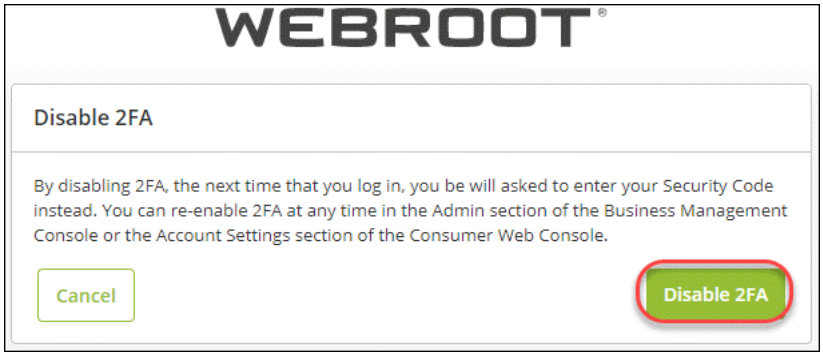
3. アカウントに関連付けられた電子メールアドレスまたは電話番号とパスワードを入力し、[**続行**] をクリックします。



4. モバイル認証用アプリを開き、そこに表示されているコードを [認証コード] ボックスに入力して [**確認**] をクリックします。

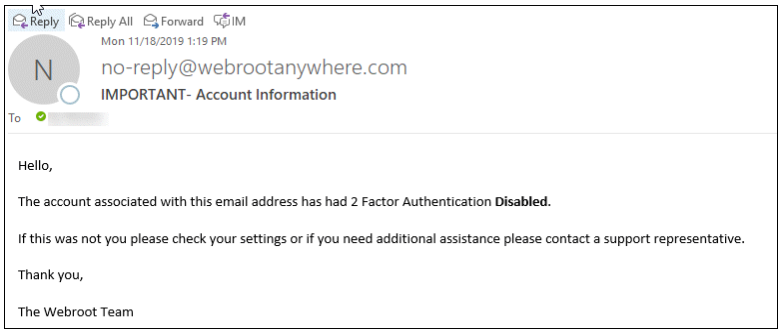


5. [**2FA を無効にする**] をクリックします。



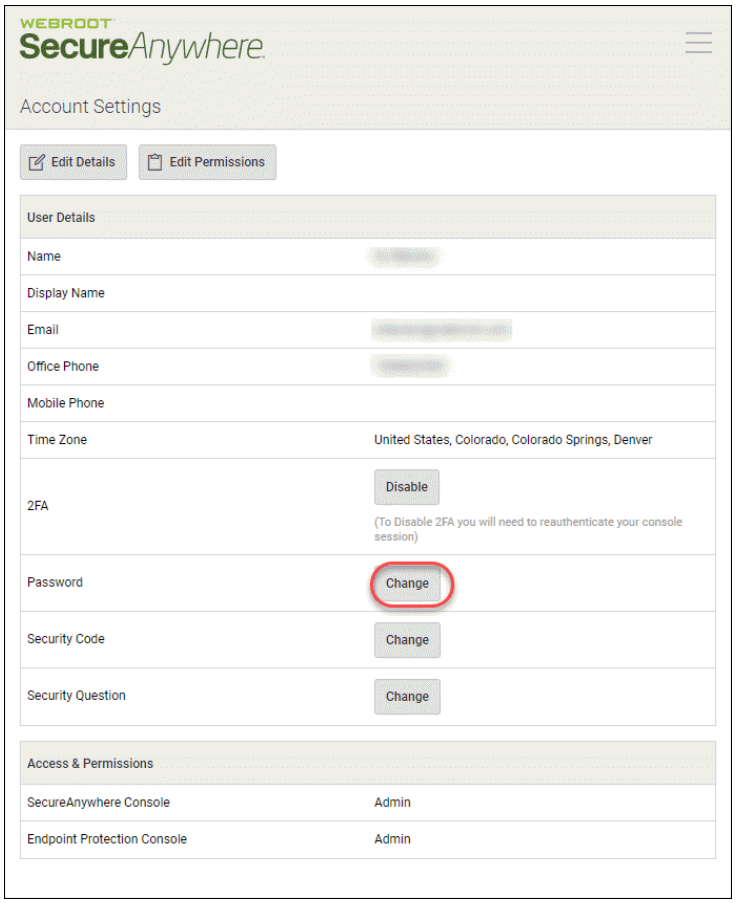
注意: 2FA を無効にする場合、アカウントの登録時に作成したセキュリティコードを入力する必要があります。2FA は、コンソールの [管理者] タブでいつでも再び有効にできます。詳細については、「*2 要素認証 (2FA) の有効化 ページ16*」を参照してください。

6. 2FA が無効になりました。アカウントで 2FA が無効になったことを通知する確認の電子メールが送信されます。

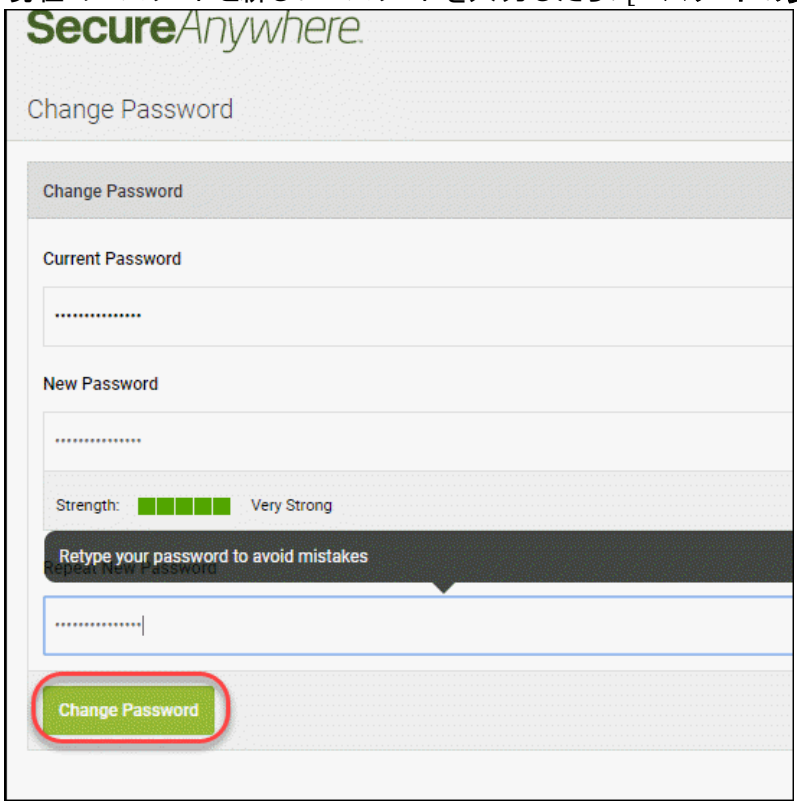


パスワードの変更

1. [アカウント設定] ページで [パスワード] の横にある [**変更**] をクリックすると、[パスワードの変更] ページが開きます。

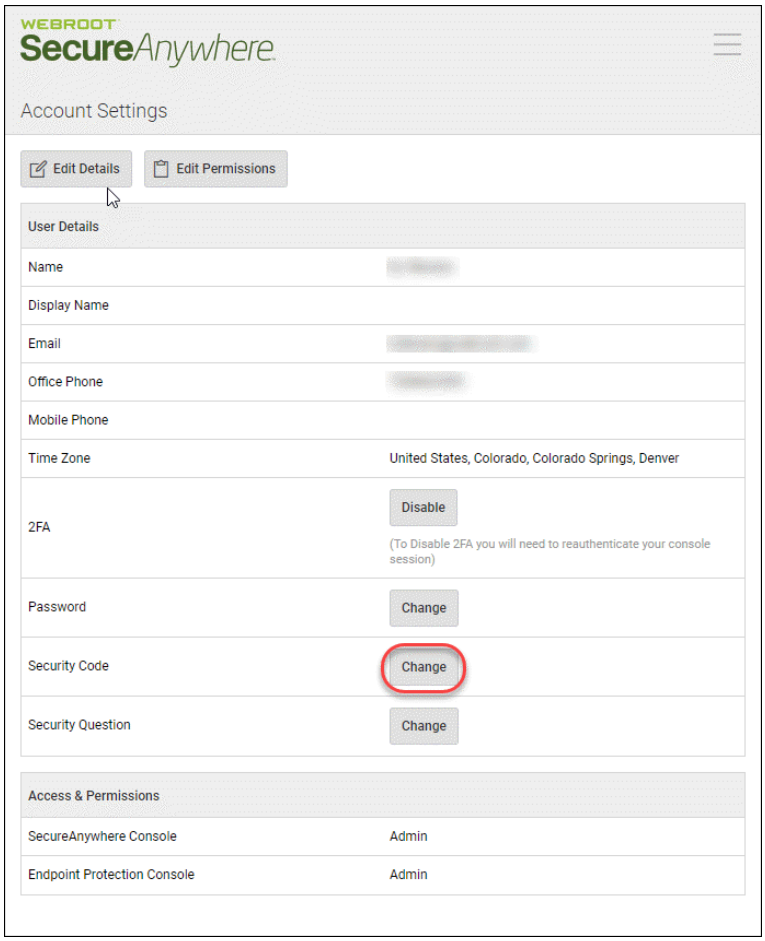

WEBROOT
SecureAnywhere
Account Settings
Edit Details
Edit Permissions
User Details
Name
Display Name
Email
Office Phone
Mobile Phone
Time Zone
United States, Colorado, Colorado Springs, Denver
2FA
Disable
(To Disable 2FA you will need to reauthenticate your console session)
Password
Change
Security Code
Change
Security Question
Change
Access & Permissions
SecureAnywhere Console
Admin
Endpoint Protection Console
Admin

2. 現在のパスワードと新しいパスワードを入力したら、[**パスワードの変更**] をクリックします。

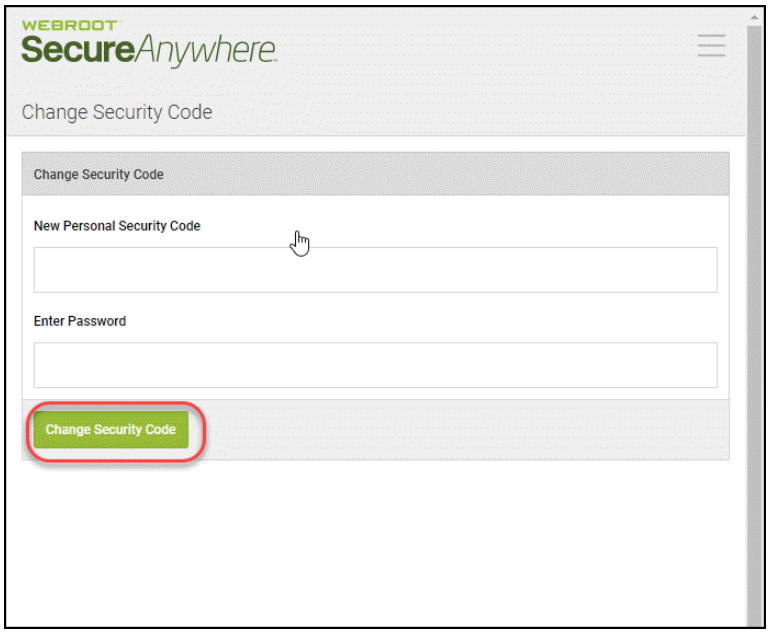


セキュリティコードの変更

1. [アカウント設定] ページで [セキュリティコード] の横にある [**変更**] をクリックすると、[セキュリティコードの変更] ページが開きます。

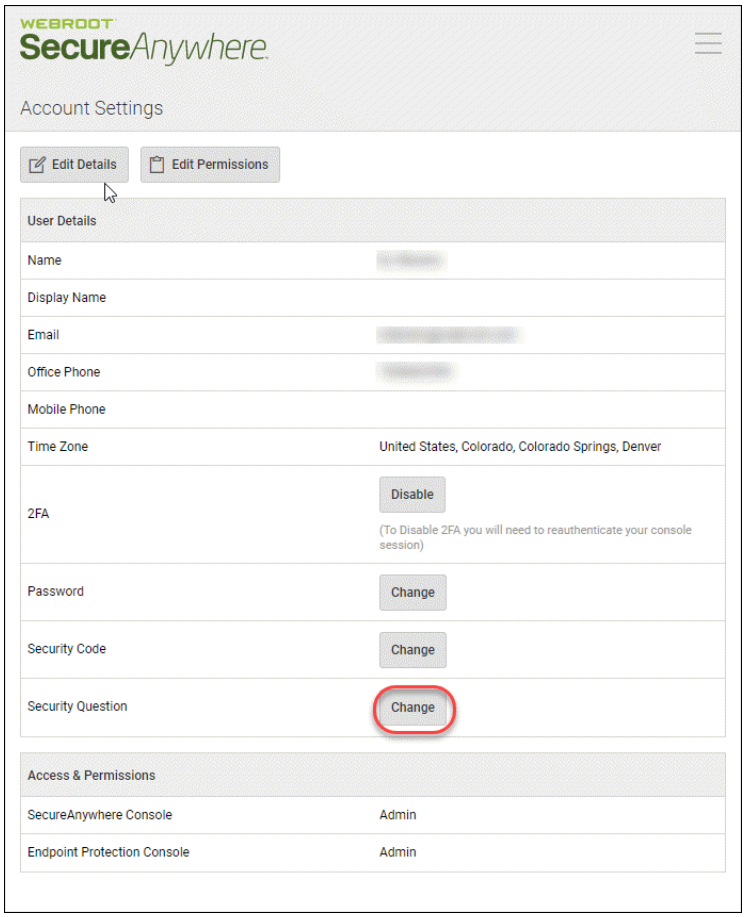

WEBROOT
SecureAnywhere
Account Settings
Edit Details
Edit Permissions
User Details
Name
Display Name
Email
Office Phone
Mobile Phone
Time Zone
United States, Colorado, Colorado Springs, Denver
2FA
Disable
(To Disable 2FA you will need to reauthenticate your console session)
Password
Change
Security Code
Change
Security Question
Change
Access & Permissions
SecureAnywhere Console
Admin
Endpoint Protection Console
Admin

2. 新しい個人用セキュリティコードをボックスに入力し、パスワードを入力したら、[**セキュリティコードの変更**] をクリックします。



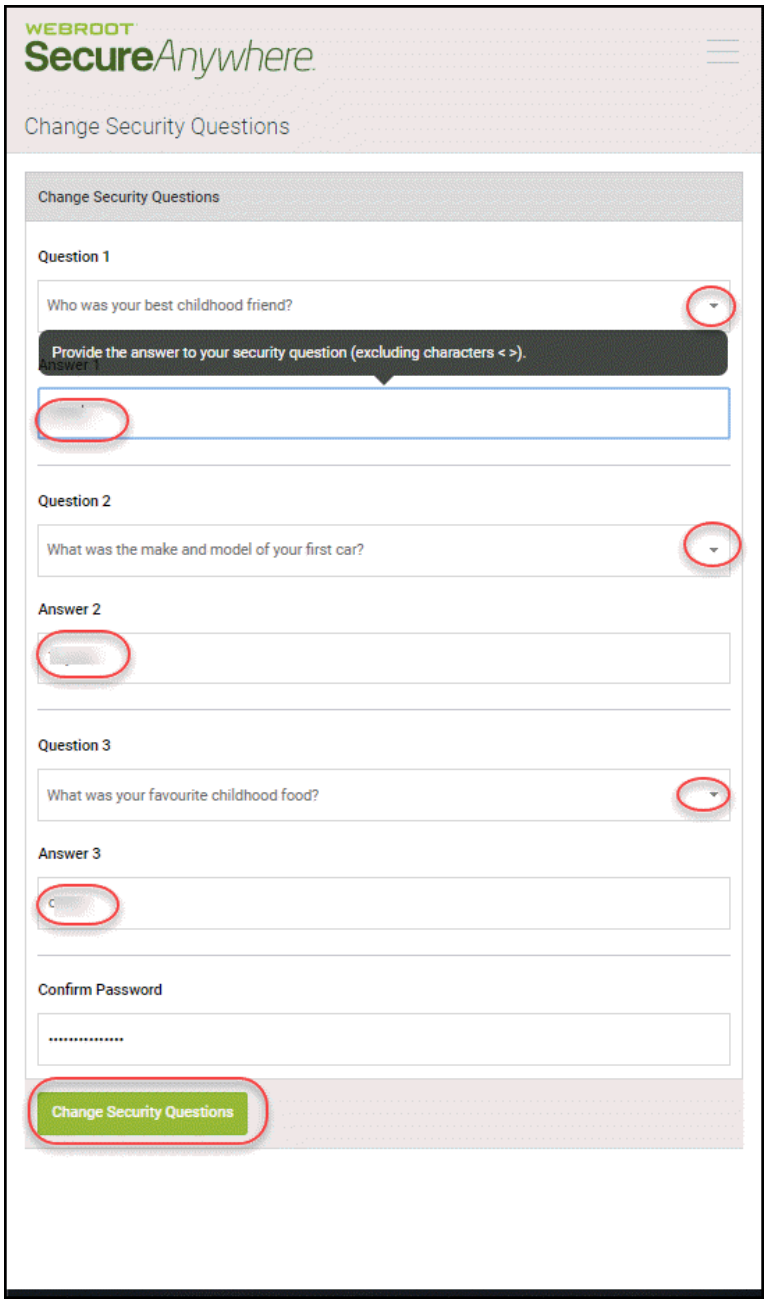
セキュリティの質問の変更

1. [アカウント設定] ページで [セキュリティの質問] の横にある [**変更**] をクリックすると、[セキュリティの質問の変更] ページが開きます。



2. セキュリティの質問を選択するには、それぞれのドロップダウンの矢印をクリックしてリストから質問を選択します。また、該当するボックスにその回答も入力します。最後に [**セキュリティの質問の変更**] をクリック

すると、アカウントのセキュリティの質問が更新されます。



ポータルユーザーの管理

エンドポイントプロテクションの管理者権限を持っている場合、管理ポータルの新規ユーザーを作成し、そのアクセス権限を設定したり情報を編集したりできます。新規ユーザーを作成すると、エンドポイントプロテクションから、パスワードの作成とログインに関する詳細情報が記載された電子メールが新規ユーザーに送信されます。

詳細については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

このトピックでは、次の手順について説明します。

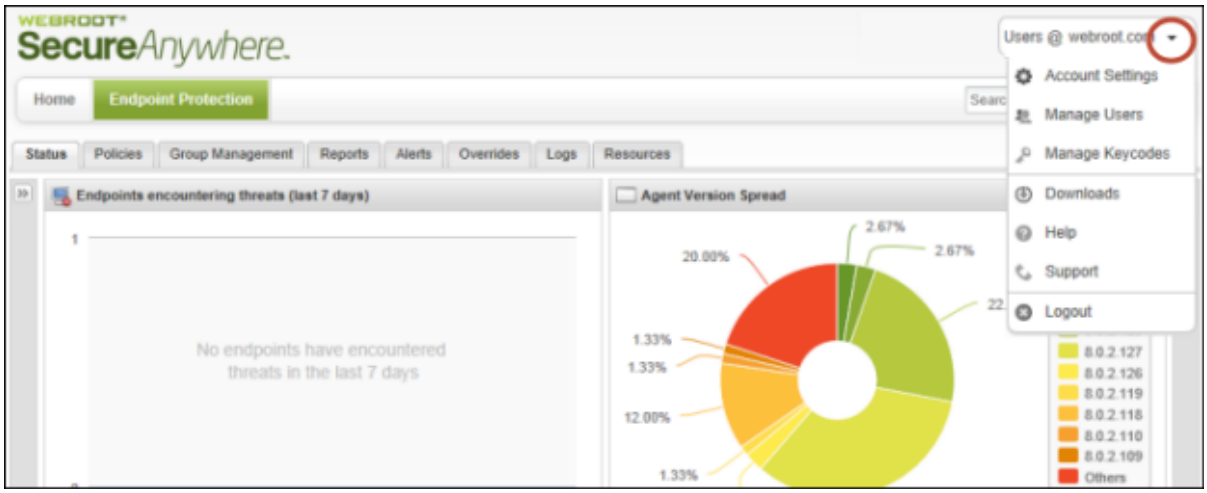
- 新規ポータルユーザーの作成
- ユーザー情報の編集

新規ポータルユーザーの作成

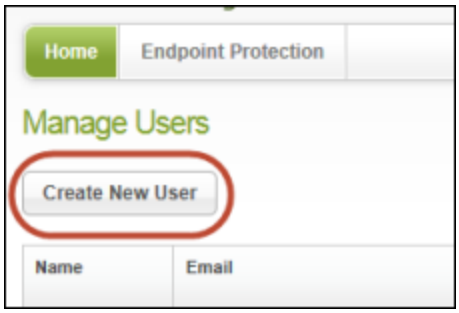
他の管理者を追加して、その管理者がエンドポイントプロテクションのレポートにアクセスできるようにした方がよい場合もあります。また、データの表示のみが可能で変更はできないように、追加したユーザーの権限を制限することもできます。

新規ポータルユーザーを作成するには

1. ログイン ID の横にある**下向き**矢印をクリックし、[**ユーザーの管理**] を選択します。



2. [ユーザーの管理] パネルで [**新規ユーザーの作成**] ボタンをクリックします。



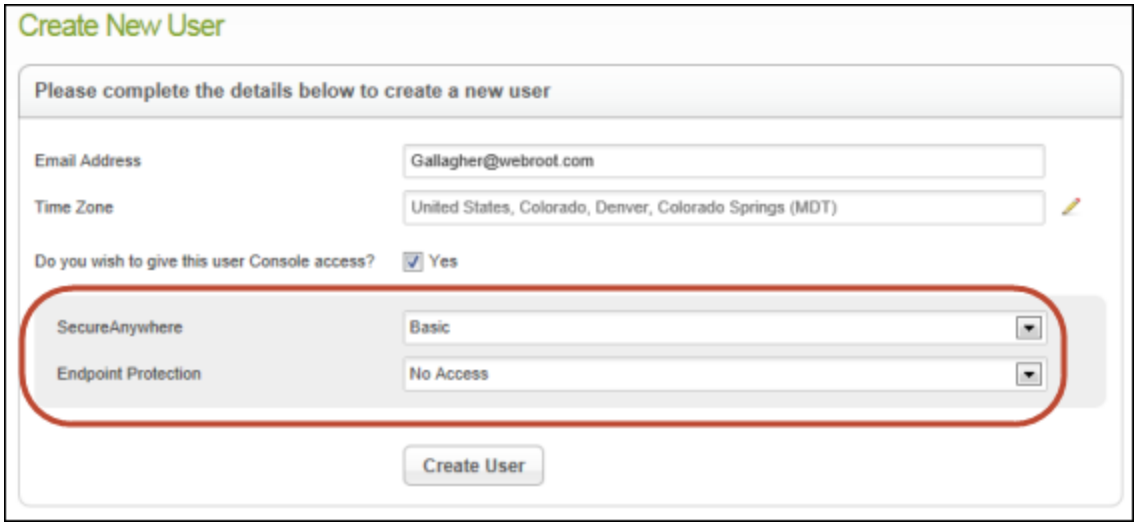
3. [新規ユーザーの作成] パネルで、ユーザーの電子メールアドレスを入力します。これは、ユーザーが確認メッセージを受信するアドレスで、ユーザーのログイン名としても使用されます。

   間違った電子メールアドレスを入力したためにメッセージを受信できない場合は、後から電子メールアドレスを変更してメッセージを再送信することができます。詳細については、「ユーザー情報の編集」を参照してください。

4. [タイムゾーン] フィールドの右側の**鉛筆**アイコンをクリックして、国、地域、または主要都市を入力すると、タイムゾーンのドロップダウンメニューが開き、ユーザーの所在地を選択できます。

5. [**はい**] チェックボックスを選択します。

   ペインの下部にさらに 2 つのフィールドが表示されます。



- **SecureAnywhere** - my.webrootanywhere.comのホームページです。ユーザーはこのページから、モバイルプロテクションポータル(モバイルプロテクションを購入した場合)など、ウェブルートの他のポータルにアクセスできます。詳細については、WSA Business - モバイルプロテクション管理者ガイドを参照してください。

- **エンドポイントプロテクション** - エンドポイントプロテクションの管理ポータルまたは管理者コンソールです。ユーザーがこのポータルにアクセスできる場合、[**エンドポイントプロテクションに進む**] ボタンをクリックして管理ポータルにアクセスすることができます。Portal.

6. SecureAnywhere のドロップダウンの矢印で、次のいずれかを選択します。

   - **基本** - コンソールとアカウント設定への制限付きアクセス権を付与します。
   - **管理者** - ウェブルートポータルのすべてのキーコード、ユーザー、アカウント設定への完全なアクセス権を付与します。

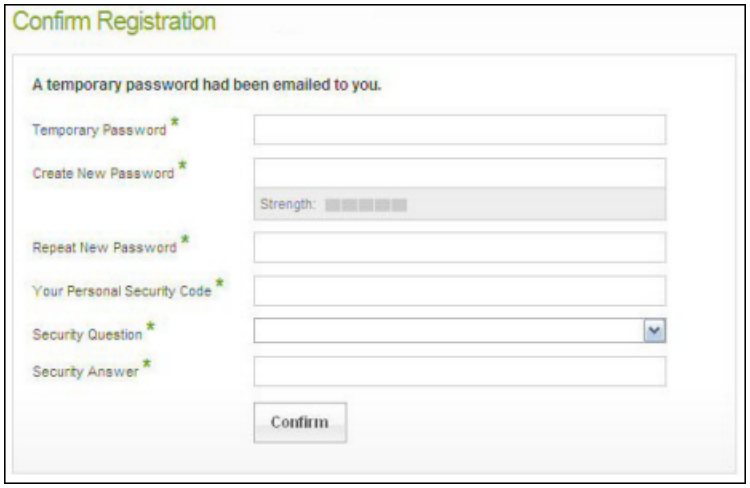
7. エンドポイントプロテクションのドロップダウンメニューで、次のいずれかを選択します。

   - **アクセス不可**
   - **基本** - エンドポイントスキャンへの読み取り専用アクセス権
   - **管理者** - すべての設定への完全なアクセス権

   このユーザー権限を後から変更する方法の詳細については、「*コンソールユーザーの権限設定 ページ 75*」を参照してください。

8. 完了したら、[**ユーザーを作成**] ボタンをクリックします。

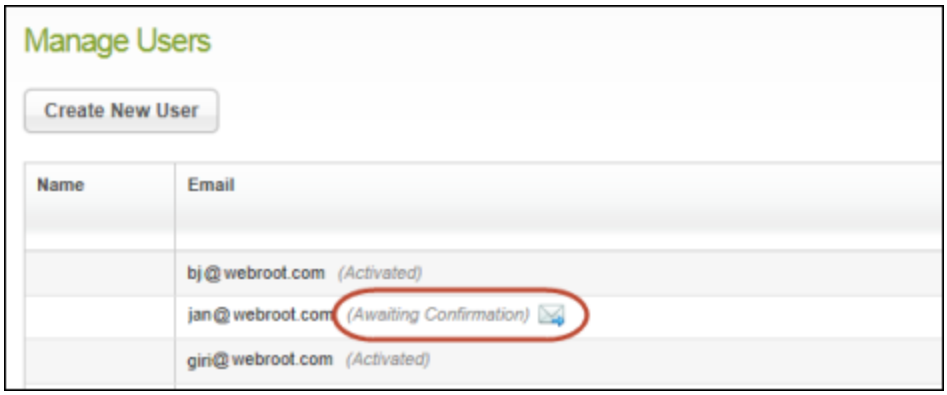
   新しいユーザーに確認の電子メールが送信されます。この電子メールメッセージには、初回にログインするための仮のパスワードが記載されています。ユーザーが電子メールに記載された確認のリンクをクリックすると、[登録確認] パネルが開き、ログイン情報を入力できます。



ユーザー情報の編集

ユーザーが登録を確認すると、[ユーザーの管理] パネルに戻り、そのユーザーの情報を編集することができます。他のユーザーのパスワード、セキュリティコード、セキュリティの質問を表示または編集することはできません。これらの情報にアクセスできるのはそのユーザーのみです。

ユーザーが登録を確認していない場合、ユーザーの状態は [確認待ち] と表示されます。ユーザーが電子メールを受信して登録を確認すると、状態が [アクティブ] に変わります。必要に応じて、[確認待ち] 状態の横にある封筒のアイコンをクリックすると、確認の電子メールを再送信できます。



ポータルユーザーを編集するには

1. 編集する必要のあるユーザーの行を探し、右端にあるそのユーザーの**編集**アイコンをクリックします。

> **注意:** アカウントに複数のコンソールがある場合、現在アクティブなコンソールのキーコードに関連付けられたユーザーのみが表示されます。コンソールの詳細については、「*アカウントへのコンソールの追加 ページ84*」を参照してください。

2. [ユーザーの詳細] パネルでは、必要に応じて名前や電話番号を変更できます。

   ユーザーの状態が [確認待ち] の場合、このウィンドウの上部に電子メールフィールドが表示されます。ユーザーの電子メールアドレスを間違って入力したために登録を再送信する必要がある場合は、電子メールアドレスを変更してください。

注意: [アクセスおよび権限] の設定を変更する方法の詳細については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

3. 完了したら、[**情報を保存**] ボタンをクリックします。

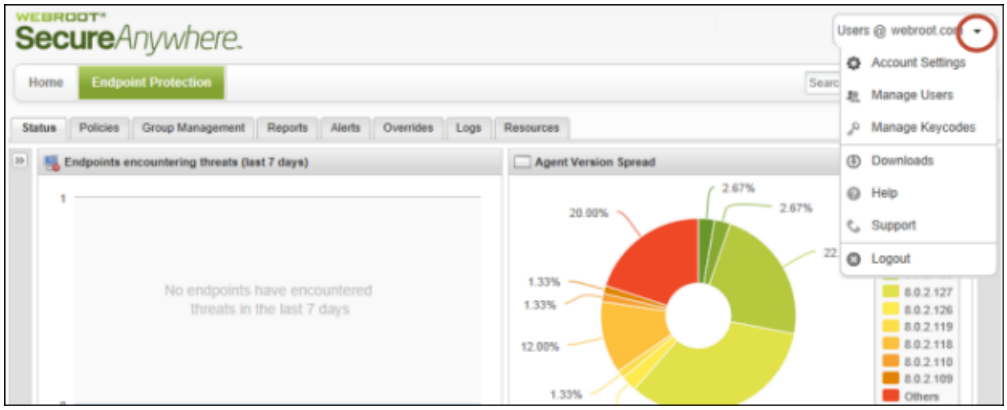
コンソールユーザーの権限設定

エンドポイントプロテクションの管理者権限を持っている場合、他の管理ポータルのユーザーについて、次のような権限を編集することができます。

- **サイトへのアクセス** - SecureAnywhere Web サイト、my.secureanywhere.com のホームパネル、エンドポイントプロテクションの管理ポータルのアクセスレベルを基本レベルと管理者レベルの間で切り替えます。
- **グループ** - ユーザーがエンドポイントのグループの作成および修正、エンドポイントの非アクティブ化または再アクティブ化、グループへのエンドポイントの割り当てを実行できるかどうかを指定します。
- **ポリシー** - ユーザーがポリシーの作成および修正、またはエンドポイントへのポリシーの割り当てを実行できるかどうかを指定します。
- **オーバーライド** - ユーザーがファイルを [正当] または [不当] としてオーバーライドできるかどうかを指定します。
- **コマンド** - ユーザーがエンドポイントに対して発行できるコマンドの種類を指定します。
- **警告** - ユーザーが警告メッセージを作成および編集できるようにします。

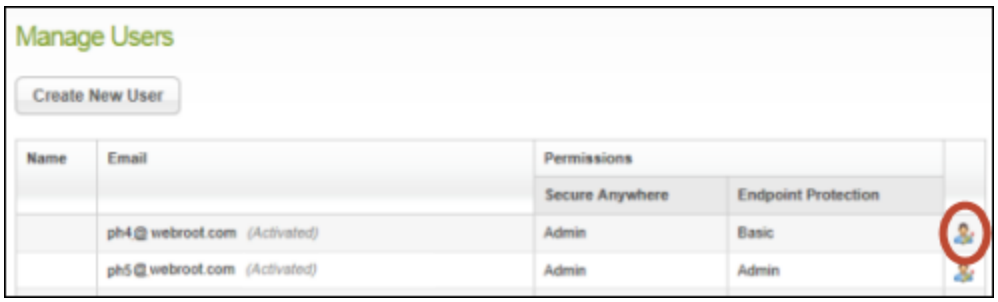
ポータルユーザーの権限を設定するには

1. ログイン ID の横にある**下向き**矢印をクリックし、[**ユーザーの管理**] を選択します。



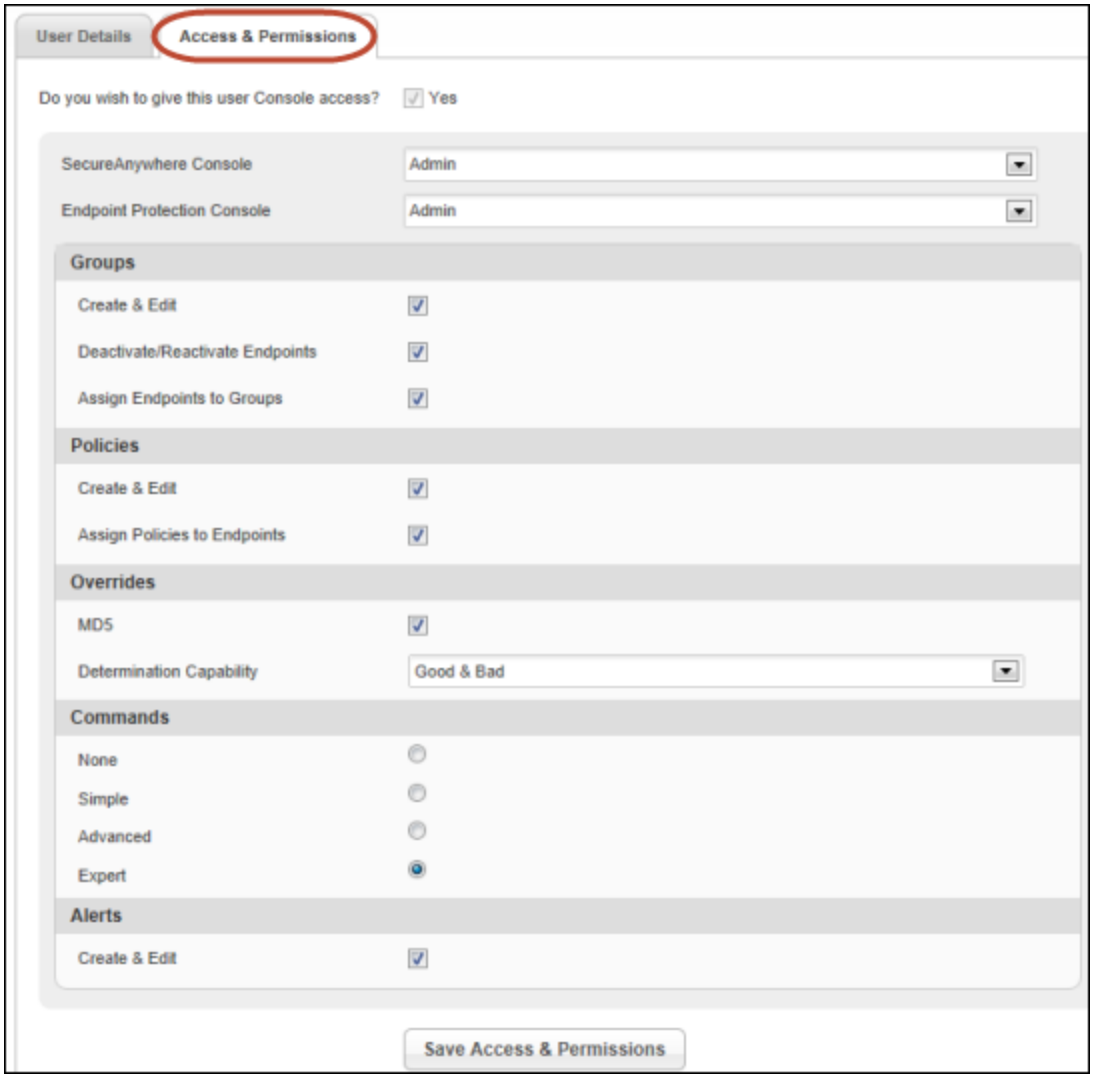
2. 編集する必要のあるユーザーの行を探し、そのユーザーの**編集**アイコンをクリックします。

   編集アイコンは右端に表示されています。



[ユーザーの詳細] パネルが表示されます。

3. [**アクセスおよび権限**] タブをクリックして、エンド ポイント プロテクションの各種機能とそれらに関連するアクセス権限の一覧を表示します。



4. このユーザーにアクセス権限を割り当てます。次の表で各権限について説明します。

オプション	説明
グループ	• **作成・編集** - エンドポイントのグループを定義および修正します。 • **エンドポイントの非アクティブ化 / 再アクティブ化** - 管理ポータルからエンドポイントを非アクティブ化および再アクティブ化します。詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。 • **グループへのエンドポイントの割り当て** - ポータルユーザーが、あるグループの 1 つ以上のエンドポイントを別のグループに移動できるようにします。 詳細については、「*エンドポイントをグループに整理 ページ330*」を参照してください。
ポリシー	• **作成・編集** — ポリシーの定義、削除、名前変更、コピー、エクスポートを行います。 • **エンドポイントへのポリシーの割り当て** - ポリシーをエンドポイントまたはエンドポイントのグループに関連付けます。 詳細については、「*ポリシーの導入 ページ222*」を参照してください。

オプション	説明

オーバーライド	• **MD5** - ファイルの MD5 値を入力して、ファイル検出方法をオーバーライドします。MD5 (メッセージダイジェストアルゴリズム 5) とは、指紋のように動作してファイルを一意に識別する暗号学的ハッシュ関数です。
	• **判定の範囲** - 次のような設定に基づいてオーバーライドを指定します。
	  • **正当** - 指定した MD5 値を含むファイルを許可します。
	  • **不正** - 指定した MD5 値を含むファイルをブロックします。スキャン中に該当するファイルが検出された場合、フラグが付けられ、SecureAnywhere ユーザーによる対応が求められます。
	  • **正当 & 不正** - [正当] または [不正] のいずれかを許可します。
	詳細については、「*オーバーライドの導入 ページ424*」を参照してください。

コマンド	• **なし** - このユーザーがエンドポイントにコマンドを送信することを許可しません。 • **シンプル** - エージェントコマンドとデータ消去コマンドにアクセスし、選択したエンドポイントのコマンドを表示できます。 • **高度** - エージェント、データ消去、キーコード、電源 & ユーザーアクセス、マルウェア対策ツール、ファイル & プロセスの各コマンドにアクセスし、選択したエンドポイントのコマンドを表示できます。 • **エキスパート** - エキスパート上級オプションを含むすべてのコマンドへのアクセスが可能です。 詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

オプション	説明
警告	**作成・編集** - エンドポイントのアクティビティに対する警告の即時発行やスケジュールを設定できます。 詳細については、「*警告の導入 ページ405*」を参照してください。

5. 完了したら、[**アクセスおよび権限を保存**] ボタンをクリックします。

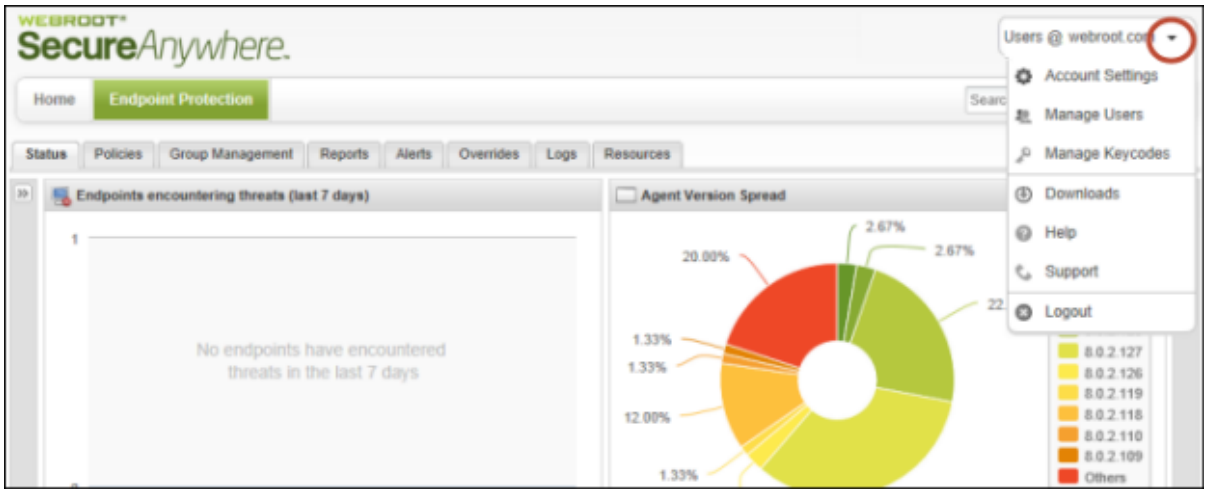
アカウントへのキーコードの追加

ウェブルートアカウントには 1 つまたは複数のキーコードを指定できます。キーコードは、SecureAnywhere をエンドポイントにインストールする際に使用される 20 文字から成るライセンスで、インストールで利用可能なシートの数を識別します。キーコードを追加購入する場合は、このセクションの説明に従って手動で追加する必要があります。

注意: 既存のキーコードを参照して新しいコードを追加するには、エンドポイントプロテクションの管理者権限を持っている必要があります。詳細については、「*コンソールユーザーの権限設定 ページ75*」を*参照してください*。

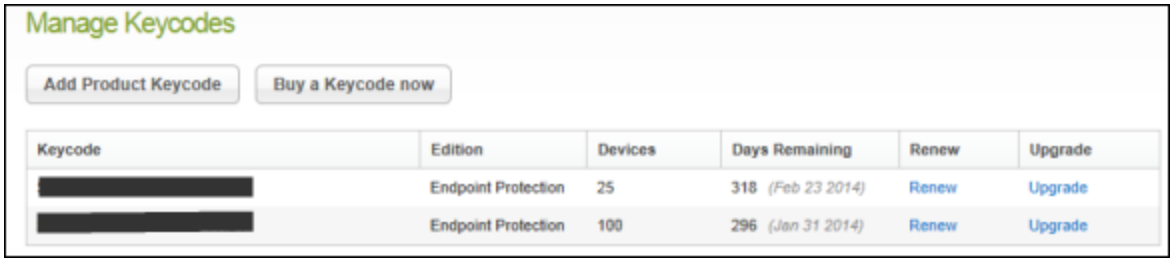
アカウントにキーコードを追加するには

1. ログイン ID の横にある**下向き**矢印をクリックし、[**キーコードの管理**] を選択します。



[キーコードの管理] パネルが表示されます。

- それぞれのエンドポイントプロテクションのライセンスに関する属性がキーコードの一覧に表示されます。
- アカウントに複数のコンソールがある場合、現在アクティブなコンソールに関連付けられたキーコードのみが表示されます。



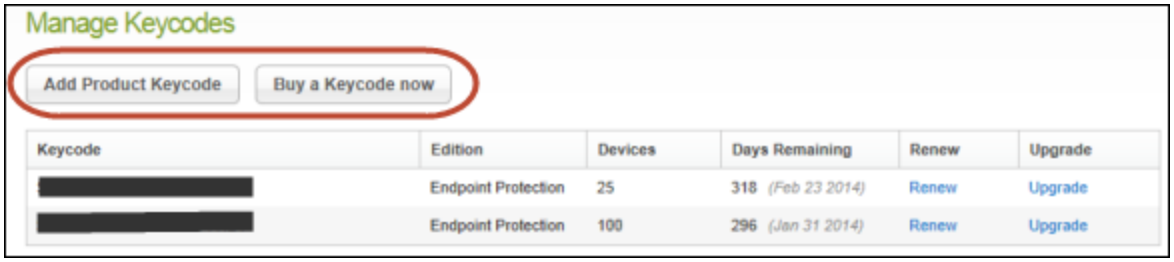
それぞれのエンドポイントプロテクションのライセンスに関する属性がキーコードの一覧に表示されます。

属性	説明
キーコード	エンドポイントプロテクション購入時に受け取った 20 文字のライセンス。
エディション	購入したエンドポイントプロテクションまたは他のウェブルート製品。
デバイス	このキーコードを使用できるエンドポイントの数。
有効期限までの日数	このキーコードの使用期限が切れるまでの日数と有効期限の期日。
更新	定期購入契約を更新するためのリンク。 詳細については、「*アカウントの更新またはアップグレード ページ91*.
アップグレード	このライセンスに対してエンドポイントのシートを追加購入するためのリンク。 詳細については、「*アカウントの更新またはアップグレード ページ91*」を参照してください。

2. キーコードを追加購入するには、[**キーコードを今すぐ購入**] ボタンをクリックします。

   ウェブルートビジネスの Web サイトが開きます。ここで別のキーコードを購入できます。

3. キーコードの購入後、[**製品キーコードを追加**] ボタンをクリックしてエンドポイントプロテクションにそのキーコードを追加します。



4. [キーコードを追加する] ダイアログで購入したキーコードを入力し、[**追加**] をクリックします。

   新しいキーコードが [キーコードの管理] パネルと [リソース] タブに表示されます。

アカウントへのコンソールの追加

初めてアカウントを作成するときに、管理中のデバイスはエンドポイントプロテクションによって 1 つのコンソールにまとめられます。コンソールは、SecureAnywhere または他のウェブルート製品を実行している 1 つまたは複数のエンドポイントをひとまとめにした単位です。数百のエンドポイントを含む大規模なネットワークでは、複数のコンソールを作成してデバイスのグループの簡略化されたビューを使用した方がよい場合もあります。たとえば、リモートオフィスのエンドポイントや別々の部門のエンドポイントに対してそれぞれ別のコンソールを作成できます。

注意: コンソールを追加するには、ウェブルートから新しいキーコードを取得する必要があります。エンドポイントプロテクションの請求システムは、キーコードの数ではなくシートの数に基づいていることに注意してください。エンドポイントのシート数が上限に達していなければ、新たにキーコードを購入する必要はありません。詳細については、ウェブルートの販売部門までご連絡ください。

このトピックでは、次の手順について説明します。

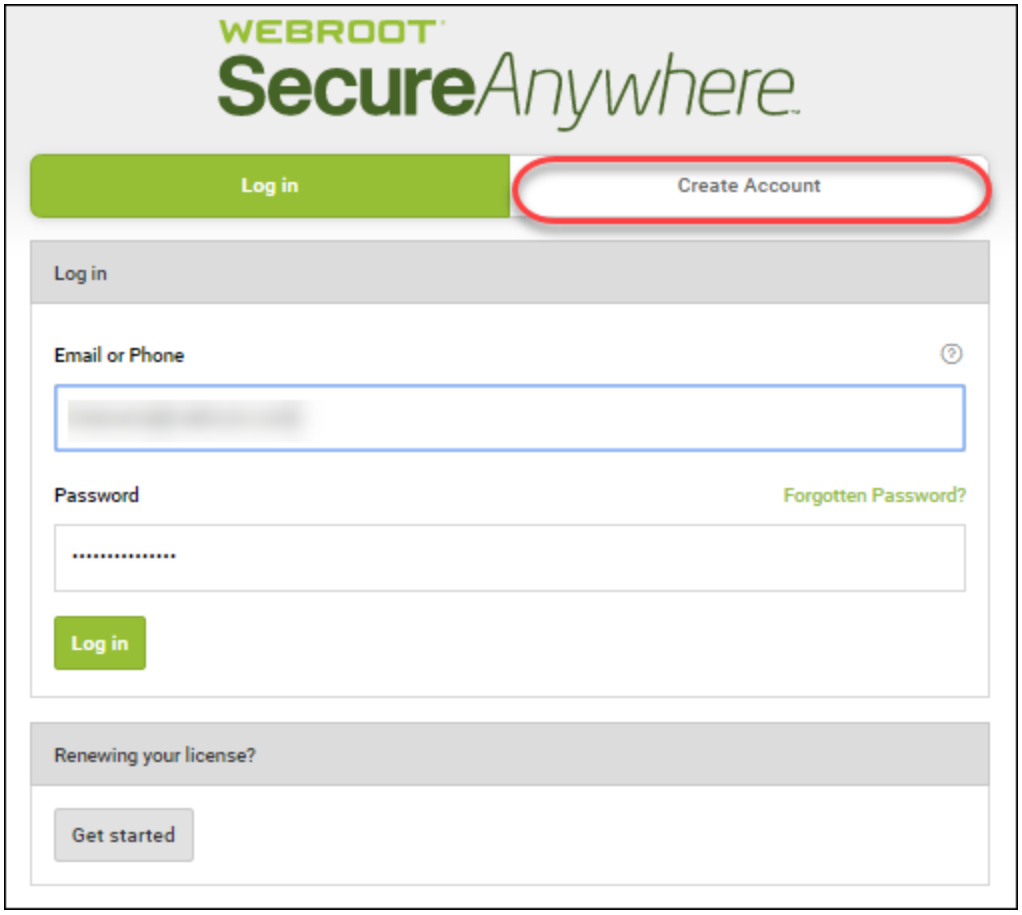
- コンソールの追加
- コンソールの名前の変更
- コンソールの切り替え

コンソールの追加

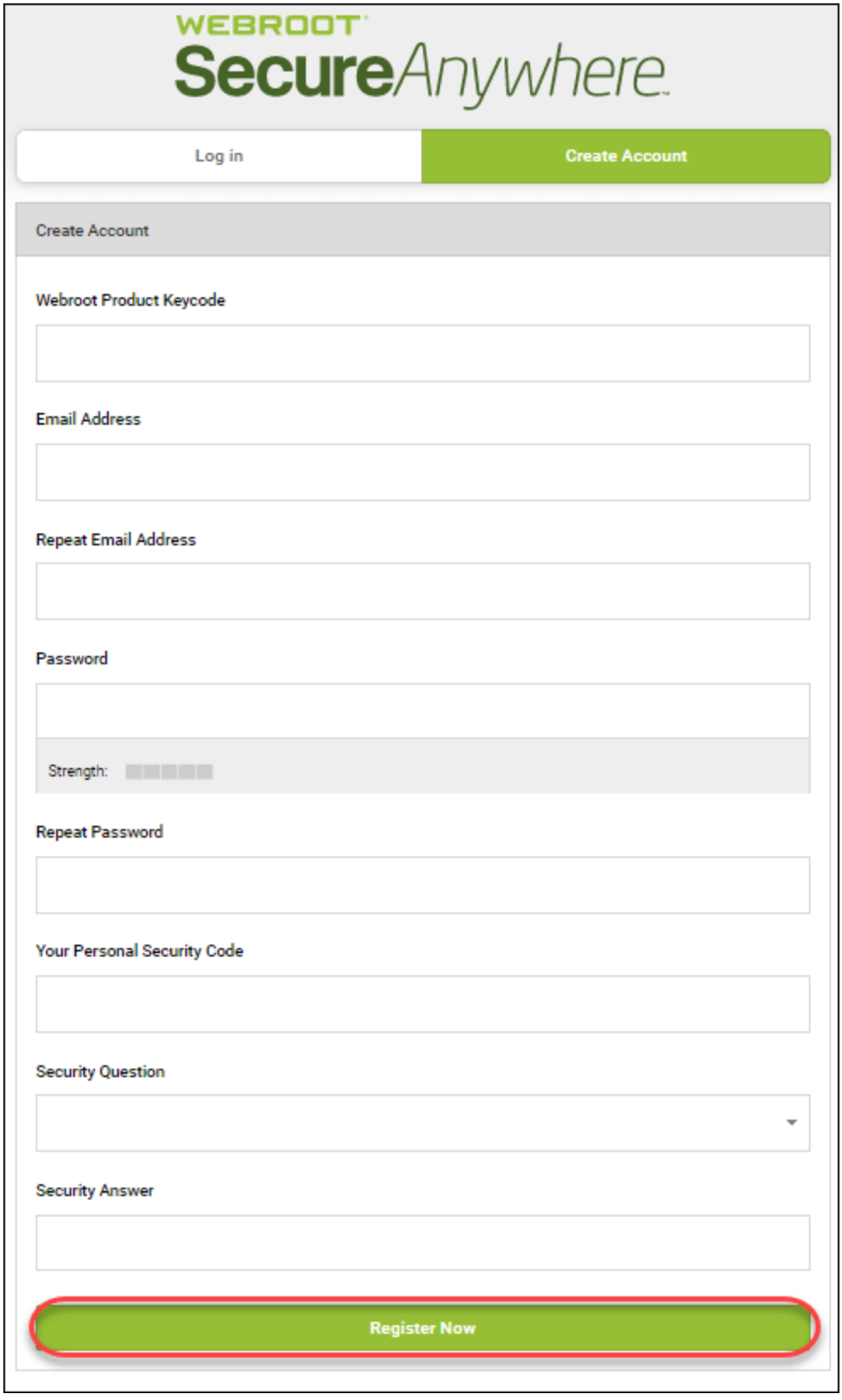
コンソールを作成する前に、まず新しいキーコードを取得し、そのキーコードを使用して SecureAnywhere をエンドポイントに配備する必要があります。コンソールを作成すると、新しいキーコードを使用するエンドポイントが自動的に検出されます。既存のエンドポイントを別のコンソールへ移行する必要がある場合は、*ウェブルート法人向けサポート*までご連絡ください。

アカウントにコンソールを追加するには

1. SecureAnywhere の管理コンソールに移動します: https://my.webrootanywhere.com.
2. アカウントにはログインせずに [**アカウントの作成**] ボタンをクリックします。



3. [**ウェブルート製品のキーコード**] フィールドに新しいキーコードを入力します。


WEBROOT
SecureAnywhere
Log in
Create Account
Create Account
Webroot Product Keycode
Email Address
Repeat Email Address
Password
Strength:
Repeat Password
Your Personal Security Code
Security Question
Security Answer
Register Now

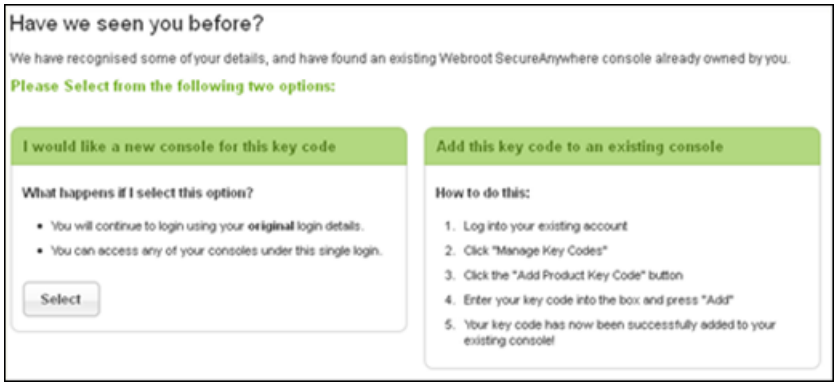
4. その他のフィールドについては、電子メールアドレス、パスワード、セキュリティコード、セキュリティの質問と回答に関して既存のアカウント情報を指定します。

フィールド	説明
電子メールアドレス	エンドポイントプロテクションを管理する管理者の電子メールアドレスを入力します。 アカウントをアクティブ化するための確認のメッセージがこの電子メールアドレスに送信されます。このメールアドレスは、管理コンソールにログインする際のユーザー名にもなります。
パスワード	9 文字以上を入力してください。パスワードは、少なくともアルファベット 6 文字と数字 3 文字を含む必要があります。パスワードは最小文字数の 9 文字を超えても問題ありません。山括弧 (< >) 以外の特殊文字は使用可能です。パスワードの大文字と小文字は区別されます。 入力を始めると、強度メーターがパスワードの安全性を示します。最適なセキュリティを確保するために、パスワードはできるだけ強力なものにすることをお勧めします。
個人用セキュリティコード	文字または数字を入力してください。ログインする際に、パスワードを入力した後の追加のセキュリティ対策として使用されます。6 文字以上で、覚えやすいコードを使用してください。 管理ポータルへのログイン時には毎回、このコードからランダムな 2 文字を入力するように求められます。たとえば、コードが *123456* で、4 番目と 6 番目の文字を入力するよう求められた場合、「4」と「6」を入力します。この個人用セキュリティコードでは大文字と小文字が区別されます。

フィールド	説明
セキュリティの質問	ドロップダウンリストから質問を選択します。 ログインの詳細情報を忘れた場合に、この質問に答えることで情報を取得できます。
セキュリティの回答	セキュリティの質問に対する回答を入力します。セキュリティの回答では大文字と小文字が区別されます。

5. [**今すぐ登録**] ボタンをクリックします。

   ウェブルートでユーザーのアカウント情報が認識されます。ここで、キーコードに対して新しいコンソールを作成するか、既存のコンソールにキーコードを追加します。

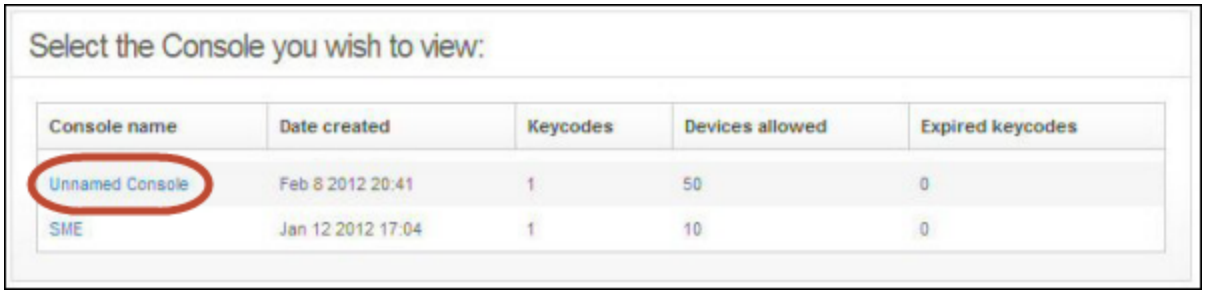


6. 左側のパネルの [**選択**] ボタンをクリックして、新しいコンソールを追加します。

   コンソールが作成され、ログインを促すプロンプトが表示されます。

7. アカウント情報を使ってログインした後、新しく作成された [**名前のないコンソール**] を選択します。名前の変更については、「コンソールの名前の変更」セクションで説明します。

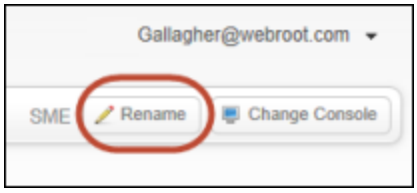
   新しいコンソールに、入力したキーコードを使用するすべてのエンドポイントの一覧が表示されます。



コンソールの名前の変更

コンソールの名前を変更するには

1. 右上のログイン名の下にある [**名前変更**] ボタンをクリックします。

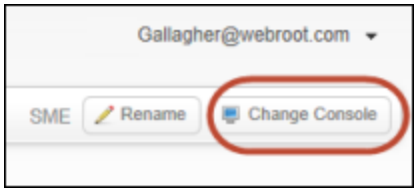


2. 新しい名前を入力し、[**保存**] ボタンをクリックします。名前には数字とスペースを使用できますが、特殊文字は使用できません。

コンソールの切り替え

コンソールを切り替えるには

1. 右上のログイン名の下にある [**コンソールを変更する**] ボタンをクリックします。



2. 表示された表でコンソールの名前を選択します。

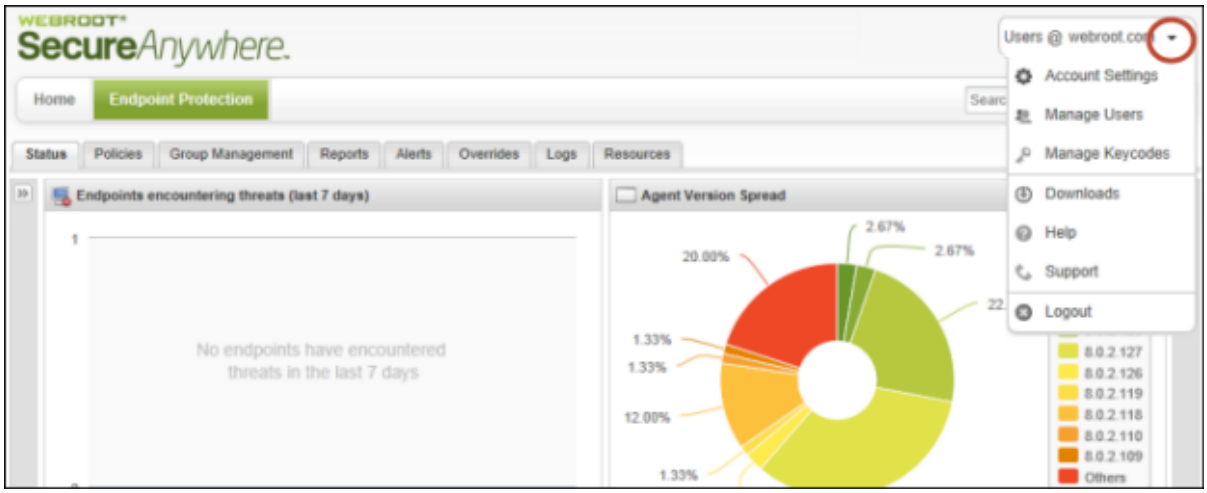
アカウントの更新またはアップグレード

管理ポータルから、エンドポイントプロテクションのライセンスの更新またはライセンスへのシートの追加を簡単に行うことができます。ライセンスの有効期限がもうすぐ切れる場合、またはすでに切れている場合、[状態] パネルに警告メッセージが表示されます。

このメッセージに表示されている [アップグレード/更新] をクリックするか、以下の手順に従って [キーコードの管理] パネルに進みます。

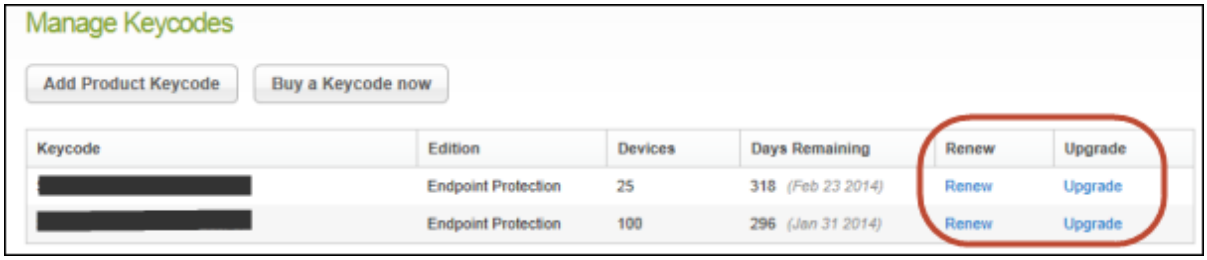
アカウントを更新またはアップグレードするには

1. ログイン ID の横にある**下向き**矢印をクリックし、[**キーコードの管理**] を選択します。



2. [キーコードの管理] ペインで、次のいずれかをクリックします。

   - **更新** - ライセンスを更新する場合。
   - **アップグレード** - ライセンスにシートを追加する場合。



注意: ライセンスはキーコードに関連付けられているため、更新またはアップグレードするキーコードに該当する行を選択してください。

ウェブルートの Web サイトが開き、詳細な手順が表示されます。

サイト管理者の追加

エンドポイントプロテクションの管理者は、追加の管理者を作成できます。追加された管理者は、エンドポイントプロテクションのレポートやデータを閲覧することができます。

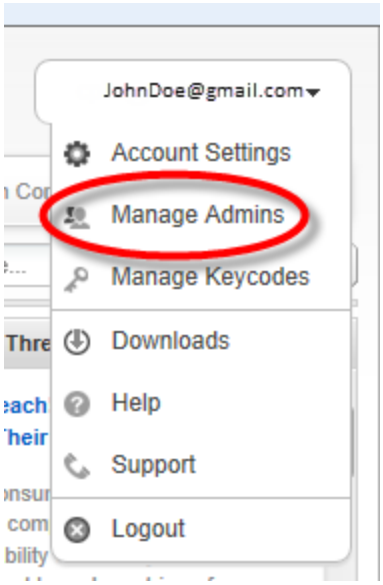
新規ユーザーを作成すると、エンドポイントプロテクションから、パスワードの作成とログインに関する詳細情報が記載された電子メールが新規ユーザーに送信されます。

サイト管理者を追加するには

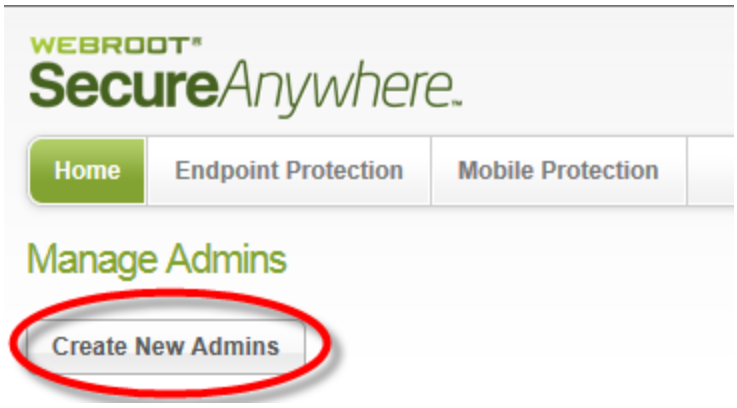
1. ja-my.webrootanywhere.com にログインします。
2. [**エンドポイントプロテクション**] タブをクリックします。

   エンドポイントプロテクションのコンソールが表示されます。

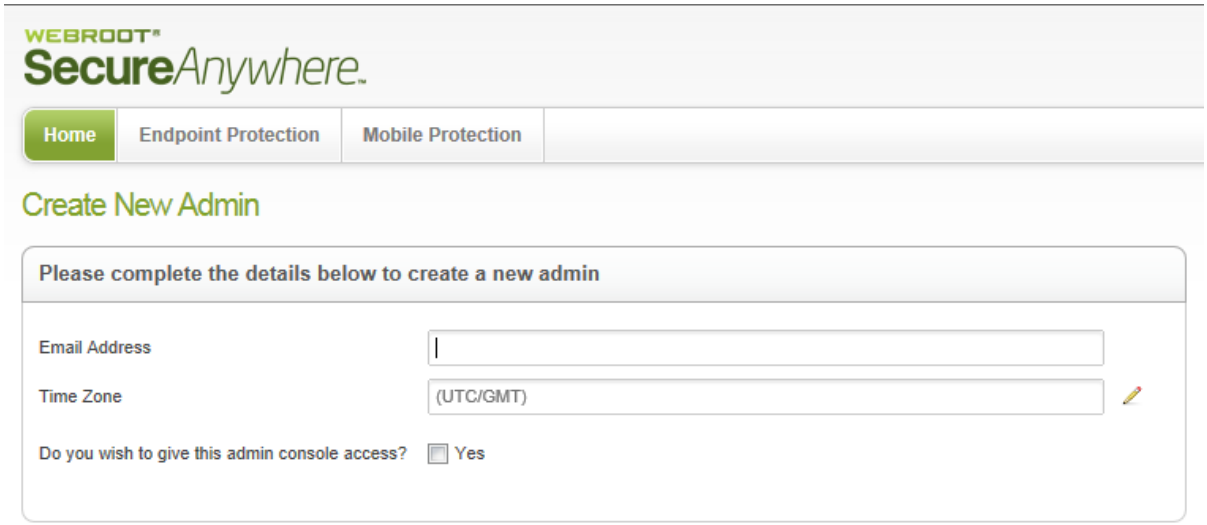
3. ログイン ID の横にあるドロップダウンメニューで [**管理者の管理**] を選択します。



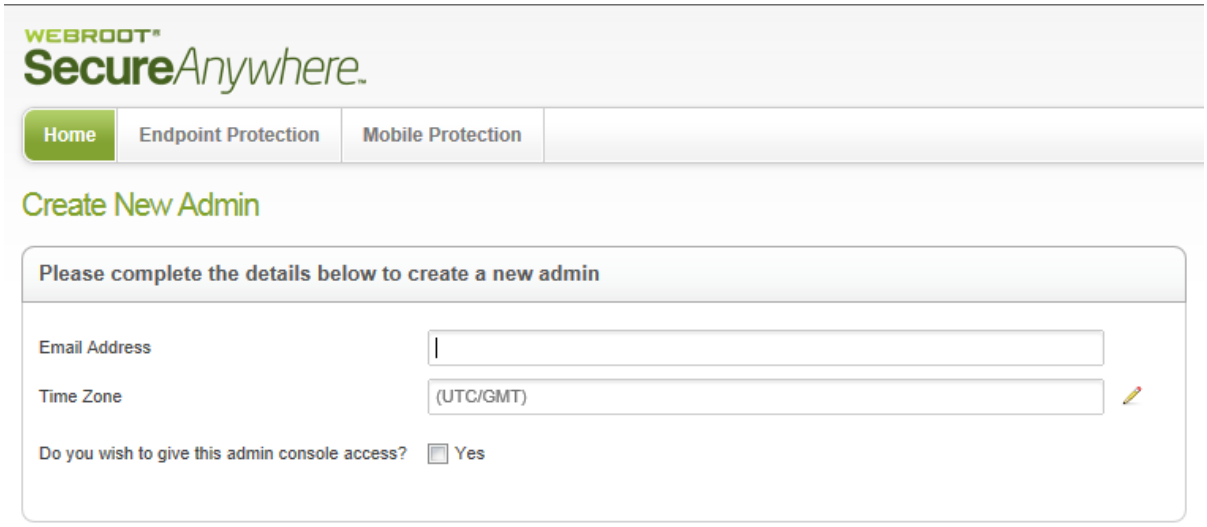
4. [**新規管理者の作成**] ボタンをクリックします。



[新規管理者の作成] パネルが表示されます。



5. [電子メールアドレス] フィールドにユーザーの電子メールアドレスを入力します。



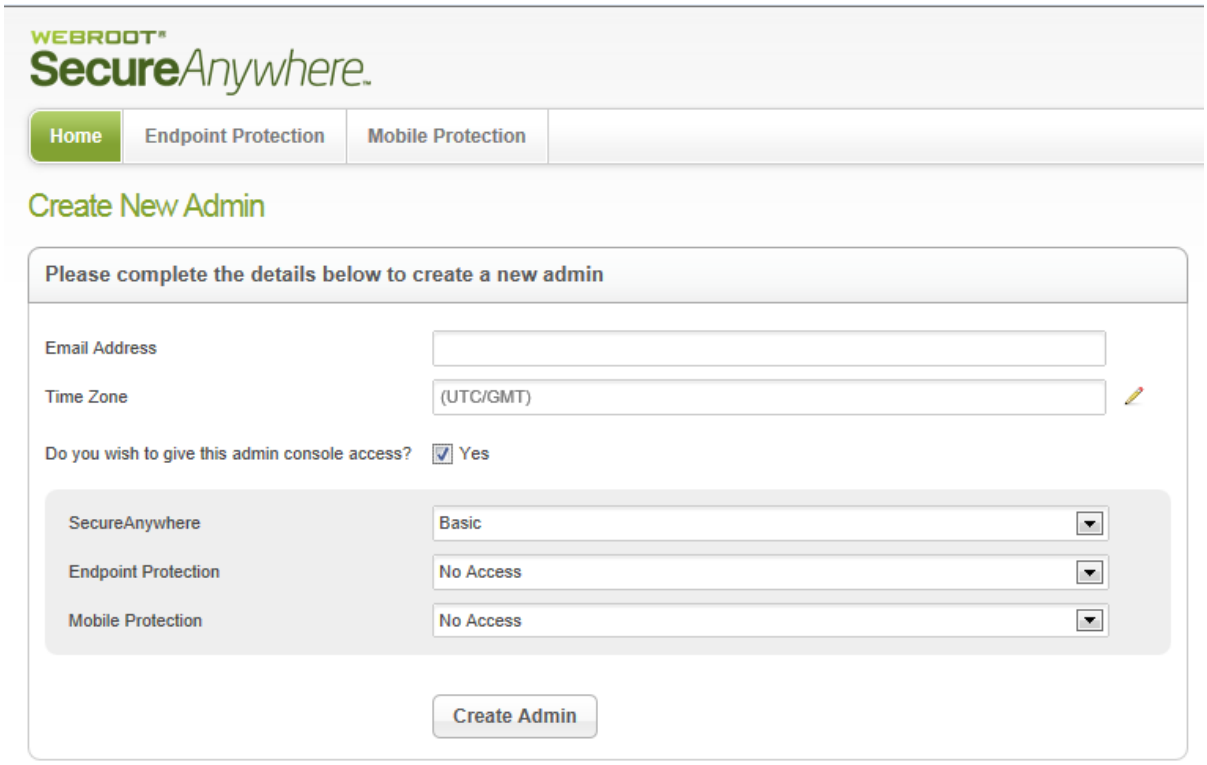
ユーザーが確認メッセージを受信するアドレスを入力します。この電子メールアドレスは、ユーザーのログイン名としても使用されます。間違った電子メールアドレスを入力したためにメッセージを受信できない場合は、電子メールアドレスを変更してメッセージを再送信することができます。詳細については、「*サイト管理者設定の編集 ページ98*」を参照してください。

6. タイムゾーンのフィールドで右側の**鉛筆**のアイコンをクリックし、国、地域、または主要都市を入力すると、ドロップダウンメニューに選択肢が表示されます。ドロップダウンメニューで、新しい管理者のタイムゾーンを選択します。

7. [このユーザーにコンソールへのアクセス権を付与しますか?] **チェックボックスを選択します。**checkbox.

次のフィールドが表示されます。

- SecureAnywhere
- エンドポイントプロテクション
- モバイルプロテクション



8. SecureAnywhere のドロップダウンメニューで、次のいずれかを選択します。

   - **基本** - コンソールとアカウント設定への制限付きアクセス権を付与します。
   - **管理者** - ウェブルートポータルのすべてのキーコード、ユーザー、およびアカウント設定への完全なアクセス権を付与します。

9. エンドポイントプロテクションのドロップダウンメニューで、次のいずれかを選択します。

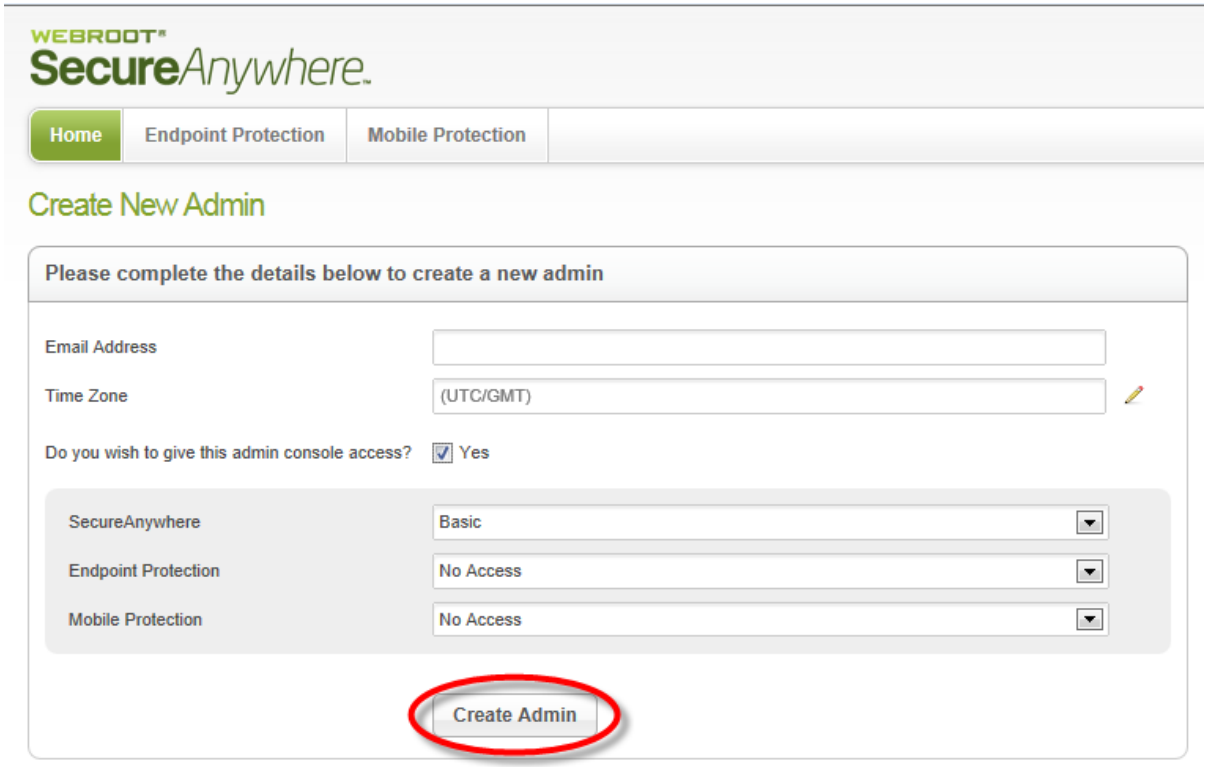
   - **アクセス不可**
   - **基本** - エンドポイントスキャンへの読み取り専用アクセス権を付与します。
   - **管理者** - すべての設定への完全なアクセス権を付与します。

10. モバイルプロテクションのドロップダウンメニューで、次のいずれかを選択します。

    - **アクセス**

- **アクセス不可**

11. 設定が完了したら、[**管理者を作成**] ボタンをクリックします。管理者となる新規ユーザーに確認の電子メールが送信されます。



この電子メールメッセージには、初回にログインするための仮のパスワードが記載されています。

電子メールに記載された確認のリンクをクリックすると、管理者がログイン情報を入力するための [登録確認] パネルが表示されます。

サイト管理者設定の編集

管理者が登録を確認したら、[管理者の管理] パネルに戻り、そのユーザーの情報を編集することができます。

ユーザーが電子メールを受信して登録を確認すると、状態が [アクティブ] に変わります。

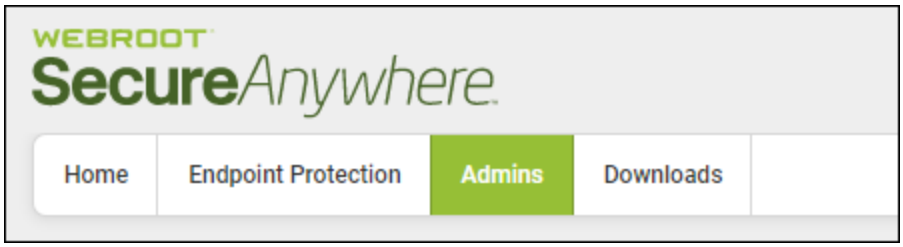
ユーザーが登録を確認していない場合、ユーザーの状態は [確認待ち] と表示されます。必要に応じて、[確認待ち] 状態の横にある封筒のアイコンをクリックすると、確認の電子メールを再送信できます。

サイト管理者設定を編集するには

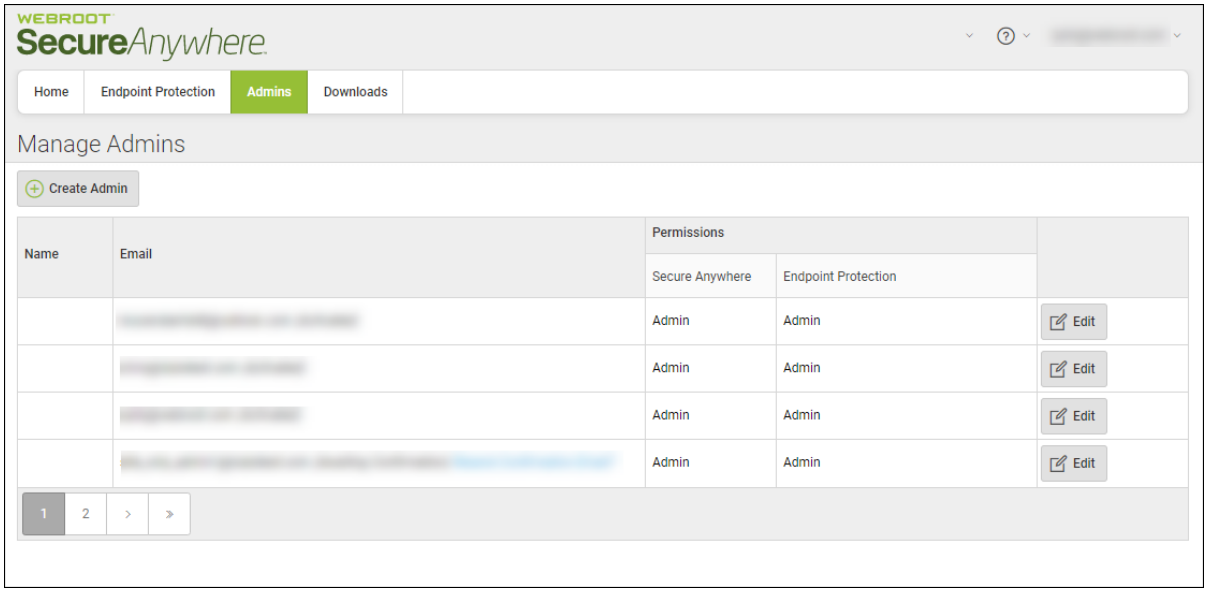
1. ja-my.webrootanywhere.com にログインします。
2. [**エンドポイント プロテクション**] タブをクリックします。

   エンドポイント プロテクションのコンソールが表示されます。

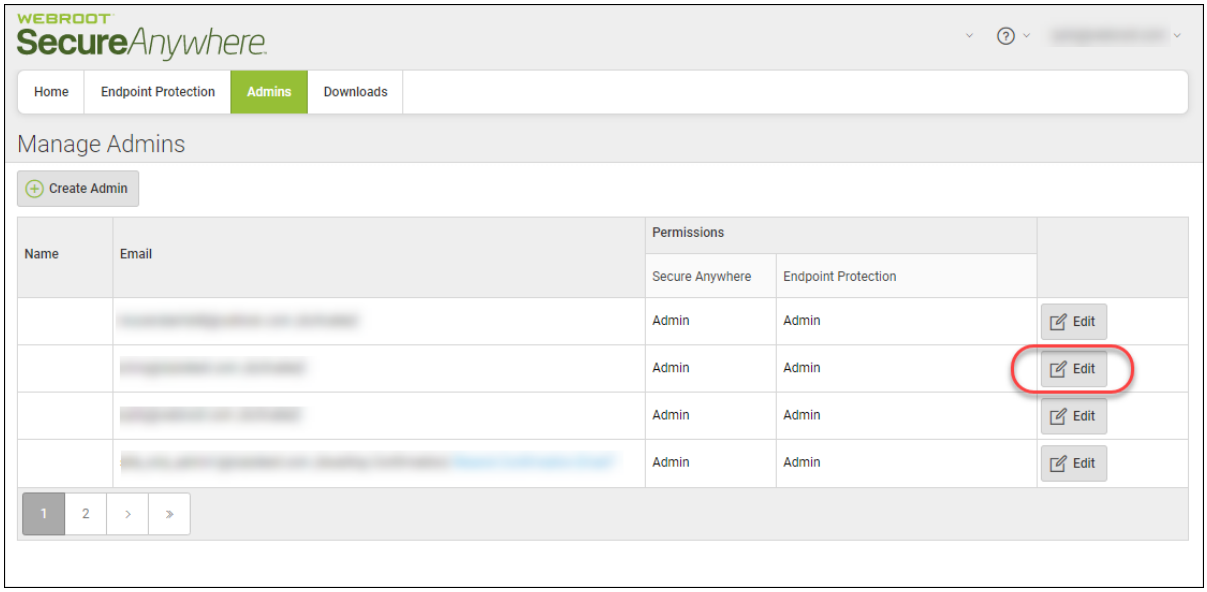
3. メインメニューの [*管理者*] タブをクリックします。



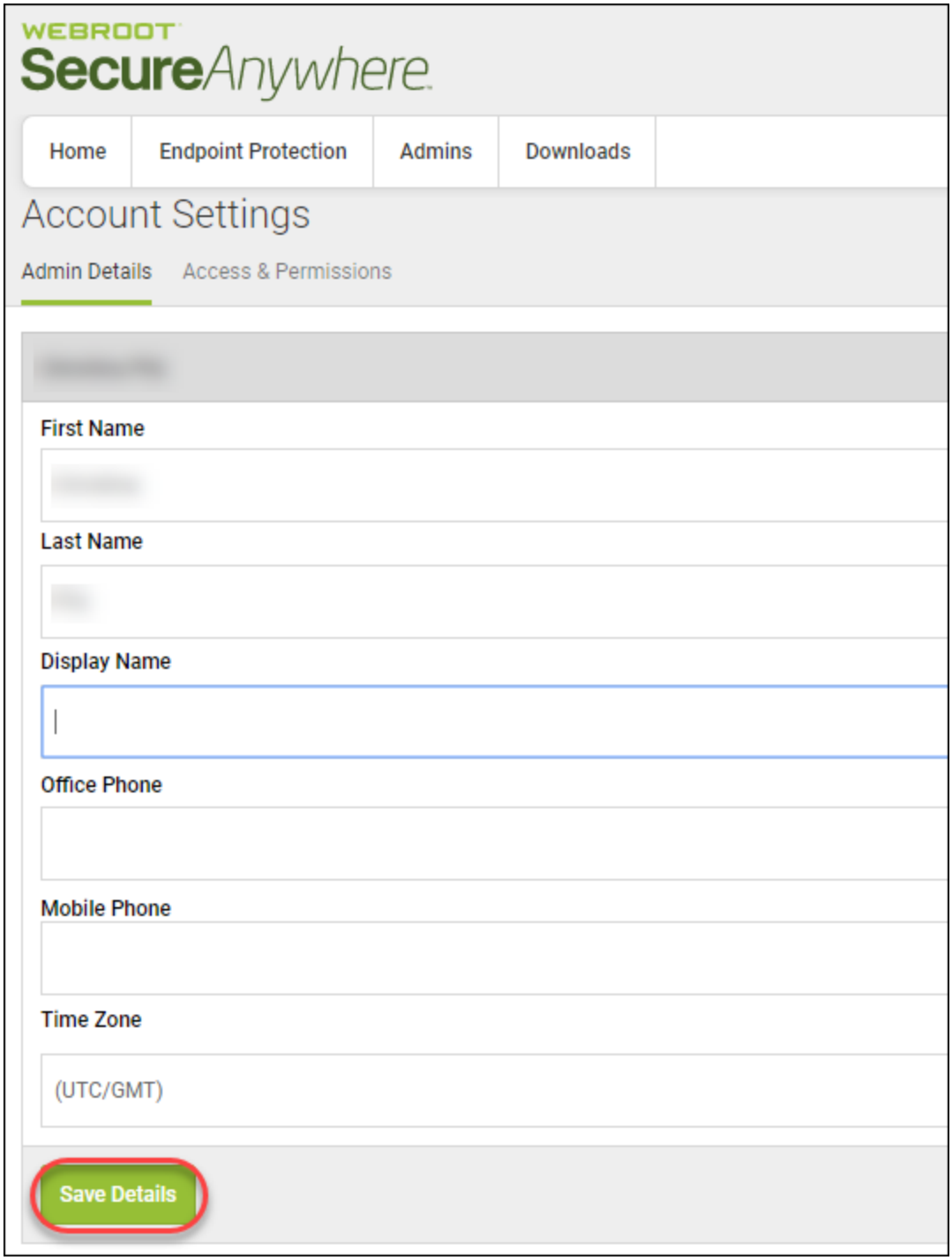
   管理者のリストが表示されます。



4. 編集する必要のあるユーザーの行を探し、そのユーザーの [**編集**] ボタンをクリックします。

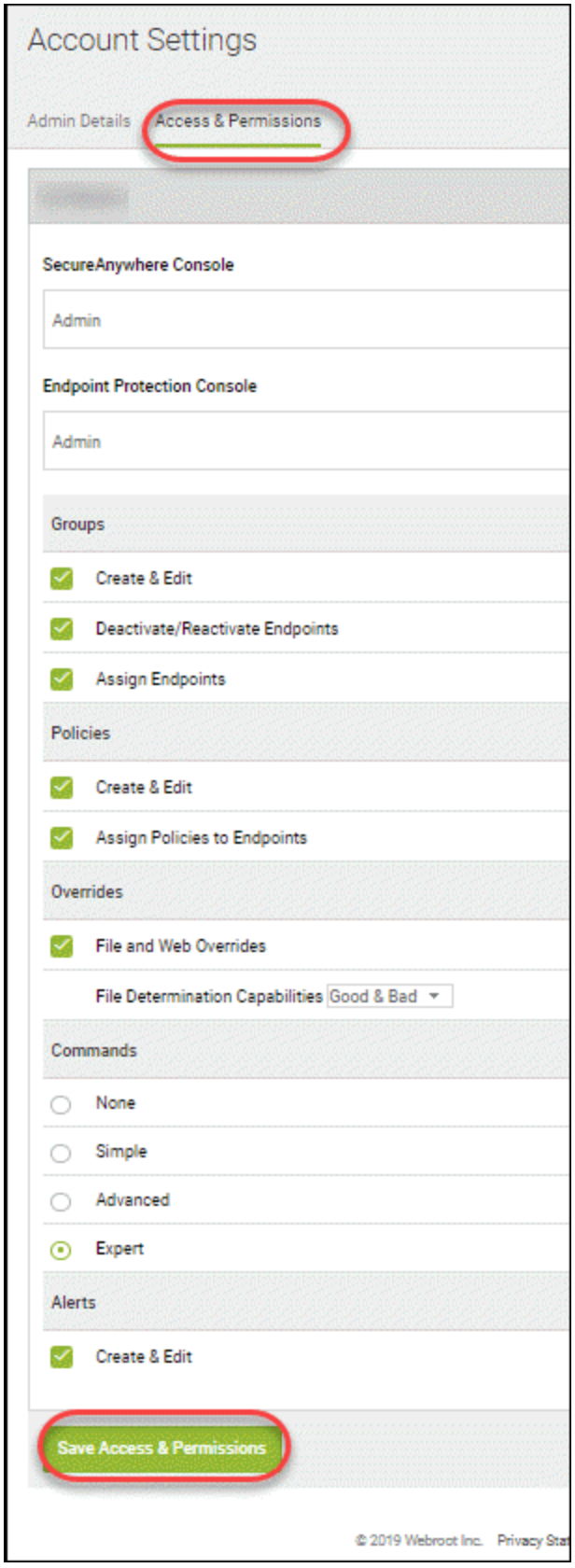


[アカウント設定] ウィンドウが、[管理者の詳細] タブがアクティブになった状態で表示されます。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Admins
Downloads
Account Settings
Admin Details
Access & Permissions
First Name
Last Name
Display Name
Office Phone
Mobile Phone
Time Zone
(UTC/GMT)
Save Details

5. 完了したら、[**情報を保存**] ボタンをクリックします。

6. **アクセスおよび権限**] タブをクリックします。


Account Settings
Admin Details
Access & Permissions
SecureAnywhere Console
Admin
Endpoint Protection Console
Admin
Groups
Create & Edit
Deactivate/Reactivate Endpoints
Assign Endpoints
Policies
Create & Edit
Assign Policies to Endpoints
Overrides
File and Web Overrides
File Determination Capabilities
Good & Bad
Commands
None
Simple
Advanced
Expert
Alerts
Create & Edit
Save Access & Permissions
© 2019 Webroot Inc.

7. 必要に応じて、次の表の情報に従って設定を変更します。

設定	説明
SecureAnywhere コンソール	次の権限レベルのいずれかを選択します。 • **アクセス不可** • **基本** • **管理者**
エンドポイントプロテクションのコンソール	次の権限レベルのいずれかを選択します。 • **アクセス不可** • **基本** • **管理者**
グループ	
作成・編集	このチェックボックスを選択すると、管理者がエンドポイントのグループを定義したり修正したりできるようになります。
エンドポイントの非アクティブ化 / 再アクティブ化	このチェックボックスを選択すると、管理者が管理ポータルからエンドポイントを非アクティブ化したり再アクティブ化したりできるようになります。 詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。

設定	説明
グループへのエンドポイントの割り当て	このチェックボックスを選択すると、管理者があるグループの 1 つ以上のエンドポイントを別のグループに移動できるようになります。 詳細については、「*エンドポイントをグループに整理 ページ330*」を参照してください。
ポリシー	
作成・編集	このチェックボックスを選択すると、管理者がポリシーの定義、削除、名前変更、コピー、エクスポートを実行できるようになります。
エンドポイントへのポリシーの割り当て	このチェックボックスを選択すると、管理者がポリシーをエンドポイントまたはエンドポイントのグループに関連付けられるようになります。 詳細については、「*ポリシーの導入 ページ222*」を参照してください。
オーバーライド	
MD5	このチェックボックスを選択すると、管理者がファイルの MD5 値を入力して、ファイル検出方法をオーバーライドできるようになります。 MD5 (メッセージダイジェストアルゴリズム 5) とは、指紋のように動作してファイルを一意に識別する暗号学的ハッシュ関数です。

設定	説明
判定の範囲	ドロップダウンメニューから次のいずれかを選択してオーバーライドを決定します。 • **正当** - 指定した MD5 値を含むファイルを許可します。 • **不正** - 指定した MD5 値を含むファイルをブロックします。スキャン中に該当するファイルが検出された場合、フラグが付けられ、SecureAnywhere ユーザーによる対応が求められます。 • **正当 & 不正** - [正当] または [不正] のいずれかを許可します。 詳細については、「*オーバーライドの導入 ページ424*」を参照してください。
コマンド	
なし	管理者がエンドポイントにコマンドを送信できないようにするには、このラジオボタンを選択します。
シンプル	管理者がエージェントコマンドとデータ消去コマンドにアクセスし、選択したエンドポイントのコマンドを表示できるようにするには、このラジオボタンを選択します。
詳細	管理者がエージェント、データ消去、キーコード、電源 & ユーザーアクセス、マルウェア対策ツール、ファイル & プロセスの各コマンドにアクセスし、選択したエンドポイントのコマンドを表示できるようにするには、このラジオボタンを選択します。
エキスパート	管理者がエキスパート上級オプションを含むすべてのコマンドにアクセスできるようにするには、このラジオボタンを選択します。

設定	説明
警告	
作成・編集	管理者がエンドポイントのアクティビティに対する警告の即時発行やスケジュールを設定できるようにするには、このチェックボックスを選択します。 詳細については、「*警告の導入 ページ405*」を参照してください。

8. 完了したら、[**アクセスおよび権限を保存**] ボタンをクリックします。

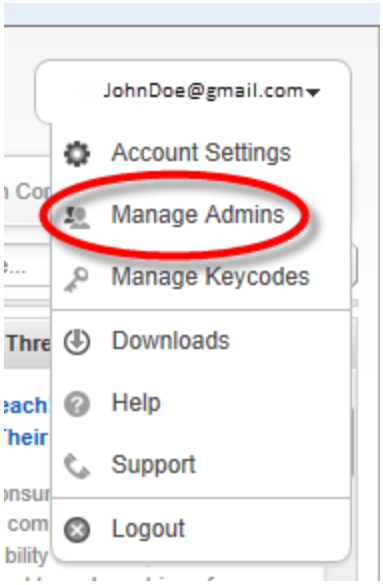
サイト管理者の削除

サイト管理者を削除するには

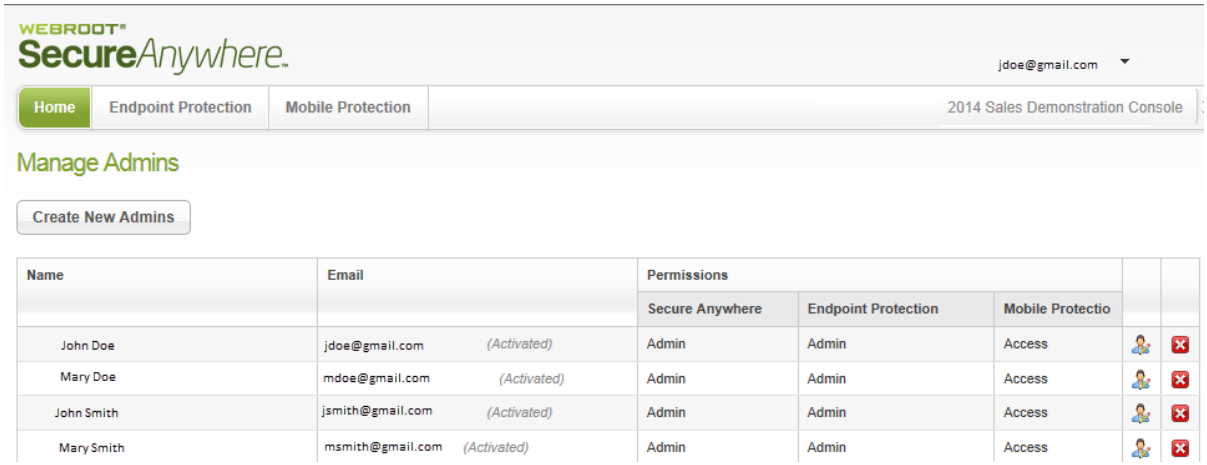
1. ja-my.webrootanywhere.com にログインします。
2. [**エンドポイントプロテクション**] タブをクリックします。

   エンドポイントプロテクションのコンソールが表示されます。

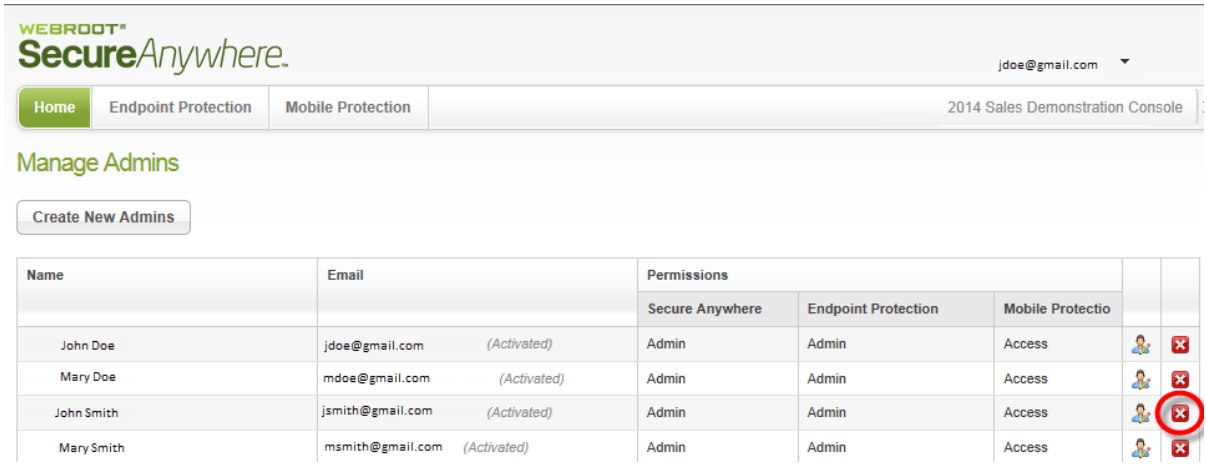
3. ログイン ID の横にあるドロップダウンメニューで [**管理者の管理**] を選択します。



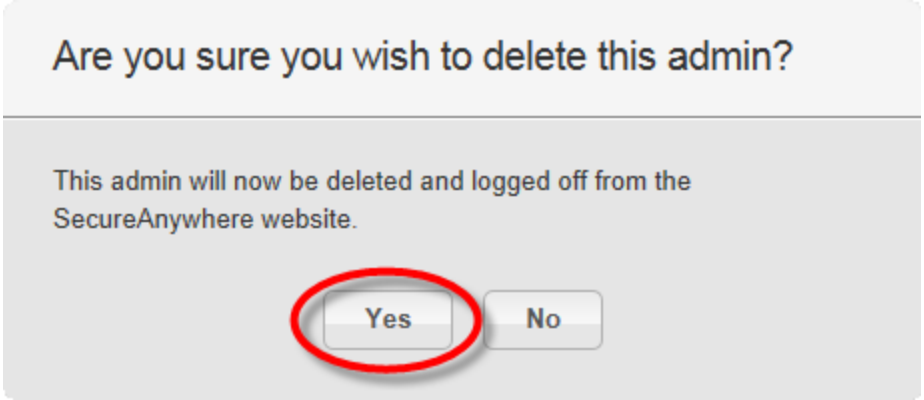
管理者のリストが表示されます。.



4. 編集する必要のあるユーザーの行を探し、そのユーザーの [**削除**] アイコンをクリックします。



警告メッセージが表示されます。



5. [**はい**] ボタンをクリックして削除を承認します。
6. ブラウザを更新し、サイト管理者がシステムから削除されたことを確認します。

第 4 章: エンドポイントの管理

エンドポイントの管理方法については、以下のトピックを参照してください。

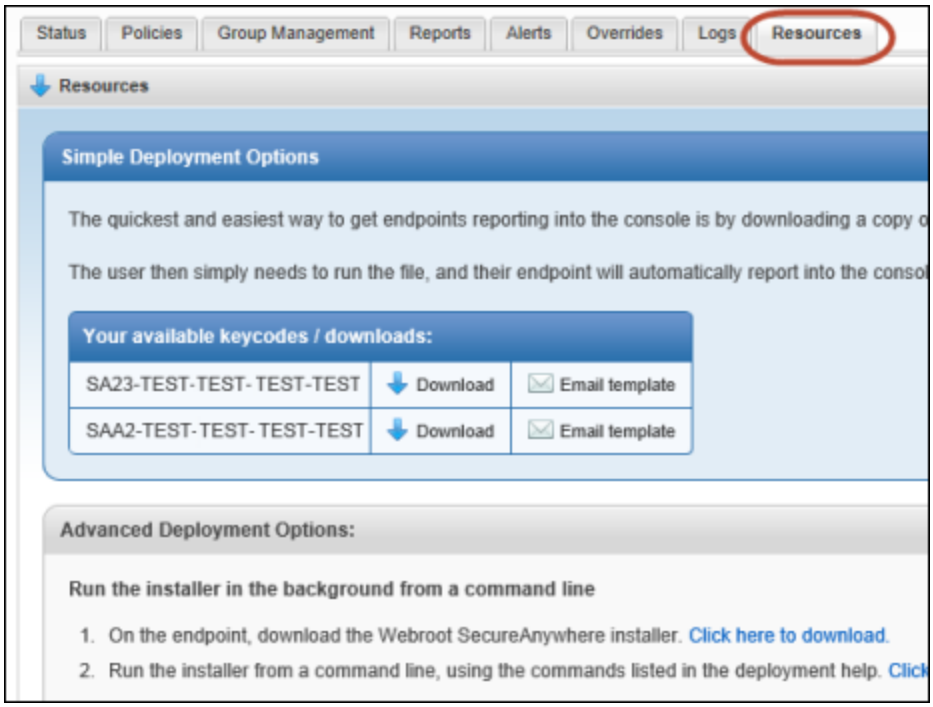
エンドポイントへの SecureAnywhere の配備

ビジネス要件やネットワークの規模に応じて、さまざまな方法で SecureAnywhere をエンドポイントに配備することができます。Windows の PC、ノートパソコン、サーバー、またはネットワークにインストールされている仮想サーバーをエンドポイントとして使用できます。エンドポイントのシステム要件については、「*セットアップの準備 ページ5*」を参照してください。

注意: 新しいエンドポイントがインストールされると管理者に通知が送信されるよう、警告を設定することができます。詳細については、「*警告の導入 ページ405*」を参照してください。

エンドポイントに SecureAnywhere を配備するには

1. キーコードを確認します。キーコードが不明な場合は、管理ポータルの [**リソース**] タブをクリックしてください。



注意: 管理ポータルへの報告を行うには、デバイスでエンドポイントプロテクションのキーコードを使用している必要があります。SecureAnywhere がすでに異なる種類のキーコードを利用してインストールされている場合は、「*エンドポイントキーコードの変更 ページ135*」を参照してください。

2. 環境に最も適した配備の方法を選択します。

   次の表では、さまざまな配備の方法について説明しています。

オプション	説明
SecureAnywhere 実行可能ファイルの配備	次のいずれかの方法で SecureAnywhere のインストーラーファイルを配備します。 • 各エンドポイントで実行可能ファイルを手動インストール。 • エンドユーザーに電子メールを送信。エンドユーザーは、電子メールテンプレートに記載されたリンクをクリックしてソフトウェアをインストールできます。 • キーコードを使用して実行可能ファイル名を変更。電子メールテンプレートでは、名前が変更された実行可能ファイルとキーコードが提供されます。 • 追加コマンドを使用して実行可能ファイルをバックグラウンドで配備。 • インストーラーでコマンドラインオプションを使用。プロキシサーバーの背後にあるエンドポイントへの配備が可能です。
MSI 配備オプションの使用	Microsoft インストーラー (MSI) を使用して SecureAnywhere インストーラーファイルを配備。
Windows グループポリシーオブジェクト (GPO) の使用	グループポリシーオブジェクト (GPO) を使用して SecureAnywhere インストーラーファイルを配備。Microsoft の Active Directory および GPO エディタに関する知識が必要です。

注意: Iエンドポイントの数が 100 未満の小規模ネットワークでは、[リソース] タブで説明するシンプルな配備オプションを使用することをお勧めします。大規模なネットワークで Active Directory を使用している場合は、高度な配備オプションを使用してください。大規模なネットワークでは、エンドポイントを別々のコンソールに整理して、小さいグループごとの簡略化されたビューを使用することもできます。詳細については、「*アカウントへのコンソールの追加 ページ84*」を参照してください。

3. 以下のいずれかのセクションの説明に従って、SecureAnywhere をエンドポイントに配備します。

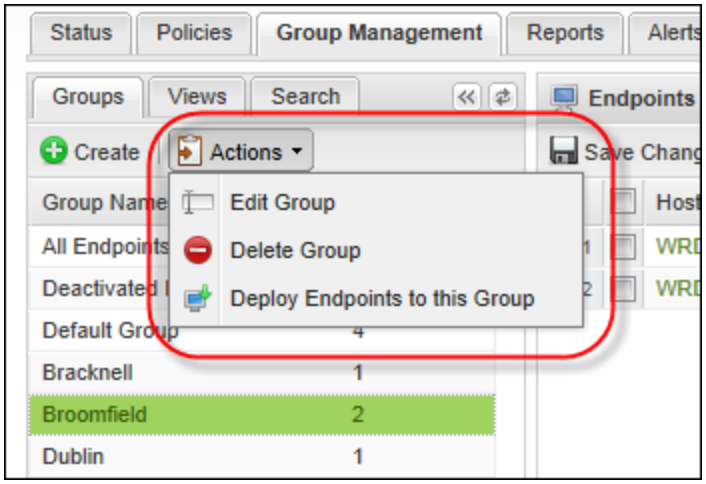
   - SecureAnywhere インストーラーの使用
   - MSI 配備オプションの使用。
   - GPO 配備オプションの使用

   注意: 管理ポータルで、エンドポイントの状態が報告されていることを確認します。詳細については、「*エンドポイントの状態の表示 ページ204*」を参照してください。

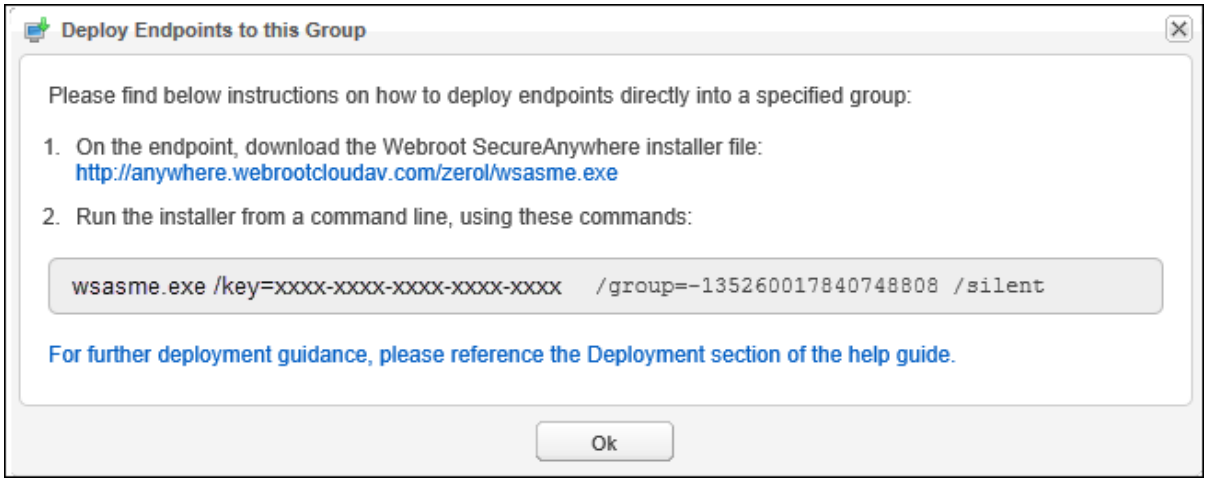
4. 以下のいずれかの操作を行います。

   - エンドポイントがデフォルトのポリシーおよびグループに割り当てられるようにします。すべてのエンドポイントはまず、デフォルトのポリシーおよびグループに割り当てられます。割り当ては、必要に応じて後で変更することができます。詳細については、「*ポリシーの導入 ページ222*」および「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

   - エンドポイントを特定のグループに割り当てるには、エンドポイントを追加するグループを選択し、[アクション] ドロップダウンメニューで [**このグループにエンドポイントを配備**] を選択します。



コマンドリンクからソフトウェアをインストールするために必要な情報が表示され、選択したグループにエンドポイントが追加されます。



5. 設定が完了したら、[**OK**] ボタンをクリックします。

SecureAnywhere インストーラーの使用

次のいずれかの方法で SecureAnywhere のインストーラーファイルを配備します。

- 各エンドポイントに SecureAnywhere をインストール。Mac にインストールする場合はこのオプションを使用してください。

- エンドユーザーに電子メールを送信。エンドユーザーは、電子メールテンプレートに記載されたリンクをクリックしてソフトウェアをインストールできます。
- キーコードを使用して実行可能ファイル名を変更。この方法は、独自の配備ツールを使用することを計画している場合や、MSI コマンドを使用せずにバックグラウンドでインストールを実行することが望ましい場合に適しています。
- 追加コマンドを使用して実行可能ファイルをバックグラウンドで配備。
- インストーラーでコマンドラインオプションを使用。プロキシサーバーの背後にあるエンドポイントへの配備が可能です。

Windows 版の SecureAnywhere インストーラーを使用するには

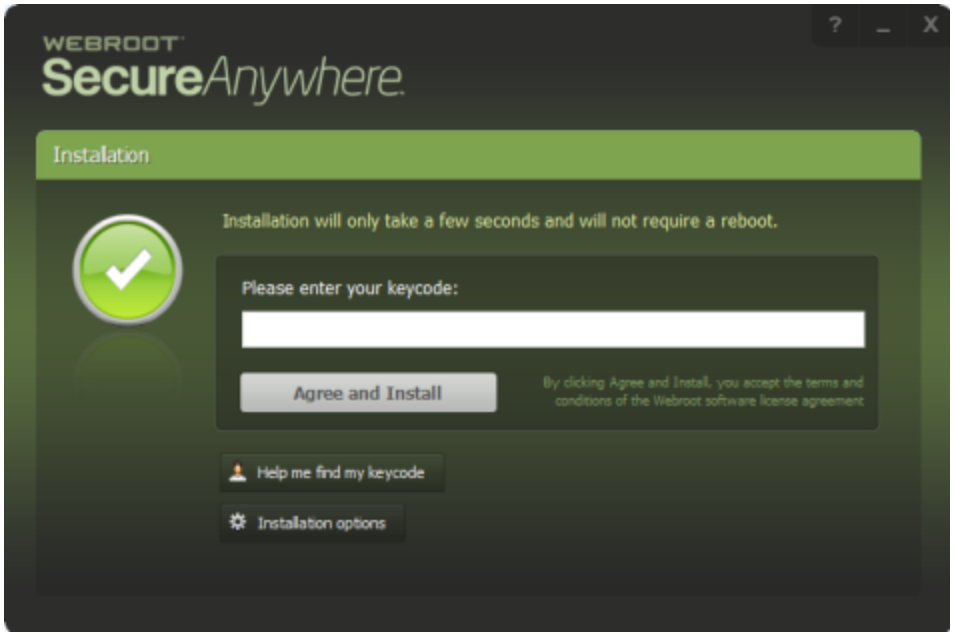
1. エンドポイントで、SecureAnywhere のインストーラーファイルをダウンロードします。

   インストーラーファイルは [リソース] タブにあります。または、次のリンクをクリックしてください。

   http://anywhere.webrootcloudav.com/zerol/wsasme.exe

2. インストールパネルでキーコードを入力します。

   キーコードが [リソース] タブに表示されます。



3. 必要に応じて、インストールパネル下部にある [**インストールオプション**] ボタンをクリックし、次のオプションを設定できます。

   - **SecureAnywhere へのショートカットをデスクトップに作成する** - このオプションを選択すると、Windows のデスクトップに SecureAnywhere のショートカットアイコンが作成されます。

   - **感染を回避するために、インストールファイルの名前をランダムに変更する** - このオプションを選択すると、ウェブルートのインストールファイルの名前がランダムに変更されます (「QrXC251G.exe」など)。これにより、マルウェアによるウェブルートのインストールファイルの検出とブロックを回避できます。

   - **SecureAnywhere のファイル、プロセス、メモリを改ざんから保護する** - このオプションを選択すると、自己保護と CAPTCHA のプロンプトが有効になります。CAPTCHA を使用する場合、重要なアクションを実行する前に、ユーザーが画面上の歪んだ文字を読みとり、文字をフィールドに入力する必要があります。

   - **言語を変更する** — SecureAnywhere で表示される言語を変更する場合は、[**言語を変更する**] ボタンをクリックして、サポートされている言語を選択してください。表示言語はインストールの際にのみ変更できます。インストール後は変更できません。

4. [**同意してインストール**] ボタンをクリックします。

   インストール中に SecureAnywhere によるクイックスキャンがエンドポイントで実行されます。

Mac 版の SecureAnywhere インストーラーを使用するには

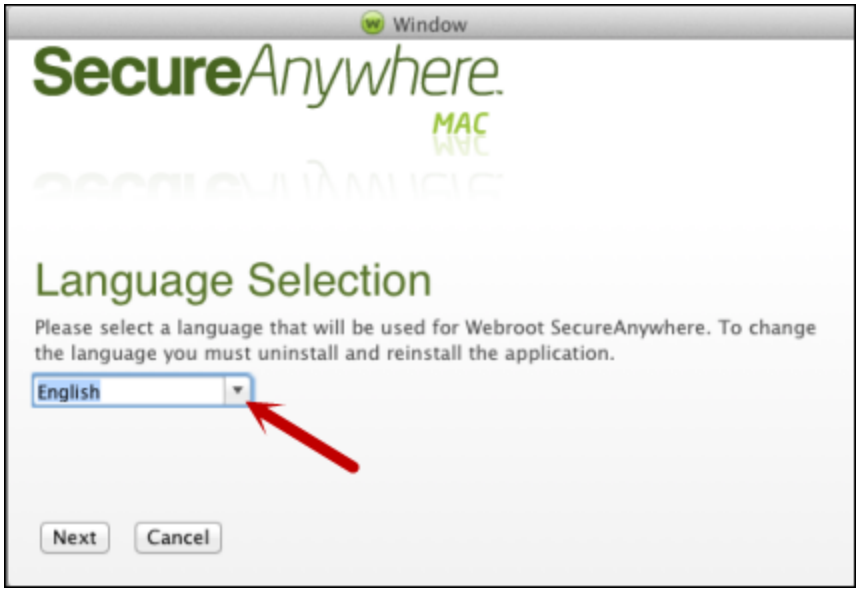
1. エンドポイントで、SecureAnywhere のインストーラーファイルをダウンロードします。

   インストーラーファイルは [リソース] タブにあります。または、次のリンクをクリックしてください。

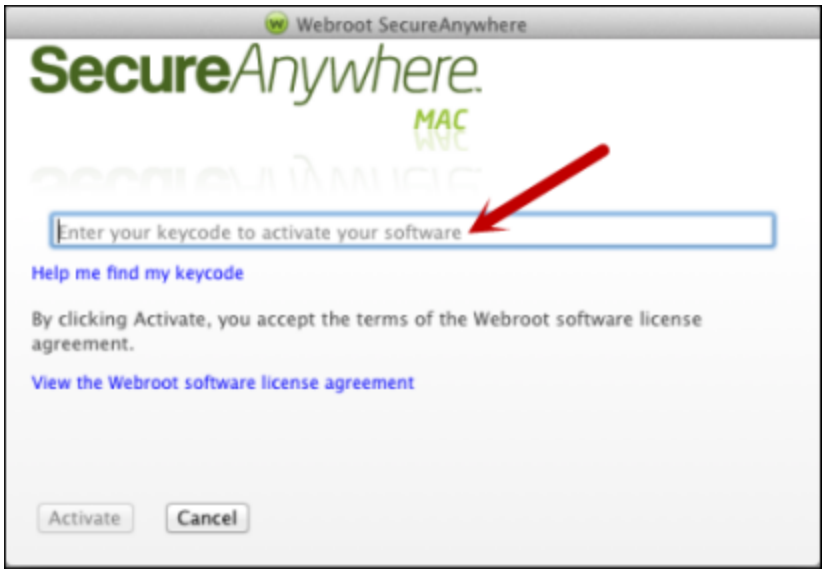
   http://anywhere.webrootcloudav.com/zerol/wsamac.dmg

2. SecureAnywhere インストーラーを Mac にダウンロードします。
3. **wsamac.dmg** をダブルクリックしてインストーラーを開きます。
4. [**アプリケーション**] フォルダをダブルクリックして開きます。
5. [アプリケーション] フォルダの **Webroot SecureAnywhere** のアイコンをダブルクリックし、アクティブ化を開始します。
6. 初期アクティブ化ウィンドウの言語選択ドロップダウンメニューで言語を選択し、[**次へ**] ボタンをクリックします。

注意: 必ず適切な言語を選択してください。SecureAnywhere のインストール後に言語を変更することはできません。



7. 次のパネルでキーコードを入力し、[**アクティブ化**] ボタンをクリックします。



8. その他の画面のプロンプトに従ってインストールを最後まで進めます。

エンドユーザーが自分で SecureAnywhere をインストールできるよう電子メールを送信するには

1. [**リソース**] タブをクリックします。
2. [**電子メールテンプレート**] リンクをクリックします。

   電子メールテンプレートが [使用を開始するには] ウィンドウに表示されます。

3. 電子メールメッセージにテキストをカット & ペーストします。正しいキーコードがリンクにより自動的に追加されます。ユーザーに電子メールを送信します。

   ユーザーがインストールを開始するリンクをクリックします。プログラムは、入力済みの正しいキーコードを使用してバックグラウンドでインストールを実行します。プロセスが完了すると、エンドポイントのシステムトレイにウェブルートのアイコンが表示されます。

実行可能ファイルの名前を変更してバックグラウンドでインストールを実行するには

キーコードを含む実行可能ファイルの名前を変更して SecureAnywhere を配備することができます。この方法は、独自の配備ツールを使用することを計画している場合や、MSI コマンドを使用せずにバックグラウンドでインストールを実行することが望ましい場合に適しています。前述の電子メールテンプレートを使用することもできます。その場合、名前を変更したインストーラーをキーコードに含めるようあらかじめ設定されています。

注意: UAC (ユーザーアカウント制御) 環境では、インストーラーの実行に使用するアカウントにローカルの管理者権限が必要です。エンドユーザーに対して UAC プロンプトが表示されないようにするには、UAC 環境で上級権限を持つプロセスからインストーラーを実行する必要があります。

1. エンドポイントで、以下の SecureAnywhere のインストーラーファイルをダウンロードします。

   http://anywhere.webrootcloudav.com/zerol/wsasme.exe

2. インストーラーファイル名の wsasme の部分をキーコードに置き換えます。

   ファイル名は XXXX-XXXX-XXXX-XXXX-XXXX.exe という形式になります。

3. 独自の配備ツールを使用して SecureAnywhere ソフトウェアをエンドポイントにインストールします。

コマンドラインからバックグラウンドでインストールを実行するには

1. エンドポイントで、以下の SecureAnywhere のインストーラーファイルをダウンロードします。

   http://anywhere.webrootcloudav.com/zerol/wsasme.exe

2. 以下の表に記載されているコマンドオプションを使用して、コマンドラインからインストーラーを実行します。他にも利用できるオプションがあります。詳細については、ウェブルート法人向けサポートまでお問い合わせください。

   Windows のコマンドラインオプション

コマンドライン	説明
/key=keycode	指定されたキーコードを使用してインストールします。ハイフンは入力しなくても構いません。 例: `wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx`
/silent	バックグラウンドでインストールします。
/nostart	SecureAnywhere を起動せずにインストールします。

コマンドライン	説明
/lockautouninstall=password	指定したパスワードを使用して SecureAnywhere を自動アンインストールできます。このオプションは、SecureAnywhere をバックグラウンドでアンインストールする必要が生じた場合に適しています。 アンインストールを実行するには、/autouninstall コマンドを使用します。 /lockautouninstall を使用する場合、コントロールパネルの [プログラムの追加と削除] に SecureAnywhere は表示されません。SecureAnywhere を [プログラムの追加と削除] に含めるには、/exeshowaddremove を使用します。
/autouninstall=password	/lockautouninstall に対応するコマンドです。例: wsasme.exe/autouninstall=password デフォルトでは、非管理モードでユーザーがソフトウェアを削除できないようにするため、コントロールパネルの [プログラムの追加と削除] には SecureAnywhere は表示されません。

コマンドライン	説明
-clone	クローン化したマシン / VM に対して使用します。ポータルで表示するマシン ID および PC のホスト名を変更するための、永続的な一意の値をエージェントが PC 上で作成できるようにします。 製品ログでは、管理者が対象の PC を認識できるよう、このフラグが示されます。たとえば、"適用された一意のマシン ID: C8137921" の場合、C8137921 はホスト名 (例: PCHOSTNAME-C8137921) に一致し、InstanceMID と DeviceMID の最初の 8 バイトに対応します。これにより、それぞれが元の ID とは異なる、特定可能な値となります。 この値は、エージェントがアンインストール / 再インストールされた場合に、既存のエージェントが他の ID に移動することがないよう保持されます。OS が再インストールされると、ID は変更されます。 例: `wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone` **注意:** InstanceMID が一致することによりコンソールまたはエンドポイントで重複が発生する場合に使用し、各ポーリング間隔でエンドポイントを置き換えます。

コマンドライン	説明
/exeshowaddremove	SecureAnywhere をコントロールパネルの [プログラムの追加と削除] に表示します。 例: `wsasme.exe /key=xxxx-xxxx-xxxx-xxxx /lockautouninstall=password/exeshowaddremove` **注意:** SecureAnywhere を [プログラムの追加と削除] に表示すると、非管理モードでエンドポイントユーザーがソフトウェアを削除できるようになります。

コマンドライン	説明

/group=groupcode	グループに直接配備するコマンドラインスイッチです。
	
	例:
	
	`wsasme.exe /key=xxxxxxxxx /group=-135260017840748808 /silent`
	
	エンドポイントを特定のグループに割り当てるには、エンドポイントを追加するグループを選択し、[アクション] ドロップダウンメニューで [このグループにエンドポイントを配備] を選択します。GROUPCODE をメモしておきます。
	
	その他の要件:
	
	• グループがコンソールに既に存在している必要があります。
	
	• コンソールで確認されたことのないシステムでの新規インストールについてのみ使用できます。
	
	コマンドラインの例:
	
	`msiexec /i "C:\wsasme.msi" GUILIC="XXXX-XXXX-XXXX-XXXX" CMDLINE="SME,quiet,Group=-135260017840748808" /qn /l*v %windir%\wsa_install_log.txt`
	
	MSI のインストールの場合は、コマンドラインと MSI エディタを使用できます。
	
	MSI エディタの場合の CMDLINE フィールドの例: Group=-135260017840748808

コマンドライン	説明
	プロキシ設定を指定します。 **注意：** エンドポイントがプロキシサーバーを使用して接続する場合、SecureAnywhere は自動的にプロキシ設定を検出します。SecureAnywhere は、エンドポイントの再起動時および 15 分おきにプロキシ設定に対する変更をチェックします。プロキシ設定については自動検出を使用することをお勧めしますが、コマンドラインオプションを使用することも可能です。
-proxyhost=X -proxyport=X -proxyuser=X -proxypass=X -proxyauth=#	プロキシのサポートを有効にするには、以下のコマンドラインオプションを使用します。wsasme.exe -proxyhost=nn.nn.nn.nn -proxyauth=n (where n can be 0=Any, 1=Basic, 2=Digest, 3=Negotiate, 4=NTLM) -proxyuser=proxyuser -proxypass=password -proxyport=port_number -proxyauth には、0 (Any) ではなく別の数値を使用することをお勧めします。Any オプションでは、エンドポイントがすべての認証タイプを検索する必要があります。このため、プロキシサーバー上で不要なエラーや通信の遅延が発生することがあります。 このコマンドラインオプションを使用する場合は、すべてのパラメータを使用し、不要なパラメータについては値を入力せずに二重引用符のみを入力してください (例: proxypass=""

コマンドライン	説明
/lang=LanguageCode	デフォルト言語の検出を許可する代わりに、製品に対して使用する言語を指定します。コードは以下のとおりです。 en - 英語 ja - 日本語 es - スペイン語 fr - フランス語 de - ドイツ語 it - イタリア語 nl - オランダ語 ko - 韓国語 zh-cn - 簡体字中国語 pt - ポルトガル語 (ブラジル) ru - ロシア語 tr - トルコ語 zh-tw - 繁体字中国語 例: `wsasme.exe /key=xxxxxxxxxxxx /silent /lang=ru`

Mac のコマンドライン

コマンドライン	説明
-silent	サイレントモードでインストールされます。 `sudo "/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere" install -keycode=<keycode> -silent`

-proxy_auth=
 	
-proxy_host=
 	
-proxy_port=
 	
-proxy_user=
 	
-proxy_pass=
	認証方式、ホスト、ポート、ユーザー、パスワードを含むプロキシのインストール引数を指定します。
	
	`auth_any_0`
	
	`auth_basic_1`
	
	`auth_digest_2`
	
	`auth_negociate_3`
	
	`auth_ntlm_4`
	
	`open "/Applications/Webroot SecureAnywhere.app" --args install -keycode=<keycode> -proxy_auth=auth_any_0 -proxy_host=<host> -proxy_port=<port> -proxy_user=<user> -proxy_pass=<password>`

-keycode=	インストールでキーコードが要求されません。 open "/Applications/Webroot SecureAnywhere.app" --args install -keycode=<keycode>

コマンドライン	説明
-language=	指定された言語でインストールします。 `open "/Applications/Webroot SecureAnywhere.app" --args install -language=en` **注意:** 言語の一覧は今後追加予定です。
文字列全体	`sudo "/Applications/Webroot SecureAnywhere.app/Contents/MacOS/Webroot SecureAnywhere" install -keycode=XXXX-XXXX-XXXX-XXXX-XXXX -language=en –silent -proxy_auth=auth_basic_1 -proxy_host=proxy.proxy.com -proxy_port=8080 -proxy_user=proxyuser.com -proxy_pass=proxypass`

MSI 配備オプションの使用

Microsoft インストーラー (MSI) を使用したインストールでは、エンドポイントプロテクションのインストールモードをアクティブにするキーコードおよびオプションを適用するために、インストール中にコマンドが必要となります。MSI インストーラーはデフォルトでは対話型であり、バックグラウンドで自動インストールを実行するには、msiexec.exe のオプション "/qn" を必要とします。

MSI コマンドの例:

```
msiexec /i wsasme.msi GUILIC=licensekey CMDLINE=SME,quiet /qn /l*v install.log
```

注意: UAC (ユーザーアカウント制御) 環境では、インストーラーの実行に使用するアカウントにローカルの管理者権限が必要です。エンドポイントのユーザーに対して UAC プロンプトが表示されないようにするには、UAC 環境で上級権限を持つプロセスからインストーラーを実行する必要があります。

後で SecureAnywhere を削除するには

SecureAnywhere ソフトウェアを後でエンドポイントから削除する必要がある場合は、次の標準の MSI コマンドを使用します。

```
msiexec /x wsasme.msi /qn /L*v uninstall.log
```

MSI エディタを使用するには

自分で SecureAnywhere ソフトウェアをエンドポイントに配備する場合は、以下の表のコマンドをインストール中に msiexec.exe に渡すことができます。

コマンド	説明
CMDLINE	SME,quiet
GUILIC	ライセンスキー。ハイフンの入力は必須ではありません。 **注意:** キーコードを入力しなくてもインストールは続行されますが、エンドポイントにキーコードが関連付けられないためエンドポイントは保護されません。キーコードなしでインストールする場合、ソフトウェアをアンインストールしてから再インストールしてキーコードを追加する必要があります。
ARPNOREMOVE	エンドユーザーがアンインストールできないようにします。

ORCA などの MSI エディタを使用して、これらのコマンドを直接変更することもできます。

- [プロパティ] テーブルで CMDLINE のプロパティを適切な値に設定します。
- [プロパティ] テーブルで GUILIC のプロパティを使用するキーコードに設定します。
- [プロパティ] テーブルで ARPNOREMOVE のプロパティを適切な値に設定します。

GPO 配備オプションの使用

GPO を使用して SecureAnywhere をインストールするには、Microsoft の Active Directory および GPO エディタに関する知識が必要です。

また、GPO の使用方法に関するビデオ「How to Deploy Using Group Policy - SecureAnywhere Business」(英語版) も参照してください。

GPO を使用して SecureAnywhere をインストールするには

1. 以下の場所から、SecureAnywhere MSI インストーラーをネットワーク共有にダウンロードします。

   http://anywhere.webrootcloudav.com/zerol/wsasme.msi

   ファイルをダウンロードし、SecureAnywhere を配備するすべてのエンドポイントからアクセスできるようにします。

2. 配備グループのドメインコントローラーとなるサーバーに移動します。
3. ドメインコントローラー上の GPO エディタを開いて、配備グループのポリシーを作成します。
4. グループポリシーを作成する組織単位に属するすべてのエンドポイントに SecureAnywhere を割り当てます。

   グループ内のエンドポイントを再起動すると、SecureAnywhere がインストールされます。

インストーラーのオプション

WSA エージェントには、EXE と MSI の 2 つの形式のインストーラーが用意されており、どちらも WSA コンソールの [リソース] タブにあります。

- **EXE** - EXE ファイル形式は、汎用 EXE ファイル *wsasme.exe* を使用するか、WSA キーコードを使用して名前が変更された EXE ファイルである Windows ダウンロードリンクを実行してダウンロード、インストールすることができます。後者は実行するとインストールプロセスにキーコードを埋め込み、操作のいらないサイレントインストールとして実行されます。
- **MSI** - MSI 形式は、「MSI を使用してインストール」セクションにある wsasme.msi リンクを利用してダウンロードすることができます。MSI は、GUILIC プロパティのキーコードや CMDLINE プロパティのコマンドラインオプションを含むインストールをカスタマイズするために編集することができ、GPO を使用して配備できます。

ターミナル (RDS) サーバーおよび Citrix XenApp へのインストール

ターミナルサーバー (RDS サーバー) あるいはデスクトップ / セッションブローカーまたはホスト共有デスクトップ用 Citrix XenApp にインストールすると、WSA エージェントが、セッション間でカーネルモジュールを共有することにより環境を保護し、それぞれにユーザープロセスを提供します。ウェブルート管理コンソールが、ホストサーバーと各セッションを組み合わせ、レポートおよび管理用に単一のエントリまたはデバイスとして表示します。WSA エージェントは、アプリケーションの仮想化を経由したストリーミングに対応していません。

複製イメージまたは VM へのインストール

Webroot SecureAnywhere Business Endpoint Protection がインストールされると、ホスト名、SID、MAC アドレスなど、さまざまなハードウェアおよびソフトウェアのデータポイントから "マシン ID" が生成されます。エンドポイ

ントイメージが "Sysprep (システム準備)" されることなく再利用される、または VM がマスターイメージからコピーまたはプロビジョニングされ、配備やプロビジョニングの一環として Sysprep されない仮想環境にある場合、エンドポイントは同じ "マシン ID" を使用してコンソールに報告し、同じポジションを奪い合うことになるか、ウェブルート管理コンソール内に複製が生成される可能性があります。

ウェブルート管理コンソールでこの事態が発生した場合、影響を受けたエンドポイントから Webroot SecureAnywhere Business Endpoint Protection をアンインストールしてください。構成ファイルが残らないように %PROGRAMDATA% にある"WRDATA" フォルダを削除するか名前を変更して、コマンドラインオプション "uniquedevice" で再インストールします。

例:

実行可能ファイルを使用した方法

```
"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent –uniquedevice"
```

MSI を使用した方法

CMDLINE	-uniquedevice

これにより、SecureAnywhere がホスト名のチェックサムを取得して "マシン ID" を変更し、システムに対して一意の ID を作成します。これは、マシンの OS やハードウェアがクローンされ、ホスト名が常に異なる場合に便利です。この場合、一意のホスト名により、ウェブルート管理コンソールへの報告用に、デバイスの一意のインスタンスを存在させることが可能になります。ホスト名はそのまま残るため、OS 内で存在するとおりにコンソールに報告されます。

この理由から、まず最初に Sysprep されることなくコピーされるイメージ、またはプロビジョニングに使用されるイメージへの Webroot SecureAnywhere Business Endpoint Protection のインストールは推奨されません。非永続 VM 環境を含むほとんどの仮想環境では、グループポリシーやログオンスクリプトなどを使用して VM を配備してから、Webroot SecureAnywhere Business Endpoint Protection をインストールする必要があります。

配備内でホスト名が一意ではない場合、"clone" インストールスイッチを使用してください。例:

実行可能ファイルを使用した方法

```
"wsasme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent –clone"
```

MSI を使用した方法

CMDLINE	-clone

これによりレジストリキーが作成され、HKLM\System\CurrentControlSet\Control\CloneTimeStampFlags

これを使用して、ポータルで表示するマシン ID および PC のホスト名を変更するための、永続的な一意の値をエージェントが PC 上で作成できるようにします。

スキャンログでは、管理者が対象の PC を認識できるよう、次のようなフラグが示されます。

"適用された一意のマシン ID: C8137921"

C8137921 はウェブルート管理コンソールに報告されたホスト名に一致します (例: PCHOSTNAME-C8137921 など)。この値は、エージェントがアンインストール / 再インストールされた場合に、既存のエージェントが他の ID に移動することがないよう保持されます。OS が再インストールされると、ID は変更されます。

Citrix 環境内での配備方法に関する詳細については、次のドキュメントを参照してください。

http://download.webroot.com/Citrix/Citrix.pdf

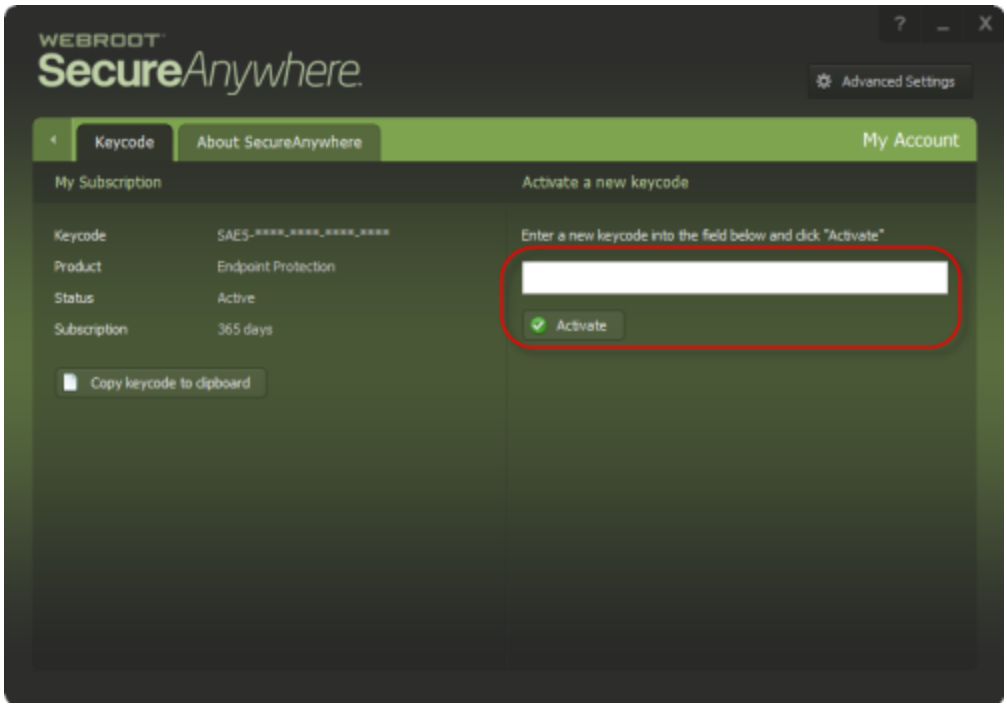
エンドポイントキーコードの変更

管理ポータルへの報告を行うには、エンドポイントでエンドポイントプロテクションのキーコードを使用している必要があります。ネットワーク内のエンドポイントに、SecureAnywhere の消費者向けバージョンなど、異なる種類のキーコードを利用して SecureAnywhere がすでにインストールされている場合は、新しいキーコードをエンドポイントから直接アクティブ化してキーコードを変更します。詳細については、以下の手順を参照してください。

キーコードを変更するコマンドの発行方法の詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

エンドポイントのキーコードを変更するには

1. エンドポイントから、システムトレイの**ウェブルート**のアイコンをダブルクリックして SecureAnywhere を開きます。
2. **マイアカウント**の歯車のアイコンをクリックします。
3. [新しいキーコードのアクティブ化] フィールドでキーコードを入力します。
4. [**アクティブ化**] ボタンをクリックします。

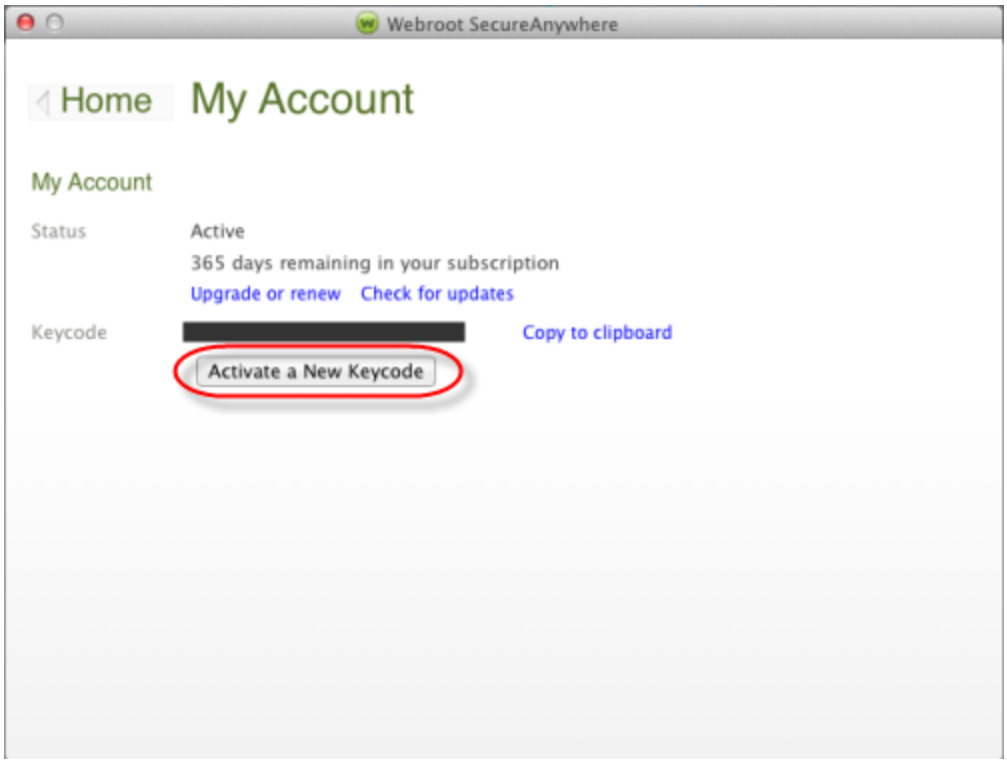


新しいキーコードを入力すると、SecureAnywhere がスキャンを開始します。システムで自動的にスキャンが開始されない場合は、[PC セキュリティ] タブの [**コンピュータをスキャン**] をクリックします。スキャンが完了すると、SecureAnywhere は管理ポータルへの報告を行います。

Mac のエンドポイントキーコードを変更するには

1. エンドポイントから、メニューバーの**ウェブルート**のアイコンをクリックし、続けてドロップダウンメニューで [**Webroot SecureAnywhere を開く**] を選択します。
2. メインウィンドウで [**マイアカウント**] を選択します。

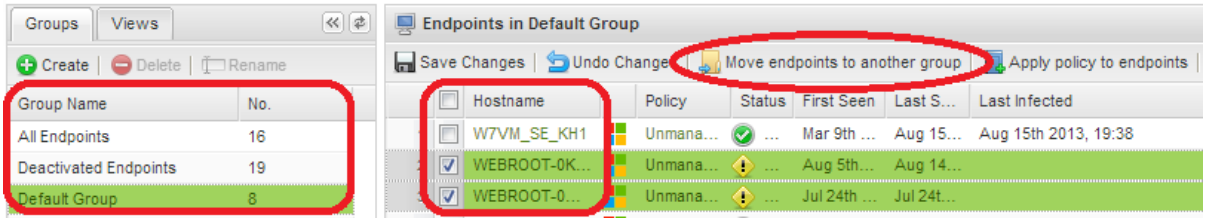
3. [マイアカウント] ウィンドウで [**新しいキーコードのアクティブ化**] ボタンをクリックします。



4. ダイアログでエンドポイントプロテクションのキーコードを入力し、[**アクティブ化**] ボタンをクリックします。

   新しいキーコードがアクティブ化されたら管理ポータルに戻り、デフォルトのグループで新しいエンドポイントを探します。

   必要に応じて、別のグループにエンドポイントを再割り当てします。詳細については、「*グループ間でのエンドポイントの移動 ページ328*」を参照してください。



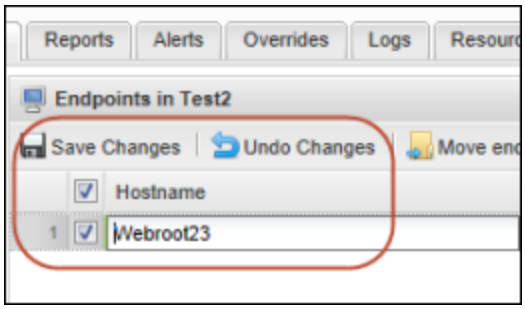
エンドポイントの名前の変更

エンドポイントを追加する際、SecureAnywhere は、管理ポータルでそのエンドポイントを識別するためにマシンの名前を使用します。このため、"*Winchester-Laptop*" や "*LabTest-1*" など、分かりやすい名前に変更することをお勧めします。

注意: 仮想マシンでは、エンドポイントの名前を変更しないでください。名前を変更すると、管理ポータルに新しいエンドポイントとして表示され、不要なライセンスのシートが使用されます。

エンドポイントの名前を変更するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、名前を変更するエンドポイントを含むグループを選択します。
3. 右側の [エンドポイント] パネルで、エンドポイントの名前をダブルクリックします。



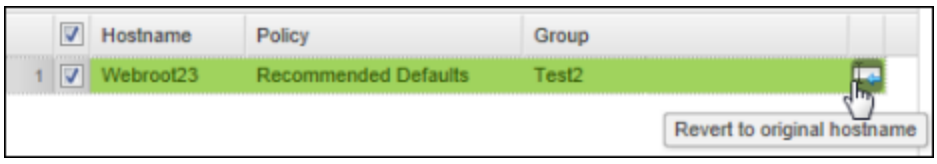
4. 新しい名前を入力して **Enter** キーを押します。

   フィールドの左上に赤いフラグが付き、変更がまだ保存されていないことを示します。

5. コマンドバーの [**変更を保存**] ボタンをクリックします。

   [ホスト名] カラムに新しい名前が表示されます。

6. 元の名前に戻す場合は、行の右端にある [**戻す**] ボタンをクリックします。



エンドポイントの検索

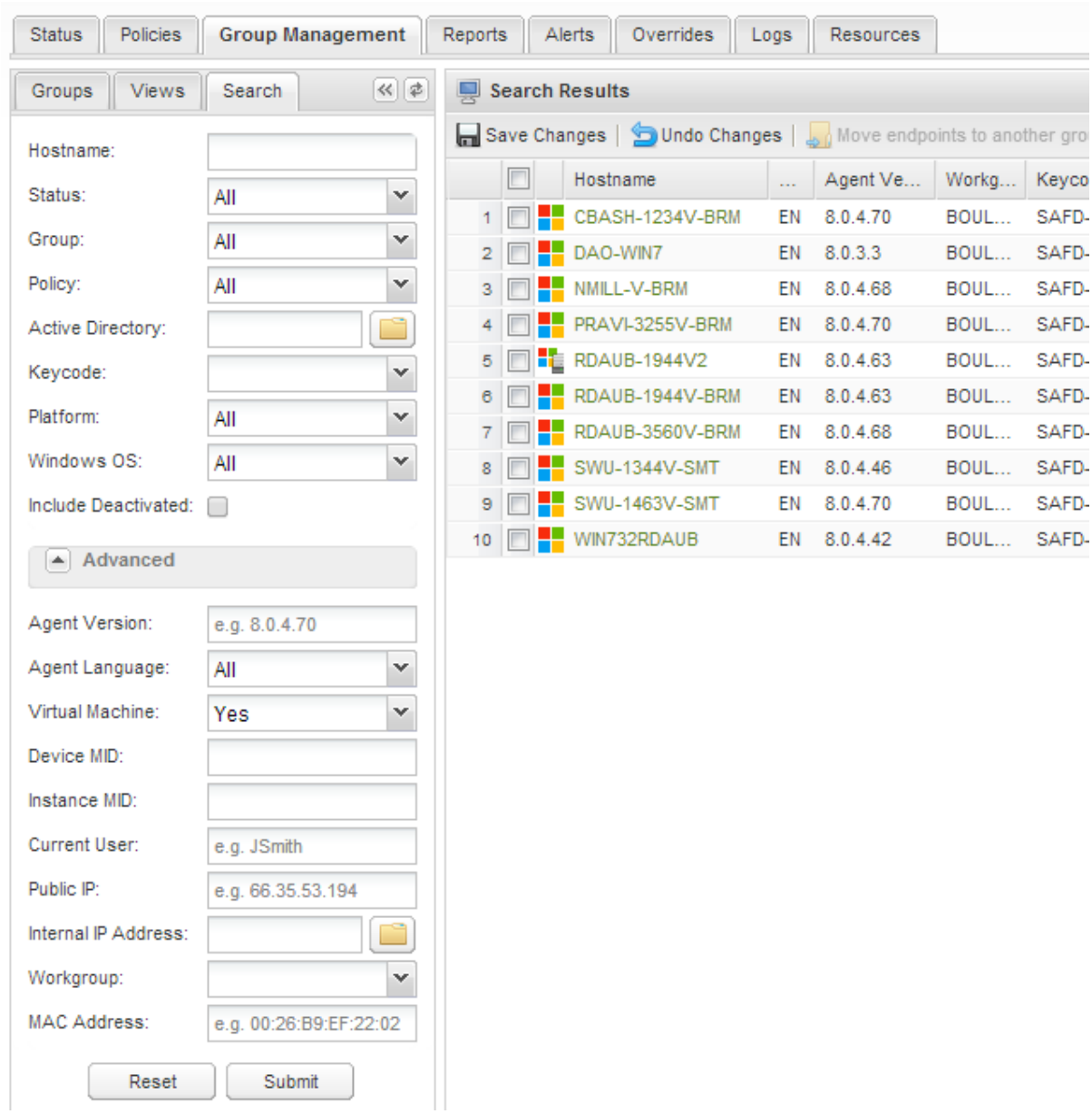
ダイナミックでフレキシブルな検索機能を使用して、単一または複数のエンドポイントを検索することができます。また、高度な検索オプションも利用できます。

各フィールドまたはドロップダウンメニューでは、あらゆる条件を組み合わせて対象を絞り込むことができます。たとえば、状態のタイプとポリシーのタイプを検索する場合は、これら 2 つのフィールドのみを使用します。さらにフィルタリング機能を使用するには、追加情報を入力します。

エンドポイントを検索するには

1. [エンドポイントプロテクション] パネルで [**グループの管理**] タブをクリックします。
2. [**検索**] タブをクリックします。

   [検索] パネルが表示されます。



3. [ホスト名] フィールドにホスト名を入力します。

   このフィールドには自由形式でテキストを入力でき、大文字と小文字は区別されません。

4. [状態] ドロップダウンメニューで以下のいずれかを選択します。

   - **保護**

- **感染あり**
- **期限切れ**
- **感染および期限切れ**
- **最近確認されていません**

5. [グループ] ドロップダウンメニューで、検索するグループを選択します。
6. [ポリシー] ドロップダウンメニューで、検索するポリシーを選択します。
7. [アクティブディレクトリ] フィールドで、以下のいずれかの操作を行います。

   - Active Directory 名を入力する。

   - Active Directory の場所を参照する。

8. [キーコード] ドロップダウンメニューで、検索するキーコードを選択します。
9. [プラットフォーム] ドロップダウンメニューで、検索するプラットフォームを選択します。
10. [Windows OS] ドロップダウンメニューで、以下のいずれかの OS を選択します。

    - **Windows XP**
    - **Windows Vista**
    - **Windows 7**
    - **Windows 8**
    - **Windows Server**
    - **MacOS**
    - **その他**

11. 以下のいずれかの操作を行います。

    - 非アクティブ化されたエンドポイントを含める場合は、[**非アクティブ化されたエンドポイントを含む**] チェックボックスを選択する。

    - 非アクティブ化されたエンドポイントを含めない場合は、[**非アクティブ化されたエンドポイントを含む**] チェックボックスの選択を解除する。

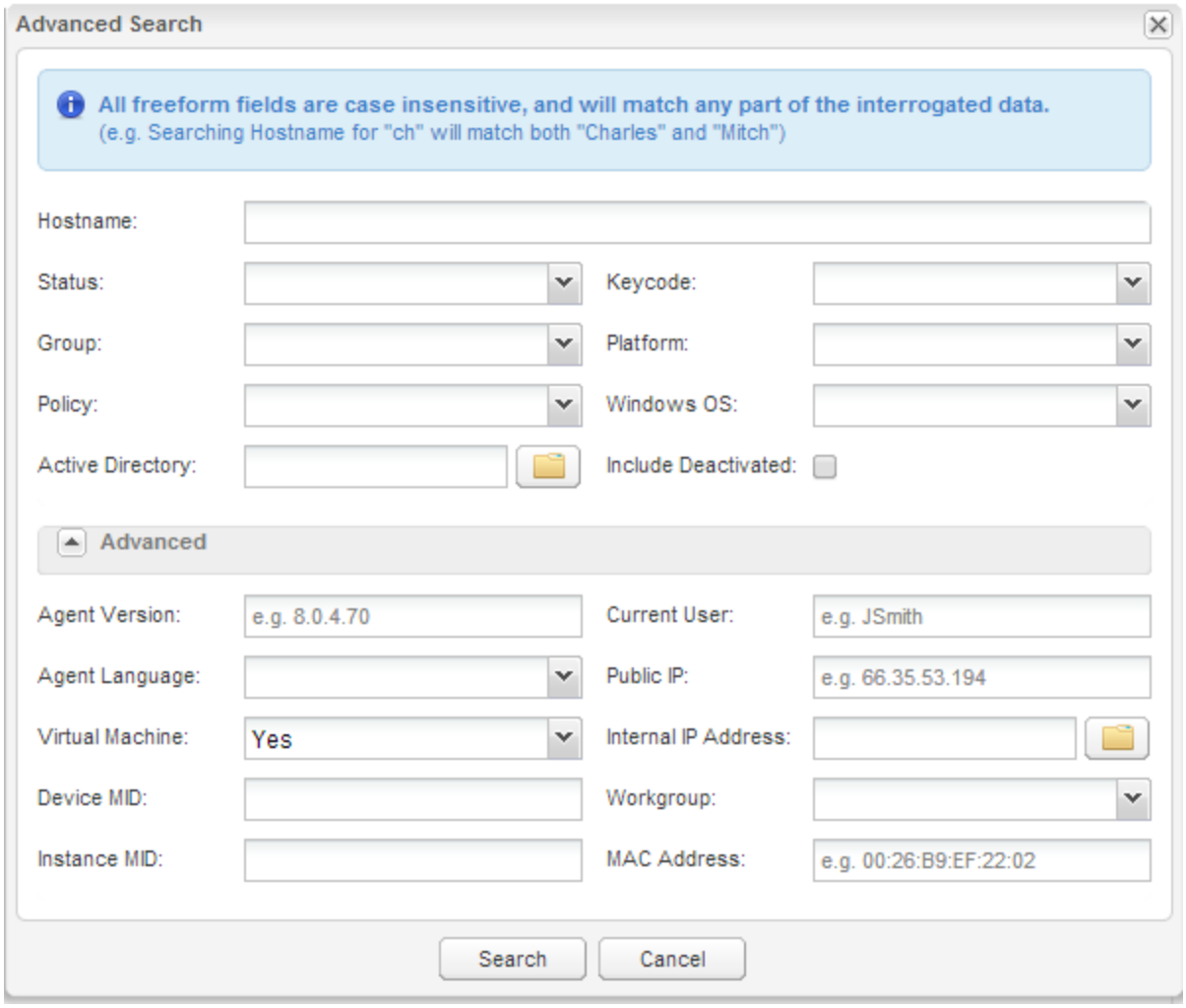
12. 設定が完了したら、[**送信**] ボタンをクリックして結果を絞り込みます。

    管理ポータルの右のパネルに、検索条件に一致するすべてのエンドポイントが表示されます。

高度な検索を実行するには

1. [エンドポイントプロテクション] パネルで、パネル右上にある [**高度な検索**] ボタンをクリックします。

   [高度な検索] パネルが表示されます。



2. [エージェントのバージョン] フィールドにエージェントの番号を入力します。

   これは自由形式のフィールドです。

3. [エージェントの言語] ドロップダウンメニューで、あらかじめ設定されたサポートされている言語のリストから選択します。

4. [VM] ドロップダウンメニューで、以下のいずれかを選択します。

   - **はい** - デフォルトです。
   - **いいえ**

5. [デバイス MID] フィールドに、デバイスのウェブルートベースの一意の識別子を入力します。

   これは自由形式のフィールドです。

6. [インスタンス MID] フィールドに、インスタンスのウェブルートベースの識別子を入力します。

   これは自由形式のフィールドです。

7. [現在のユーザー] フィールドに現在のユーザー名を入力します。

   これは自由形式のフィールドです。

8. [パブリック IP アドレス] フィールドにパブリック IP アドレスを入力します。

   これは自由形式のフィールドです。

9. [ローカル IP アドレス] フィールドにローカル IP アドレスを入力します。

   これは自由形式のフィールドです。

10. [ワークグループ] ドロップダウンメニューで、あらかじめ設定された利用可能なワークグループのリストから選択します。
11. [MAC アドレス] フィールドに MAC アドレスを入力します。

    これは自由形式のフィールドです。

12. 設定が完了したら、[**送信**] ボタンをクリックして結果を絞り込みます。

    管理ポータルの右のパネルに、検索条件に一致するすべてのエンドポイントが表示されます。

エンドポイントへのコマンドの発行

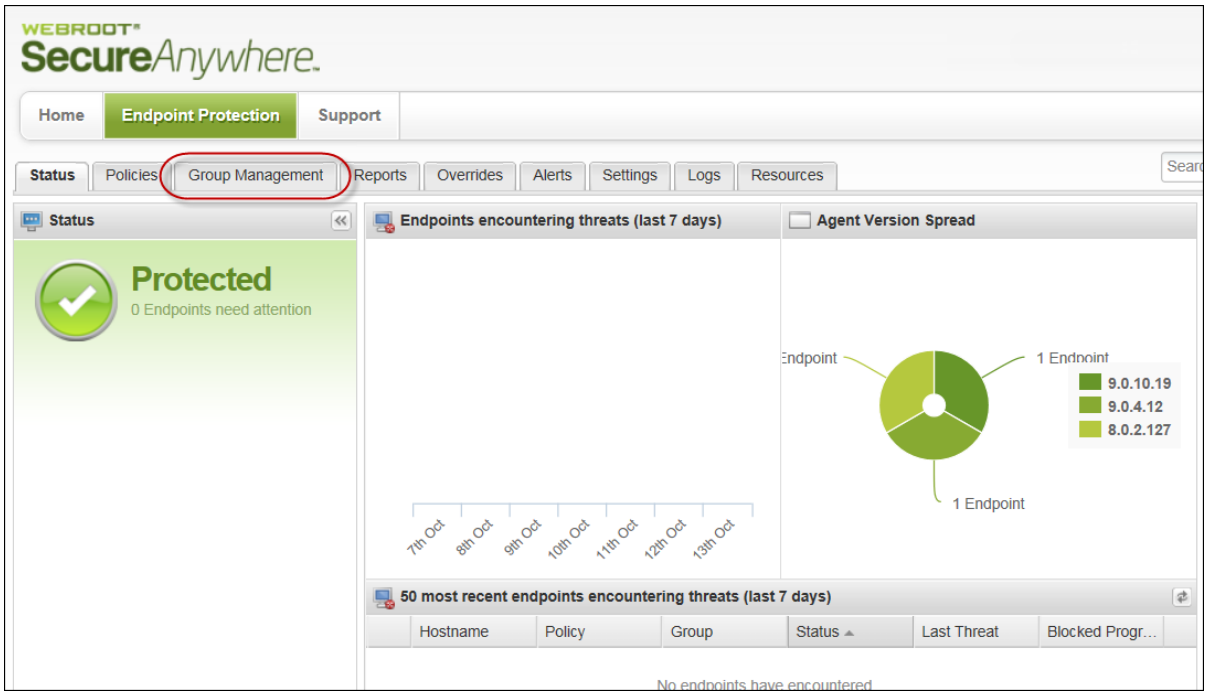
管理ポータルでは、個々のエンドポイントまたはエンドポイントのグループに対してコマンドを発行することが可能です。たとえば、遠隔地のエンドポイントをスキャンすることができます。ここで紹介するコマンドを使用すると、エンドポイントの SecureAnywhere ソフトウェア上で利用できるものと同じコマンドを簡単に実行することができます。

ただし、エンドポイントは次回のポーリング間隔までコマンドを受信できないことに注意してください。必要に応じて、関連するポリシーでポーリング間隔を変更するか、即時のポーリングを強制することができます。詳細については、「*ポリシー設定の変更 ページ247*」または「*即時のアップデートの強制実行 ページ180*」を参照してください。

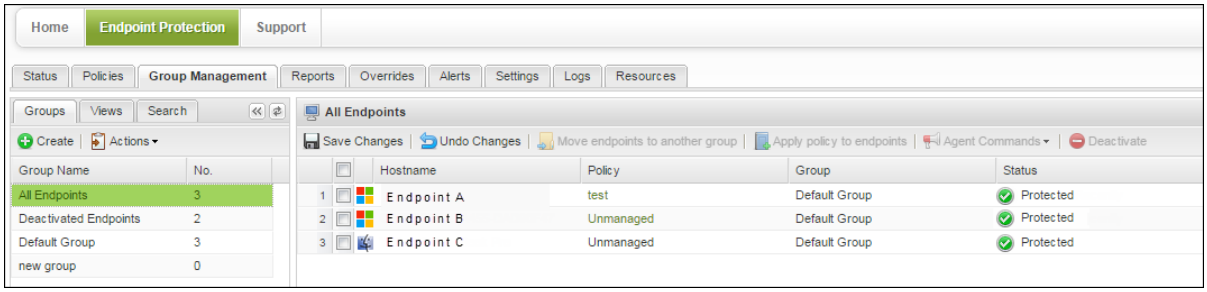
注意: コマンドに対するアクセス権限 (シンプル、アドバンスト、またはエキスパート) によっては、このセクションで紹介するコマンドの一部が表示されない場合があります。管理者は、アクセス権限を変更することができます。詳細については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

エンドポイントにコマンドを発行するには

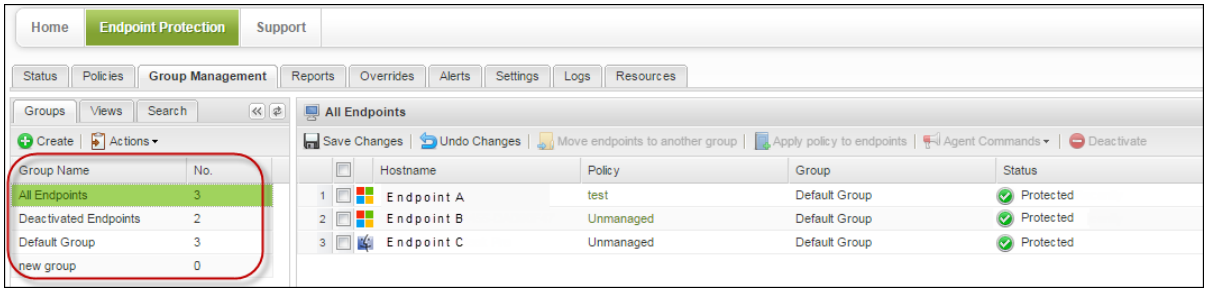
1. エンドポイントのコンソールで [**グループの管理**] タブをクリックします。



[グループの管理] タブが表示されます。

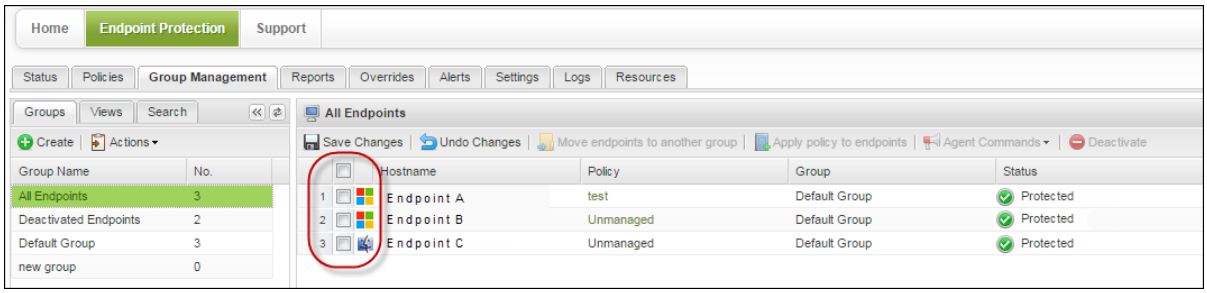


2. [**グループ**] カラムで、コマンドを発行するエンドポイントが含まれるグループを選択します。

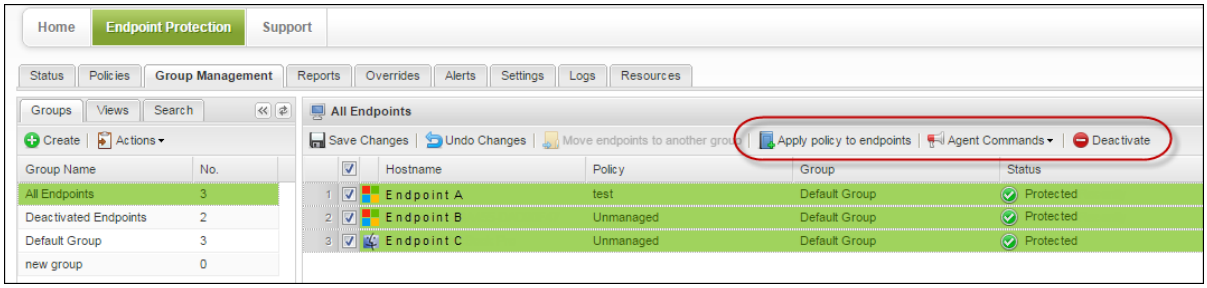


3. [**エンドポイント**] パネルで次のいずれかを実行して、エンドポイントの情報を表示します。

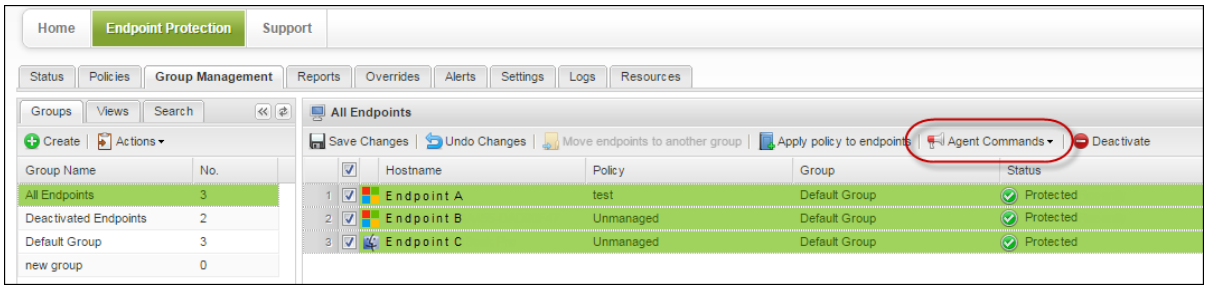
- 1 つのエンドポイントの横にあるチェックボックスを選択します。
- **チェックボックス**のカラムの一番上にあるチェックボックスを選択します。



1 つまたは複数のチェックボックスを選択すると、コマンドバーの追加コマンドがアクティブになり、使用できる状態になります。

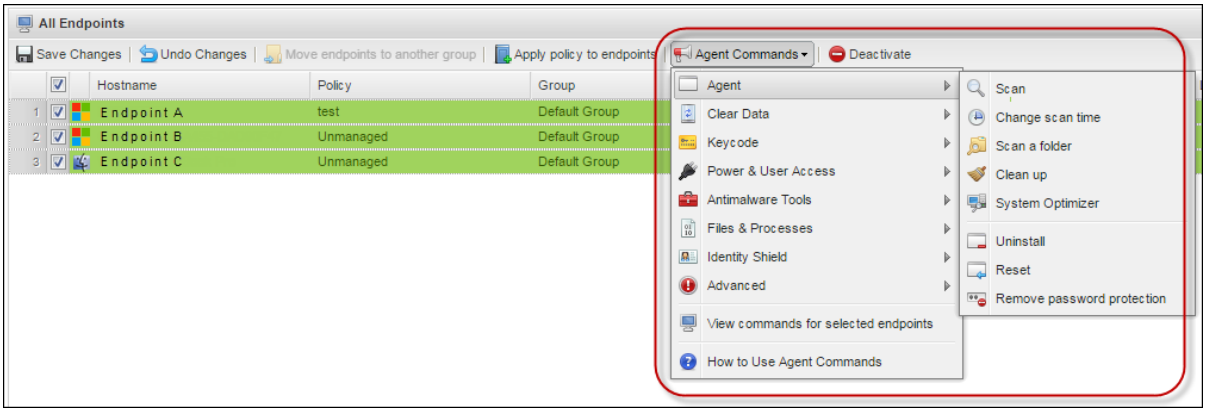


4. コマンドバーで、[**エージェントコマンド**] の下向きの矢印をクリックします。

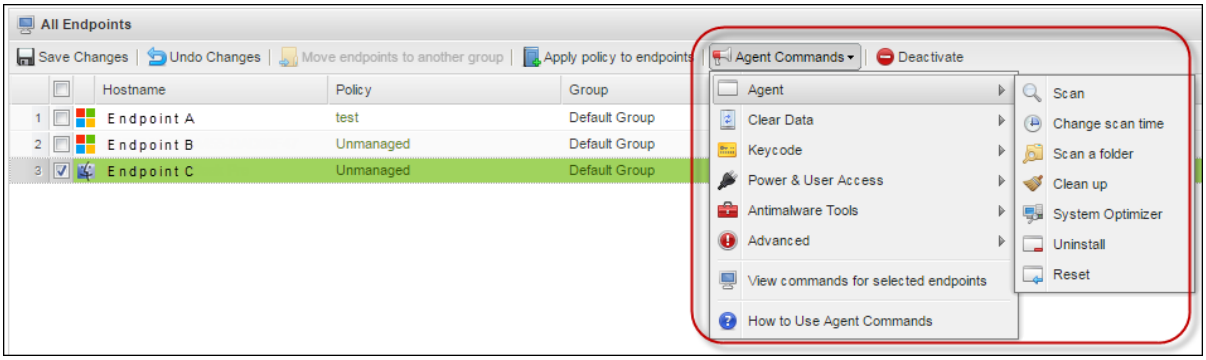


選択した項目に応じた [エージェントコマンド] メニューが表示されます。

- PC エンドポイント、または PC と Mac エンドポイントの組み合わせを選択した場合、表示される [エージェントコマンド] メニューは次のとおりです。



- Mac エンドポイントのみを選択した場合、次のような [エージェントコマンド] メニューが表示されます。ID シールドコマンドやパスワード保護を削除するためのオプションは含まれません。



5. エージェントコマンドのカテゴリーを選択し、展開されるメニューから実行するコマンドを選択します。

   各コマンドの説明については、以下の表を参照してください。

コマンド	説明
エージェントコマンド	
スキャン	エンドポイントがコマンドを受信した後、ただちにバックグラウンドでディープスキャンを実行します。 スキャンが完了すると[スキャン履歴]パネルが開き、ディープスキャンの結果が表示されます。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。 **注意:** 検出された脅威は自動的に隔離されません。ポータルで、クリーンアップの実行またはオーバーライドの作成のいずれかの操作を実行する必要があります。

コマンド	説明
スキャン時間を変更	エンドポイントをスキャンする新しい時間を選択します。 デフォルトでは、SecureAnywhere はインストールされた時刻とほぼ同じ時刻に毎日スキャンを実行します。たとえば、SecureAnywhere をエンドポイントに正午にインストールしたとすると、スキャンは常に正午 12 時頃に始まります。このコマンドを使用すると、この時刻を別の時刻に変更できます。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。

フォルダをスキャン	指定のフォルダ内の全ファイルに対してフルスキャンを実行します。フォルダの完全なパス名を入力してください。
	
	Windows システムでは次のように入力します。
	
	`C:\Documents and Settings\Administrator\My Documents`
	
	Mac システムでは次のように入力します。
	
	`/Applications`
	
	このコマンドは PC および Mac 両方のエンドポイントで実行できます。

コマンド	説明
クリーンアップ	スキャンを開始して、悪意のあるファイルを自動的に隔離します。 スキャンが完了すると [スキャン履歴] パネルが開き、[クリーンアップ後のスキャン] の結果が表示されます。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
システム最適化ツール	システム最適化ツールをエンドポイントで実行します。このツールは、ウェブ閲覧履歴、ユーザーアクティビティを記録するファイル、ごみ箱内のファイルや Windows の一時ファイルなど貴重なディスク容量を消費するファイルの痕跡をすべて削除します。 システム最適化ツールのオプションは、ポリシー設定で変更することができます。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。

コマンド	説明
アンインストール	SecureAnywhere をエンドポイントからアンインストールします。 このコマンドを使用しても、エンドポイントは管理ポータルに表示されたままとなります。 SecureAnywhere をアンインストールしてライセンスのシートを解放するには、エンドポイントを非アクティブ化します。詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
リセット	エンドポイントでの SecureAnywhere の設定をデフォルト値に戻します。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
パスワード保護を削除	エンドポイントのユーザーによる制御でパスワードの保護を無効にします。これにより、管理者はロックアウトされてもエンドポイントにアクセスすることができます。 このコマンドは PC エンドポイントでのみ実行できます。
Showgui	ポリシーで許可されている場合に UI を表示します。 例: "c:\program files\webroot\wrsa.exe" –showgui `This command runs only on PC endpoints.`

コマンド	説明

Silentscan	サイレントモードでスキャンを開始します。スキャン用 UI はユーザーには表示されませんが、トレイアイコンにカーソルを合わせると表示されます。
	
	コマンドの例:
	
	`WRSA.exe -silentscan="c:\foldername"`
	
	フォルダをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop"`
	
	ファイルをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop\eicar.com"`
	
	このコマンドは PC エンドポイントでのみ実行できます。

データ消去コマンド	
ファイルを消去	現在のログファイルを消去して、エンドポイントの領域を解放します。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。

コマンド	説明
プロキシ設定を無効化	エンドポイントのユーザーがエンドポイント上で設定したプロキシ設定を無効にします。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。 **注意:** プロキシサーバーを経由するほかにインターネットへのアクセス方法を持たないエンドポイントに対しては、このコマンドを使用しないでください。使用すると、そのエンドポイントはクラウドと通信できなくなります。
キーコードコマンド	
キーコードを変更	別のキーコードを入力します。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。 **注意:** ドロップダウンリストには、このコンソールに割り当てられているキーコードのみが表示されます。

コマンド	説明
キーコードを一時的に変更	このエンドポイントで使用するキーコードを一時的に切り替えます。これは、テストなどの場合に必要になることがあります。 ダイアログボックスでドロップダウンリストからキーコードを選択し、SecureAnywhere で使用する日付を指定します。指定した変更日が終了すると、キーコードは元のキーコードに戻ります。 このコマンドは PC エンドポイントでのみ実行できます。
電源およびユーザーアクセスコマンド	
エンドポイントをロック	ログイン画面を起動して、このエンドポイントをロックします。再びログインする際は、ユーザー名とパスワードを入力する必要があります。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
ログオフ	アカウントからユーザーをログオフします。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
再起動	報告時にこのエンドポイントを再起動します。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。

コマンド	説明
[セーフモードとネットワーク] で再起動する	[セーフモードとネットワーク] でこのエンドポイントを再起動します。 このコマンドは PC エンドポイントでのみ実行できます。
シャットダウン	報告時にこのエンドポイントをシャットダウンします。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
マルウェア対策ツールコマンド	
デスクトップの壁紙をリセット	デスクトップの壁紙をデフォルト設定にリセットします。これは、エンドポイントが最近マルウェアに感染して、壁紙が変更された場合に必要となることがあります。 このコマンドを送信した後、PC エンドポイントを再起動する必要があります。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。
スクリーンセーバーをリセット	スクリーンセーバーをデフォルト設定にリセットします。これは、エンドポイントが最近マルウェアに感染して、スクリーンセーバーが変更された場合に必要となることがあります。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。

コマンド	説明
システムポリシーをリセット	Windows システムポリシーをデフォルト設定にリセットします。これは、エンドポイントが最近マルウェアに感染し、タスクマネージャー設定などのポリシーが変更された場合に必要となることがあります。 このコマンドは PC エンドポイントでのみ実行できます。 **注意:** このコマンドは、エンドポイントプロテクションのポリシーではなく、Windows のポリシーをリセットします。
ファイルを復元	MD5 値を使用して、隔離されたファイルを元の場所に復元します。 ファイルの MD5 値を確認する方法の詳細については、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。 このコマンドは PC エンドポイントでのみ実行できます。
ファイルおよびプロセスコマンド	
すべてのファイルとプロセスを再検証する	次回のスキャン時に、このファイルの分類を再検証します。 このコマンドは、設定したオーバーライドをエンドポイントで有効にする必要がある場合に便利です。 このコマンドは PC エンドポイントでのみ実行できます。

コマンド	説明
すべてのアイテムを正当と評価	このエンドポイントで検出されたすべてのファイルを安全に実行可能とみなします。 このコマンドは、エンドポイントで数多くの誤検出が確認され、それらに素早く"正当"とタグ付けする必要がある場合に便利です。 このコマンドは PC エンドポイントでのみ実行できます。
ファイアウォールによりブロックされたプロセスを許可	ファイアウォールの設定によりブロックされたすべてのプロセスについて通信を許可します。 このコマンドは PC エンドポイントでのみ実行できます。
信頼できないプロセスの強制終了	信頼できないプロセスを停止します。これは、マルウェアプログラムの痕跡を通常のスキャンで完全に削除できなかった場合に必要となることがあります。 プロセスはただちに停止されますが、再実行を防止することはできません。 このコマンドは PC エンドポイントでのみ実行できます。
ID シールドコマンド	

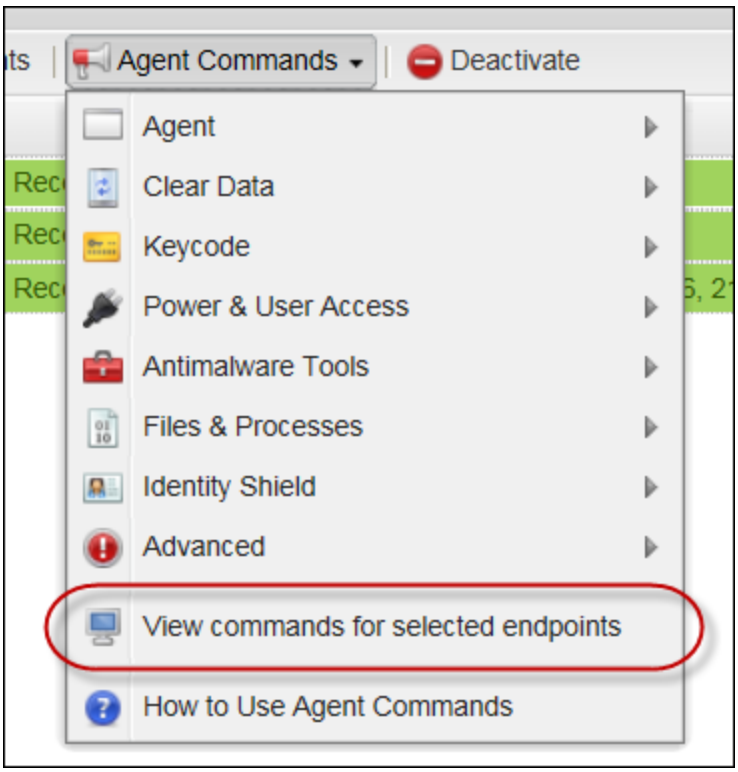
コマンド	説明
アプリケーションを許可	エンドポイントでのアプリケーションの実行を許可します。 • アプリケーションを特定するには、その MD5 値を入力する必要があります。 • MD5 値を確認するには、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。 このコマンドは PC エンドポイントでのみ実行できます。
アプリケーションを拒否	エンドポイントでのアプリケーションの実行をブロックします。 • アプリケーションを特定するには、その MD5 値を入力する必要があります。 • MD5 値を確認するには、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。 このコマンドは PC エンドポイントでのみ実行できます。
拒否されているすべてのアプリケーションを許可	ブロックされたすべてのアプリケーションをリセットして、エンドポイントで実行できるようにします。 このコマンドは PC エンドポイントでのみ実行できます。

コマンド	説明
アプリケーションを保護	エンドポイントで実行されているアプリケーションにセキュリティを追加します。 • アプリケーションを特定するには、その MD5 値を入力する必要があります。 • MD5 値を確認するには、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。 このコマンドは PC エンドポイントでのみ実行できます。
アプリケーションの保護を解除	以前に [アプリケーションを保護] コマンドを使用してセキュリティを追加した場合に、アプリケーションを標準の保護にリセットします。 • アプリケーションを特定するには、その MD5 値を入力する必要があります。 • MD5 値を確認するには、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。 このコマンドは PC エンドポイントでのみ実行できます。
高度なコマンド	

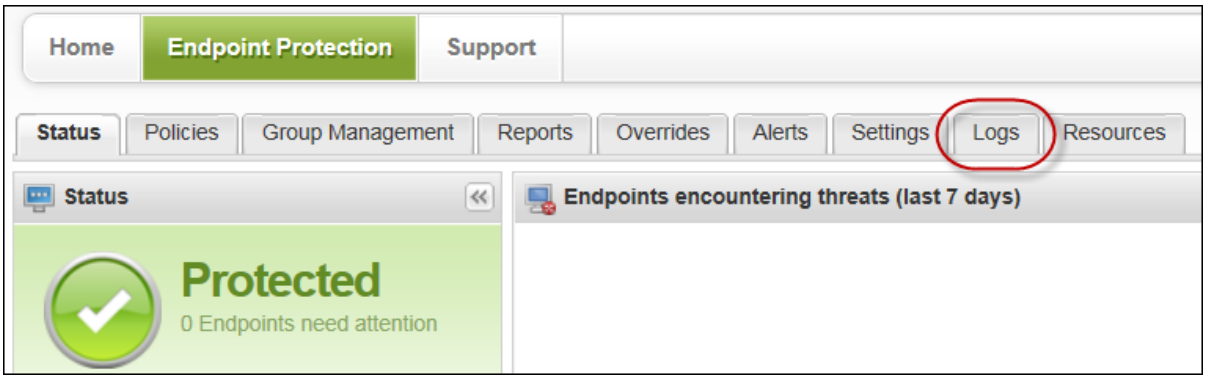
コマンド	説明
カスタマーサポートスクリプトを実行	実行可能ファイルをエージェントにダウンロードする際の URL を指定して、リモートで実行します。 このコマンドは PC エンドポイントでのみ実行できます。
カスタマーサポートの診断	WSABLogs ユーティリティを実行して、感染したエンドポイントに関する情報を収集します。 [カスタマーサポートの診断] ダイアログには、ユーティリティの実行可能ファイルの場所と、エンドポイントアカウントに関連付けられている電子メールアドレスが表示されます。 [送信] をクリックするとユーティリティが実行され、結果がウェブルート法人向けサポートに送信されます。 また、オプションの詳細設定を指定すると、追加のファイルを送信したり、ログを送信する代わりにローカルに保存したり、メモリダンプを収集したりできます。 このコマンドは PC および Mac 両方のエンドポイントで実行できます。 **注意:** オプションの設定は Mac には適用されないため、Mac には必要ありません。

6. 必要に応じて、以下のいずれかを実行します。

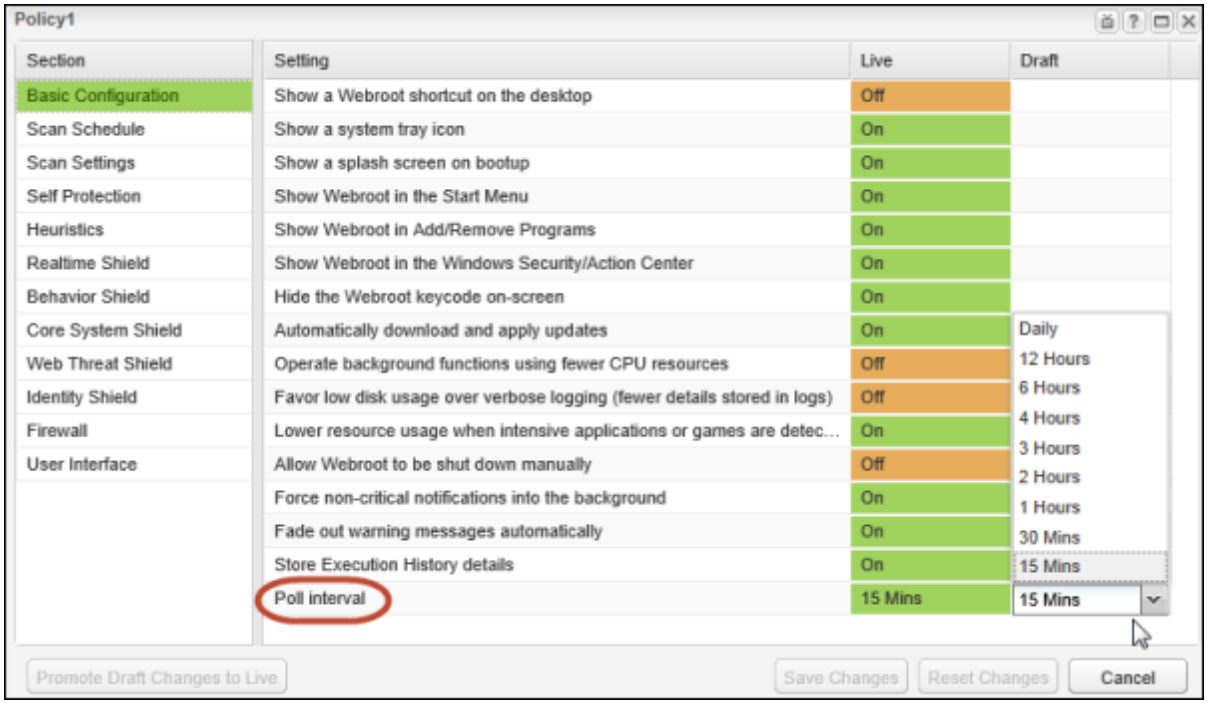
   - 送信したコマンドの状態を表示するには、[エージェントコマンド] メニューで [**選択したエンドポイントのコマンドを表示**] を選択します。



- コマンドログを確認するには、メインのエンドポイントプロテクションのコンソールで [**ログ**] タブをクリックします。詳細については、「*コマンドログの表示 ページ520*」を参照してください。



次回のポーリング間隔で、エンドポイントプロテクションが Windows コンピュータに対してコマンドを発行します。必要に応じて、グループのポリシーの [基本設定] でポーリング間隔を変更したり、「*即時のアップデートの強制実行 ページ180*」の説明に従って即時の変更を強制したりできます。


Policy1
Section
Setting
Live
Draft
Basic Configuration
Scan Schedule
Scan Settings
Self Protection
Heuristics
Realtime Shield
Behavior Shield
Core System Shield
Web Threat Shield
Identity Shield
Firewall
User Interface
Show a Webroot shortcut on the desktop
Show a system tray icon
Show a splash screen on bootup
Show Webroot in the Start Menu
Show Webroot in Add/Remove Programs
Show Webroot in the Windows Security/Action Center
Hide the Webroot keycode on-screen
Automatically download and apply updates
Operate background functions using fewer CPU resources
Favor low disk usage over verbose logging (fewer details stored in logs)
Lower resource usage when intensive applications or games are detec...
Allow Webroot to be shut down manually
Force non-critical notifications into the background
Fade out warning messages automatically
Store Execution History details
Poll interval
Off
On
On
On
On
On
On
On
Off
Off
On
Off
On
On
On
15 Mins
Daily
12 Hours
6 Hours
4 Hours
3 Hours
2 Hours
1 Hours
30 Mins
15 Mins
15 Mins
Promote Draft Changes to Live
Save Changes
Reset Changes
Cancel

エンドポイントのアップデートとその他の変更の管理

このセクションでは、エンドポイントのハードウェアや OS を変更する際に発生する可能性のある、いくつかの特殊な状況について説明しています。

新しい OS への移行

エンドポイントに新しい OS をインストールすると、その変更によって管理ポータル内にエンドポイントのエントリの複製が作成されます。新しい OS をインストールする前に、エンドポイントを非アクティブ化してください。詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。

OS をインストール済みの場合は、管理ポータルで最も古いエントリを非アクティブ化してください。余分なライセンスは削除され、エンドポイントの複製は [非アクティブ化されたエンドポイント] のグループに追加されます。

注意: ほとんどの場合、OS をアップグレードするだけではエントリの複製が作成されることはありません。

エンドポイントのハードウェアの変更

エンドポイントに新しいハードドライブを取り付け、SecureAnywhere を再インストールすると、管理ポータルでは新しいエントリとして表示されます。ハードドライブを交換する前に、余分なライセンスの使用を避けるため、まず管理ポータルでエンドポイントを非アクティブ化してください。詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。

その他のタイプのハードウェアをエンドポイントで変更する場合 (新しいマザーボードやプロセッサ、ネットワークアダプタを取り付ける場合など)、アップグレードされたコンピュータが管理ポータルで新しいエントリとして表示されることはありません。その場合は最初にエンドポイントを非アクティブ化にする必要はありません。

新しいサブネットへのエンドポイントの移動

エンドポイントを新しいサブネットへ移動する際は、それまでのサブネットと同じ通信回線を使用できるようにします。以下のドメインをファイアウォールで許可する必要があります。

*.webrootcloudav.com

*.webroot.com

*.s3.amazonaws.com

WSAWebFilteringPortal.elasticbeanstalk.com

*.webrootanywhere.com

ファイアウォールを介した通信

ファイアウォールがある場合、以下の表に記載されたウェブルートのパスマスクを許可してください。

ファイアウォールの詳細については、「セットアップの準備 ページ5」を参照してください。

パス	詳細
***.webrootcloudav.com**	エージェントの通信とアップデート。 **注意:** 一部のファイアウォールでは、単一のワイルドカードマスクを使用したダブルドットを含むサブドメイン名 (例: 「g1.p4.webrootcloudav.com」を「*.webrootcloudav.com」で表示) をサポートしていません。このため、一部の環境では「*.p4.webrootcloudav.com」または「*.*.webrootcloudav.com」のいずれかにしなければならないことがあります。
***.webroot.com**	エージェントのメッセージ送受信。
***.s3.amazonaws.com**	エージェントのファイルのダウンロードとアップロード。

パス	詳細
WSAWebFilteringPortal.elasticbeanstalk.com	エージェントの Web フィルタリングに必要。 elasticbeanstalk は Amazon の AWS ドメイン。
***.webrootanywhere.com**	管理ポータルとサポートチケットログのアップロード。

エンドポイントでの SecureAnywhere の使用

状況により、設定変更のため SecureAnywhere インターフェイスからエンドポイントにアクセスする必要が生じる場合があります。これは、エンドポイントを非管理ポリシーに割り当てている場合など、管理ポータルからは制御できない場合に必要となることがあります。

このトピックでは、次の手順と情報を紹介します。

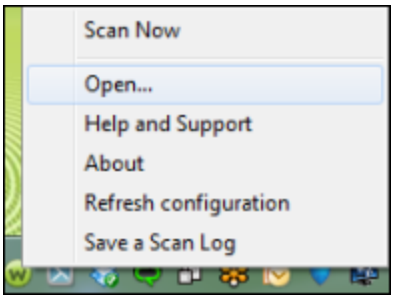
- Windows コンピュータで SecureAnywhere を開く
- Mac コンピュータで SecureAnywhere を開く
- Mac の [Webroot SecureAnywhere] メニュー
- Mac の [システムツール] ドロップダウンメニュー

注意: エンドポイントで SecureAnywhere インターフェイスを使用する手順の詳細については、Webroot SecureAnywhere の PC ユーザーガイドを参照してください。Mac コンピュータをお使いの場合は、SecureAnywhere の Mac ユーザーガイドを参照してください。

Windows コンピュータで SecureAnywhere を開く

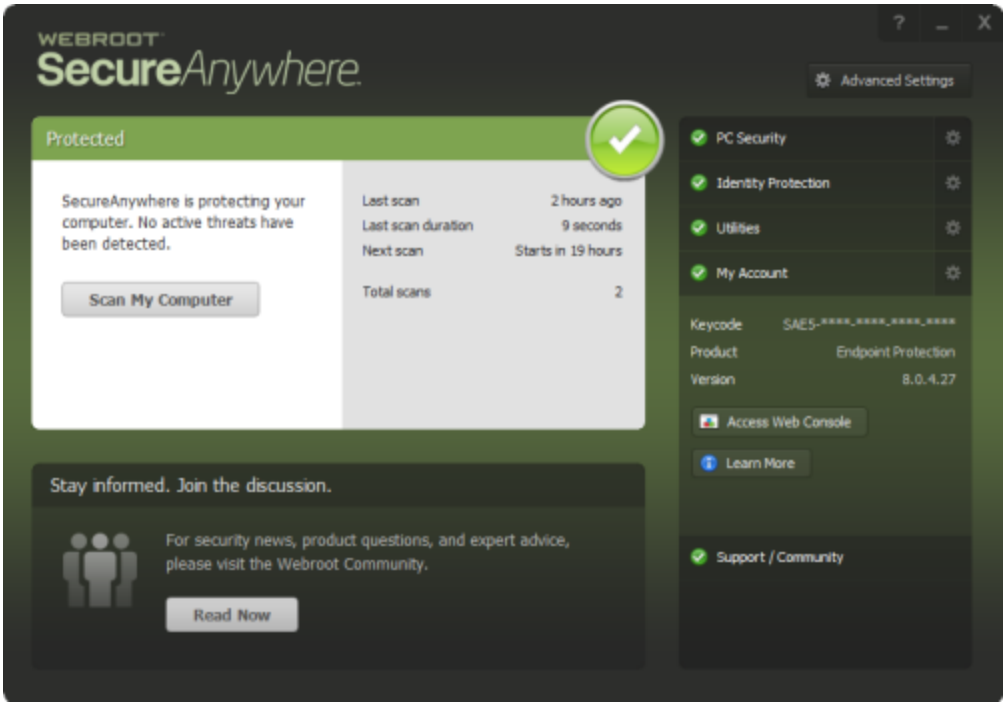
Windows コンピュータで SecureAnywhere のメインインターフェイスを開くには

1. エンドポイントで次のいずれかの操作を行います。
   - デスクトップにある**ウェブルート**のショートカットアイコンをダブルクリックする。
   - システムトレイメニューの**ウェブルート**アイコンを右クリックし、[**開く**] を選択する。



注意: システムトレイのアイコンが見つからない場合は、Windows の [スタート] メニューを開き、**[すべてのプログラム] > [Webroot SecureAnywhere] > [Webroot SecureAnywhere]**の順に選択します。

[概要] ウィンドウが表示されます。



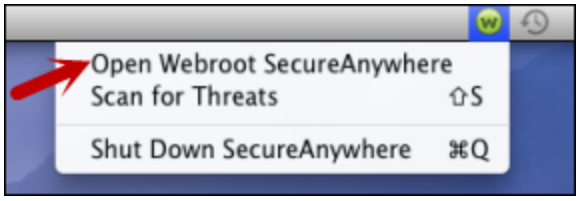
パネルの右側には、ナビゲーションタブを含むメインインターフェイスが表示されています。

歯車のアイコン	説明
PC セキュリティ	カスタムスキャン、シールド設定の変更、隔離の管理を実行できます。
ID とプライバシー	オンライントランザクション中に脅威にさらされる可能性のある重要なデータを保護します。
ユーティリティ	ツールを使用して、プロセスとファイルの管理、レポートの表示、ウェブルートサポートへのファイルの提供を実行できます。また、システム最適化ツールを使用して、インターネットブラウザのアクティビティや一時ファイルを削除できます。
マイアカウント	SecureAnywhere のアカウント情報を表示したり、アップデートをチェックしたりできます。
サポート / コミュニティ	カスタマーサポートおよびウェブルートコミュニティにアクセスできます。

Mac コンピュータで SecureAnywhere を開く

Mac コンピュータで SecureAnywhere のメインインターフェイスを開くには

1. エンドポイントで次のいずれかの操作を行います。
   - メインウィンドウを表示するには、メニューバーにある **ウェブルート** のアイコンをクリックします。
   - ドロップダウンメニューで [**Webroot SecureAnywhere を開く**] を選択します。



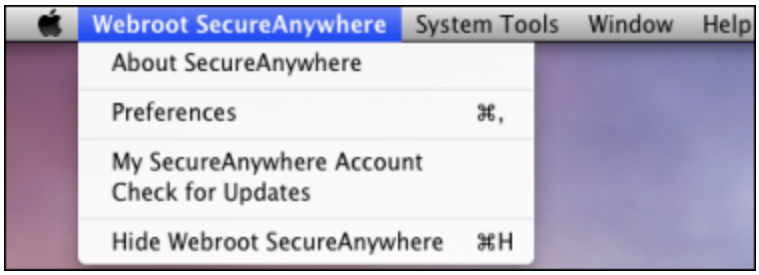
システムが安全な場合、次のようなメインウィンドウが表示されます。

ウェブルートのインターフェイスでは、コンピュータの保護の状態を反映して、次のように表示の色を使い分けます。

- **緑** - Mac は安全です。
- **黄** - 1 つあるいは複数の潜在的なリスクへの対応が必要です。
- **赤** - 1 つまたは複数の重要なアイテムについてユーザーが対応する必要があります。

Mac の [Webroot SecureAnywhere] メニュー

SecureAnywhere のインターフェイスがアクティブな場合、メニューバーには SecureAnywhere に関するオプションが表示されます。



Mac の Webroot SecureAnywhere ドロップダウンメニュー項目の詳細については、以下の表を参照してください。

オプション	説明
SecureAnywhere について	SecureAnywhere のバージョン番号を表示します。
設定	システム設定、スキャンのスケジュール、その他の設定を変更することができます。
My SecureAnywhere アカウント	キーコードおよびその他のアカウント詳細を表示します。
アップデート情報を確認する	最新のプログラムアップデートをダウンロードおよび適用します。
Webroot SecureAnywhere を非表示にする	メインウィンドウが表示されなくなりますが、SecureAnywhere の保護はシャットダウンされません。保護をシャットダウンする場合は、メニューバーにあるウェブルートのアイコンをクリックし、[**SecureAnywhere をシャットダウン**] を選択してください。

Mac の [システムツール] ドロップダウンメニュー

Mac の [システムツール] ドロップダウンメニュー項目の詳細については、以下の表を参照してください。

項目	説明
システム制御	Mac で実行中のすべてのプログラムとプロセスに対する脅威検出の設定を調整できます。
レポート	スキャンログを保存できます。スキャンログは、問題の原因特定のためにウェブルートサポートに問い合わせをする際に役立つ場合があります。
ファイルの提供	ファイルを分析のためにウェブルートに送信できます。ファイルが問題を起こしていると考えられる場合や、ファイルが安全と分かっていてそれを再分類する必要がある場合に、ファイルを送信できます。
システムアナライザ	脅威、セキュリティ上の脆弱性、その他のコンピュータの問題を検出するシンプルなユーティリティです。完了後のレポートでは、システムパフォーマンス、プライバシー、保護を強化するための推奨事項が提案されます。

スキャンの結果確認と脅威の管理

[グループの管理] で、エンドポイントのスキャン履歴を表示し、検出された脅威を管理できます。ファイルが正当なものだとわかっている場合は、隔離されたファイルを復元できます。詳細については、「*ファイルの隔離からの復元*」を参照してください。

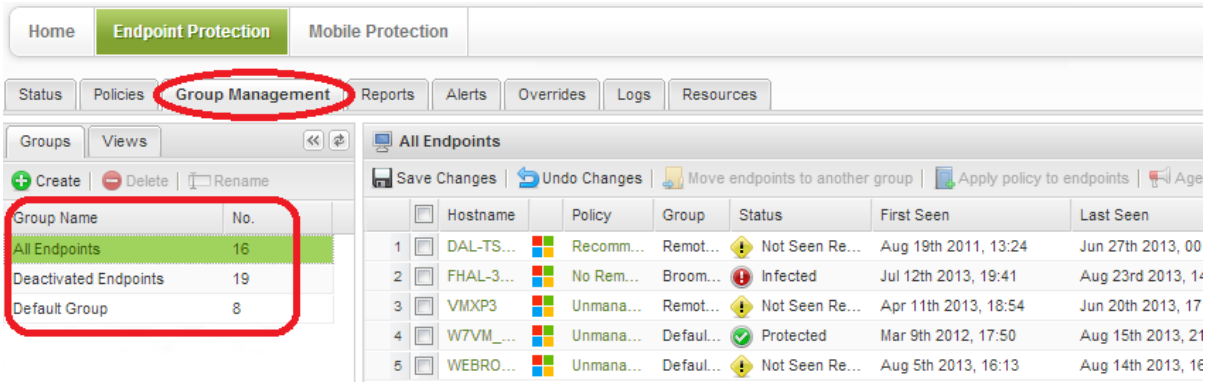
また、ファイルを [*正当*] (実行を許可)、または [*不正*] (自動隔離) に再分類することもできます。詳細については、「*ファイルのオーバーライドの設定*」を参照してください。

スキャン履歴の表示

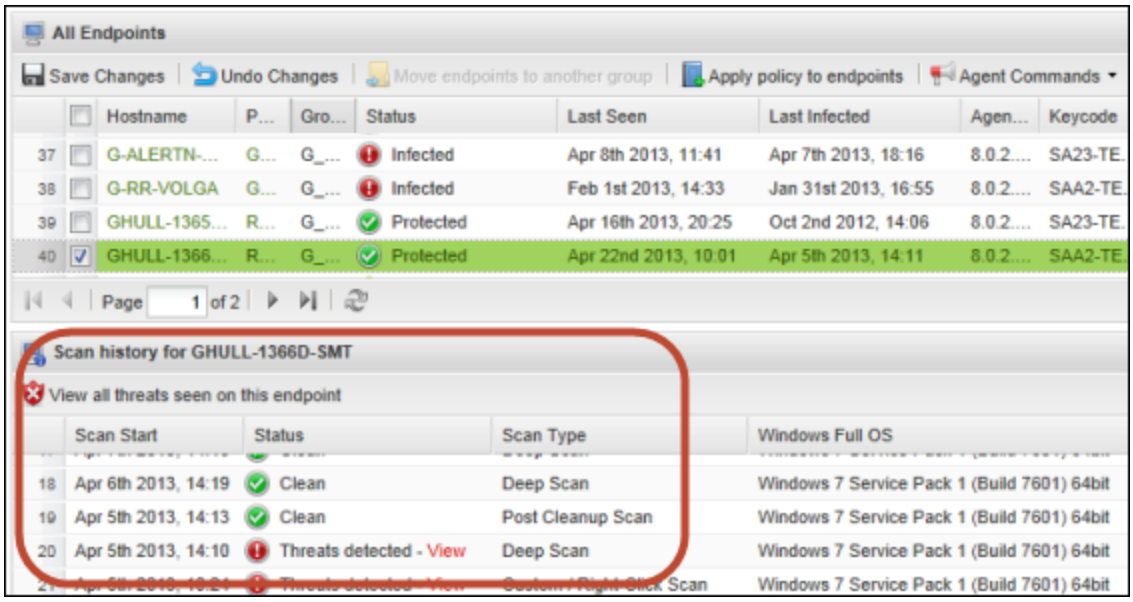
[グループの管理] パネルでエンドポイントのスキャン履歴を表示することができます。これは、脅威が見つかった場所を確認する際に役立ちます。

スキャン履歴を表示するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、必要なエンドポイントを含むグループを選択します。

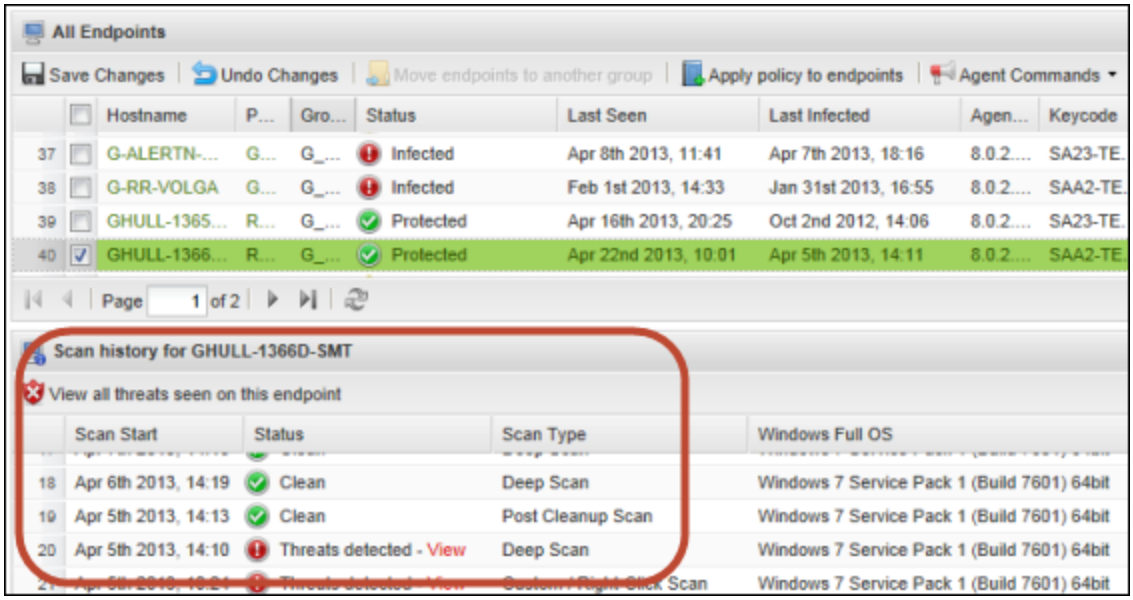


3. 右側の [エンドポイント] パネルで、いずれかのエンドポイントを選択します。



[スキャン履歴] パネルが表示され、エンドポイントにおけるスキャンアクティビティと検出された脅威が提示されます。

注意： 脅威が検出された場所のパス名にドライブを示す文字が含まれている場合、この文字は ”?” マークに置換されます。たとえば、?:\users\user1\desktop のようなパス名が表示される場合があります。



4. 必要に応じて、エンドポイントとスキャン履歴に関する追加データを表示または非表示にできます。カラム見出しをクリックしてドロップダウンメニューを開き、追加または削除するカラムのチェックボックスを選択します。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

ファイルの隔離からの復元

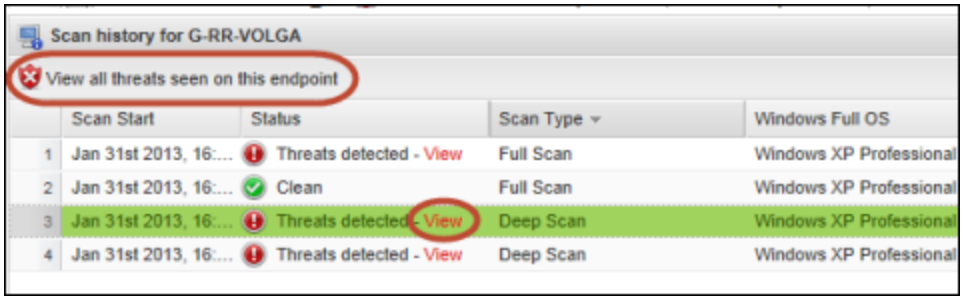
[スキャン履歴] パネルで、ファイルを隔離から復元できます。ファイルはエンドポイントの元の場所に自動的に戻ります。

また、[確認されたすべての脅威] レポートからファイルを復元することもできます。詳細については、「*[確認されたすべての脅威] レポートの生成 ページ342*」を参照してください。

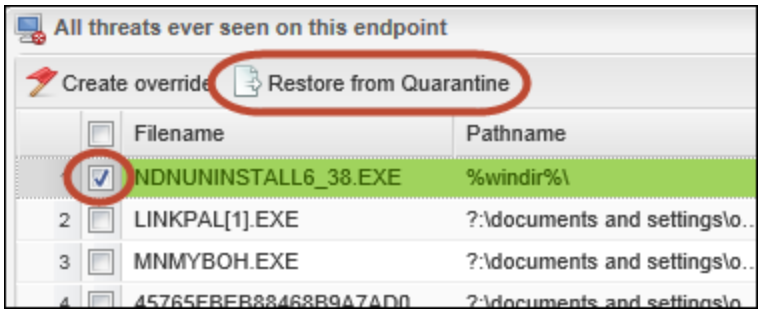
ファイルを復元するには

1. このセクションの前述の説明に従って、特定のエンドポイントのスキャン履歴を表示します。
2. [スキャン履歴] パネルで、次のいずれかを実行して該当するファイルを探します。

   - [状態] カラムで [**表示**] をクリックして、脅威が検出された日付を確認する
   - [**このエンドポイントで確認されたすべての脅威を表示**] ボタンをクリックする



3. 表示されるダイアログで、チェックボックスを選択してファイルを選択します。
4. [**隔離先から復元する**] ボタンをクリックします。



ファイルがエンドポイントの元の場所に戻されます。

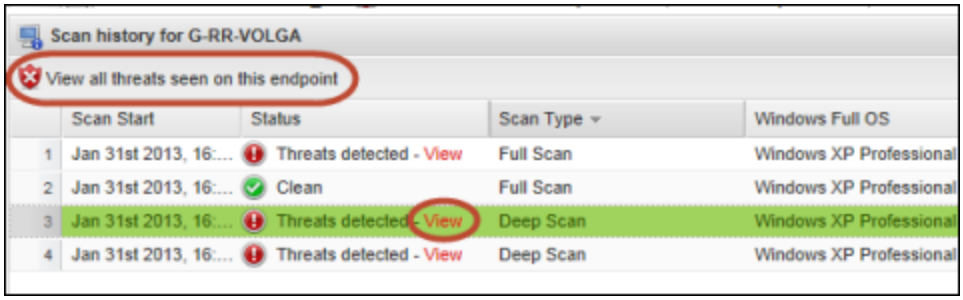
ファイルのオーバーライドの設定

[スキャン履歴] パネルで、ファイルのオーバーライドを設定できます。また、[オーバーライド] タブでオーバーライドを設定することもできます。詳細については、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。

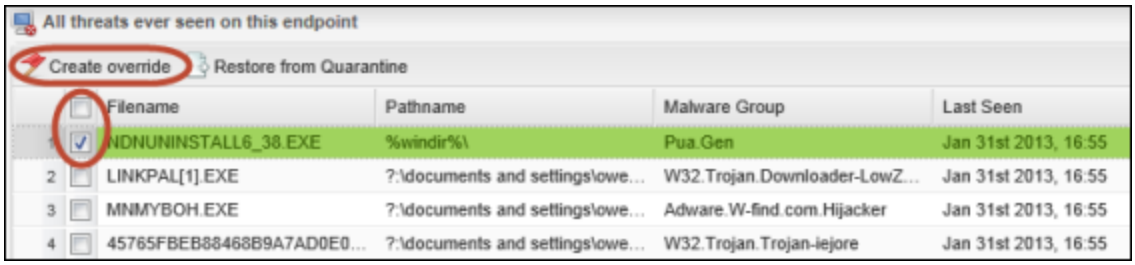
ファイルのオーバーライドを設定するには

1. このセクションの前述の説明に従って、特定のエンドポイントのスキャン履歴を表示します。
2. [スキャン履歴] パネルで、次のいずれかを実行して該当するファイルを探します。

- [状態] カラムで [**表示**] をクリックして、脅威が検出された日付を確認する
- [**このエンドポイントで確認されたすべての脅威を表示**] ボタンをクリックする



3. 表示されるダイアログで、リストからファイルを選択します。
4. [**オーバーライドの作成**] ボタンをクリックします。



[オーバーライドの作成] ウィンドウが表示されます。

5. [判定] ドロップダウンメニューで、次のいずれかを選択します。
   - **正当** - ファイルの実行を常に許可します。
   - **不正** - 常にファイルを隔離します。
6. 次の手順に従って、このオーバーライドをポリシー全体または個々のポリシーに適用できます。
   - すべてのポリシーにオーバーライドを適用するには、[**オーバーライドをグローバルに適用**] チェックボックスを選択します。

- オーバーライドの対象となるポリシーを個別に選択するには、[**オーバーライドをグローバルに適用**] チェックボックスの選択を解除します。[ポリシー] フィールドが表示されたら、ドロップダウンメニューでポリシーを選択します。

アップデートのダウンロードと強制実行

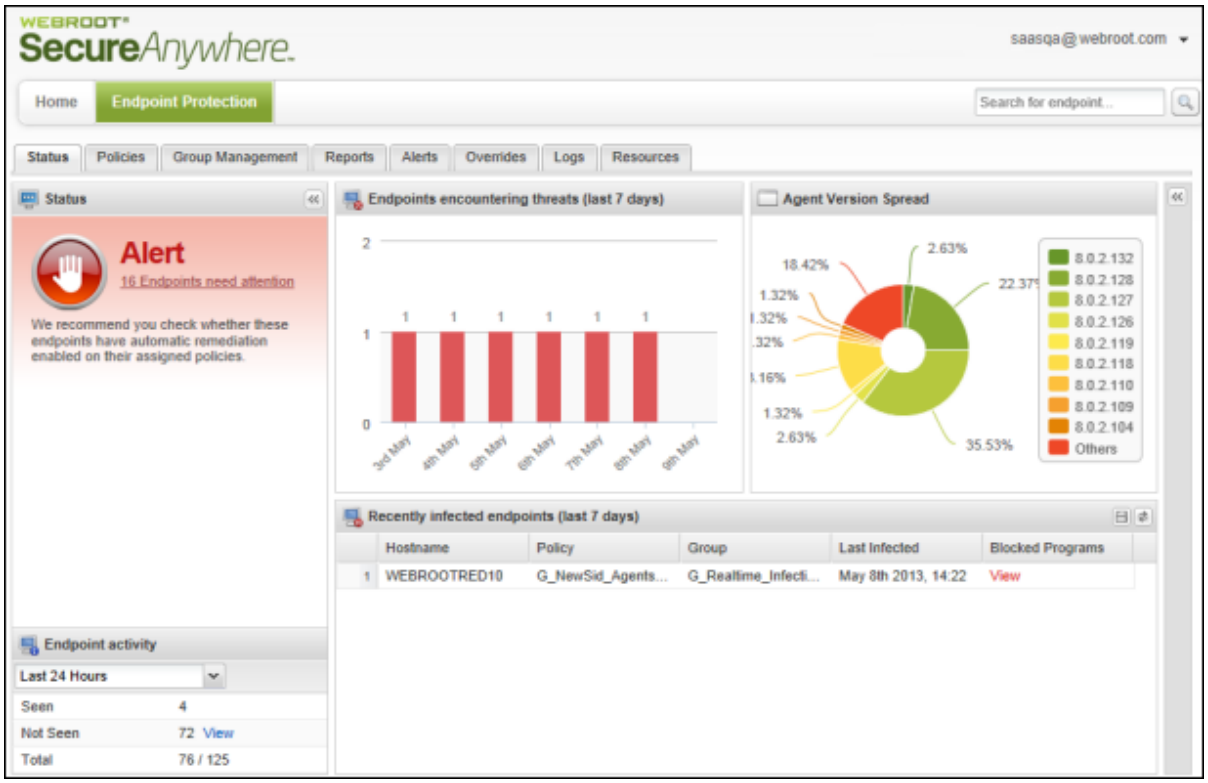
ウェブルートソフトウェアの過去のバージョンとは異なり、Webroot SecureAnywhere はデフォルトですべてのアップデートを自動的にダウンロードおよびインストールします。バージョンのアップデートは、リリース時に全世界のユーザーベース全体で負荷が分散されるため、すべてのエンドポイントに適用されるまで最大 72 時間かかる場合があります。

スキャンを実行するたびにお使いのウェブルートソフトウェアがクラウドと通信し、新しい判定やアップデートがあれば、それをダウンロードしてマシンに適用します。SecureAnywhere はアップデートがリリースされるとすぐに対応するため、コンピュータがインターネットに接続されている限り、常に最新の保護状態が維持されます。

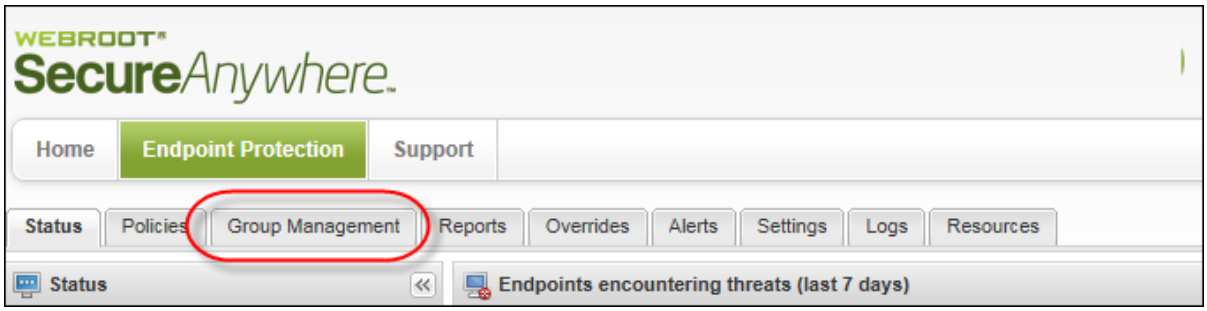
注意: 詳細については、「*エンドポイントへのコマンドの発行 ページ144*」の「高度なコマンド」の表を参照してください。

アップデートをダウンロードして強制適用するには

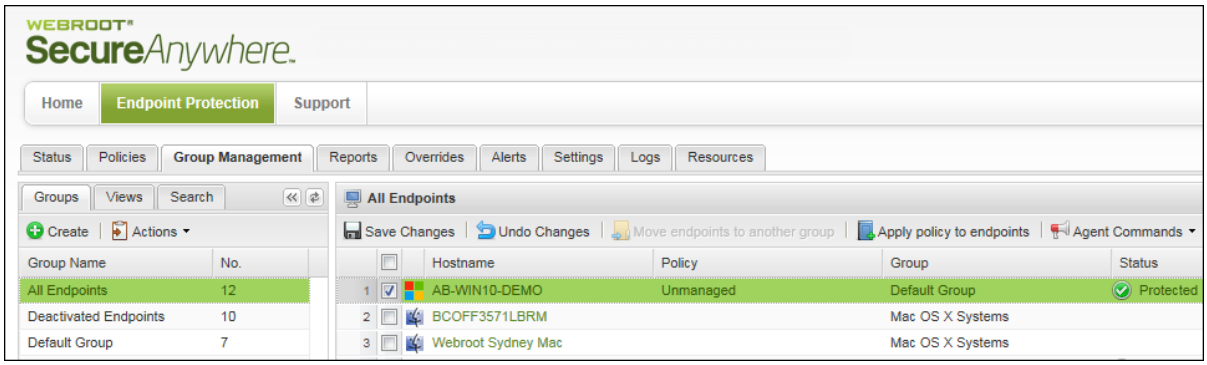
1. エンドポイントプロテクションにログインします。



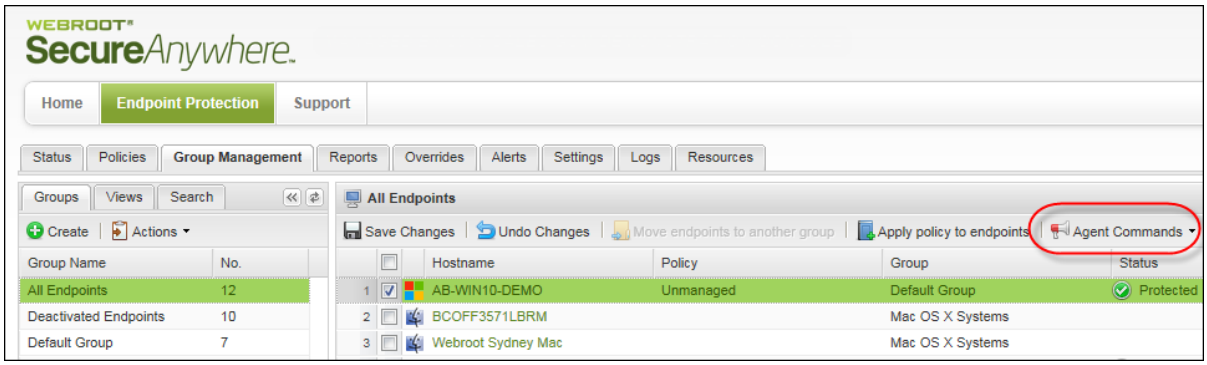
2. [**グループの管理**] タブをクリックします。



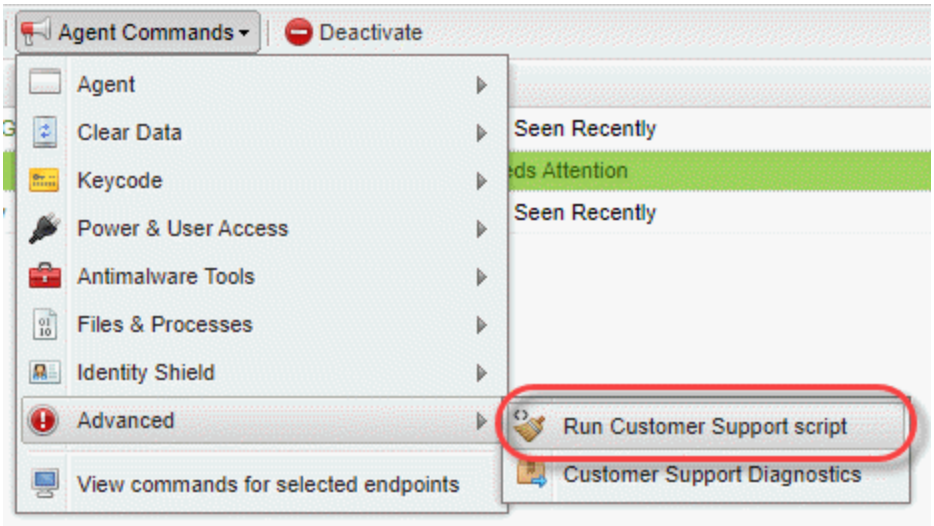
3. 左側の [グループ] パネルで [**すべてのエンドポイント**] を選択し、右側のペインで 1 つ以上のエンドポイントを選択します。



メニューバーに [エージェント コマンド] ボタンが表示されます。

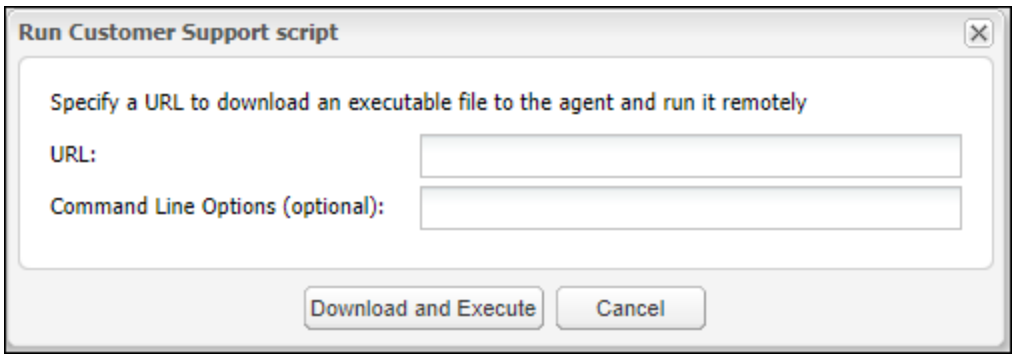


4. [エージェントコマンド] ドロップダウンメニューで、**[詳細] >3 [カスタマーサポートスクリプトを実行]** を選択します。



5. [URL] フィールドに次の URL を入力します。:

   http://anywhere.webrootcloudav.com/zerol/wsasme.exe



注意: この URL を使用して、インストーラーをエンドポイントにローカルでダウンロードし、手動で実行することも可能です。

6. ダウンロードのウィザードに従って最新のアップデートをインストールします。

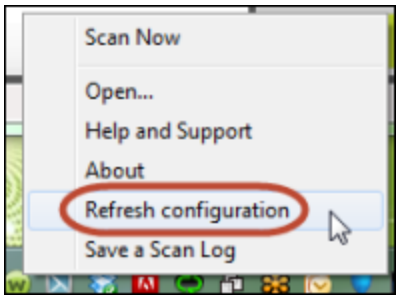
即時のアップデートの強制実行

ポーリング間隔によって、エンドポイントがその状態を送信しコマンドを受信する頻度 (15 分毎、1 時間毎など) が決まります。必要に応じて、グループのポリシーの [基本設定] でポーリング間隔を変更したり、以下の手順に従って即時のアップデートを強制実行したりできます。

詳細については、「*ポリシー設定の変更 ページ247*」を参照してください。

アップデートを強制するには

1. エンドポイントで、システムトレイにある**ウェブルート**のアイコンを右クリックします。
2. 表示されるドロップダウンメニューで [**設定のリフレッシュ**] を選択します。



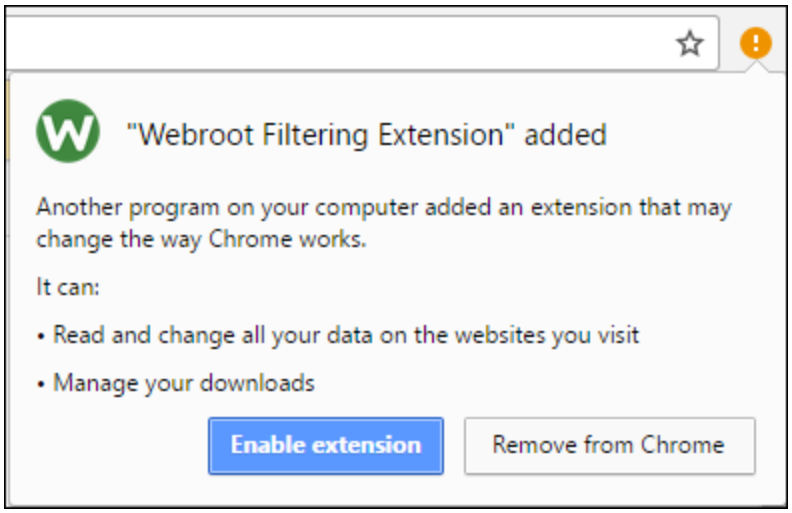
システムがアップデートされます。

Web 脅威シールド Chrome ブラウザエクステンションのインストール

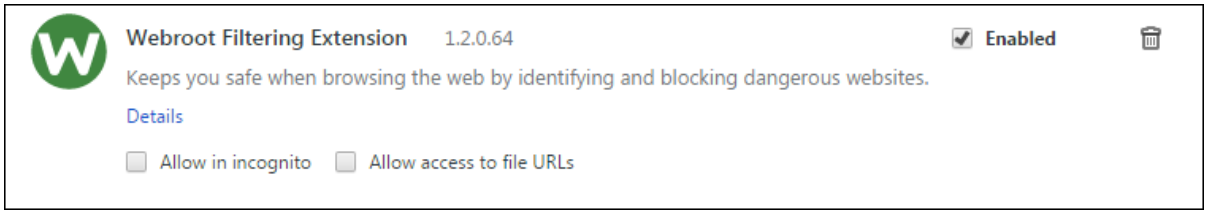
ウェブルートではブラウザエクステンションの配備に関して、Google と Chromium プロジェクトのベストプラクティスを採用しています。そのため、ウェブルートがエンドユーザーに通知することなくブラウザエクステンションを配備することはできません。管理された環境での Chrome ブラウザエクステンションのサイレントモードのインストールを希望する場合は、以下の手順に従って強制インストールを実行できます。

管理された環境での Webroot SecureAnywhere の強化 Web 脅威シールド (EWTS) 向け Chrome ブラウザエクステンションの強制インストールは簡単です。強制インストールではユーザーにエクステンションのアクティブ化や承諾を促さず、ユーザーによる無効化も回避されます。

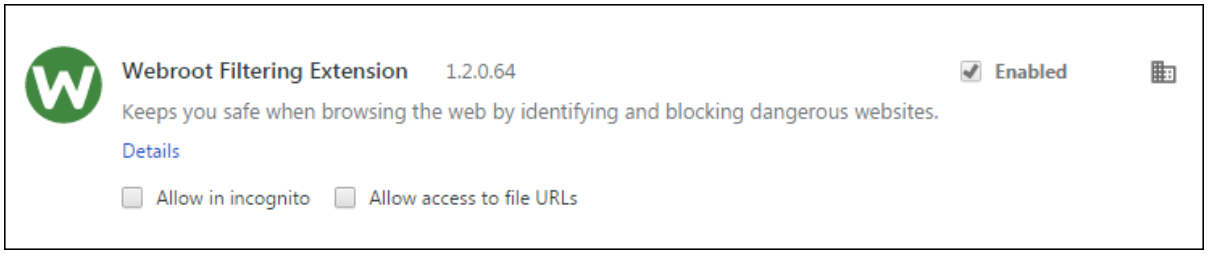
非強制の環境では、Chrome のエクステンションを有効化するように促す、次の図のようなプロンプトが表示されます。



非強制のエクステンションは、chrome://extensions/ を介してユーザーが有効化、無効化、削除を実行できるようになっています。次の図を参照してください。



管理された環境でサイレントモードにより配備した Chrome エクステンションは、次の図のように表示されます。この場合、ユーザー側で無効化や削除を行うことはできず、管理者が行います。ユーザーに対してエクステンションの有効化を促すプロンプトは表示されません。



Active Directory グループポリシーの使用

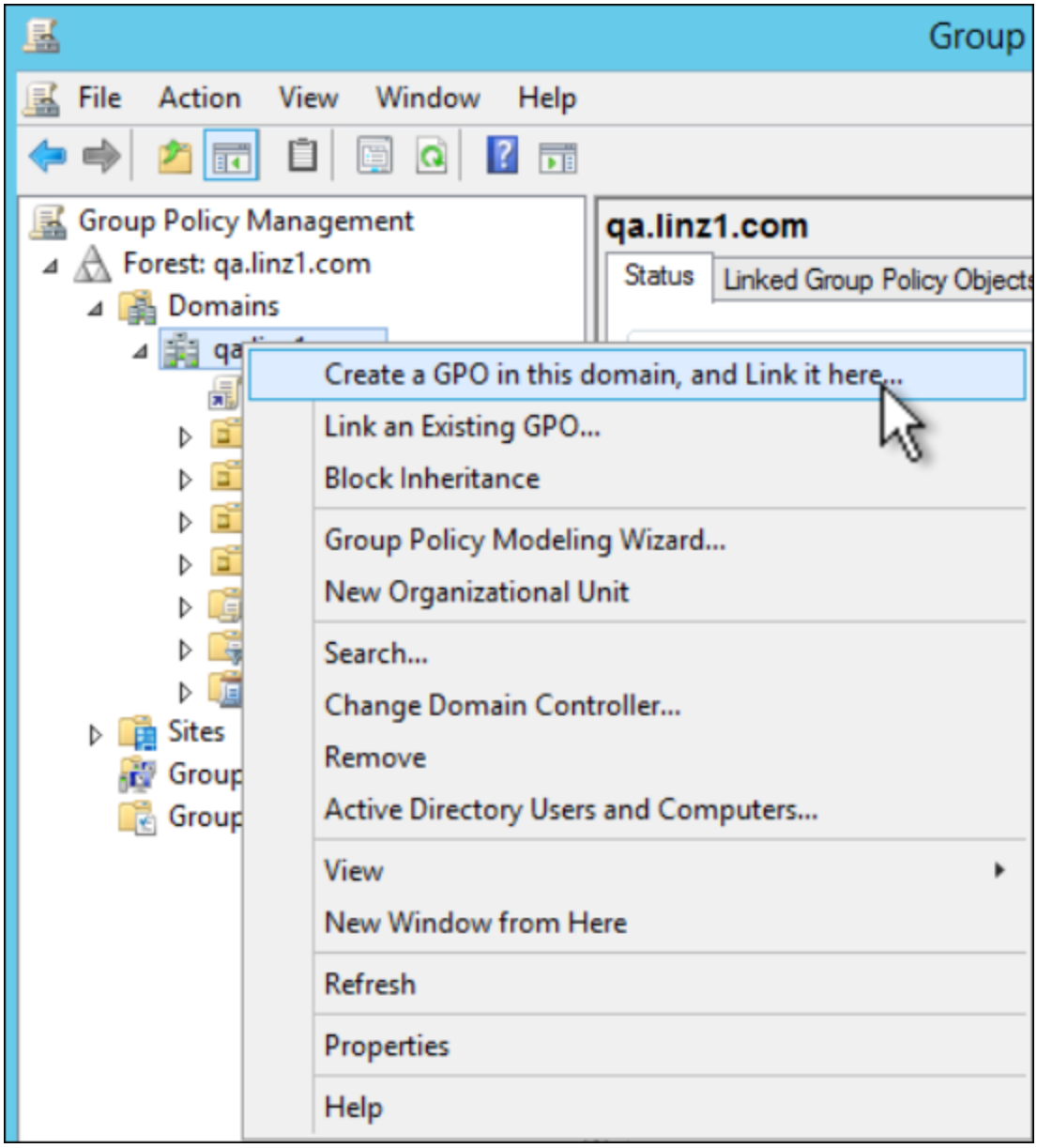
Google は Windows Server 2003 (ADM テンプレート) と Windows Server 2008+ (ADMX テンプレート) の管理用テンプレートを提供しており、これをインポートすることでグループポリシー向けの Chrome 固有のポリシーを使用できるようになります。

次の Google のリンクから該当する管理用テンプレートをダウンロードしてください。

Google Chrome テンプレート / ドキュメントの Zip ファイル

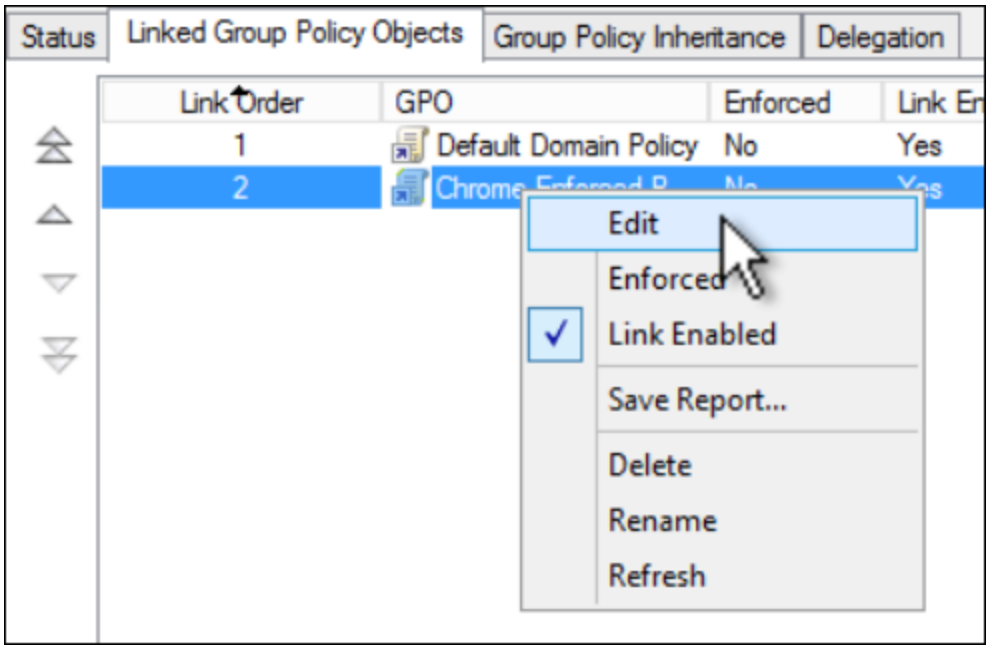
Active Directory グループポリシーを介して Chrome ブラウザエクステンションの強制インストールを行うには

1. [グループポリシー管理] コンソールを開きます。ドメインを右クリックし、[**このドメインに GPO を作成し、ここでリンクする**] を選択します。



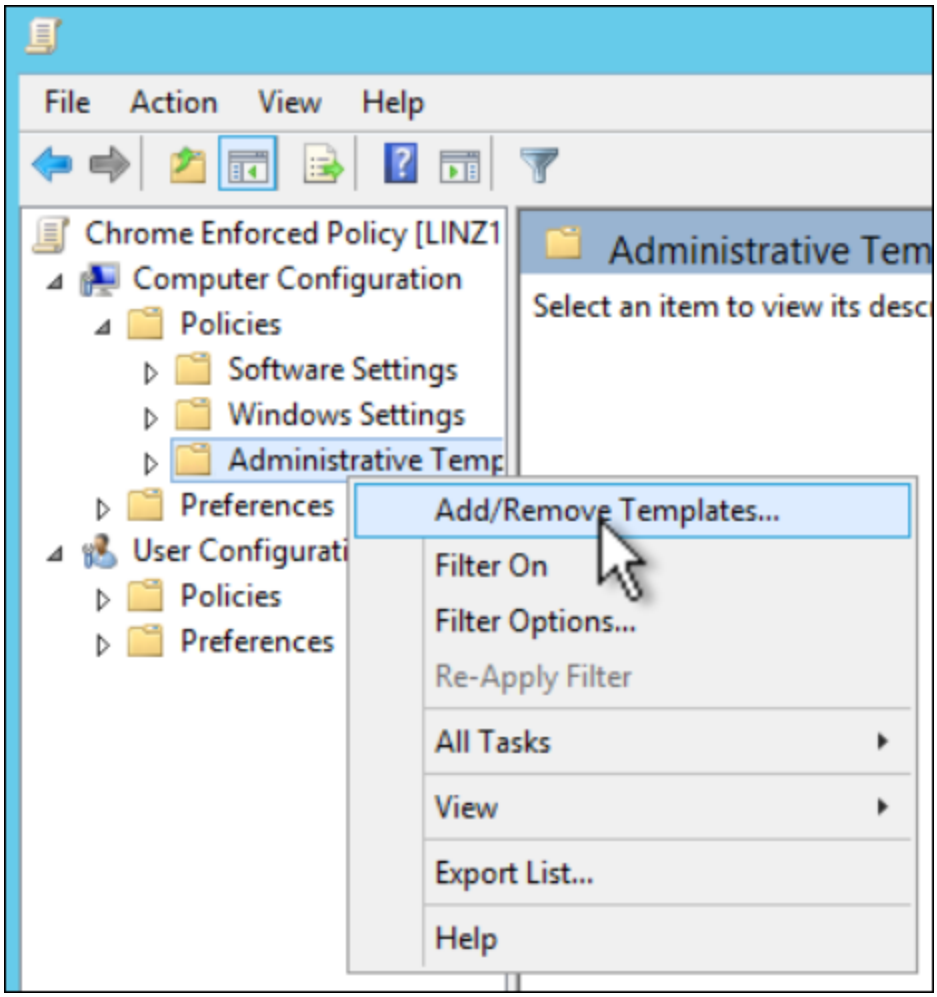
2. 新しい GPO に名前を付けます。ここでは仮に "Chrome Enforced Policy" とします。

3. 新しい GPO を右クリックし、[**編集**] を選択します。以下のようなウィンドウが開きます。

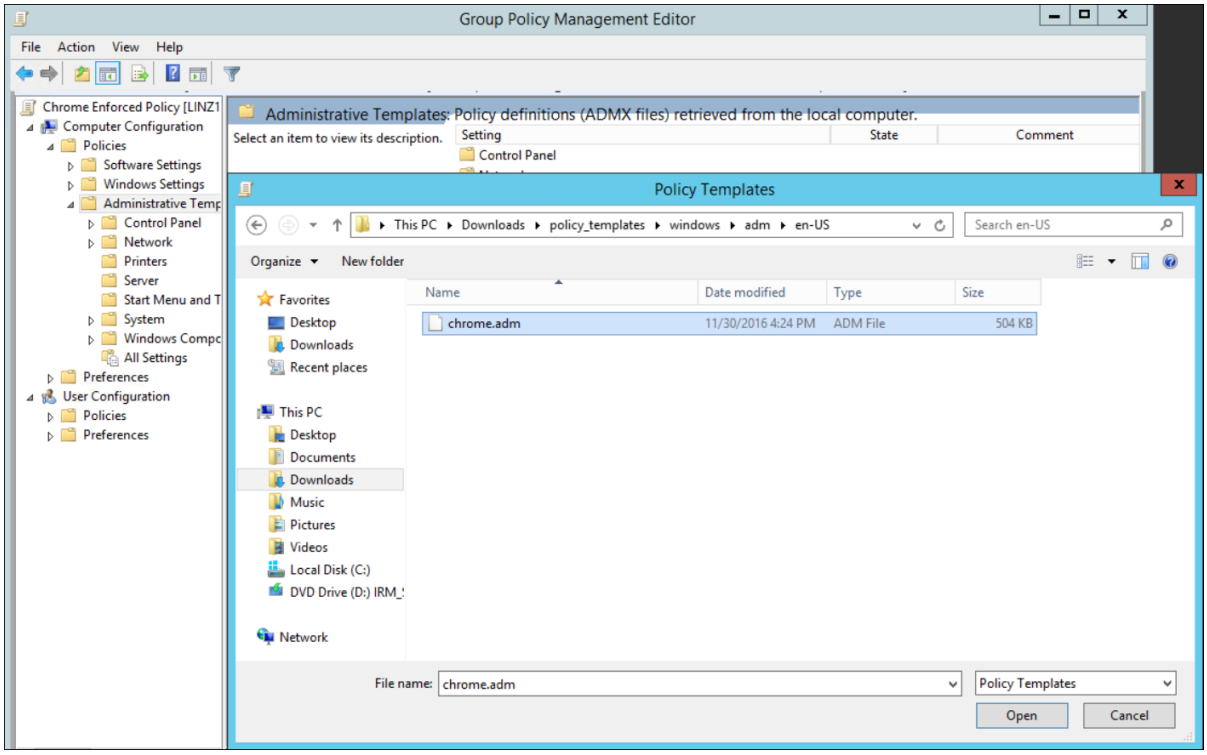


4. [コンピュータの設定] を展開します。
5. [**管理用テンプレート**] を右クリックします。

6. [**テンプレートの追加 / 削除**] をクリックします。



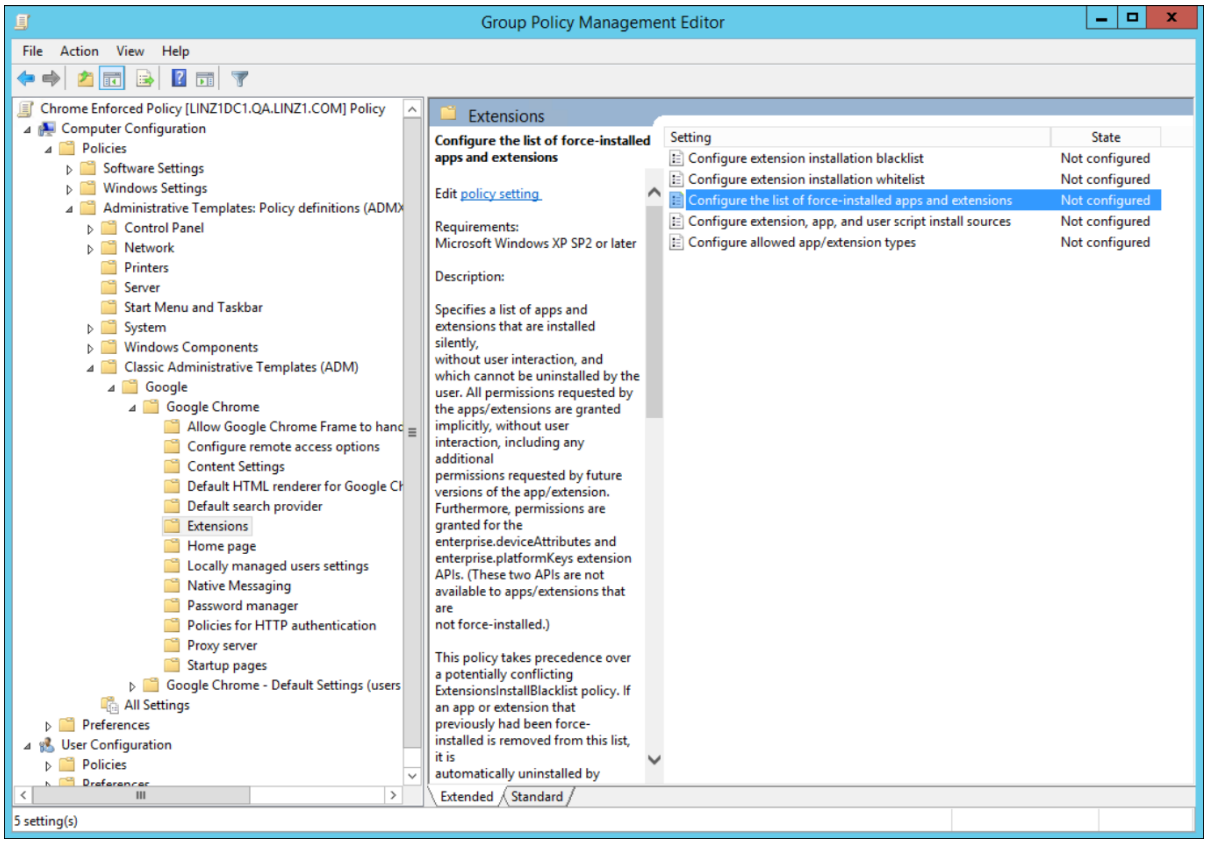
7. [**追加**] をクリックします。
8. Google Chrome テンプレート アーカイブにあるダウンロード済みの ADM ファイルまたは ADMX ファイルを指定します。



9. [**開く**] をクリックしてから [**閉じる**] をクリックします。

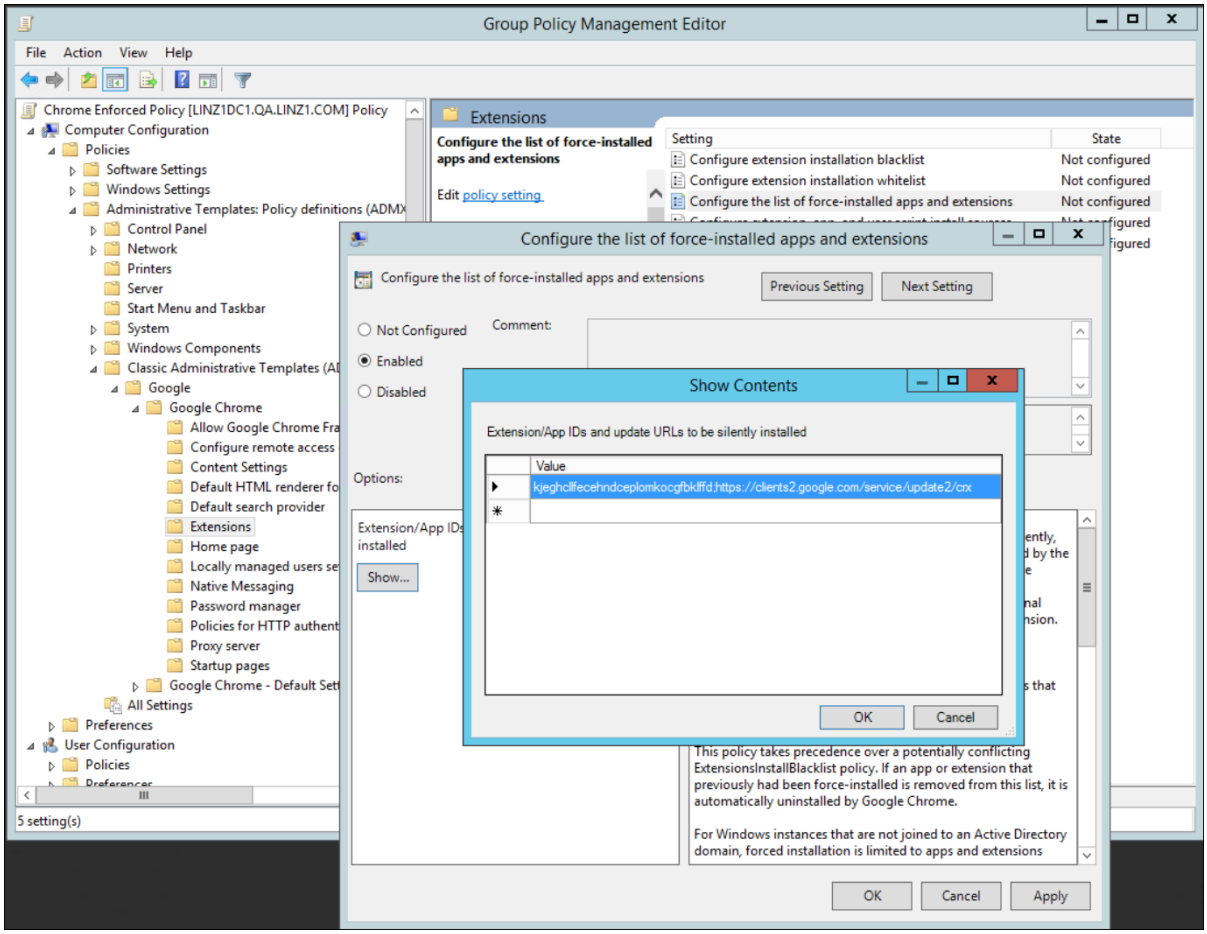
   管理用テンプレートの中に Google のフォルダが追加されていることを確認します。

10. 管理用テンプレート内の **Google\Google Chrome\Extensions** を展開します。



11. [**強制インストールエクステンションのリスト設定**] をクリックします。
12. [**有効化**] をクリックします。
13. [**表示**] をクリックします。
14. インストールがサイレントモードで行われるようにするため、[エクステンション / アプリ ID] のリストに下のテキストを入力して URL をアップデートします。

```
kjeghcllfecehndceplomkocgfbklffd;https://clients2.google.com/service/update2/crx
```



15. すべてのダイアログ / ボタンを確認します。

    これで、ウェブルートの Chrome EWTS エクステンションが、このポリシーが適用されるすべてのドメインコンピュータにインストールされます。

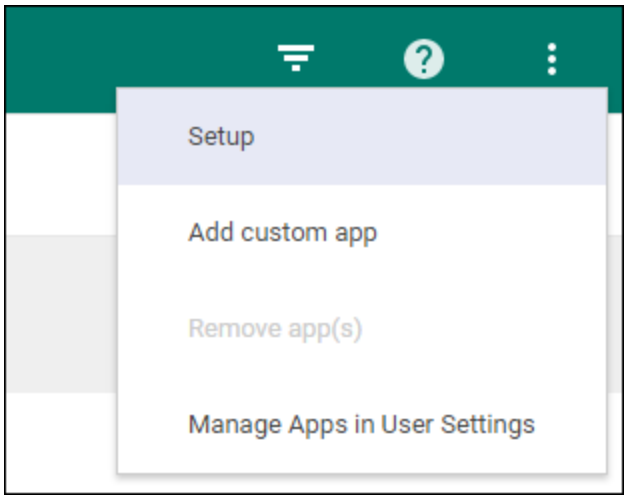
Google スイートを利用した単一カスタムアプリの強制インストール

Google スイートで管理された環境であれば、EWTS 向け Chrome エクステンションの強制インストールを実行できます。エクステンションとアプリケーションの一般的なインストール手順については、Google ヘルプを参照してください。

EWTS 向け Chrome エクステンションをインストールするには、以下の手順に従ってカスタムアプリを追加する必要があります。.

Chrome エクステンションをインストールするには

1. Google管理コンソールにサインインします。
2. 管理コンソールのダッシュボードにある [**デバイス管理**] をクリックします。
3. 左側の [**Chrome 管理**] をクリックします。
4. [**アプリ管理**] をクリックします。
5. 右側にある 3 つの点をクリックしてオーバーフローメニューを開きます。



6. [**カスタムアプリの追加**] を選択します。
7. カスタムアプリのダイアログで次の ID を入力します。

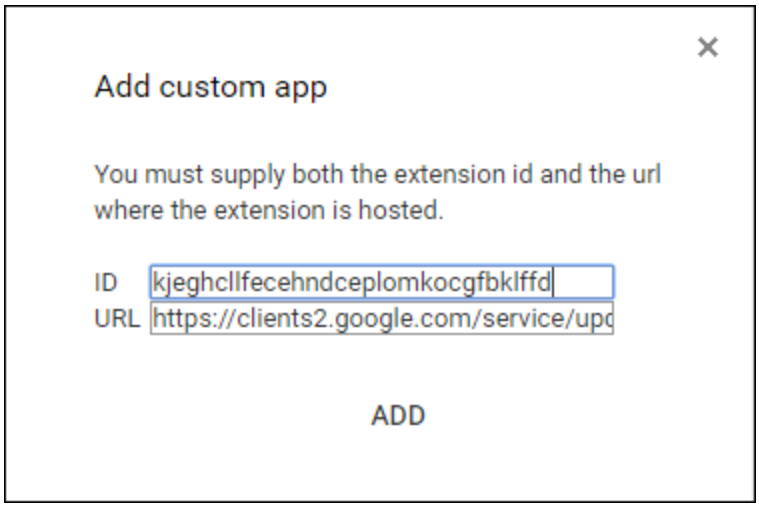
   `kjeghcllfecehndceplomkocgfbklffd`

8. 以下を入力します。

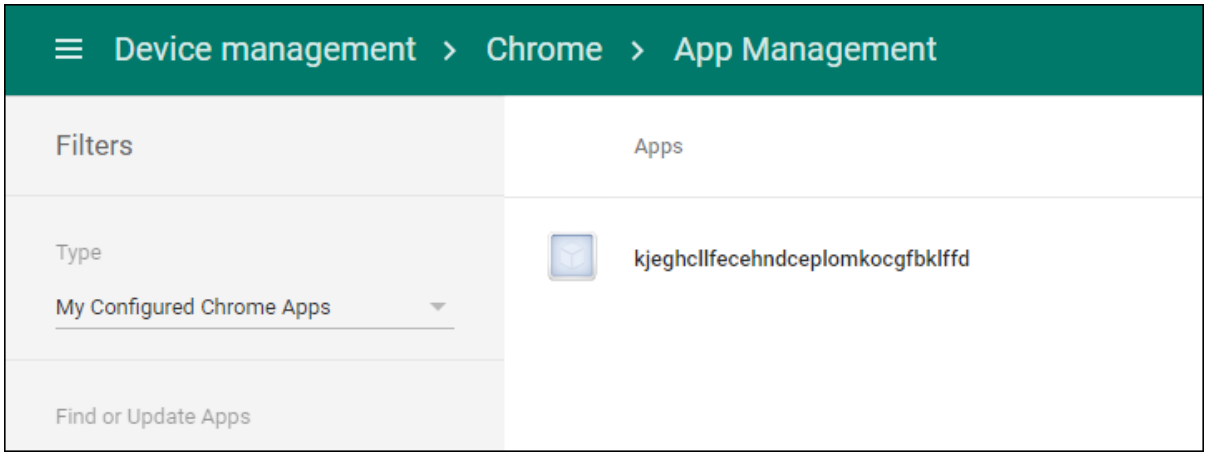
   `URL:https://clients2.google.com/service/update2/crx`

   これは、ウェブルートの Filtering Extension 用です。

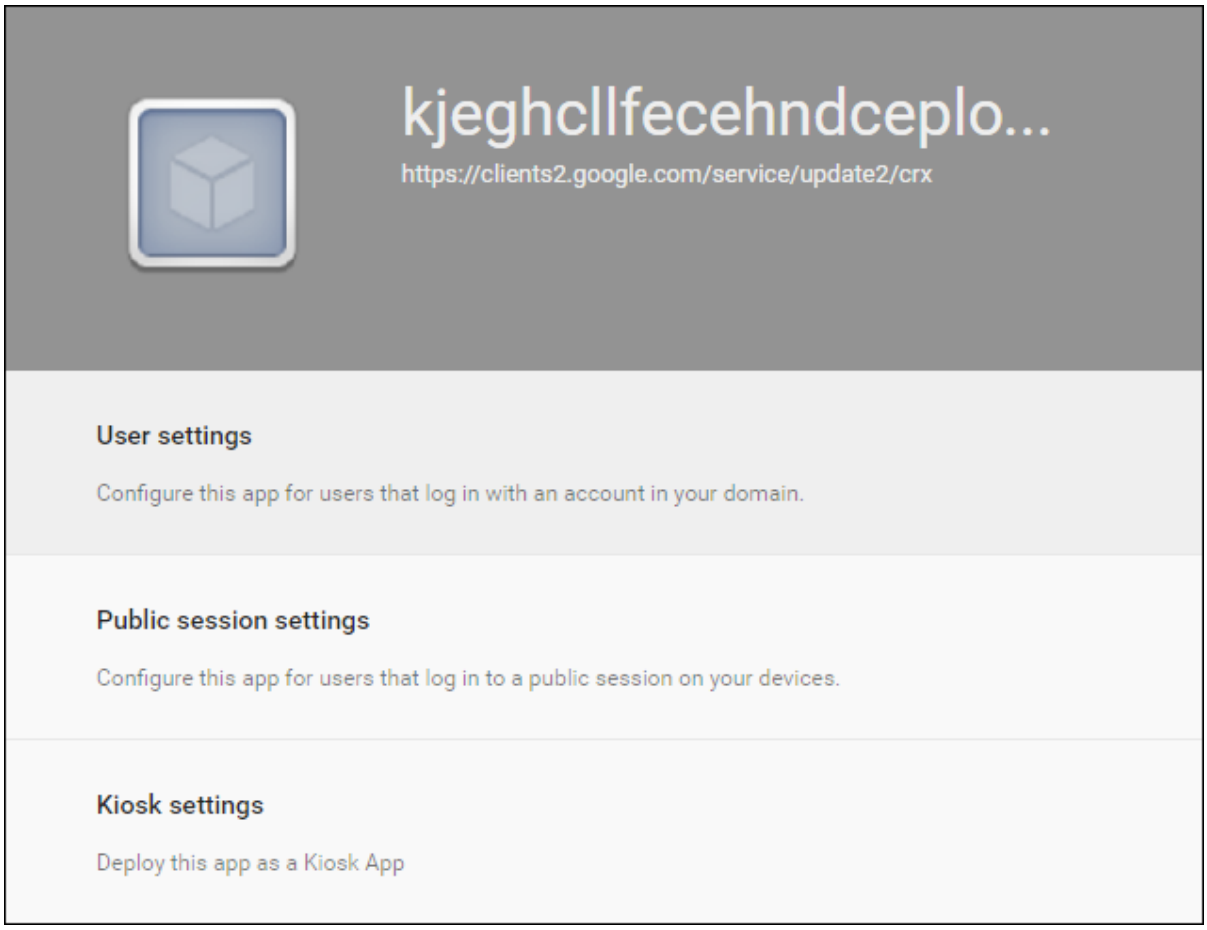
9. [**追加**] をクリックします。



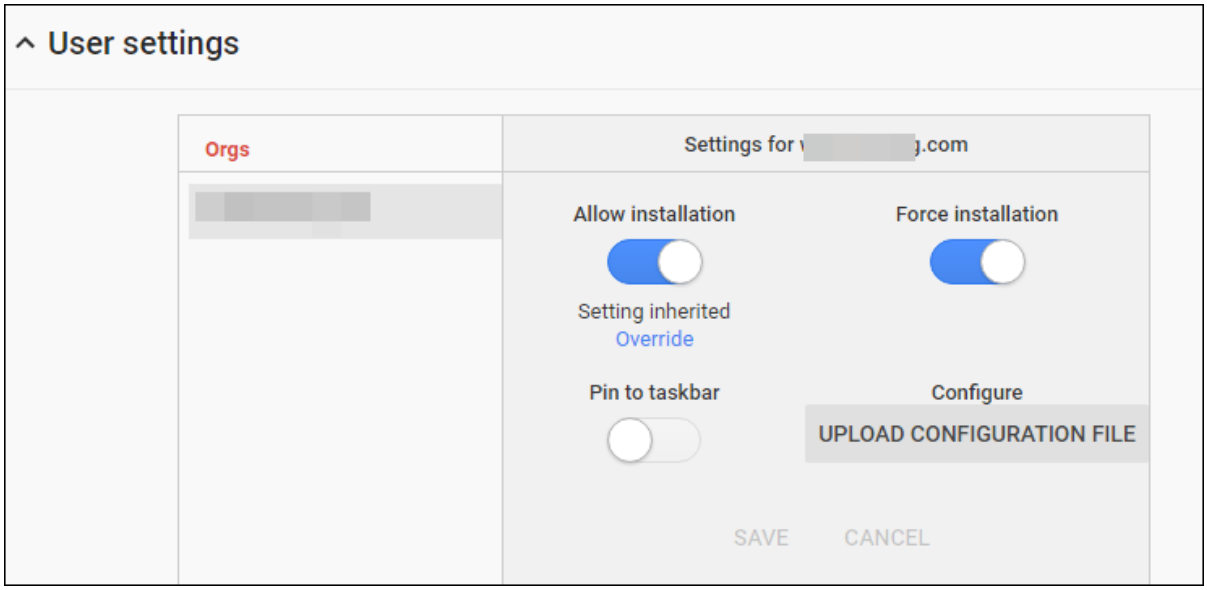
10. アプリ管理の画面で、新しく追加されたエクステンションの ID を選択します。



11. アプリのオプションで [**ユーザー設定**] を選択します。



12. EWTS 向け Chrome エクステンションをインストールする Org を選択し、[**インストール許可**] と [**強制インストール**] をオンにします。



13. [**保存**] をクリックします。

ここで選択した Org の認証情報を使用して Chrome にログインしているユーザーは、使用している Chrome ブラウザでウェブルートフィルタリングエクステンションが適用されます。Org の構成やアプリケーション管理の詳細オプションについては、Google の G Suite ドキュメントを参照してください。

注意: ウェブルートは現在、Chromebooks での Webroot SecureAnywhere の使用をサポートしていません。これらのデバイスを使用する場合は、トラブルを回避するために G Suite のポリシー制御を使用してください。詳細については、G Suite ヘルプドキュメントを参照してください。

レジストリの使用

WTS 向け Chrome エクステンションのサイレントモードでのインストールに Active Directory や Google Suite を使用することが適切でない場合は、Windows レジストリで代用できることもあります。ただし、コンピュータが Microsoft Windows ドメインの一部であることが条件となります。

注意: この方法は、Active Directory グループポリシーや G Suite で管理された環境に対応していない場合があります。

Chrome に使用できるポリシー設定の詳細については、以下のリンクを参照してください。

http://dev.chromium.org/administrators/policy-list-3#ExtensionInstallForcelist

Windows レジストリエディター (regedit.exe) の使用

1. 以下のレジストリキーが存在するかどうかを確認します。

   ```
   [HKEY_LOCAL_
   MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]
   ```

   このキーが存在する場合、他の管理アプリケーション (特に強制インストールしたエクステンション) が Chrome ポリシーを強制適用している可能性があります。この場合、以下の手順に進むと競合が発生することがあります。

2. 次のレジストリ値を追加します。

   Windows レジストリエディター バージョン 5.00

   ```
   [HKEY_LOCAL_
   MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist]"1"
   ="kjeghcllfecehndceplomkocgfbklffd;https://clients2.google.com/servic
   e/update2/crx"
   ```

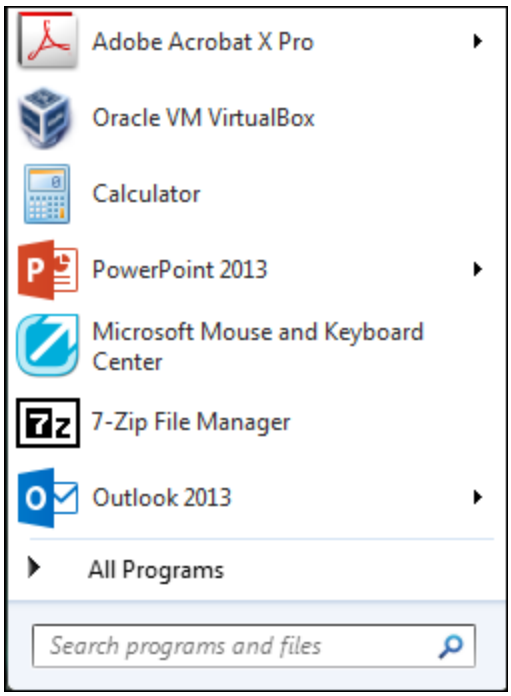
   エクステンションを追加登録する場合は、番号が連続するようにしてください。

エンドポイントでのコマンドの実行

Windows の PC、ノート パソコン、サーバー、またはネットワークにインストールされている仮想サーバーをエンドポイントとして使用できます。コマンドをエンドポイントでローカル実行するには、次の手順に従ってください。

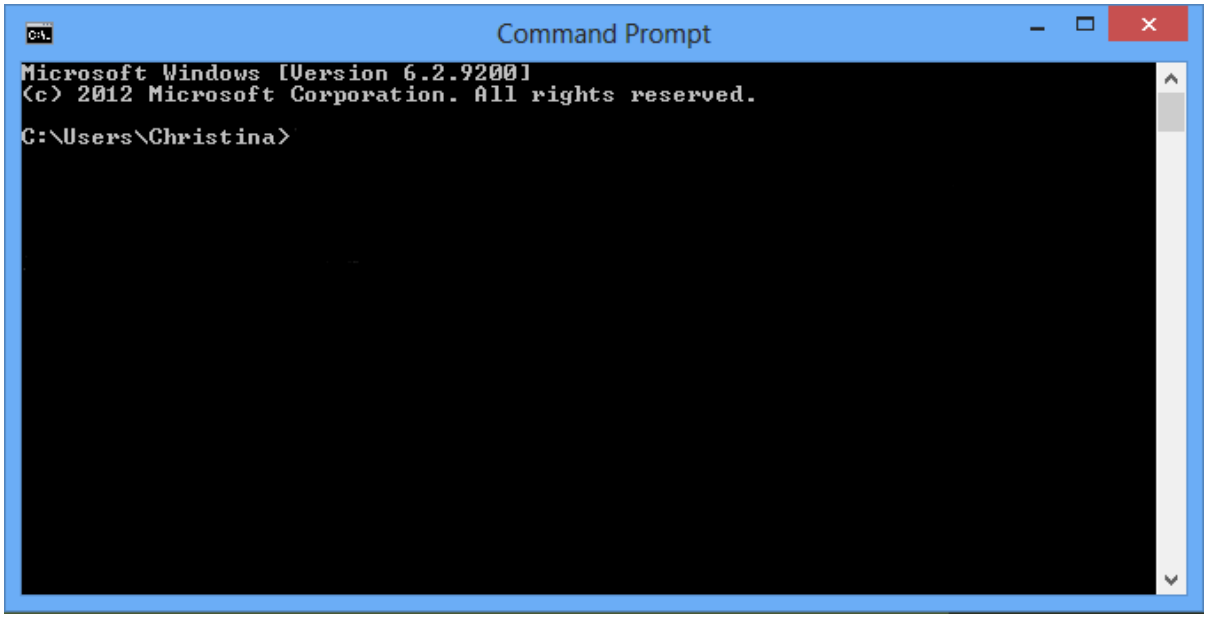
エンドポイントでコマンドを実行するには

1. [**スタート**] メニューをクリックします。

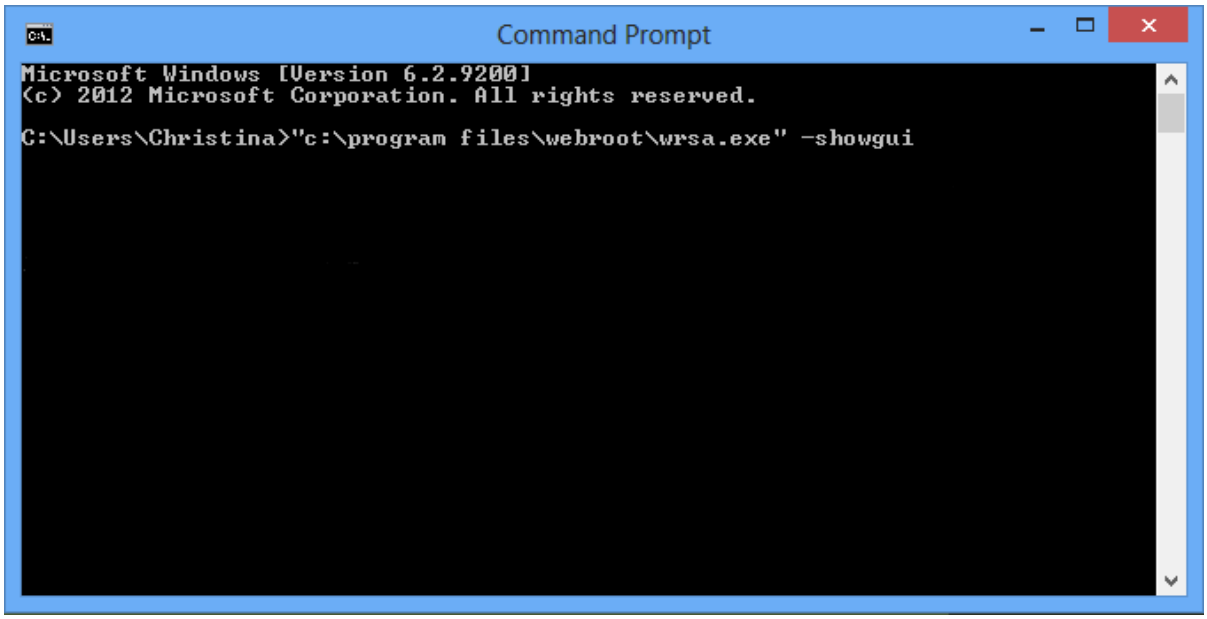


2. [プログラムとファイルを検索] 欄に「**CMD**」と入力します。

   [コマンド] ウィンドウが表示されます。



3. コマンドラインに次のコマンドのいずれかを入力します。



コマンド	説明
-poll	コマンドラインオプションでポーリングを行います。 例: `"c:\program files\webroot\wrsa.exe" -poll` これによりポーリングを必要に応じて実行でき、SME のお客様は、現在使用しているソフトウェア実行手段 (例: psexec) でポーリングを強制的に実行できるようになります。ソフトウェアのアップデート、設定のアップデート、エージェントコマンドのアップデート、ライセンスの確認を同時に行うことができます。
-showgui	ポリシーで許可されていれば、UI が起動し表示されます。 例: `"c:\program files\webroot\wrsa.exe" -showgui`

-silentscan	サイレントモードでスキャンを開始します。スキャン用 UI はユーザーには表示されませんが、トレイアイコンにカーソルを合わせると表示されます。コマンドの例: `WRSA.exe -silentscan="c:\foldername"`
	
	フォルダをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop"`
	
	ファイルをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -silentscan="c:\Documents and Settings\Administrator\Desktop\eicar.com"`
	
	注意: コマンドは 8.0.1.196 以降のビルドでのみ利用可能です。

コマンド	説明

-scan	特定のロケーションのスキャンを開始し、開始後にスキャン進捗状況の UI をユーザーに表示します。
	
	形式: WRSA.exe -scan="c:\foldername"
	
	フォルダをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop"`
	
	ファイルをスキャンする実行コマンドの例:
	
	`"C:\Program Files\Webroot\WRSA.exe" -scan="c:\Documents and Settings\Administrator\Desktop\eicar.com"`
	
	注意: コマンドは 8.0.1.196 以降のビルドでのみ利用可能です。

-uninstall	製品がインストールされている場合、アンインストールします。WRSA.exe でも実行できます。
	
	アンインストールはサイレントモードでは実行されません。エンドポイントが非管理の場合のみ有効です。エンドポイントが管理されている場合、コマンドは Windows の [セーフモードとネットワーク] でのみ動作します。実際にネットワークに接続されている必要はありません。
	
	例:
	
	`wsasme.exe -uninstall`
	
	`"c:\program files\webroot\wrsa.exe" -uninstall`

4. 終了したら、[コマンド] ウィンドウ右上の赤い **X** マークをクリックしてウィンドウを閉じます。

エンドポイントの非アクティブ化

エンドポイントを非アクティブ化して、エンドポイントプロテクションに報告を行わないようにすることができます。必要に応じて、後からエンドポイントを再アクティブ化することができます。エンドポイントを非アクティブ化することにより、ライセンスシートを解放して別のエンドポイントをインストールすることができます。

注意: 管理ポータルでエンドポイントを非アクティブ化せずに、エンドポイントにアンインストールコマンドを送信することもできます。この場合、管理ポータルにエンドポイントのエントリが維持されます。ただし、7 日が経過すると [*未確認*] と表示されます。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

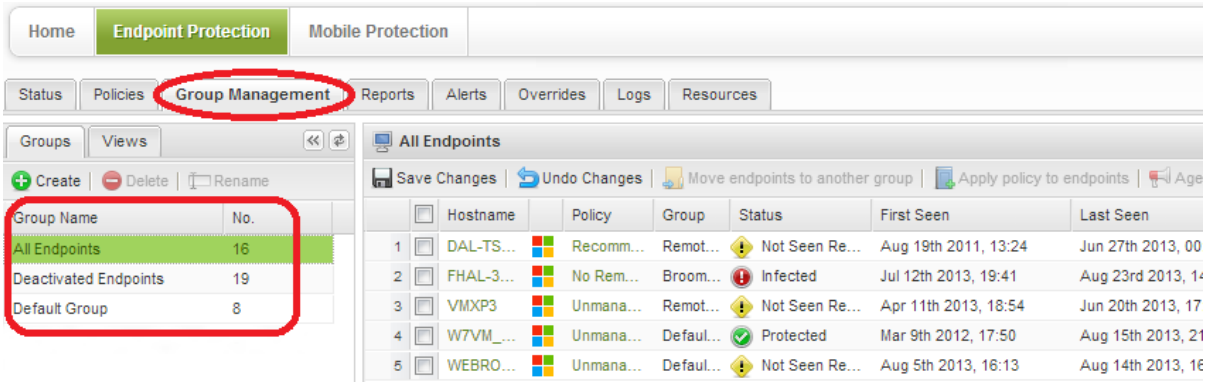
このトピックでは、次の手順について説明します。

エンドポイントの非アクティブ化

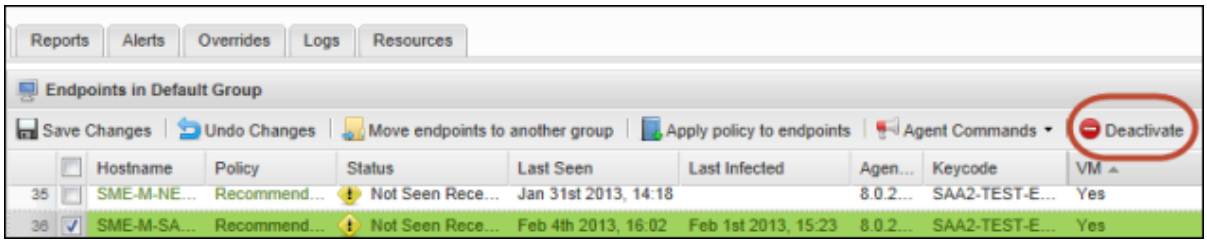
非アクティブ化するとエンドポイントにアンインストールコマンドが送信され、管理ポータルからエンドポイントのエントリが削除されます。

エンドポイントを非アクティブ化するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、必要なエンドポイントを含むグループを選択します。



3. コマンド バーで 1 つまたは複数のエンドポイントを選択して、[**非アクティブ化**] ボタンをクリックします。



非アクティブ化したエンドポイントはエンドポイントプロテクション対して報告を行えなくなることを示す警告メッセージが表示されます。

4. [**はい**] をクリックするとエンドポイントにアンインストールコマンドが送信され、SecureAnywhere が削除されます。

SecureAnywhere が削除されると、エンドポイントは [非アクティブ化されたエンドポイント] グループに表示されます。7 日間が経過すると、状態が [*最近確認されていません*] に変わります。

> **注意：** [非アクティブ化されたエンドポイント] グループから自分でエンドポイントを完全に削除することはできません。このリストをクリーンアップして古いアイテムを削除する場合は、*ウェブルート テクニカルサポート*までご連絡ください。

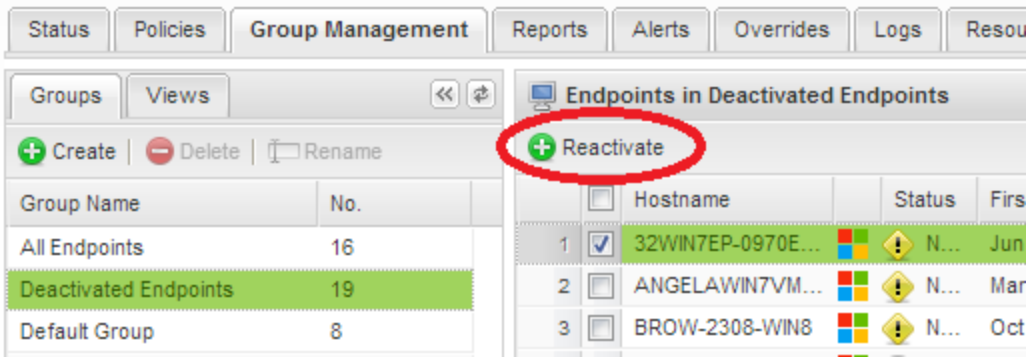
エンドポイントでの SecureAnywhere の再アクティブ化

[グループの管理] タブでエンドポイントを非アクティブ化する場合は、必要に応じて後から再アクティブ化することができます。

エンドポイントを再アクティブ化するには

1. エンドポイントに SecureAnywhere を再インストールします。
2. 管理ポータルを開き、[**グループの管理**] タブをクリックします。
3. [非アクティブ化されたエンドポイント] グループで目的のエンドポイントを選択します。

4. コマンド バーの [**再アクティブ化**] ボタンをクリックします。



エンドポイントが以前のグループに戻されます。

SecureAnywhere のアンインストール

以下のいずれかの方法で、エンドポイントから SecureAnywhere プログラムを削除することができます。

- エンドポイントを非アクティブ化し、エンドポイントプロテクションに報告しないようにします。必要に応じて、後からエンドポイントを再アクティブ化することができます。

  エンドポイントを非アクティブ化することにより、ライセンスシートを解放して別のエンドポイントをインストールすることができます。詳細については、「*エンドポイントの非アクティブ化 ページ199*」を参照してください。

- 管理ポータルからアンインストールコマンドをエンドポイントに送信します。この方法では、エンドポイントは管理ポータルに表示されたままになります。

  SecureAnywhere をアンインストールしてライセンスのシートを解放するには、エンドポイントを非アクティブ化します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

第 5 章: 状態の確認

状態を確認する方法については、以下のトピックを参照してください。

エンドポイントの状態の表示

管理ポータルですべてのエンドポイントの状態を確認できます。SecureAnywhere によるスキャン時、またはポーリング間隔の終了時に、エンドポイントから状態が報告されます。

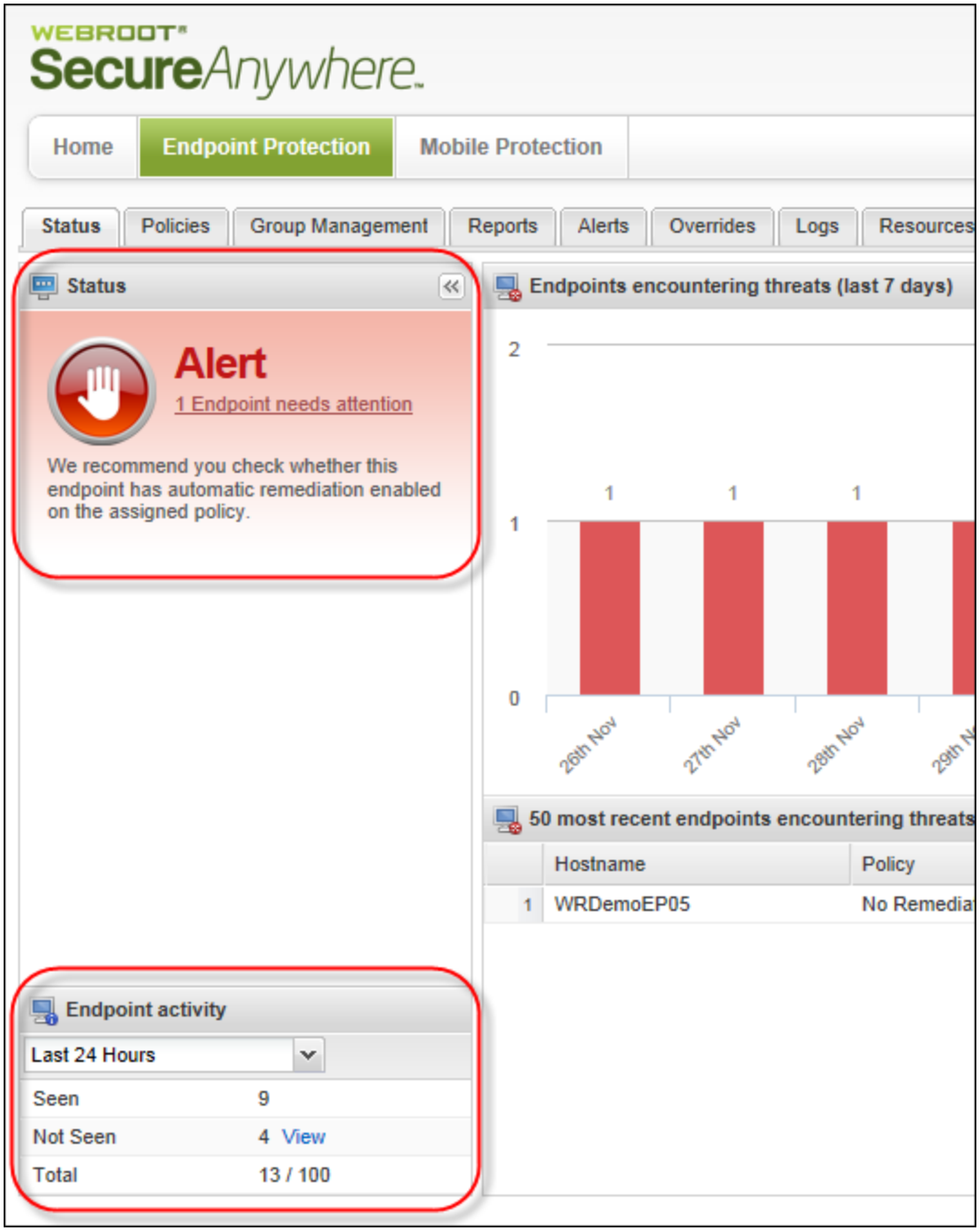
注意: エンドポイントのスキャン履歴の詳細については、「*スキャンの結果確認と脅威の管理 ページ 171*」を参照してください。

エンドポイントの状態を表示するには

1. SecureAnywhere の Web サイトにログインします。
2. [**エンドポイントプロテクションに進む**] ボタンをクリックします。

3. 感染しているエンドポイントがある場合、そのエンドポイントへのリンクをクリックして詳細パネルに直接進むことができます。

4. 管理ポータルが表示されたら、左側の [状態] パネルと [エンドポイントのアクティビティ] パネルでエンドポイントの状態を確認します。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Mobile Protection
Status
Policies
Group Management
Reports
Alerts
Overrides
Logs
Resources
Status
Alert
1 Endpoint needs attention
We recommend you check whether this endpoint has automatic remediation enabled on the assigned policy.
Endpoints encountering threats (last 7 days)
2
1
0
1
1
1
26th Nov
27th Nov
28th Nov
50 most recent endpoints encountering threats
Hostname
Policy
1
WRDemoEP05
Endpoint activity
Last 24 Hours
Seen 9
Not Seen 4 View
Total 13 / 100

5. 2 つのパネルでは、以下のいずれかの操作で、さらに詳細を確認できます。

   - [状態] パネルに警告メッセージが表示された場合は、リンクをクリックしてエンドポイントに関する詳細情報を表示できます。

   - どのエンドポイントからもポータルに報告がない場合は、[エンドポイントのアクティビティ] パネルの [未確認] 行にある [**表示**] リンクをクリックします。

6. エンドポイントは [状態] タブと [グループの管理] タブで確認できます。[グループ管理] タブの詳細については、「*エンドポイントをグループに整理 ページ330*」を参照してください。

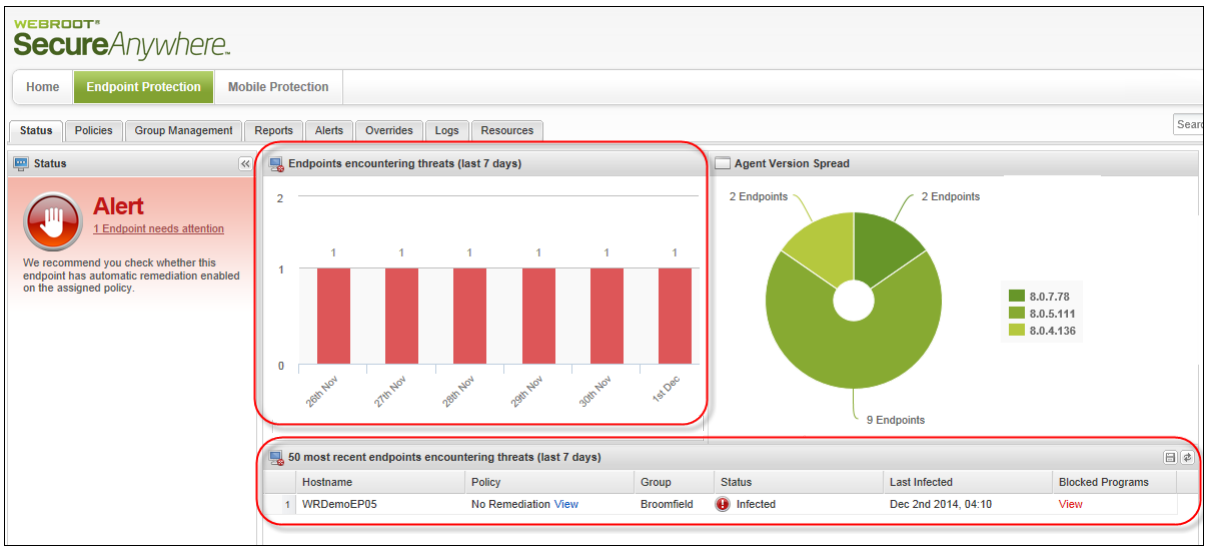
脅威の最新状況の表示

[状態] タブで、過去 1 週間に脅威を報告したエンドポイントを素早く表示できます。

脅威の最新状況を表示するには

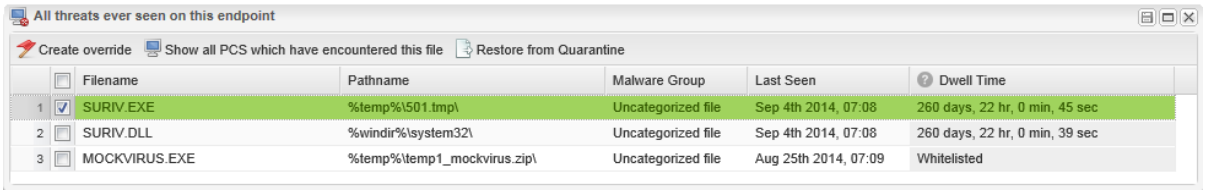
1. [**状態**] タブをクリックします。

   上部にある棒グラフは、エンドポイントで検出された脅威を示した日別概要です。パネル下部にある表には、それらのエンドポイントに関する詳細な情報が表示されます。



2. 脅威の詳細を確認するには、その脅威の行の [ブロックされたプログラム] カラムで [**表示**] リンクをクリックします。

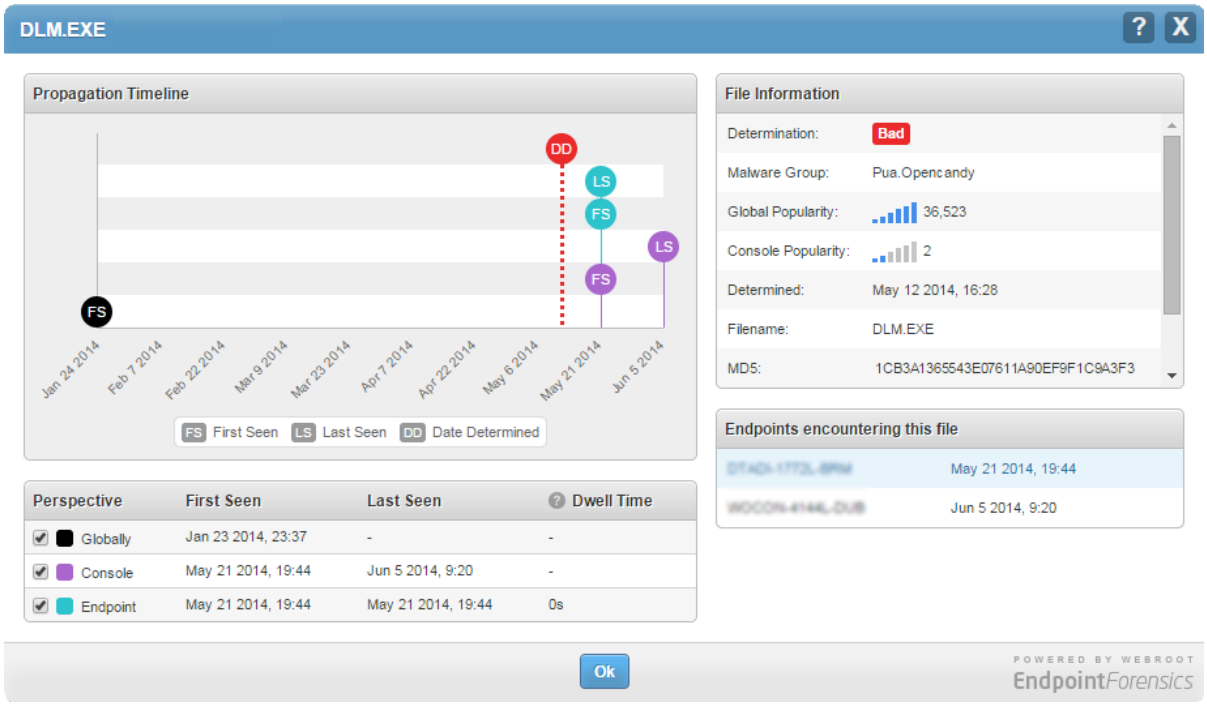
   ブロックされたプログラムが表示されます。



注意: 滞留時間の詳細については、「*滞留時間について*」を参照してください。

3. 最近感染したエンドポイントについての追加データを下部のパネルに表示したり、非表示にしたりできます。カラム見出しをクリックしてドロップダウンメニューを開き、カラムを追加する場合はチェックボックスを選択し、カラムを削除する場合はチェックボックスの選択を解除します。
4. カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。
5. 脅威や未判定のファイルタイプによるリスクについての追加情報を表示するには、ファイル名をクリックします。

   ファイルインテリジェンスのビューが表示されます。



このビューの各フィールドの詳細については、以下の表を参照してください。

フィールド	説明
判定	判定にマウスカーソルを合わせると、エージェント、ルール、クラウドに関する情報が表示されます。
グローバル頻度	WIN が初めて (FS) ファイルを確認した際の情報と、そのグローバル頻度 (他のユーザーにより確認された頻度) が表示されます。
Google 製品 / ベンダーリンク	リンクをクリックすると、ファイルの追加情報にアクセスできます。これは、分類が不明な場合に便利です。
オーバーライドの作成	このボタンをクリックすると、ファイルをオーバーライドして、ホワイトリストまたはブラックリストを作成できます。
コンソール頻度	コンソール内でファイルが確認された回数と時刻を表示します。
コンソール滞留時間	コンソール内でファイルが確認された回数と時間の長さを表示します。.
エンドポイント滞留時間	問題のデバイスでファイルが確認された時間の長さを表示します。

6. 脅威および追加オプションの詳細については、[最新のスキャンで脅威が存在したエンドポイント] レポートを作成して確認してください。このレポートから、エンドポイントのポリシーの変更、スキャンの実行、ファイルのオーバーライドの作成、隔離されたファイルの復元を実行できます。

詳細については、「*[最新のスキャンで脅威が存在したエンドポイント] レポートの生成 ページ361*」を参照してください。

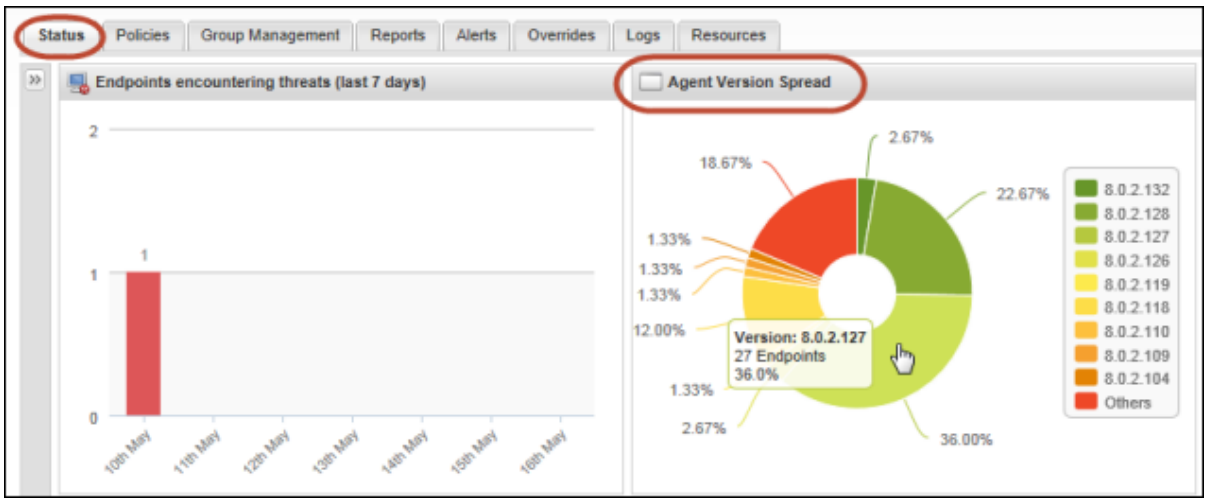
エージェントのバージョンの概要表示

[状態] タブにあるエージェントのバージョンの円グラフは、エンドポイントにインストールされた SecureAnywhere バージョンの概要を示しています。エージェントとは、エンドポイントで実行されている SecureAnywhere ソフトウェアです。

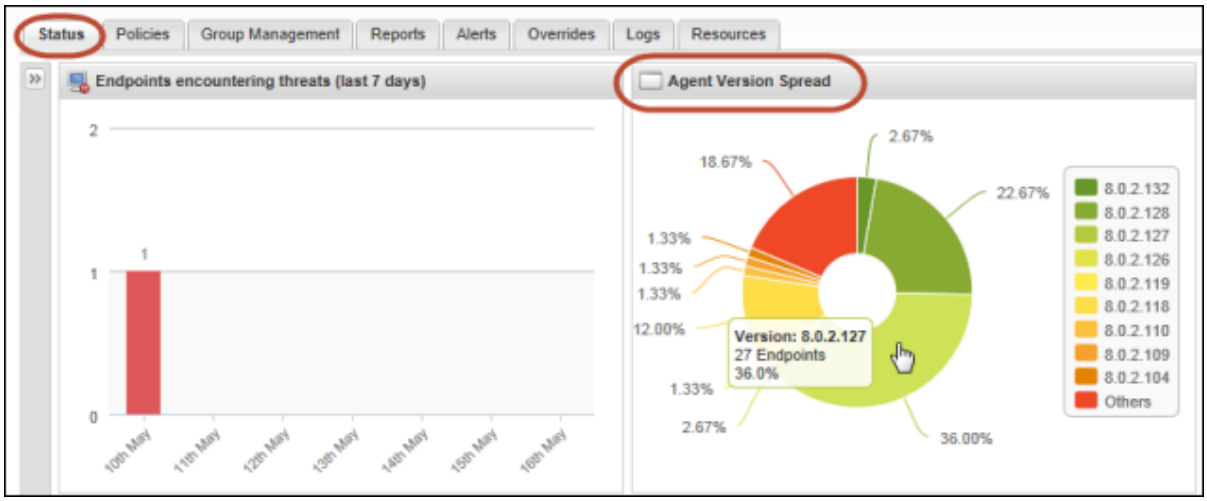
エージェントのバージョンの円グラフを表示するには

1. [**状態**] タブをクリックします。

   [状態] パネルが表示され、その右側にエージェントのバージョンの円グラフがあります。



2. 詳細を確認するには、カーソルを円グラフの各セクションに合わせます。



3. 詳細については、「*[エージェントのバージョンの使用状況] レポートの生成 ページ390*」を参照してください。

滞留時間について

ウェブルートは、複数の保護メカニズムを備えた、市場最軽量のエージェントを提供しています。エージェントは、最新の脅威に対して優れた保護機能を発揮します。

ウェブルートインテリジェンスネットワークでは 1 日に何百万ものイベントを処理し、ソリューションの検出能力を向上させています。デバイス上のすべてのマルウェアを初見で把握することは業界のどの企業にとっても困難です。ウェブルートでは別な方法で高い保護機能を実現しています。

2014 年、ウェブルートは、ガートナー社のマジッククアドラントで "滞留時間を確認する能力を持つ*唯一*のベンダー" と評価されました。

ウェブルートは、ユーザーが悪意のあるイベントに関してできる限り多くの状況を把握できるように、フォレンジック機能の導入を続けています。他のイベントベースのソリューションでレポートされるようなノイズは排除されます。

アプリケーションが未分類の場合

エージェントは未分類のアプリケーションに対して、ディスクで行われた変更を記録します。その際、永続的な変更は行われません。アプリケーションが不正として分類された場合、そのアプリケーションによって行われた記録変更をロールバックし、PC を修復します。この手法は、ウェブルートで分類が済んでいないマルウェアに対して、セーフティネットとして機能します。ID シールドなどのコンポーネントも併せて使われます。

滞留時間とは

- 滞留時間とは、脅威がデバイス上に存在していた時間です。ファイルが最初にアクティブになった時から、ファイルが最後に確認されるまでの期間で計算されます。
- ゼロ (0) 秒の滞留時間は、そのファイルが初見でブロックされたことを意味します。

滞留時間がゼロ (0) 秒より長いということは、ウェブルートが削除する前に、そのファイルがシステムに一定時間存在していたことを意味します。

滞留時間がゼロ (0) 秒を超える理由としては、ユーザーがクリーンアップ手順を完了していなかった、削除されたファイルが再びシステムに作成された、ファイルが最初は悪意のある振舞いをしていなかったためすぐに悪意があると分類されなかった、などが挙げられます。

Webroot SecureAnywhere は常にシステムを監視し、悪意がある可能性のあるファイルによって行われる変更を記録します。その後、変更をロールバックします。また、滞留時間の長さにかかわらずシステムを確実に悪意のある攻撃から保護するため、他の保護メカニズムも採用しています。

ウェブルートが最初にすべての分類を行わない理由

初見で各ファイルをブラックリスト化するモデルは実現不可能です。脅威と戦う唯一の方法は、デバイスで行われるすべての変更を監視して、その変更をロールバックできるようにすることです。これが競合他社に対するウェブルートの差別化要因になっています。

滞留時間が表示される場所

導入の最初の段階では、滞留時間はすべてのレポートと、コンソールの感染を確認できるエリアに表示されます。以降の段階では、電子メールアラートや、特定の滞留時間レポート、概要などで確認できます。

エンドポイント プロテクションからの CSV ファイルのエクスポート

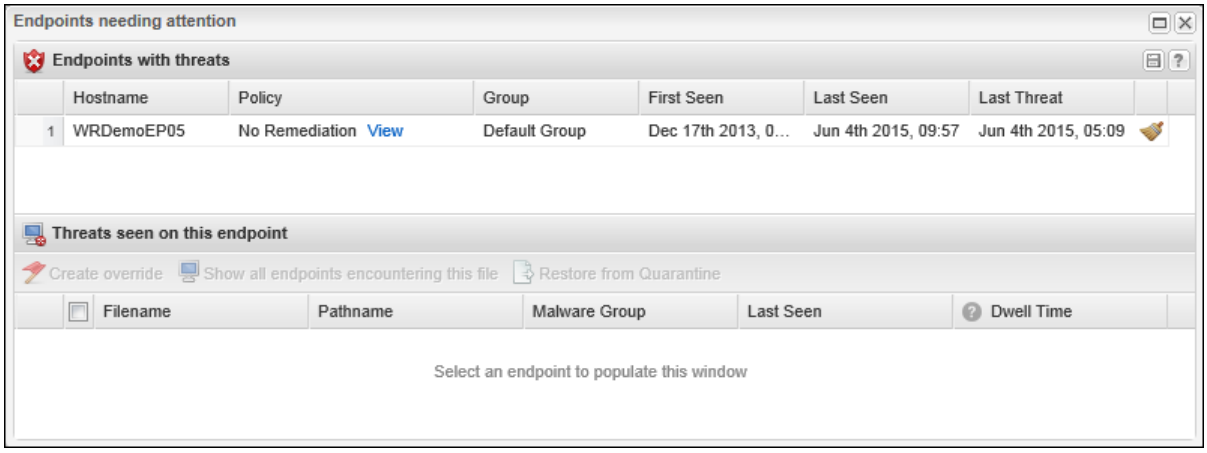
このセクションの手順に従うと、対応が必要なエンドポイントの情報が含まれる CSV ファイルをエクスポートできます。CSV ファイルを保存しておくと、必要に応じて後から参照したり共有したりできます。

CSV へのエクスポート用のアイコンが表示されていれば、この機能を使用できます。

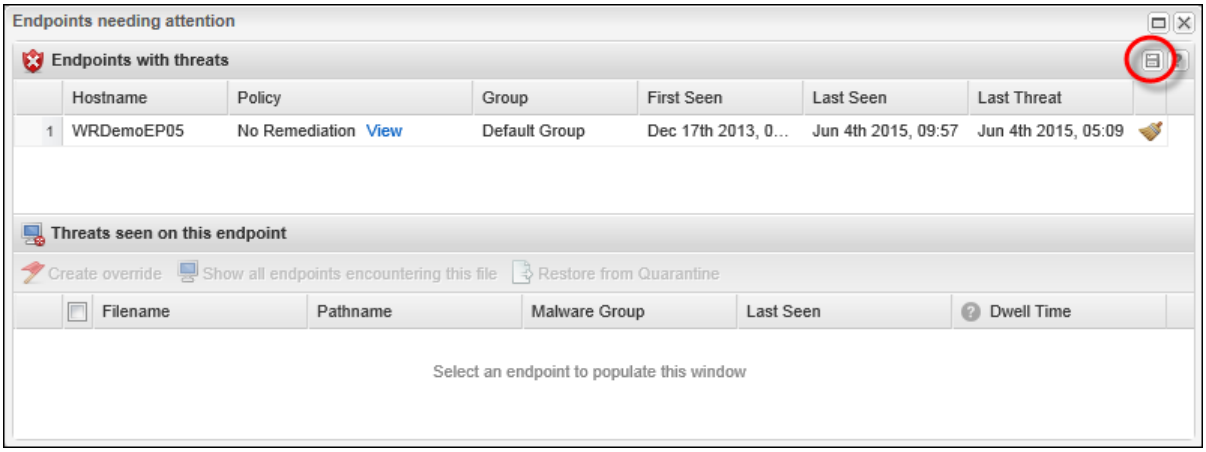
エンドポイント プロテクションで CSV ファイルをエクスポートするには

1. エンドポイントプロテクションで [**状態**] タブをクリックします。
2. [状態] エリアで [**エンドポイントに対応が必要です**] というリンクをクリックします。

対応が必要なエンドポイントのウィンドウが表示されます。

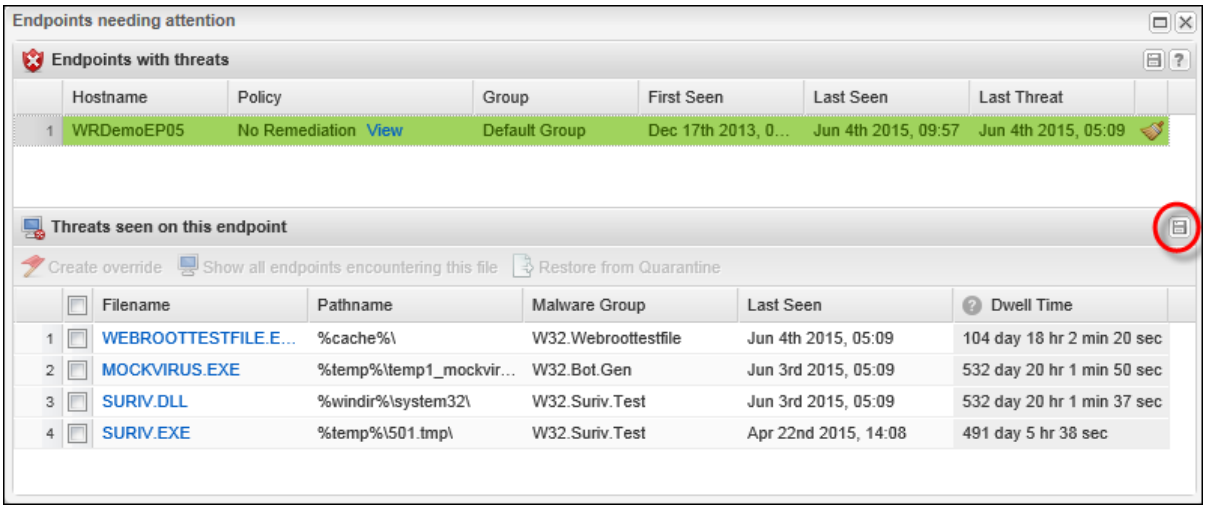


3. 以下のいずれかの操作を行います。
   - [脅威が存在したエンドポイント] の情報をエクスポートするには、右上の **CSV へのエクスポート** 用のアイコンをクリックします。

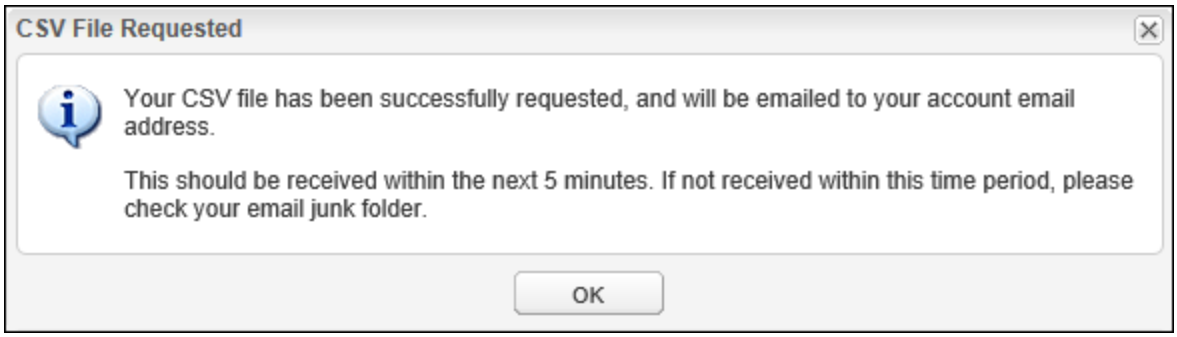


   - [このエンドポイントで確認された脅威] の情報をエクスポートするには、エンドポイントを選択して [このエンドポイントで確認された脅威] 内に情報を表示してから必要な項目を選択し、**CSV へのエク**

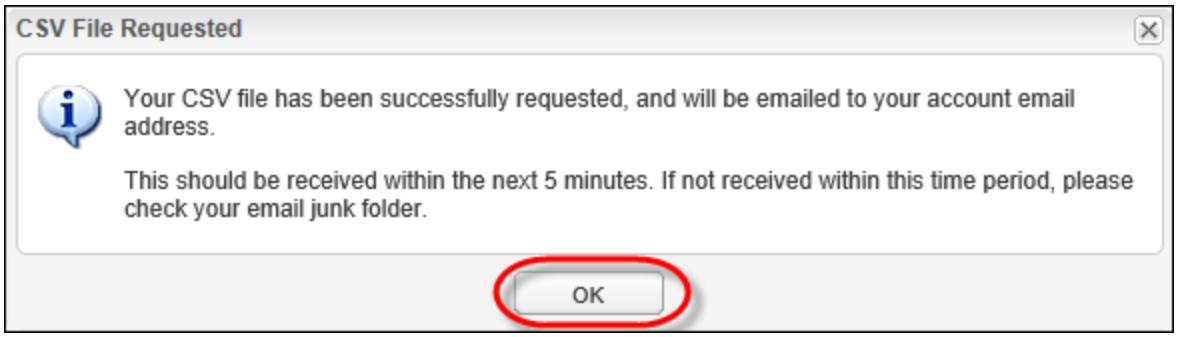
スポート 用のアイコンをクリックします。



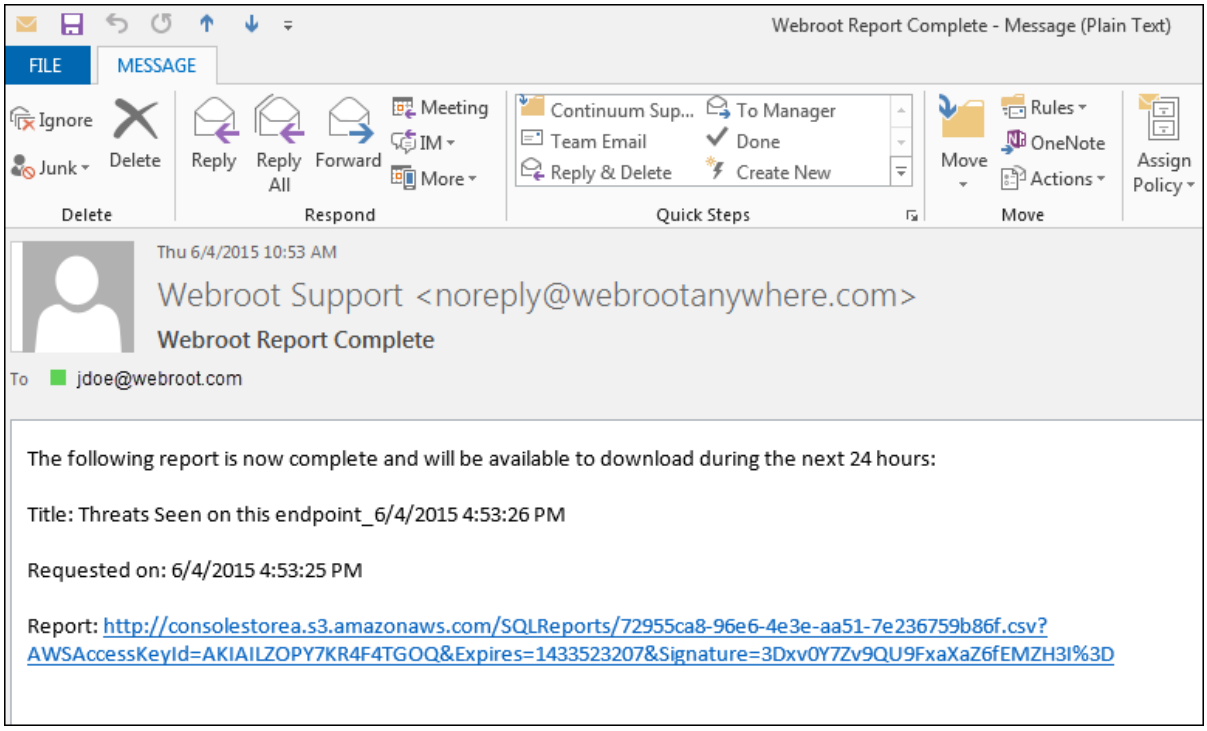
CSV ファイルがリクエストされたことを示すメッセージが表示されます。



4. [**OK**] ボタンをクリックしてウィンドウを閉じます。



ログインに使用した電子メールアドレス宛てにリンクが送信されます。s



5. CSV ファイルを表示するには、電子メールで届いたリンクをクリックします。その後、このファイルをコンピュータに保存できます。

第 6 章: ポリシーの管理

ポリシーの管理方法については、以下のトピックを参照してください。

ポリシーの導入

エンドポイントプロテクションの初期設定では、デフォルトのポリシーが選択されています。ポリシーは、スキャンのスケジュールやシールドの動作など、エンドポイントにおける SecureAnywhere の設定を定義します。

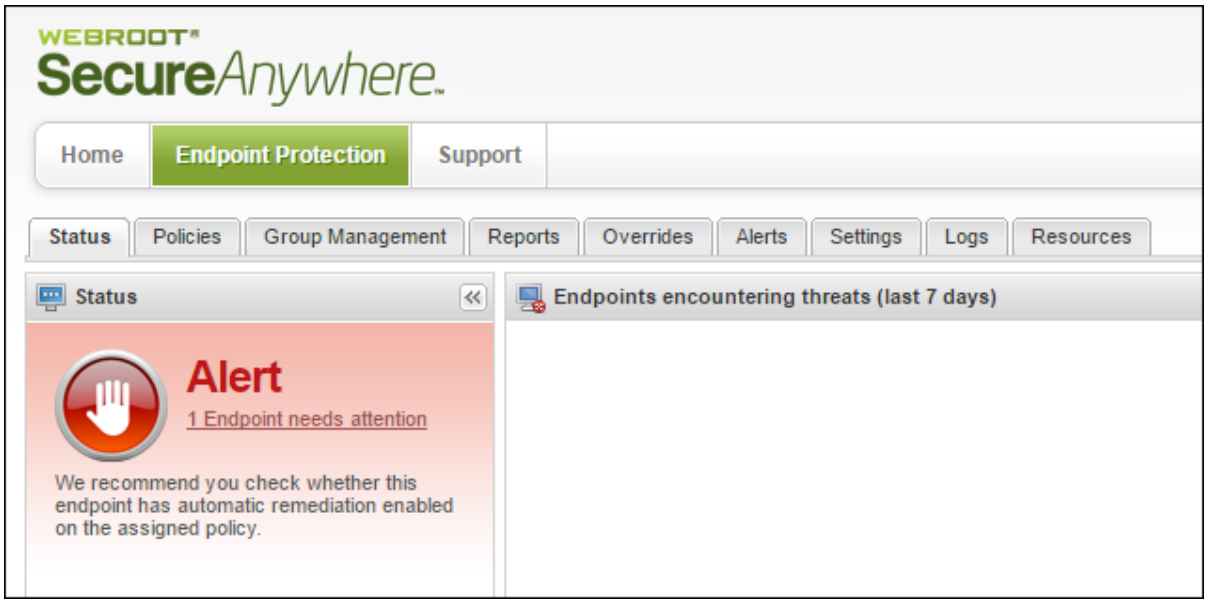
選択したデフォルトのポリシーの使用を続けるか、その他のポリシーを定義してエンドポイントに割り当てることができます。たとえば、システム管理者に対してその他の社員よりも多くの権限を与える必要がある場合があります。そのような場合は、管理者用に新しいポリシーを作成し、その他の社員に対してはデフォルトのポリシーを継続して適用することができます。

注意: ポリシーを完全に導入するには、[ポリシー] の [作成・編集] および [ポリシー] の [エンドポイントへのポリシーの割り当て] へのアクセス権限が必要です。アクセス権限の変更に関しては、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

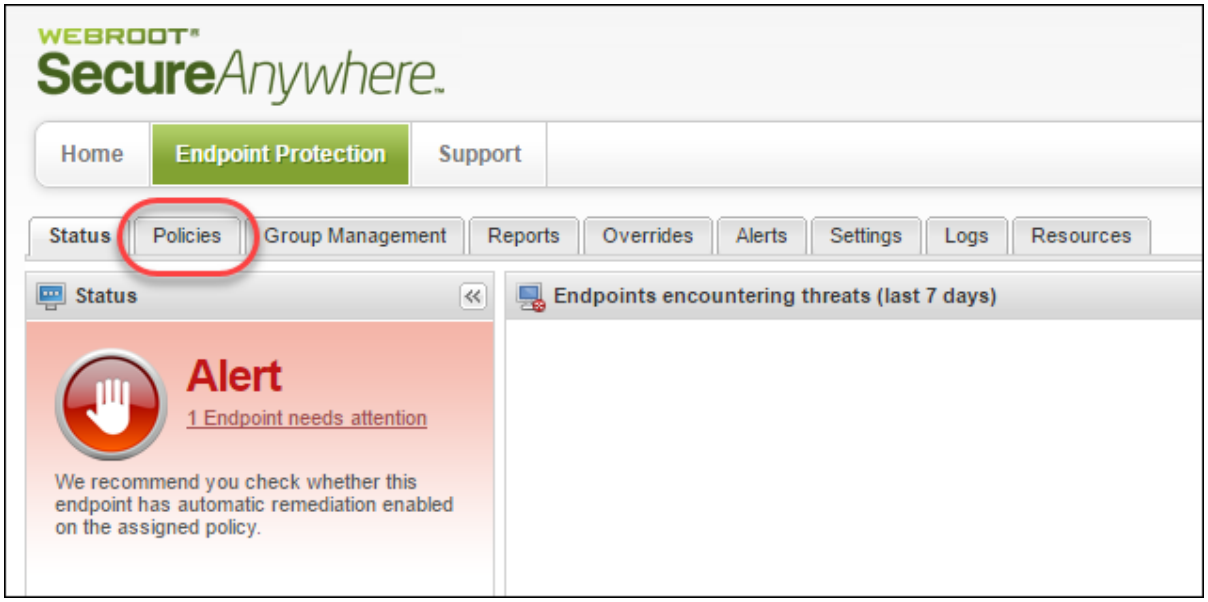
ポリシーを導入するには

1. エンドポイントプロテクションのコンソールにログインします。

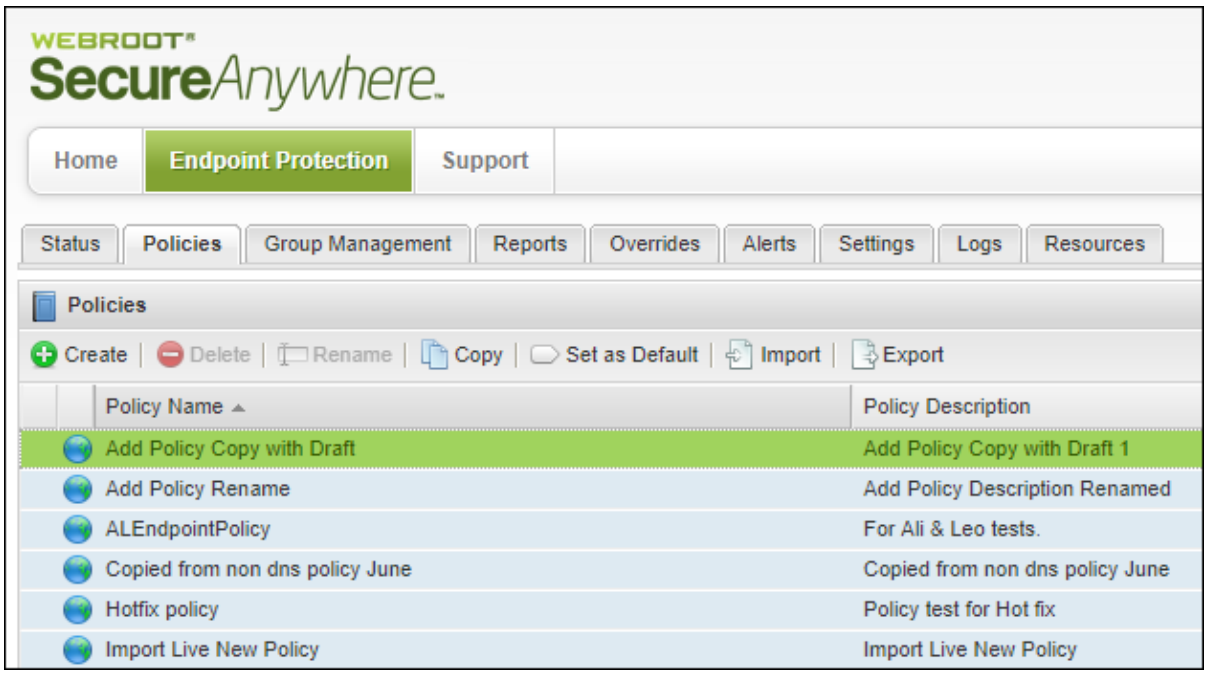
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



2. [**ポリシー**] タブをクリックします。

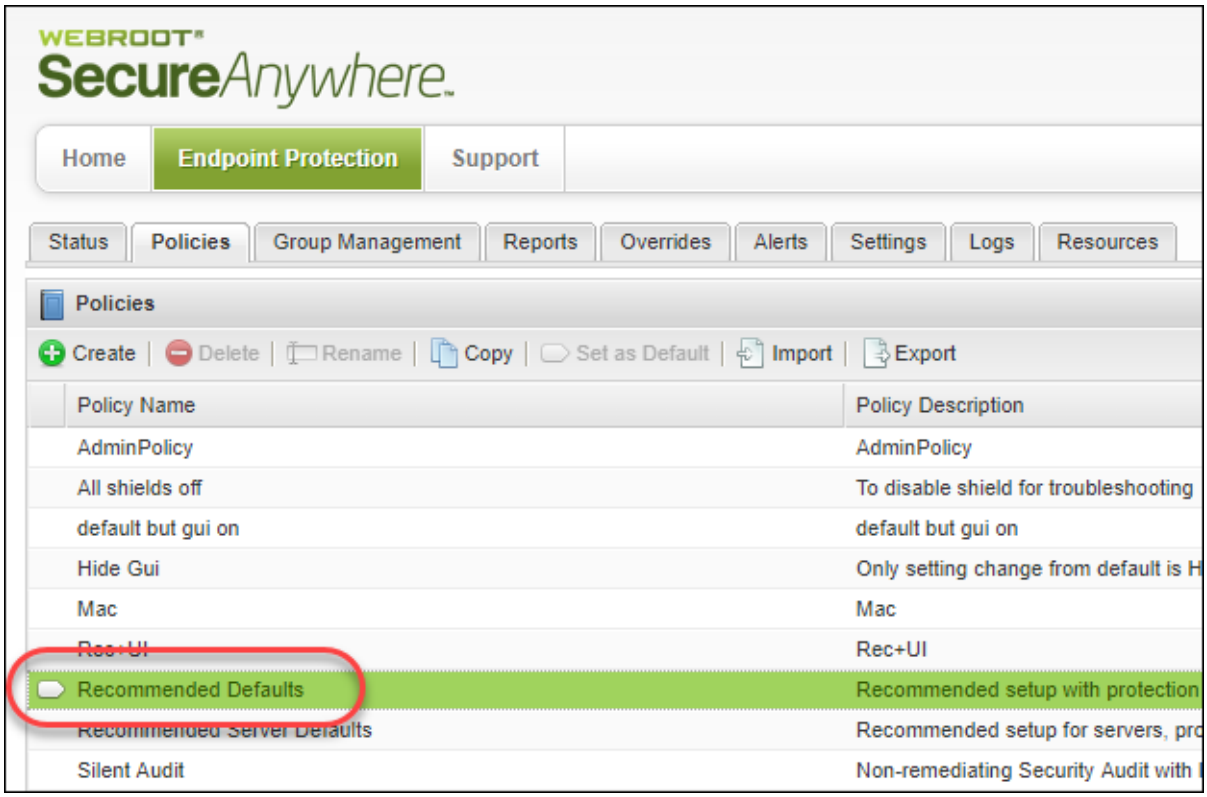


[ポリシー] タブが表示されます。

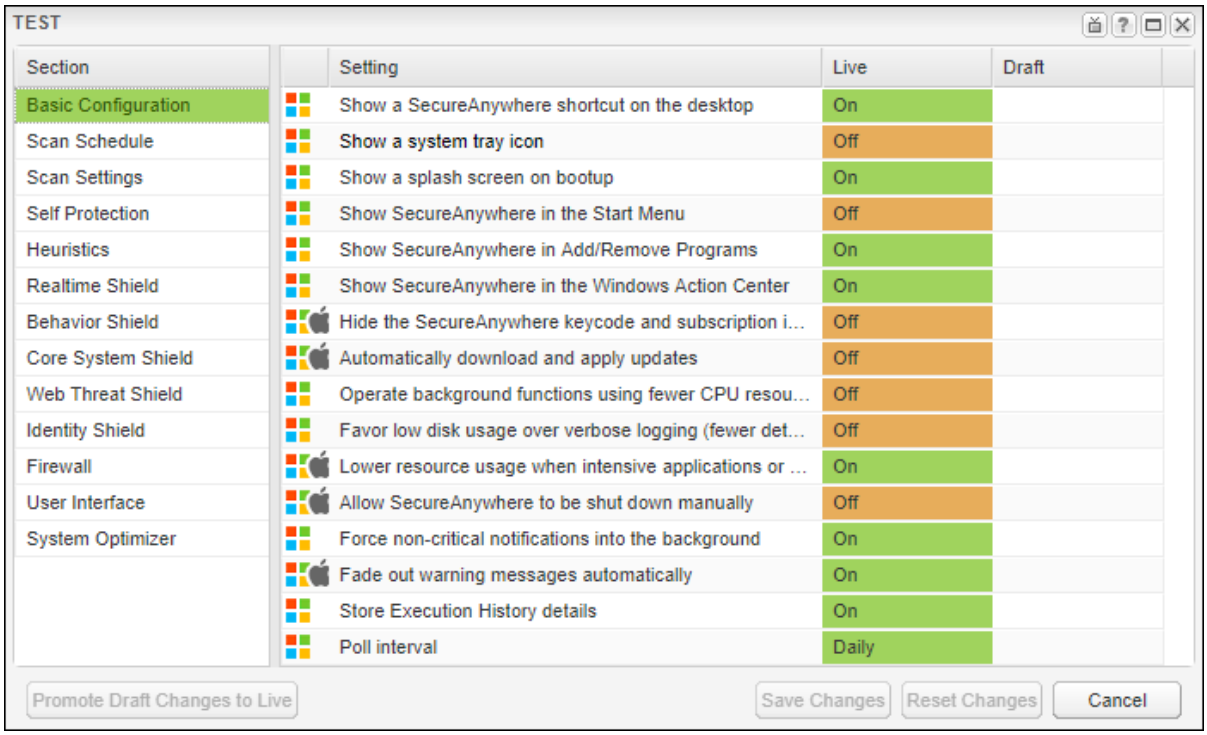


3. デフォルトのポリシーの使用を継続するかどうかを決定します。

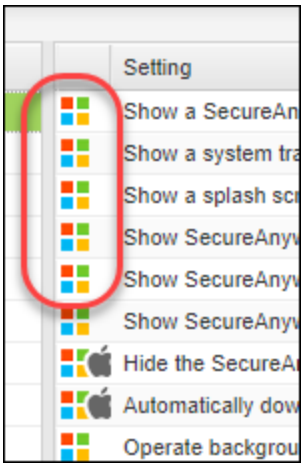
   デフォルトのポリシーはペインの左側にあり、白い水平の矢印で示されています。



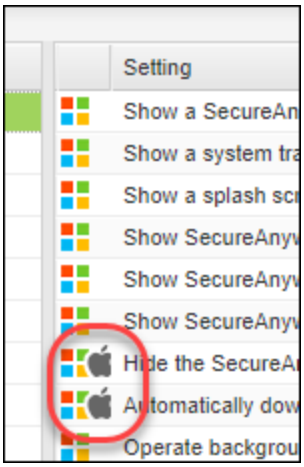
4. デフォルトのポリシー名をダブルクリックして設定を表示します。



- Windows PC のみに適用される設定には、Windows のアイコンが表示されます。



- Windows PC と Mac に適用される設定には、Windows アイコンと Mac アイコンの両方が表示されます。



注意: 非管理ポリシーの設定は、管理者ではなく、エンドポイントユーザーが権限を持つよう指定されているため、表示されません。

5. ポリシーの設定を確認して、デフォルトのポリシーがビジネス要件を満たしているかどうかを判断します。満たしていない場合、ウェブルートのデフォルトは修正できないため、新しいポリシーを作成する必要があります。

   詳細については、「*ポリシーの作成 ページ233*」を参照してください。

6. 新しいポリシーを作成したら、[グループ管理] タブのエンドポイントに割り当てることができます。

   詳細については、「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

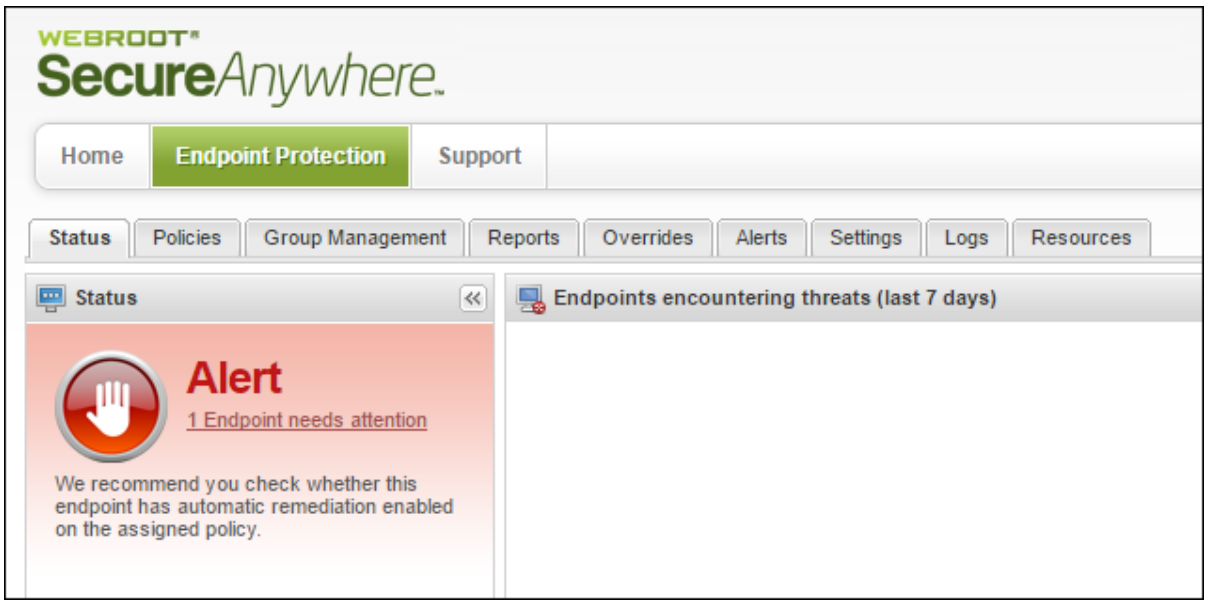
新しいデフォルトのポリシーの選択

SecureAnywhere が新しいエンドポイントにインストールされる場合は必ず、エンドポイントプロテクションによってデフォルトのポリシーに割り当てられます。必要に応じて、将来インストールするエンドポイントに対しては異なるデフォルトのポリシーを設定することができます。

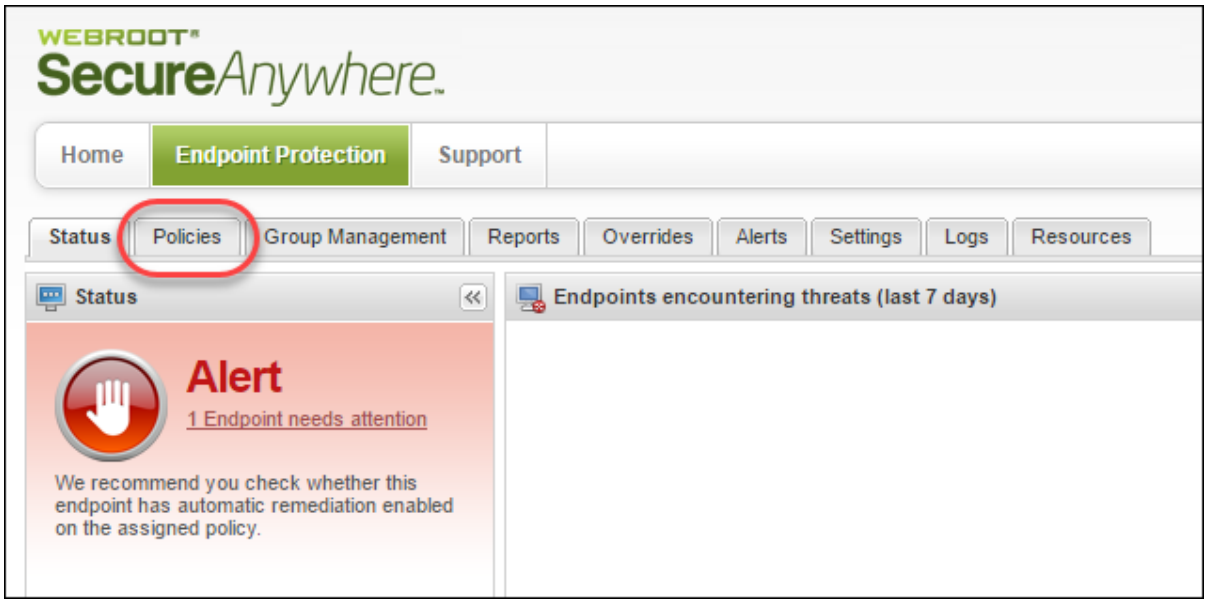
新しいデフォルトのポリシーを選択するには

1. エンドポイントプロテクションのコンソールにログインします。

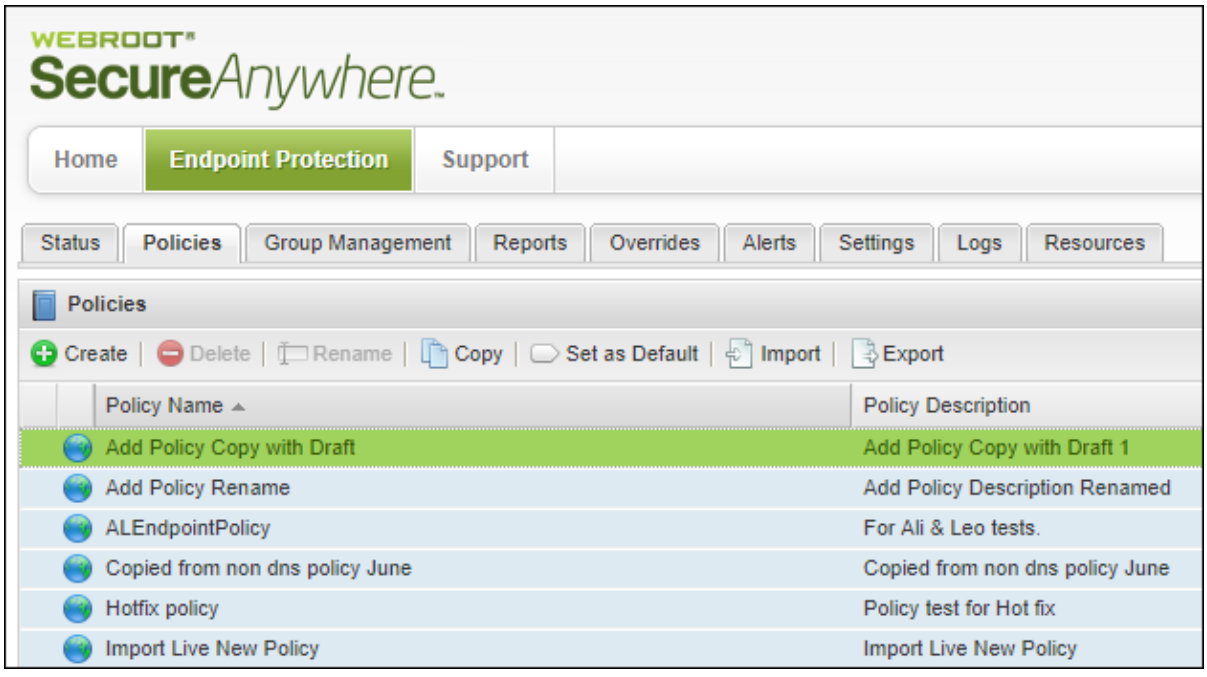
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



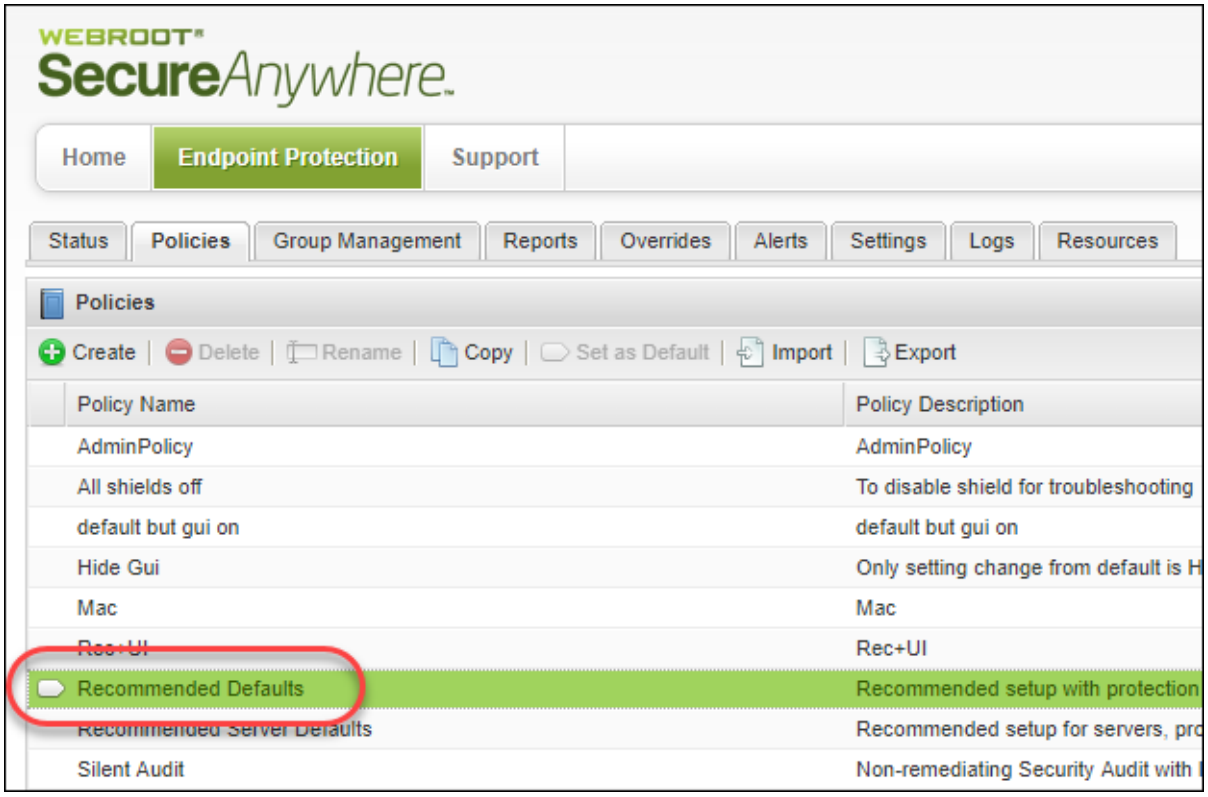
2. [**ポリシー**] タブをクリックします。



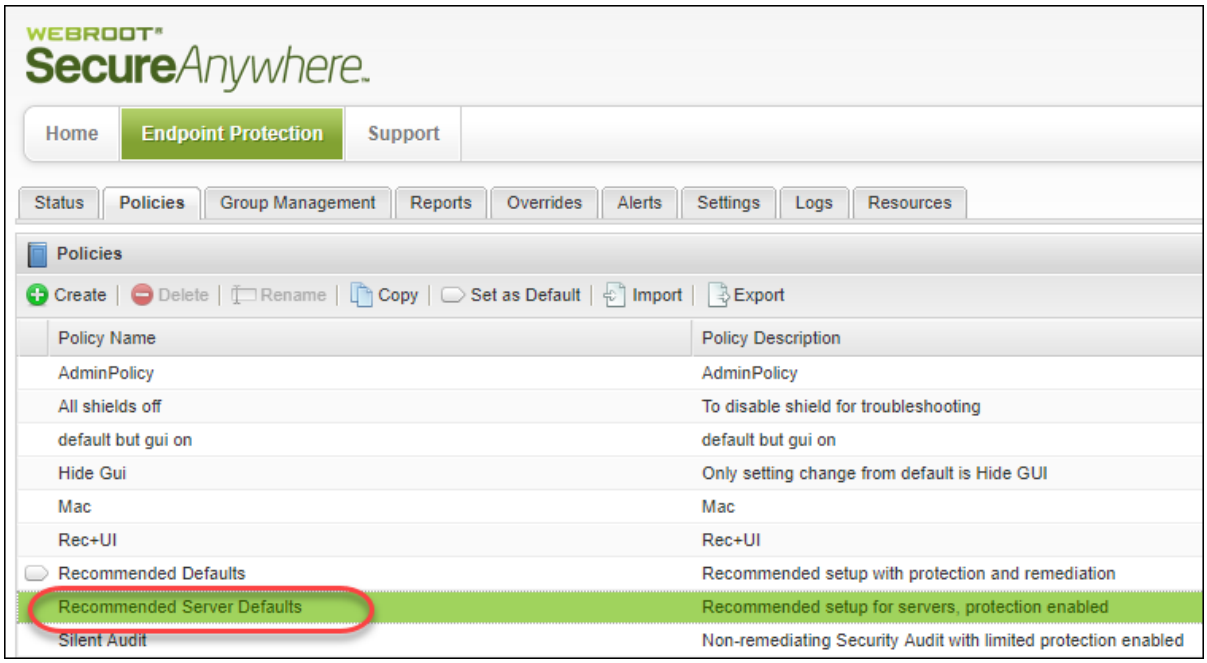
[ポリシー] タブが表示されます。



デフォルトのポリシーはペインの左側にあり、白い水平の矢印で示されています。

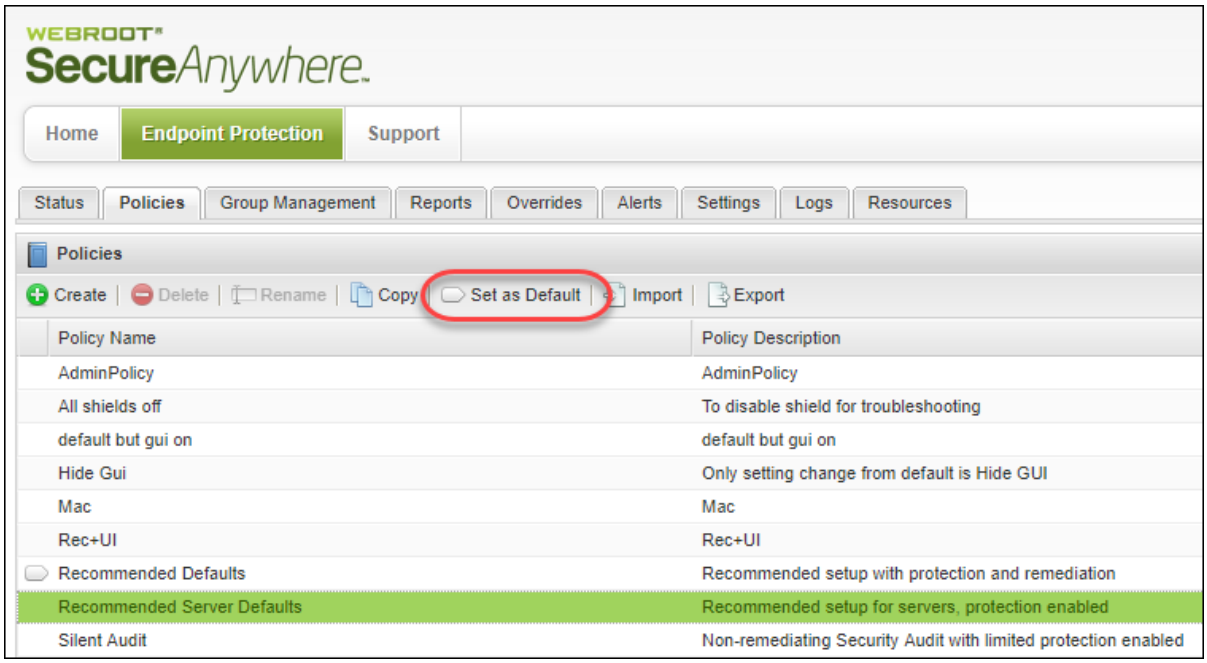


3. [ポリシー名] カラムで、新しいデフォルトとして使用するポリシーをクリックします。

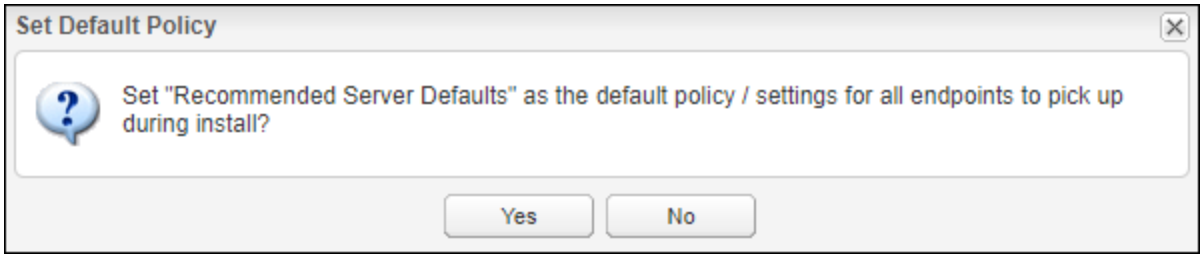


[デフォルトに設定] アイコンがアクティブになります。

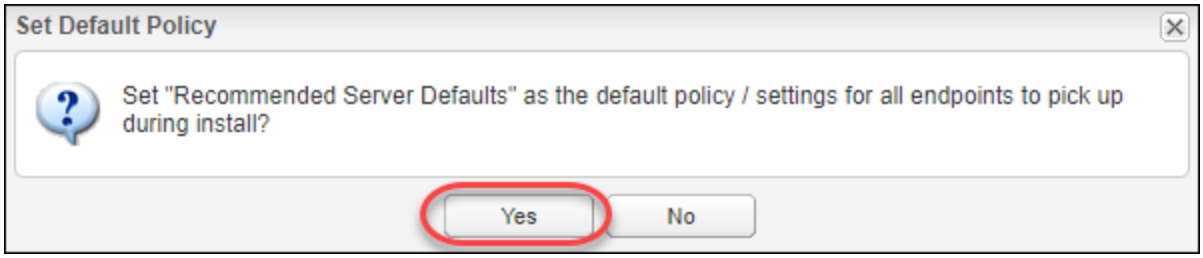
4. [**デフォルトに設定**] アイコンをクリックします。



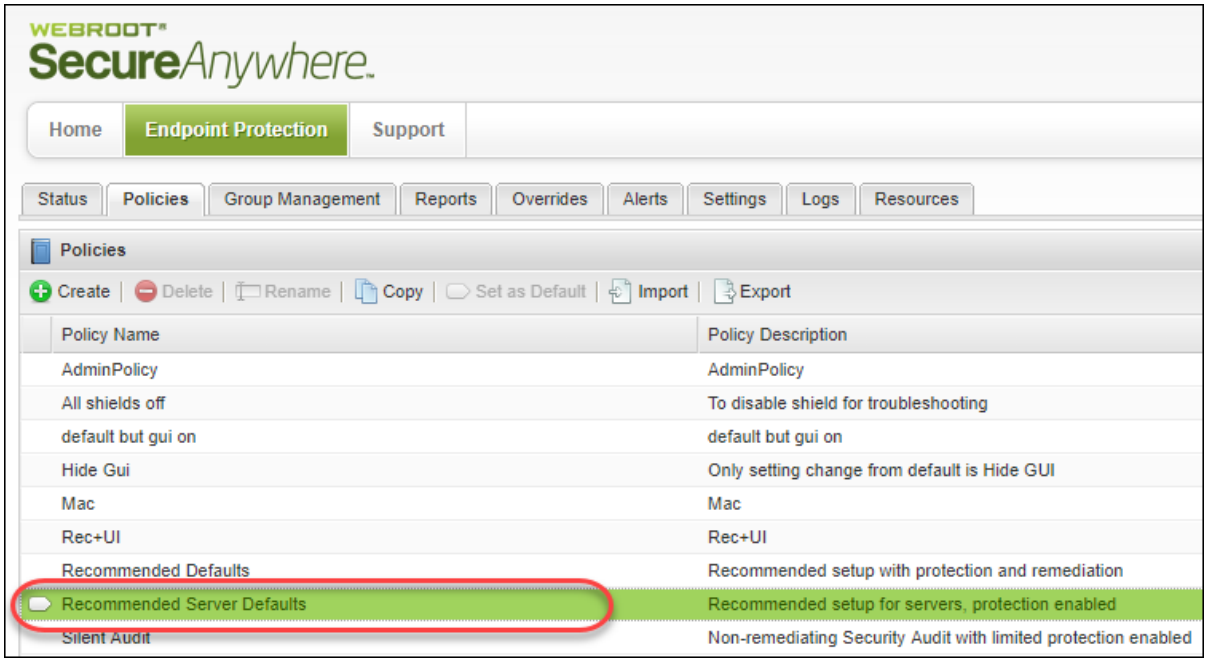
[デフォルトのポリシーを設定] ウィンドウが表示されます。



5. [**はい**] ボタンをクリックします。



白い矢印が新しいデフォルトのポリシーに移動し、このポリシーが SecureAnywhere の新しいインストールすべてに適用されるようになります。



ポリシーの作成

ポリシーを追加するには、新しいポリシーを作成するか、既存のポリシーをコピーして使用します。以下は、それぞれの手順についての説明です。ポリシー名を定義して説明を入力すると、ポリシー設定を指定できるようになります。詳細については、「*ポリシー設定の変更 ページ247*」を参照してください。

このトピックでは、次の手順について説明します。

- 新しいポリシーの作成
- ポリシーのコピー

注意: ポリシー名は一意のものである必要があるため、後で競合することがないよう、事前にポリシー名について考えておいてください。一度ポリシー名をつけると、そのポリシーを削除した後でも同じ名前を再利用することはできません。

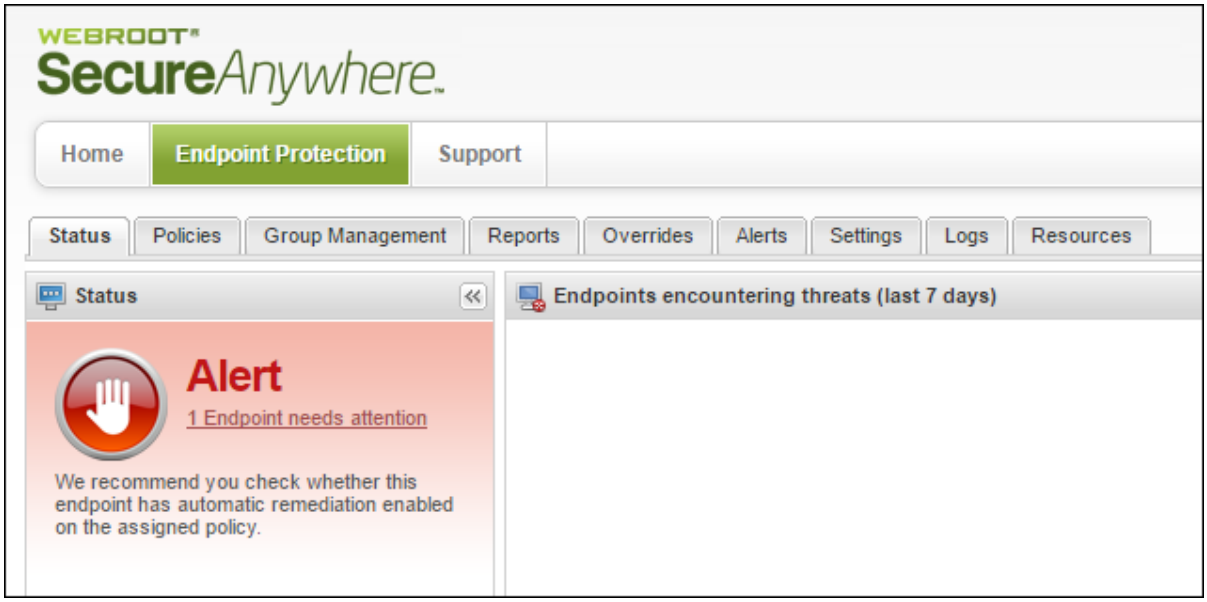
ポリシーの作成

名前と説明を指定し、新規ポリシーを作成します。新規ポリシーでは推奨されているデフォルト設定が最初に選択されますが、設定は後で変更できます。

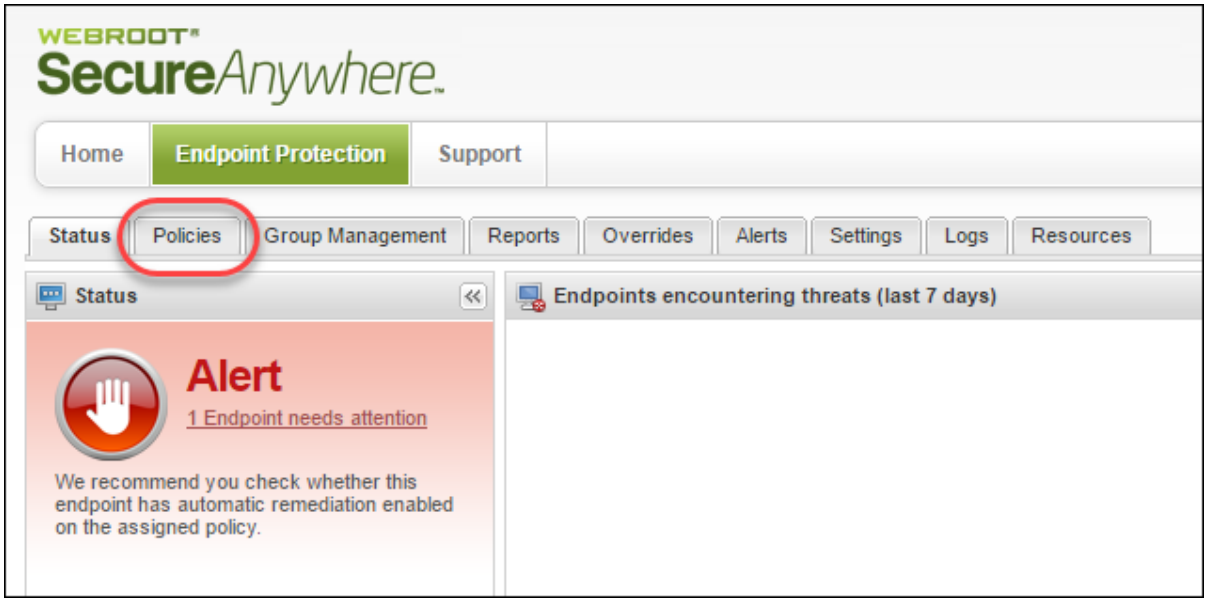
新しいポリシーを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

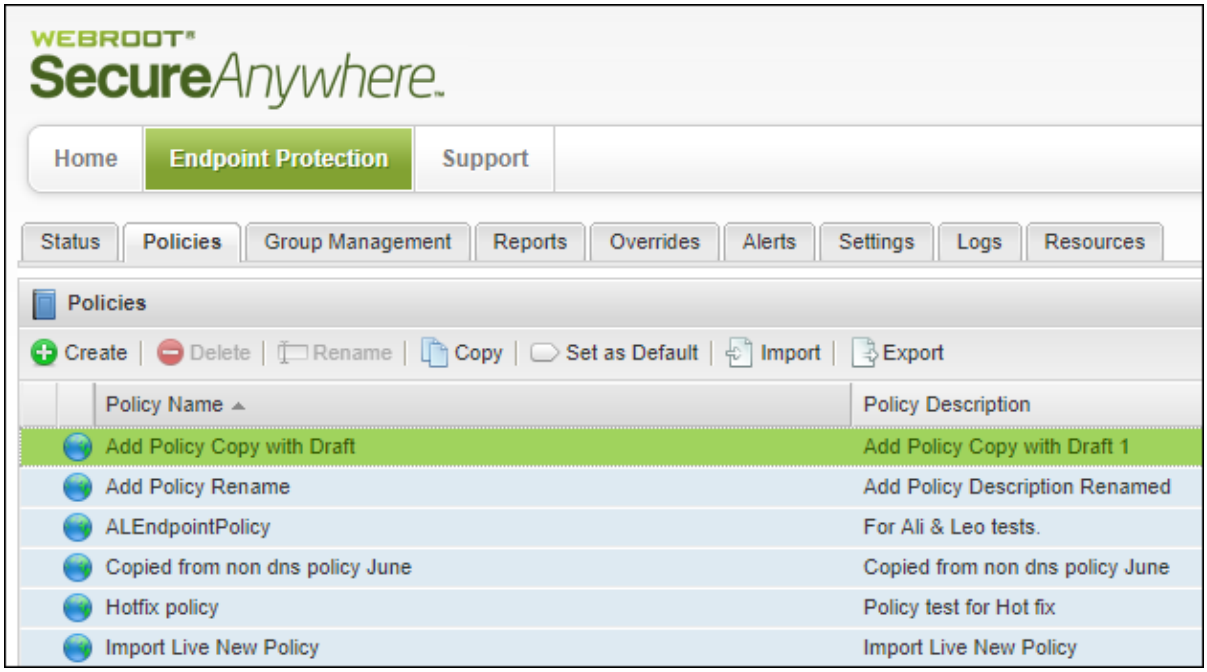
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



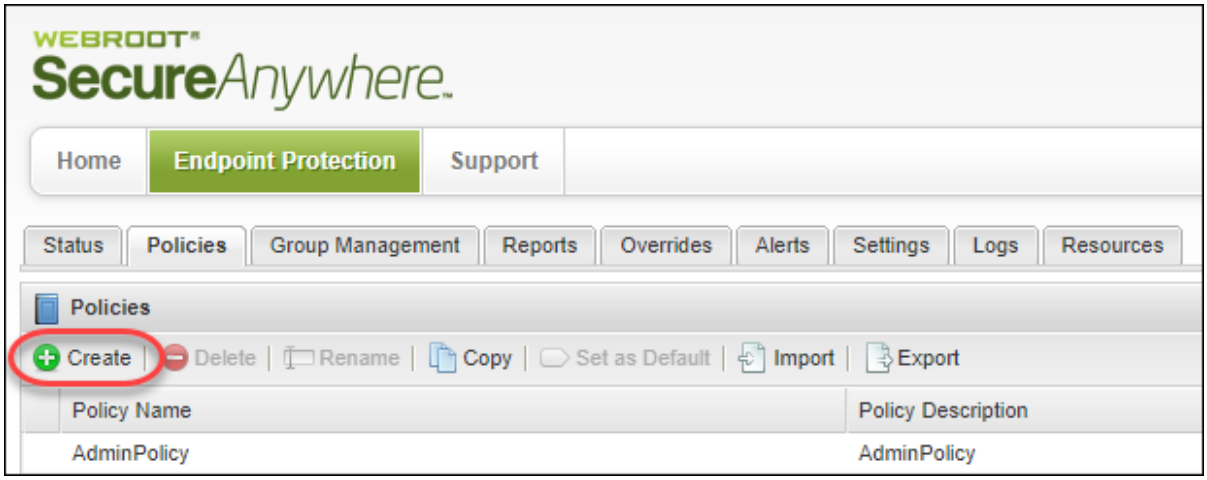
2. [**ポリシー**] タブをクリックします。



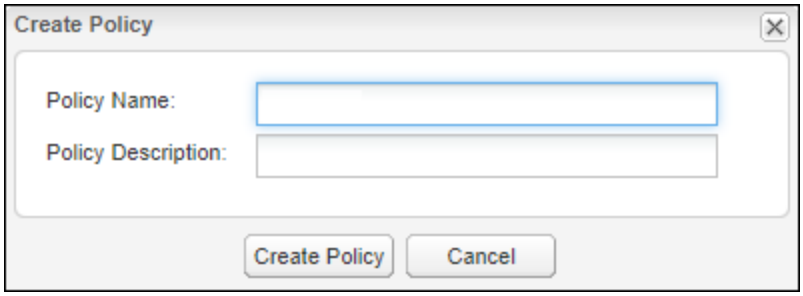
[ポリシー] タブが表示されます。



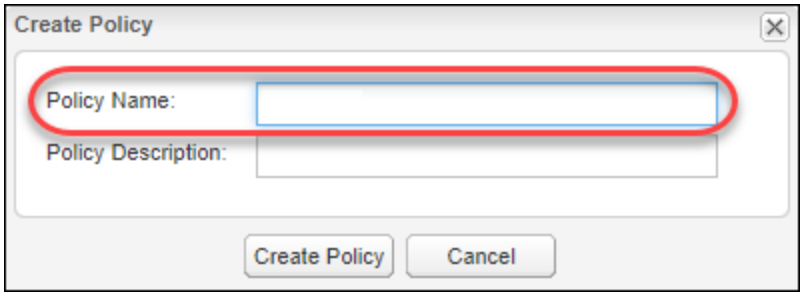
3. コマンド バーの [**作成**] ボタンをクリックします。



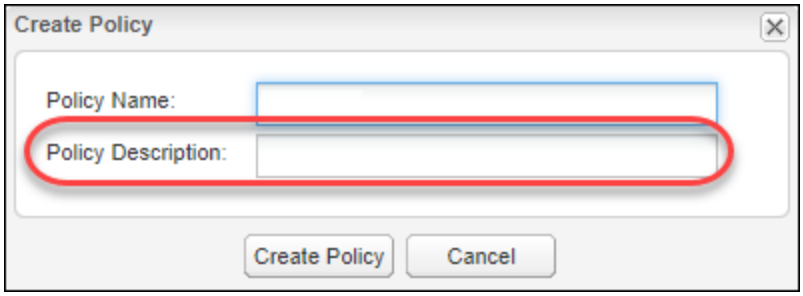
[ポリシーを作成] ウィンドウが表示されます。



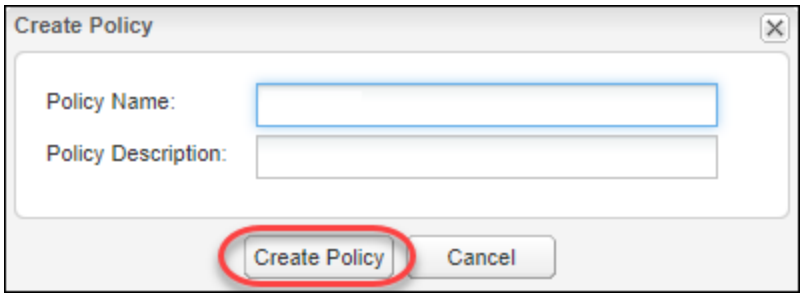
4. [ポリシー名] フィールドにポリシーの名前を入力します。



5. [新しいポリシーの説明] フィールドに、最大 50 文字 (英数字) で説明を入力します。



6. [**ポリシーを作成**] ボタンをクリックします。



7. [ポリシー名] カラムで、新しいポリシーを見つけます。

   以下のいずれかの操作を行います。

   - ポリシーをダブルクリックして設定を変更します。詳細については、「*ポリシー設定の変更 ページ247*」を参照してください。

   - ポリシーを、個々のエンドポイントまたはエンドポイントのグループに対して適用します。詳細については、「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

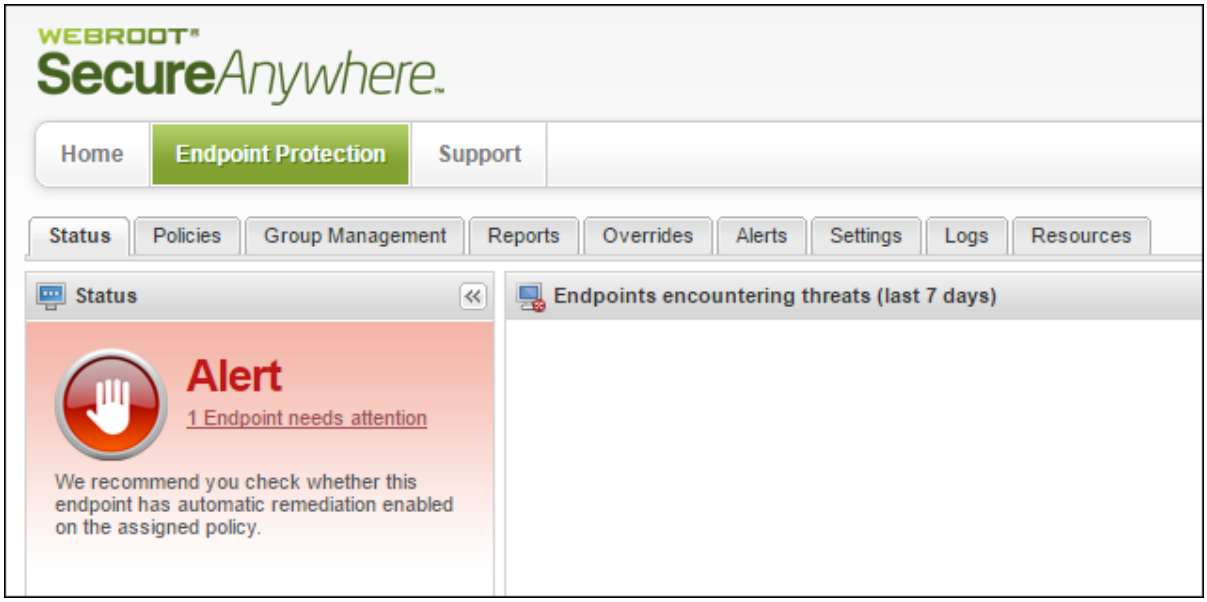
ポリシーのコピー

類似したポリシーをすでに定義している場合は、それをコピーして名前を変更することができます。新しいポリシーはコピーしたポリシーの設定を使用しますが、後でその設定を変更することができます。

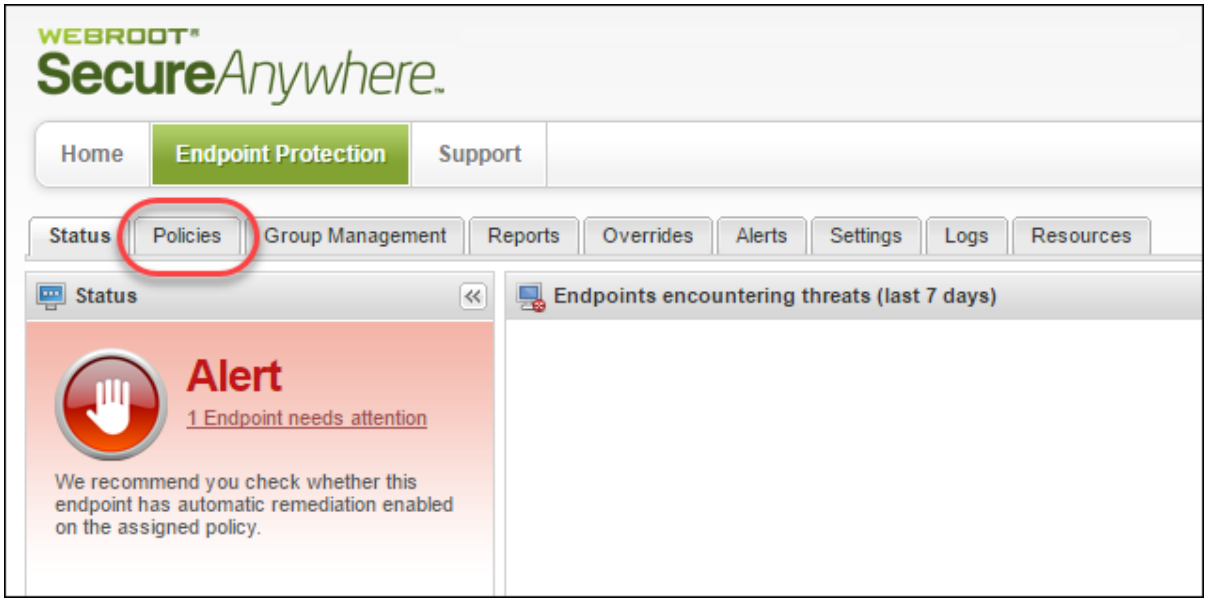
ポリシーをコピーするには

1. エンドポイントプロテクションのコンソールにログインします。

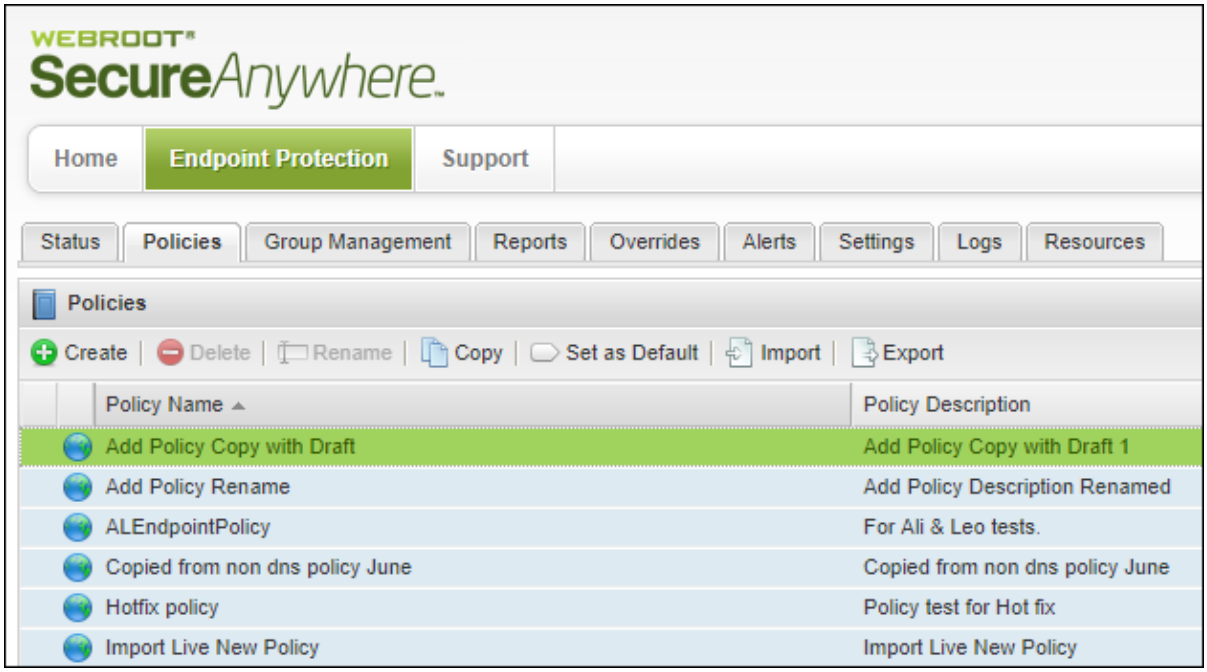
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



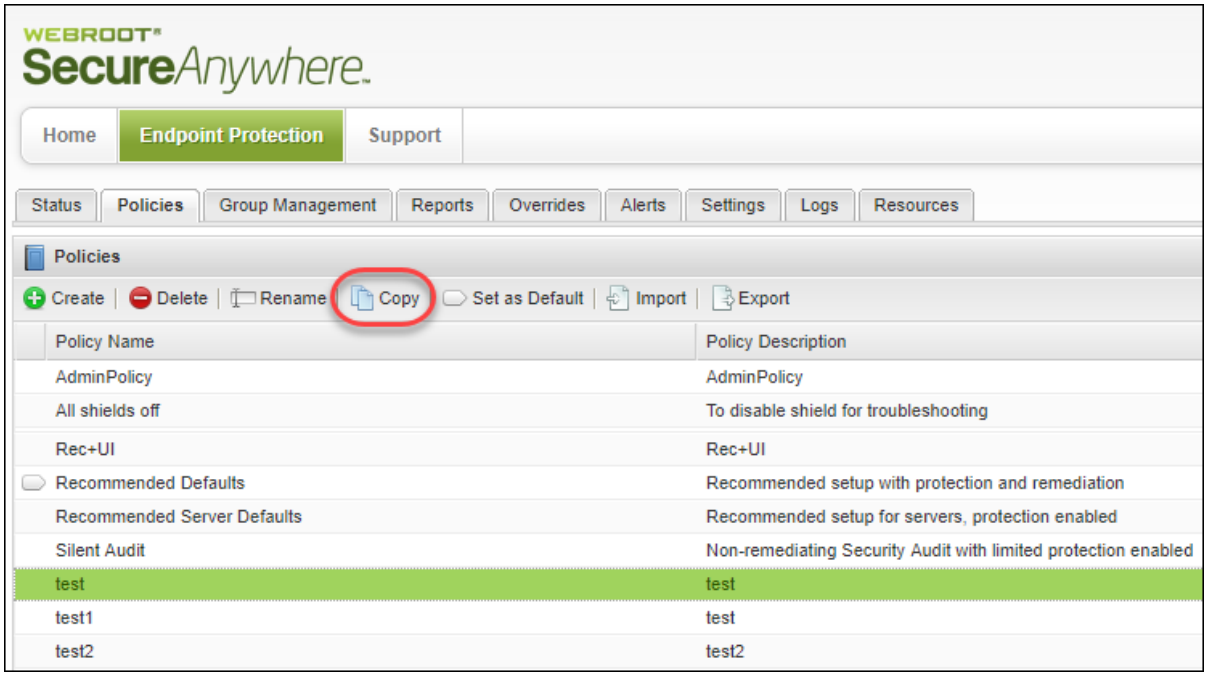
2. [**ポリシー**] タブをクリックします。



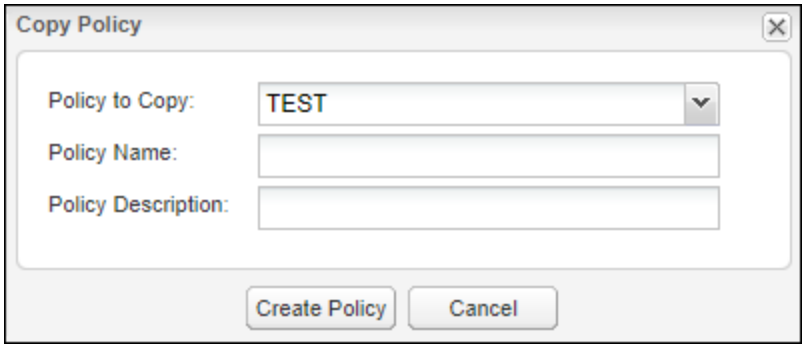
[ポリシー] タブが表示されます。



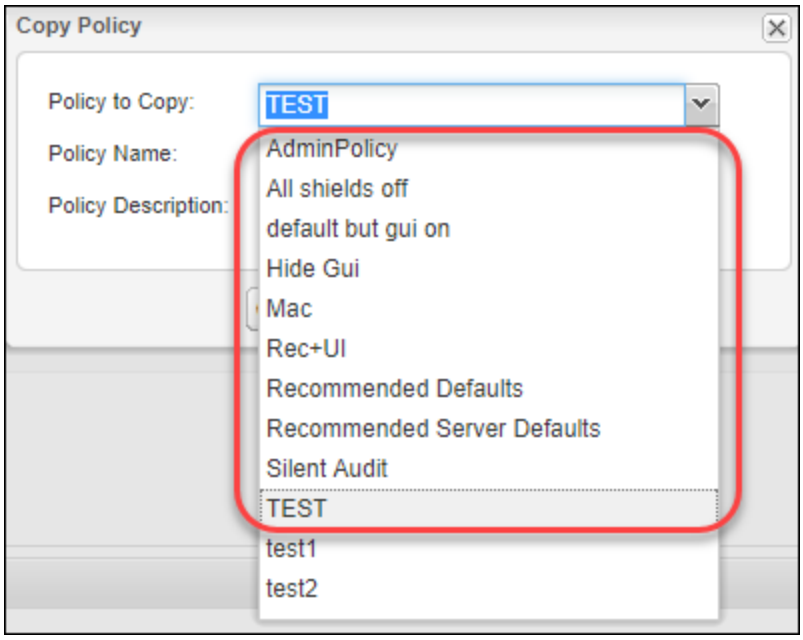
3. [ポリシー名] カラムで、元になるポリシーを選択し、[**コピー**] アイコンをクリックします。



[ポリシーのコピー] ウィンドウが表示されます。選択したポリシーが [コピーするポリシー] フィールドに表示されています。

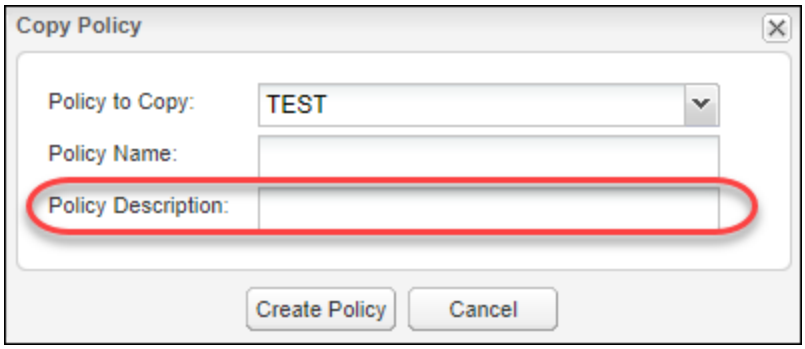


4. 必要に応じて、[**コピーするポリシー**] ドロップダウンメニューからコピー対象の別のポリシーを選択します。



5. [ポリシー名] フィールドに一意の名前を入力します。

6. [新しいポリシーの説明] フィールドに、最大 50 文字 (英数字) で説明を入力します。



7. [ポリシー名] カラムで、新しいポリシーを見つけます。

   以下のいずれかの操作を行います。

   - ポリシーをダブルクリックして設定を変更します。詳細については、「*ポリシー設定の変更 ページ247*」を参照してください。

   - ポリシーを、個々のエンドポイントまたはエンドポイントのグループに対して適用します。詳細については、「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

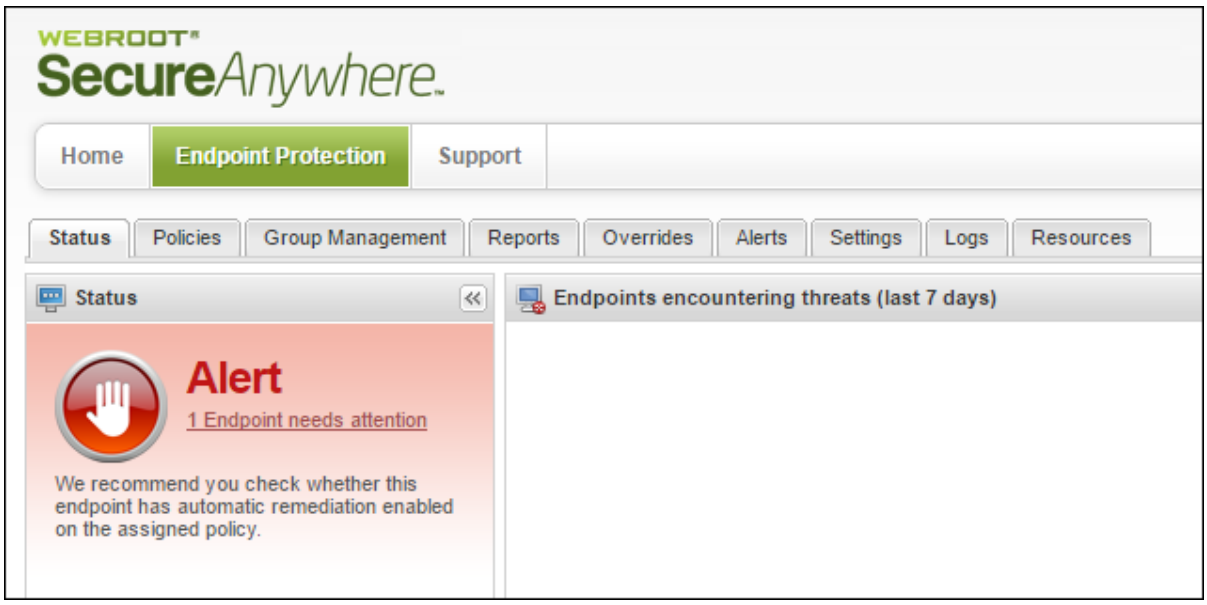
ポリシーの名前の変更

[ポリシー] タブでポリシーの名前を変更できます。ポリシー名は一意である必要があります。

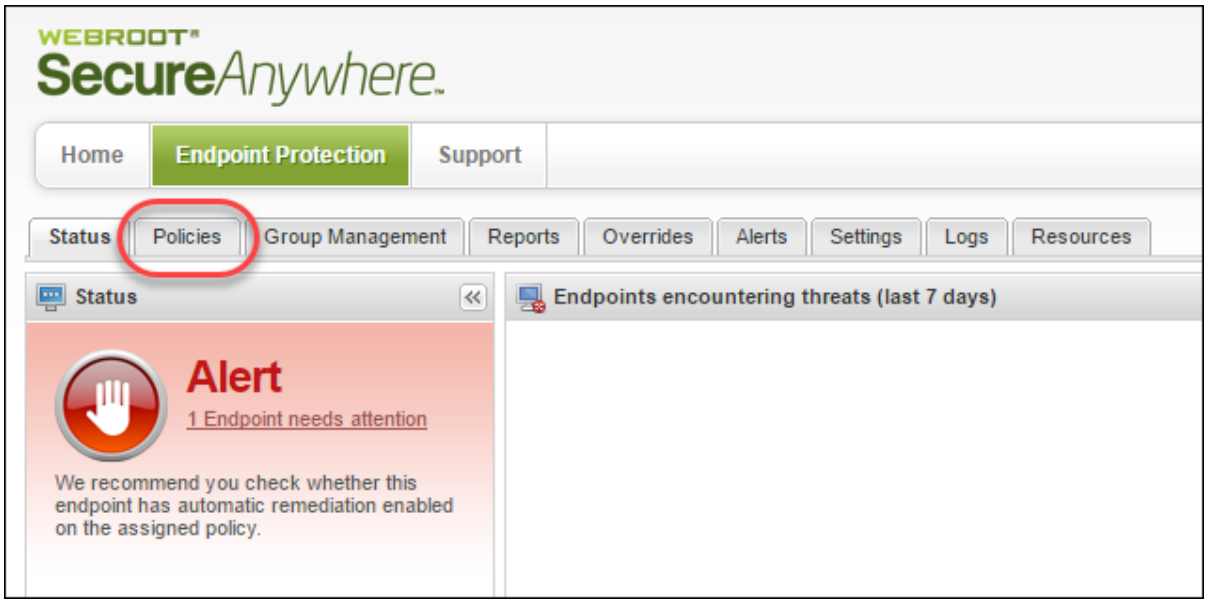
ポリシーの名前を変更するには

1. エンドポイント プロテクションのコンソールにログインします。

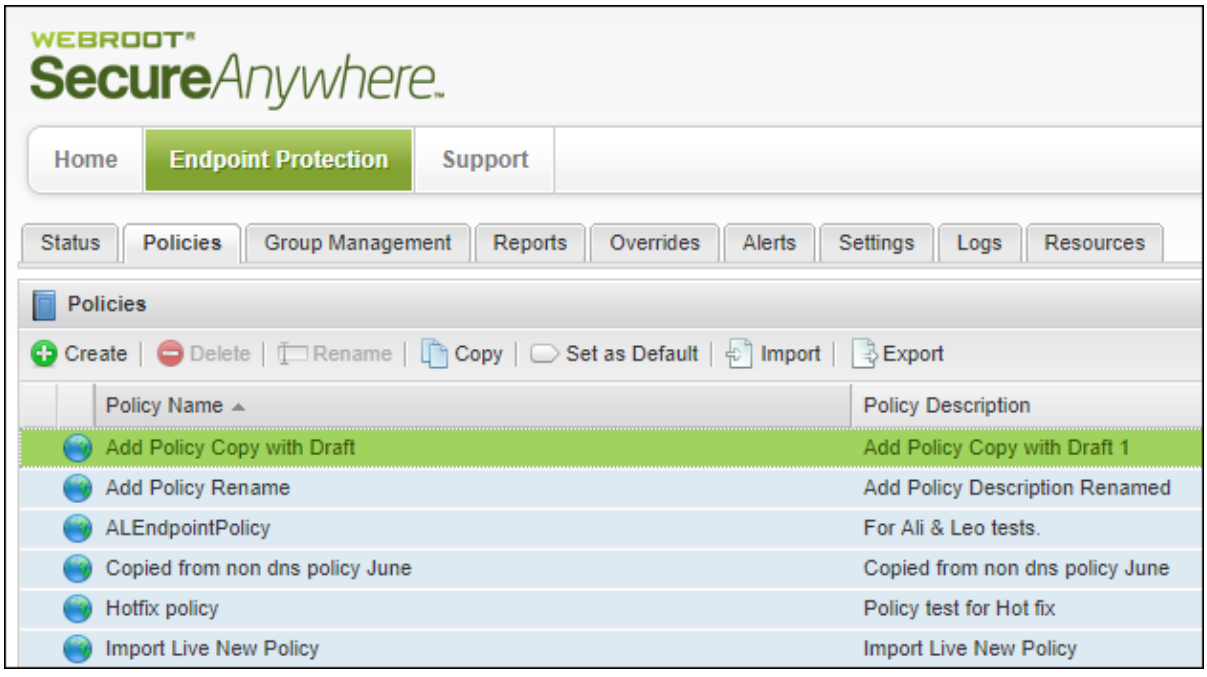
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



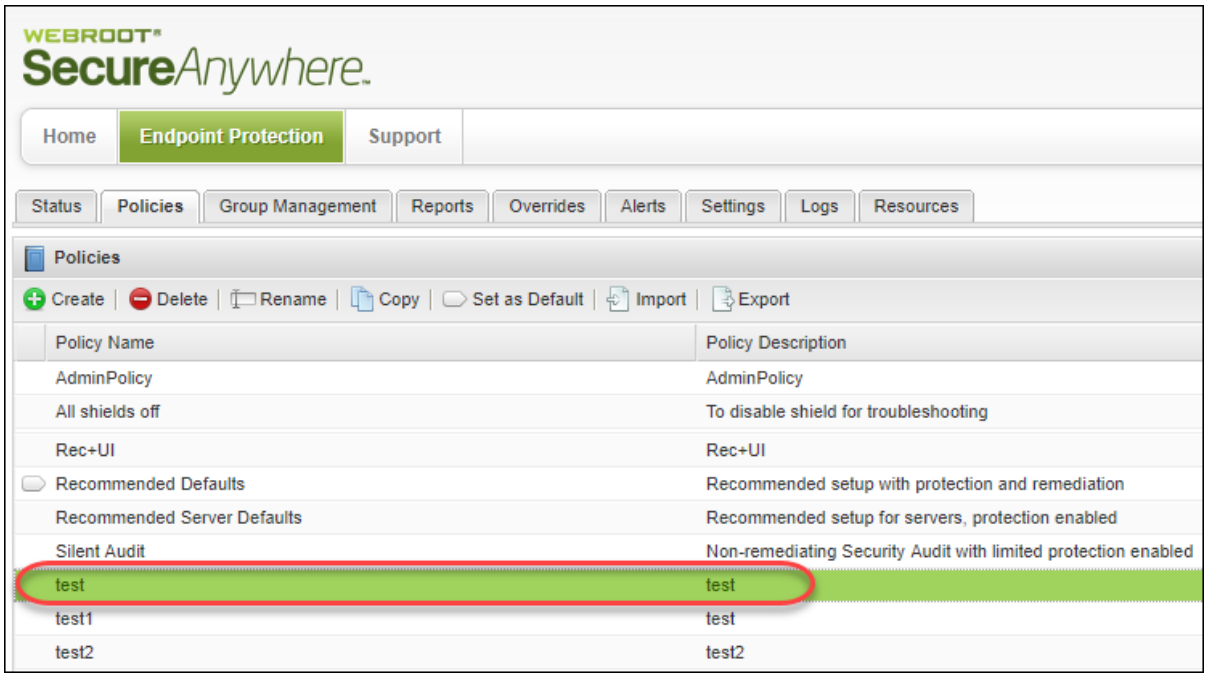
2. [**ポリシー**] タブをクリックします。



[ポリシー] タブが表示されます。

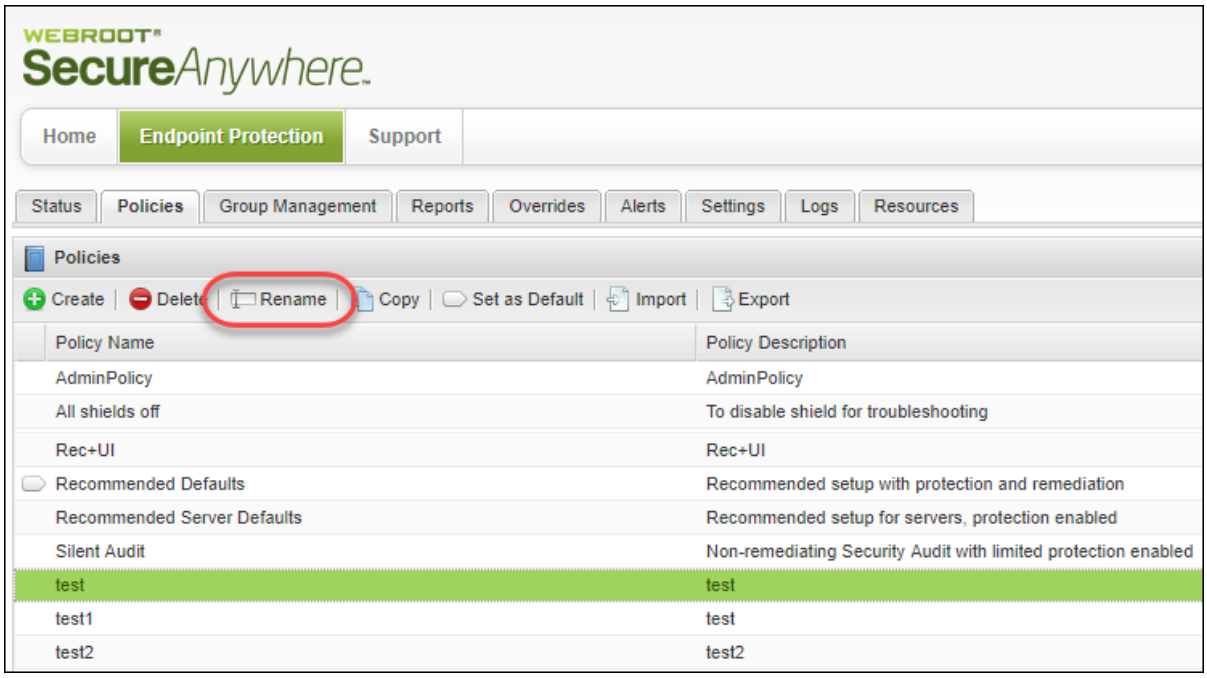


3. [ポリシー名] カラムで、名前を変更するポリシーを選択します。

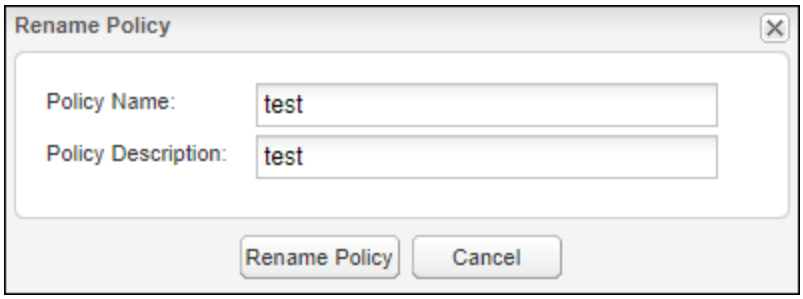


[名前変更] アイコンがアクティブになります。

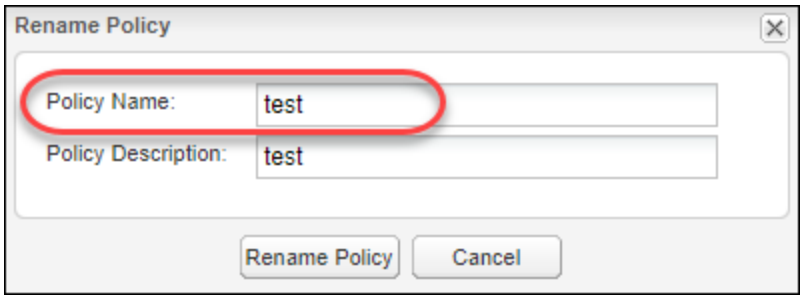
4. [**名前変更**] アイコンをクリックします。



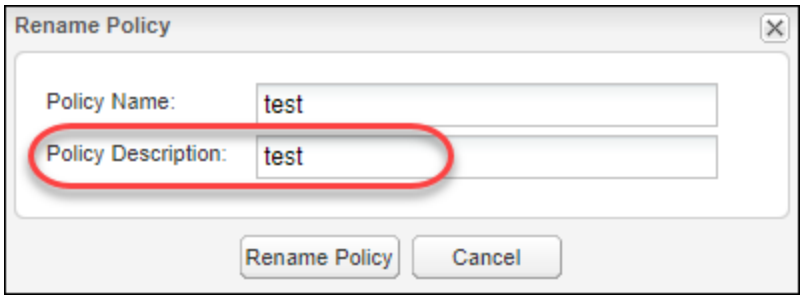
[ポリシーの名前を変更] ウィンドウが表示されます。



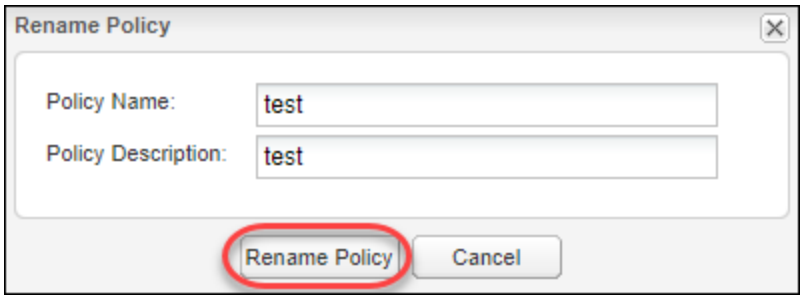
5. [ポリシー名] フィールドに、ポリシーの新しい名前と説明を入力します。



6. [ポリシーの説明] フィールドで、必要に応じてポリシーの説明をアップデートします。



7. 設定が完了したら、[**ポリシーの名前を変更**] ボタンをクリックします。



[ポリシー名] カラムに新しいポリシー名が表示されます。

ポリシー設定の変更

ポリシーを作成したら、ビジネスの目的に合わせてポリシー設定を変更することができます。必要に応じて、一時的に変更 (下書きを作成) し、後で反映 (ライブに昇格) することもできます。詳細については、「*ポリシーの作成 ページ233*」を参照してください。

注意: ウェブルートのデフォルトのポリシー設定は変更できません。

管理されているエンドポイントについて、次のような SecureAnywhere の設定をポリシーで制御することができます。

セクション	説明
基本設定	一般設定では、エンドポイントのシステムトレイにプログラムのアイコンを表示するかどうか、ユーザーがプログラムをシャットダウンできるかどうかなど、SecureAnywhere プログラムの動作を変更します。
スキャンのスケジュール	スキャンを別の時刻に実行したり、スキャン中の動作を変更したり、自動スキャンを解除したりすることができます。スキャンのスケジュールを変更しない場合、SecureAnywhere は、ソフトウェアがインストールされた時刻と同じ頃に毎日自動的にスキャンを実行します。
スキャン設定	詳細なスキャンの実行など、スキャンを細かく管理できます。
自己保護	保護を追加して、悪意のあるソフトウェアがエンドポイントで SecureAnywhere プログラムの設定やプロセスを変更できないようにします。別の製品が SecureAnywhere の機能に干渉しようとしていることが検出された場合、保護のためのスキャンを開始して脅威を特定します。

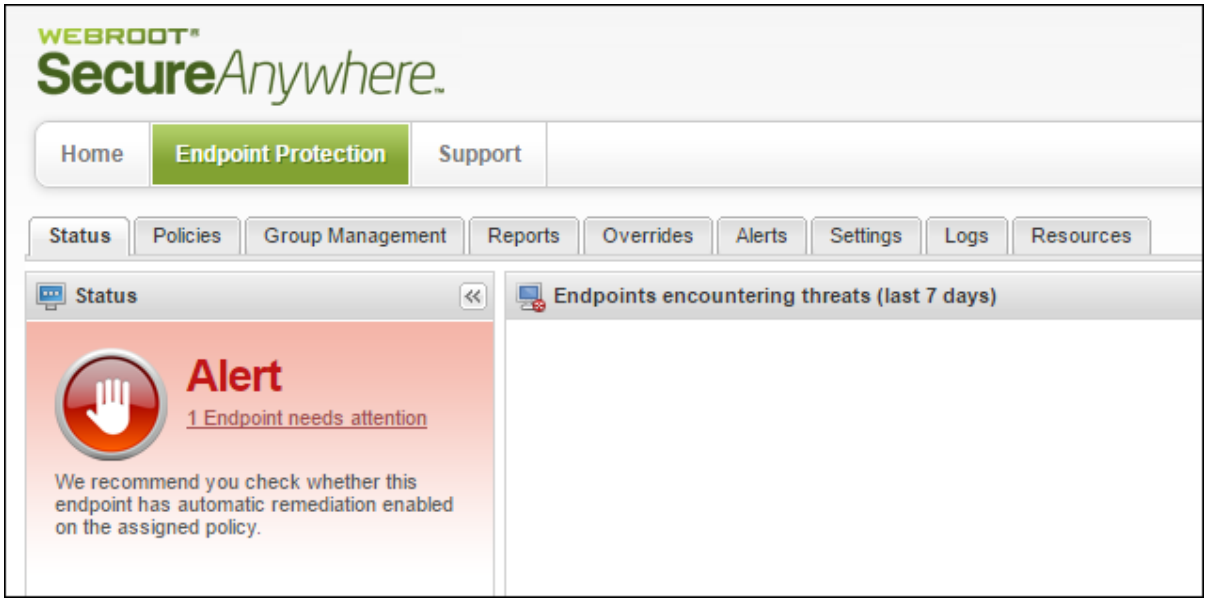
セクション	説明
ヒューリスティック	エンドポイントのスキャン中に SecureAnywhere が実行する脅威分析を設定できます。ヒューリスティックは、ローカルドライブ、USB ドライブ、インターネット、ネットワーク、CD / DVD、オフライン時の動作など、エンドポイントのさまざまなエリアに対して調整できます。
リアルタイム シールド	ウェブルートによる脅威の定義およびコミュニティのデータベースにリストされている既知の脅威をブロックします。
動作シールド	エンドポイントで実行中のアプリケーションとプロセスを分析します。
コアシステムシールド	コンピュータのシステムの構造を監視し、マルウェアによって改ざんされていないか確認します。
Web 脅威シールド	ユーザーがインターネットを閲覧したり、検索結果をクリックしたりする際に、エンドポイントを保護します。
ID シールド	個人情報の盗難や金銭的な損失からユーザーを守ります。キーロガーやスクリーングラバー、その他の情報盗用技術からユーザーを守りながら、重要なデータが確実に保護されるようにします。
ファイアウォール	コンピュータのポートから出力されるデータトラフィックを監視します。インターネットに接続して個人情報を盗もうとする、信頼できないプロセスを探します。一方で、Windows ファイアウォールは、コンピュータに入ってくるデータトラフィックを監視します。

セクション	説明
ユーザーインターフェイス	エンドポイントでの SecureAnywhere プログラムへのユーザー アクセスを設定します。
システム最適化ツール	自動クリーンアップのスケジュール、エンドポイントから削除するファイルや痕跡の種類など、システム最適化ツールの動作を制御します。

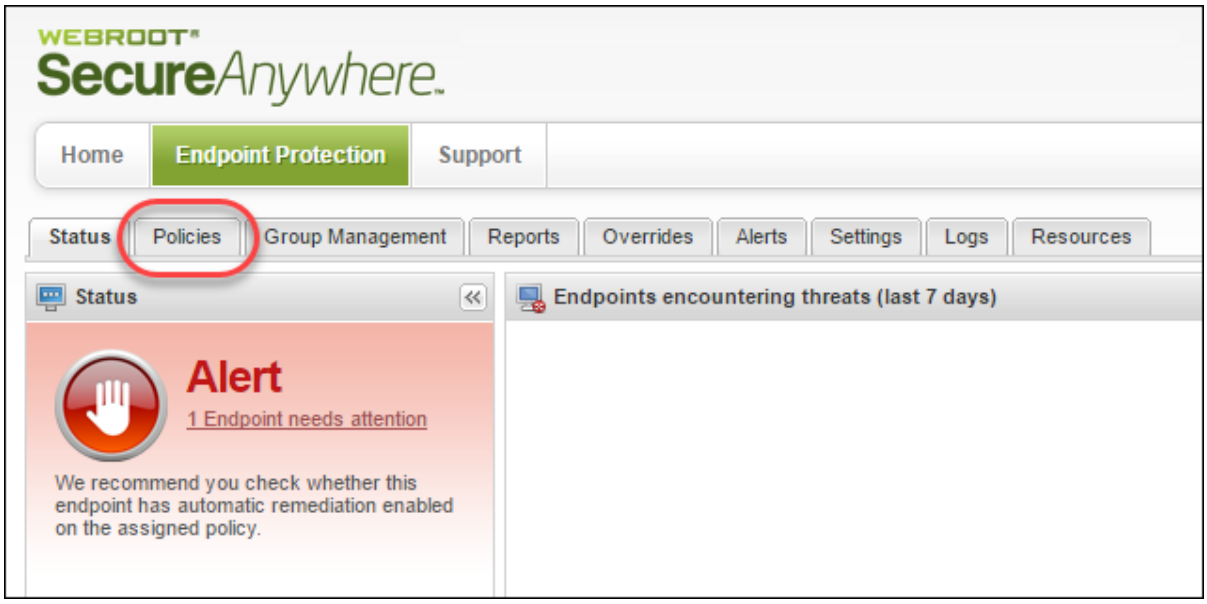
ポリシーの設定を変更するには

1. エンドポイントプロテクションのコンソールにログインします。

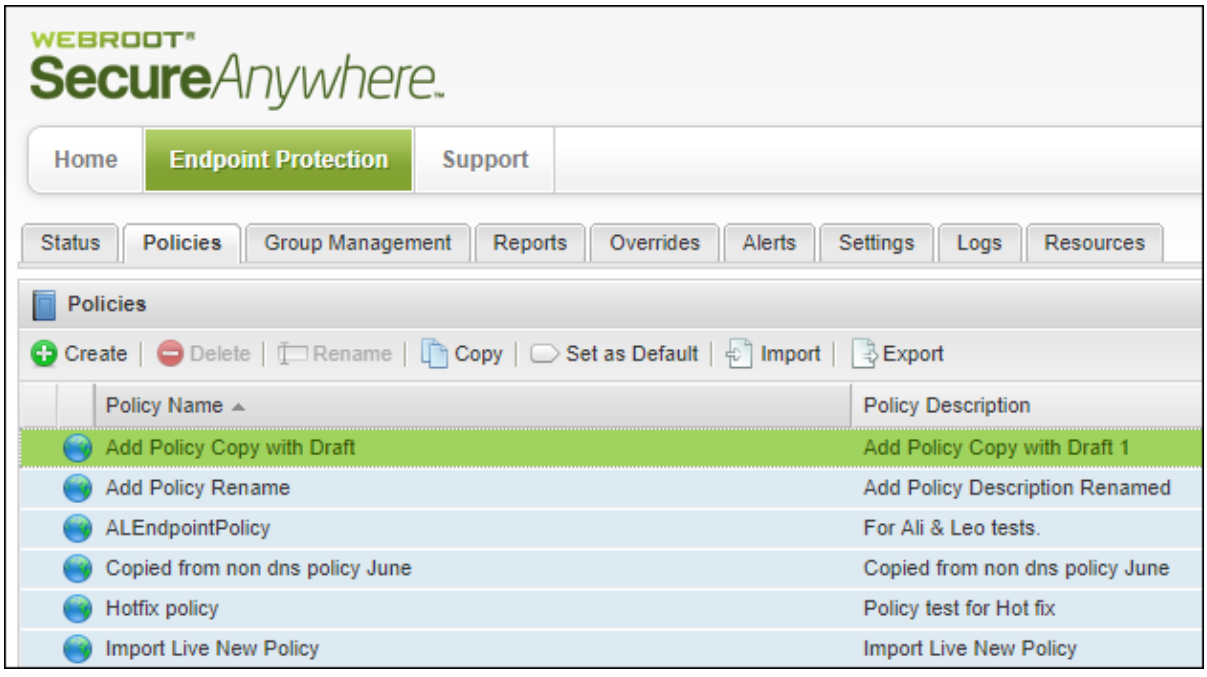
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



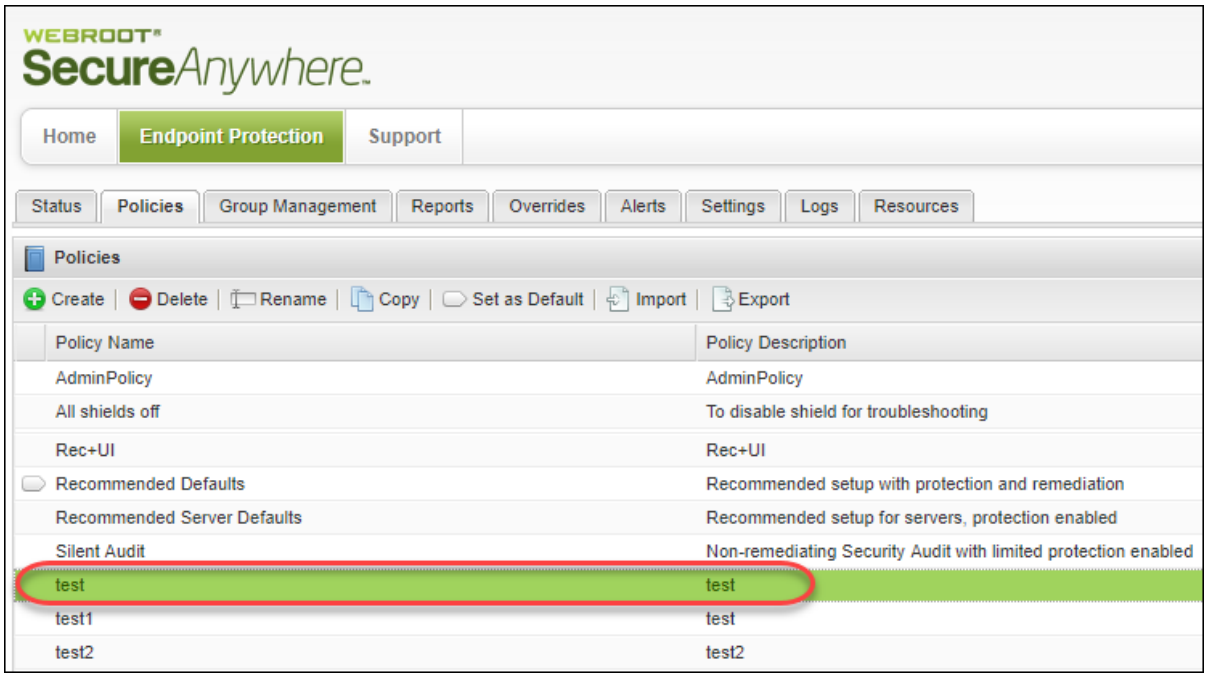
2. [**ポリシー**] タブをクリックします。



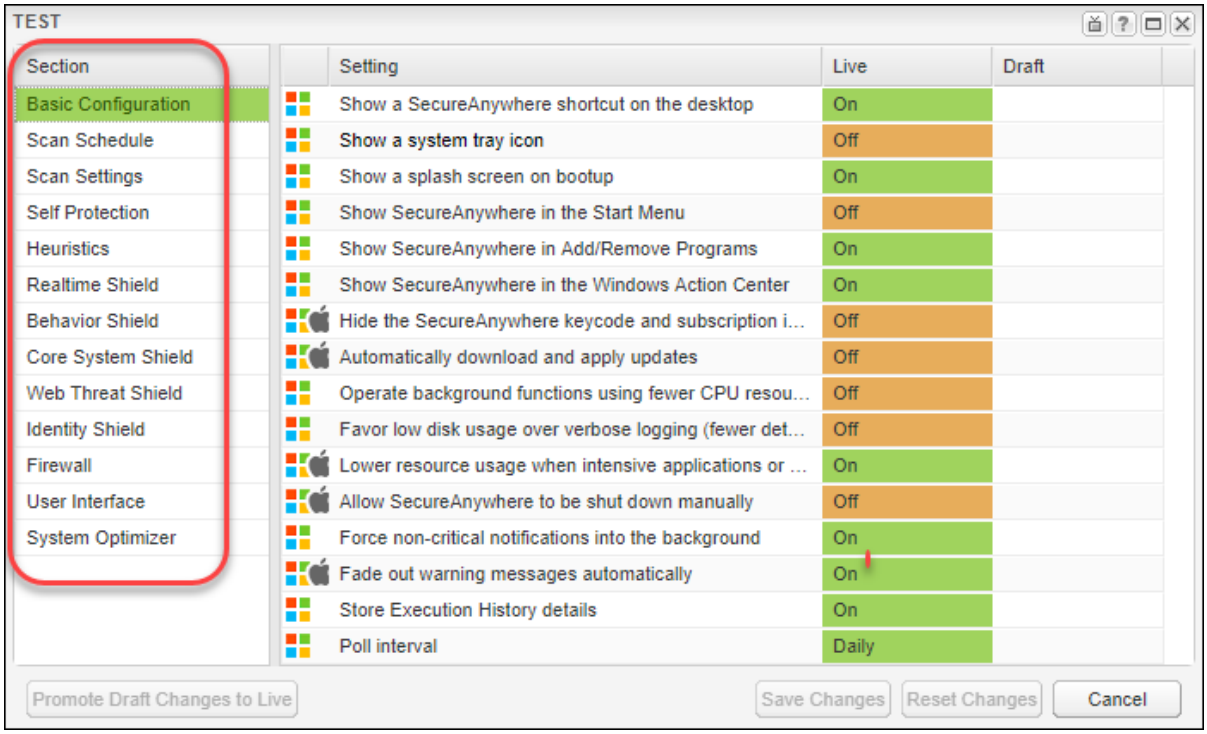
[ポリシー] タブが表示されます。



3. [ポリシー名] カラムで変更するポリシーを探して、そのポリシーをダブルクリックします。

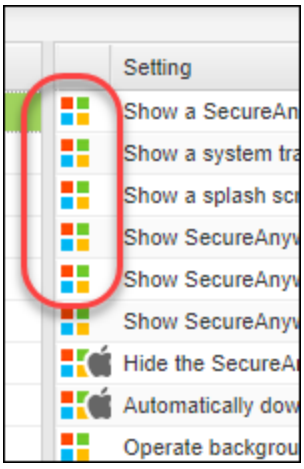


[セクション] コラムの基本設定が選択された状態で、ポリシーの設定ウィンドウが表示されます。

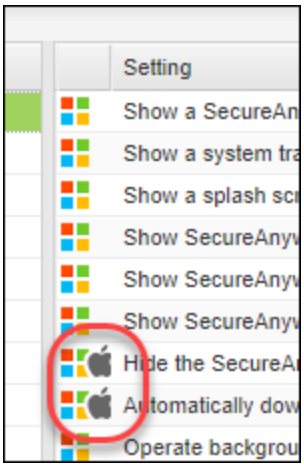


[設定] カラムにはポリシーの名前が表示されています。アイコンの意味は以下のとおりです。

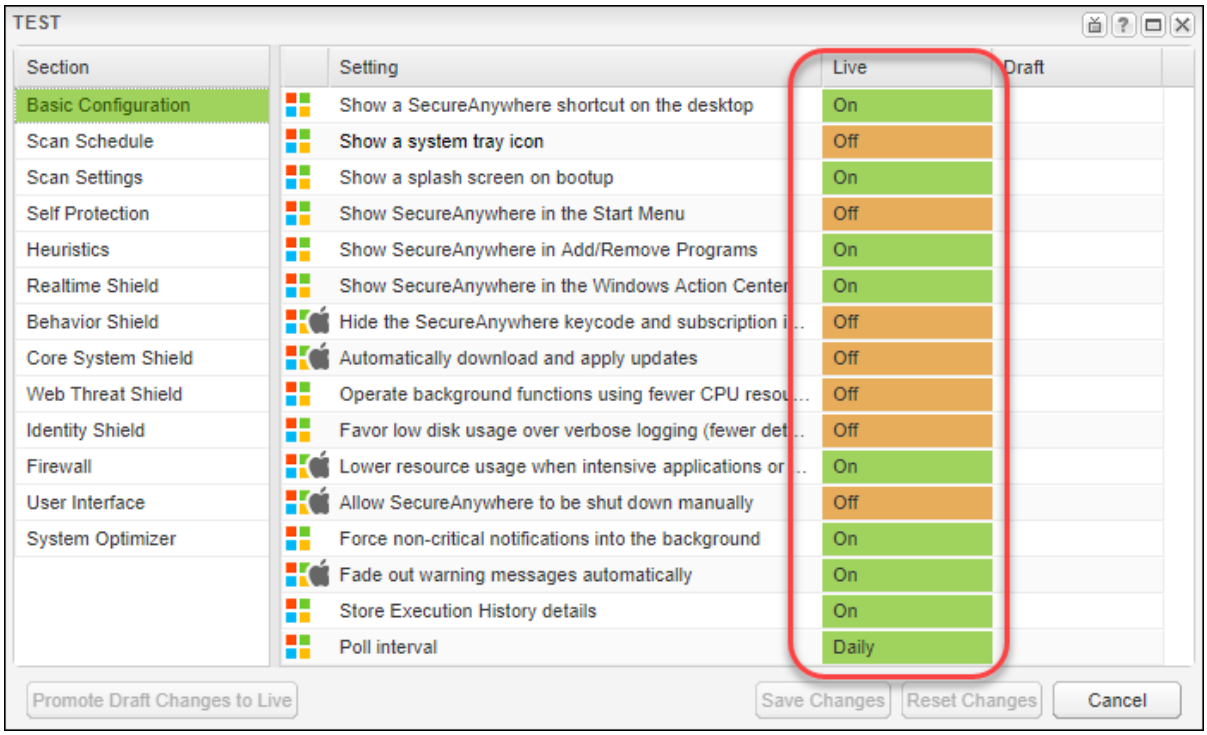
- Windows PC のみに適用される設定には、Windows のアイコンが表示されます。



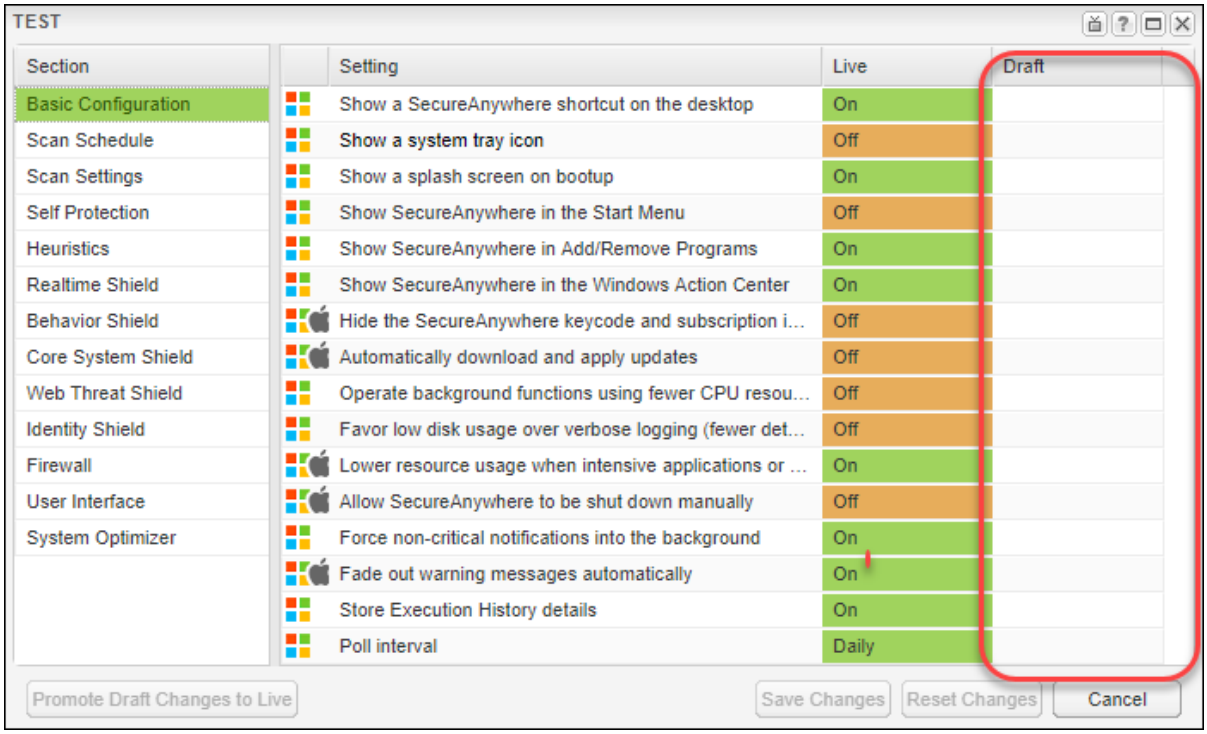
- Windows PC と Mac に適用される設定には、Windows アイコンと Mac アイコンの両方が表示されます。



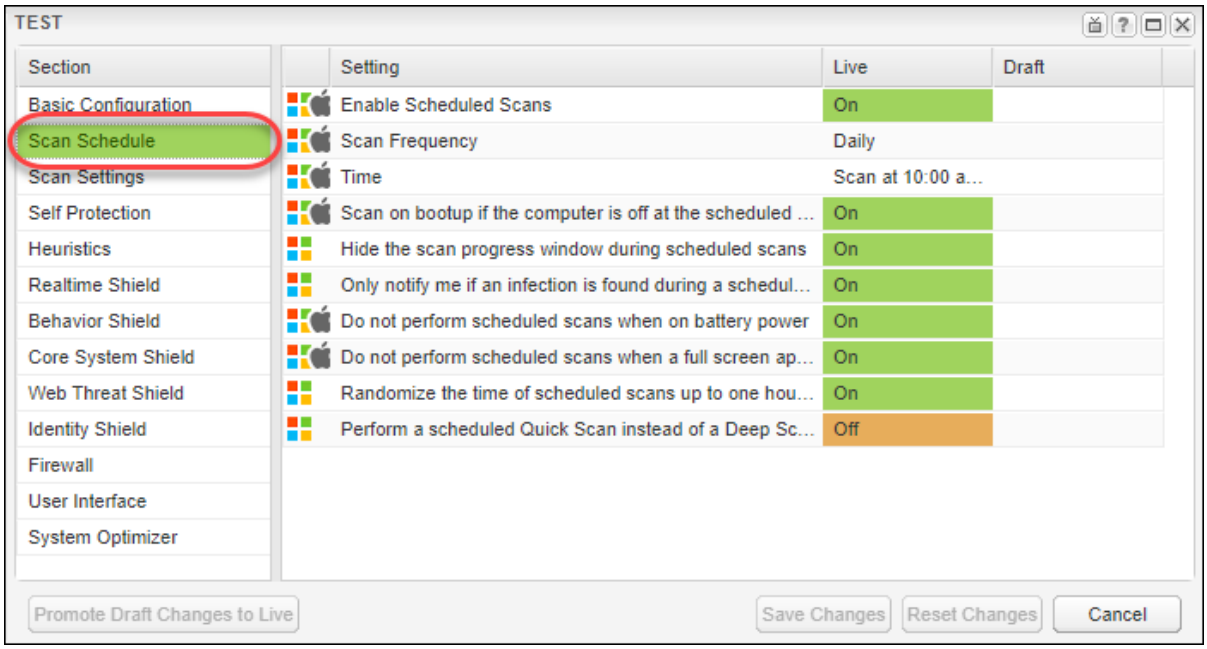
[ライブ] カラムには、設定が現在エンドポイントでどのような状態にあるかが表示されます。



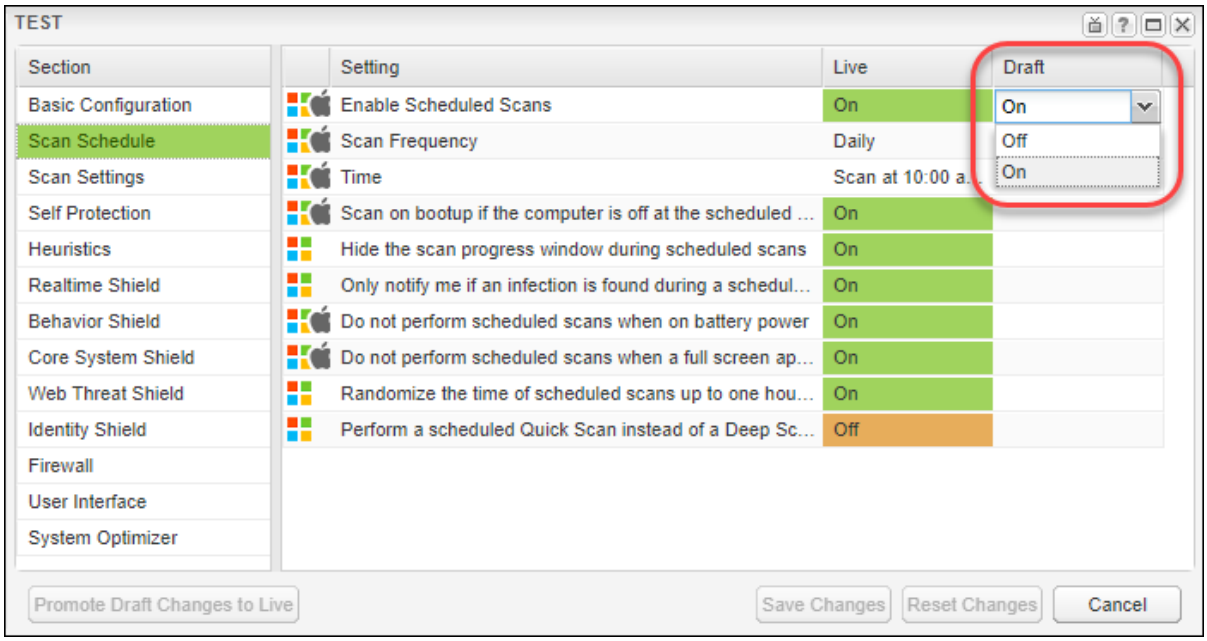
[下書き] カラムで値を変更します。



4. [セクション] カラムで編集するカテゴリを選択します。



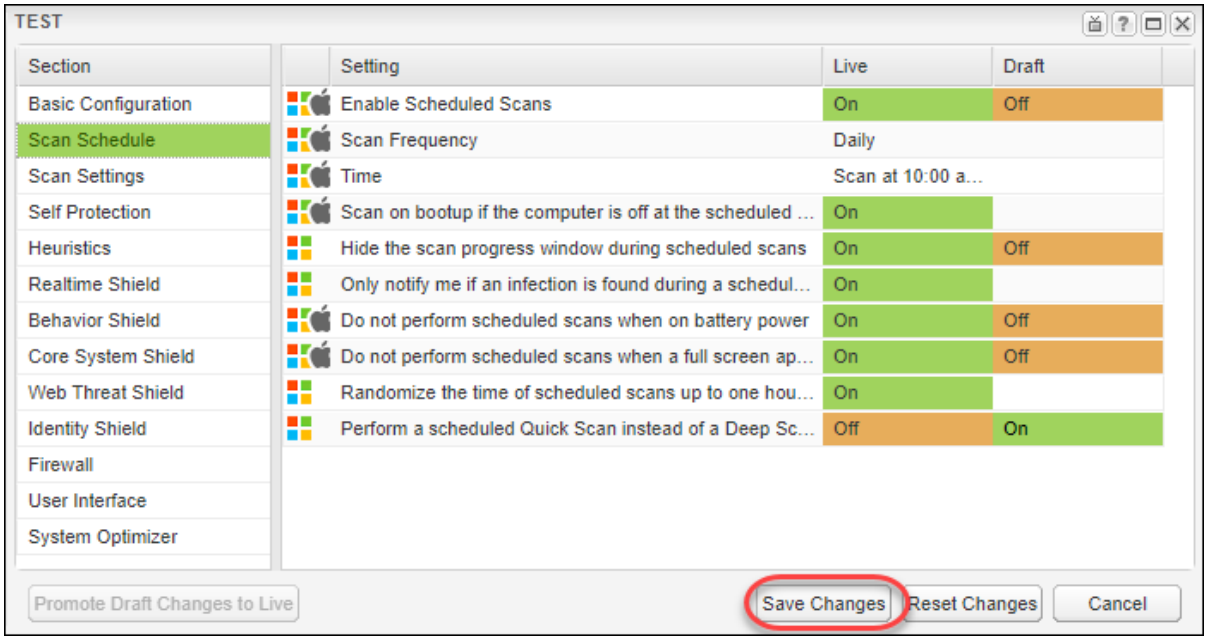
5. 各設定の [下書き] カラムでセルをダブルクリックしてオプションを表示し、ドロップダウンメニューから適切な設定を選択します。



それぞれの設定の詳細な説明については、この手順の下にある表を参照してください。

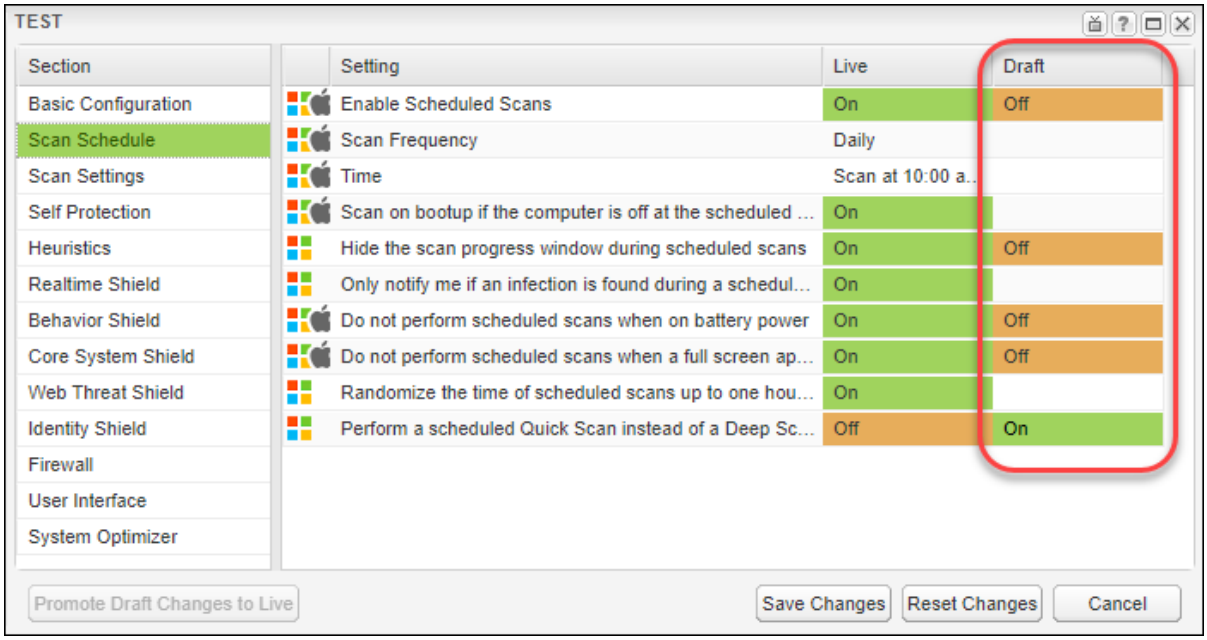
基本設定	リアルタイムシールド	ファイアウォール
スキャンのスケジュール	動作シールド	ユーザーインターフェイス
スキャン設定	コアシステムシールド	システム最適化ツール
自己保護	Web 脅威シールド	
ヒューリスティック	ID シールド	

6. 選択内容の変更を完了したら、[**変更を保存**] ボタンをクリックします。



7. ポリシーの各セクションの変更を続けます。他のセクションへ移動する前に必ず [**変更を保存**] をクリックしてください。

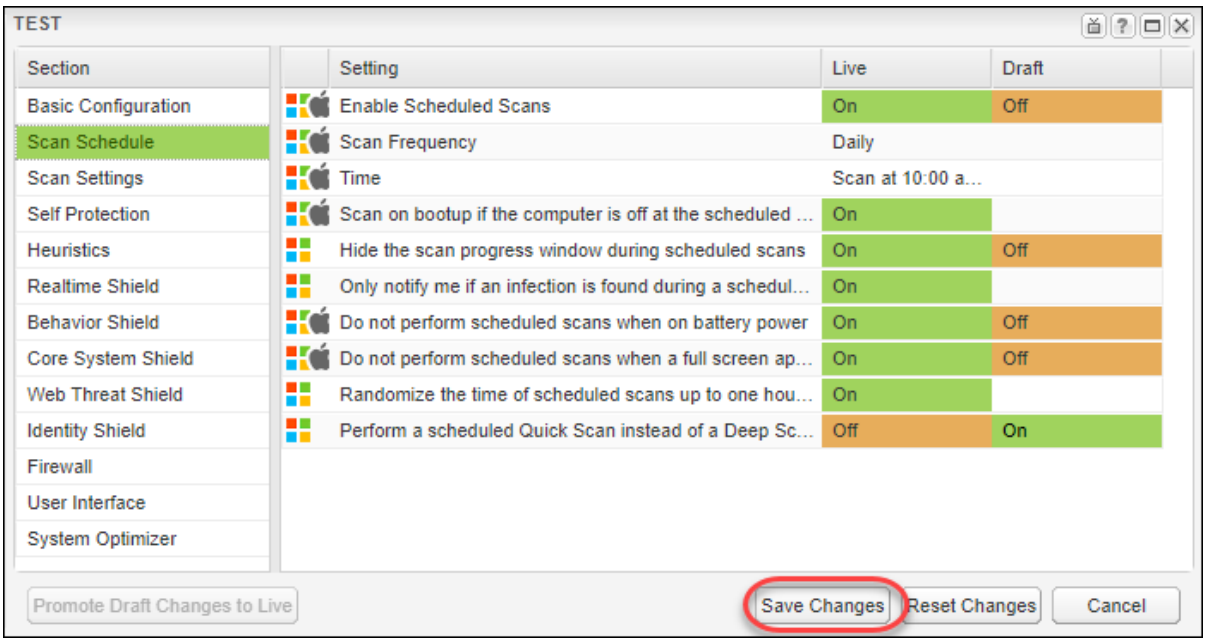
   変更が保存されていないポリシーは、[下書きの変更] カラムに表示されます。



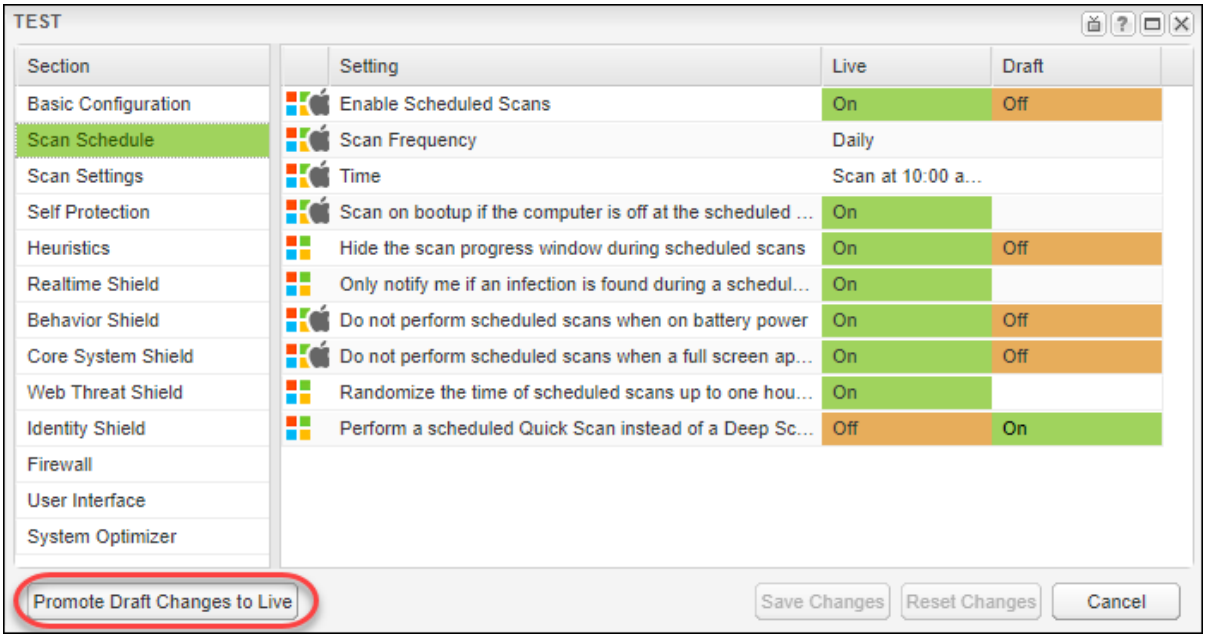
注意: 緑は設定がオンであることを示し、オレンジは設定がオフであることを示します。この色分けにより、リストを簡単に確認できます。

8. 以下のいずれかの操作を行います。

- この段階ではまだ変更を反映しない場合は、[**変更を保存**] ボタンをクリックして [ポリシー] タブに戻ります。



- 変更を反映する場合は、[**変更を保存**] ボタンをクリックしてから [**下書きの変更をライブに昇格**] ボタンをクリックします。



注意: 昇格するまで変更は有効になりません。

基本設定

基本設定は、管理されたエンドポイント上での SecureAnywhere ソフトウェアの動作を制御します。

設定	説明
SecureAnywhere へのショートカットをデスクトップ上に表示する	エンドポイントのデスクトップにショートカット アイコンを配置し、メインインターフェイスにすばやくアクセスできるようにします。 この設定は PC エンドポイントにのみ適用されます。
システムトレイ アイコンを表示する	エンドポイントのシステムトレイにウェブルートのアイコンを配置し、SecureAnywhere の各機能にすばやくアクセスできるようにします。 この設定は PC エンドポイントにのみ適用されます。
起動時にスプラッシュ画面を表示する	エンドポイントの起動時にウェブルートのスプラッシュ画面が表示されます。 この設定は PC エンドポイントにのみ適用されます。
SecureAnywhere をスタート メニューに表示する	Windows のスタート メニューに SecureAnywhere が表示されます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
[プログラムの追加と削除] パネルに SecureAnywhere を表示する	Windows の [プログラムの追加と削除] パネルに SecureAnywhere が表示されます。 この設定は PC エンドポイントにのみ適用されます。
Windows アクション センターに SecureAnywhere を表示する	Windows セキュリティ / アクション センターの [ウイルス対策] に SecureAnywhere が一覧表示されるようになります。 この設定は PC エンドポイントにのみ適用されます。
SecureAnywhere のキーコードおよび定期購入契約情報を画面上に表示しない	エンドポイントの [マイアカウント] パネルで、キーコードを非表示にします。キーコードの最初の 4 桁以外はアスタリスクで表示します。 この設定は PC および Mac エンドポイントの両方に適用されます。
アップデートを自動的にダウンロードして適用する	エンドポイント ユーザーへの警告なしに製品のアップデートを自動的にダウンロードします。 この設定は PC および Mac エンドポイントの両方に適用されます。
使用する CPU リソースを減らしてバックグラウンド機能を作動させる	スキャンに関連しない機能をバックグラウンドで実行することで、CPU リソースを節約します。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
詳細なロギングよりも低ディスク使用量を優先する (ログ情報量は少なくなります)	保存する最新のログアイテムを 4 つに制限することで、ディスク容量を節約します。 この設定は PC エンドポイントにのみ適用されます。
フル画面アプリケーションまたはゲームの検出時にリソース使用量を低減する	ゲーム、ビデオ、または大量のリソースを使用するその他のアプリケーションを実行中に、SecureAnywhere の機能を抑制します。 この設定は PC および Mac エンドポイントの両方に適用されます。
SecureAnywhere の手動シャットダウンを許可する	エンドポイントのシステムトレイメニューに終了コマンドを表示します。このオプションの選択を解除すると、終了コマンドがメニューから削除されます。 この設定は PC および Mac エンドポイントの両方に適用されます。
重要でない通知をバックグランドに表示する	情報の提供のみを目的とするメッセージがシステムトレイに表示されないようにします。 この設定は PC エンドポイントにのみ適用されます。
警告メッセージを自動的にフェードアウトする	システムトレイの警告ダイアログを数秒で閉じます。このオプションを無効にした場合、ユーザーがメッセージをクリックするまで警告が表示されたままになります。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
実行履歴の詳細を保存する	[レポート] の実行履歴ログにデータを保存します。 この設定は PC エンドポイントにのみ適用されます。
ポーリング間隔	エンドポイントがアップデートを確認する頻度を指定します。例: 15 分、30 分、1 時間、2 時間。 この設定は PC および Mac エンドポイントの両方に適用されます。

スキャンのスケジュール

SecureAnywhere は、インストールされた時刻とほぼ同じ時刻に毎日、自動的にスキャンを実行します。スキャンのスケジュールの設定を使用すると、スケジュールを変更して別の時間にスキャンを実行することができます。

設定	説明
スケジュール スキャンを有効にする	エンドポイントでのスケジュールスキャンの実行を許可します。 この設定は PC および Mac エンドポイントの両方に適用されます。
スキャン頻度	スキャンを実行する頻度を指定します。曜日を設定するか、起動時のスキャンを選択することができます。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
時間	スキャンを実行する時間を指定します。 • コンピュータの待機中のスキャン時間には、午前 8:00 前、正午前、午後 5:00 前、深夜 0:00 前のいずれかを指定できます。 • リソースが使用可能な場合のスキャン時間には、深夜 0:00 から午後 11:00 までの間の時刻を 1 時間単位で指定できます。to 11:00 p.m. この設定は PC および Mac エンドポイントの両方に適用されます。
スケジュールされた時刻にコンピュータの電源が入っていない場合、起動時にスキャンする	スケジュールした時刻にスキャンが実行されなかった場合は、ユーザーがコンピュータの電源をオンにしてから 1 時間以内にスケジュールされたスキャンを実行します。このオプションが無効になっていると、SecureAnywhere は実行されなかったスキャンを無視します。 この設定は PC および Mac エンドポイントの両方に適用されます。
スケジュール スキャン中にスキャンの進行状況ウィンドウを表示しない	スキャンをバックグラウンドで実行します。このオプションを無効にすると、ウィンドウが開いてスキャンの進捗状況が表示されます。 この設定は PC エンドポイントにのみ適用されます。
スケジュール スキャン中に感染が検出された場合にのみ通知する	脅威が発見された場合にのみ警告を発します。このオプションを無効にすると、脅威が発見されたかどうかにかかわらず、スキャンの完了時に小さなステータス ウィンドウが開きます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
バッテリ電源の場合はスケジュール スキャンを実行しない	バッテリの電力を節約します。エンドポイントがバッテリを電源としている場合に、スケジュールされたスキャンを実行するには、このオプションの選択を解除します。 この設定は PC および Mac エンドポイントの両方に適用されます。
アプリケーションまたはゲームをフル スクリーンで実行中はスケジュール スキャンを実行しない	映画やゲームなど、全画面表示のアプリケーションをユーザーが利用しているときは、スケジュールされたスキャンを無視します。このような場合もスケジュールどおりにスキャンを実行するには、このオプションの選択を解除してください。 この設定は PC および Mac エンドポイントの両方に適用されます。
スケジュール スキャン時間を最大 1 時間ランダム化してスキャンを分散する	使用可能なシステム リソースに応じてスキャンを実行するのに最適なタイミングを判断し、予定時刻の 1 時間以内にスキャンを実行します。スケジュールした時刻にスキャンを強制的に実行する場合は、このオプションの選択を解除してください。 この設定は PC エンドポイントにのみ適用されます。
ディープ スキャンではなくスケジュール クイック スキャンを実行する	メモリのクイックスキャンを実行します。すべての場所にあるあらゆるタイプのマルウェアに対して詳細なスキャンが実行されるように、このオプションの選択は解除したままにしておくことをお勧めします。 この設定は PC エンドポイントにのみ適用されます。

スキャン設定

スキャン設定では、スキャンのパフォーマンスをより詳細に制御できます。

設定	説明
リアルタイムマスターブートレコード (MBR) スキャンを有効にする	エンドポイントのマスターブートレコード (MBR) への感染を防ぎます。 MBR が感染することによって、システムのコア領域に変更が加えられ、それが OS の前に読み込まれてコンピュータを感染させる場合があります。このオプションは選択したままにしておくことをお勧めします。この機能を選択していることによるスキャン時間の増加はわずかです。 この設定は PC エンドポイントにのみ適用されます。
拡張ルートキット検出を有効化する	ディスクや保護されたエリアに隠されたルートキットや他の悪意のあるソフトウェアがないかチェックします。 スパイウェアの開発者は、検出や削除を避けるためにルートキットを使用する場合がよくあります。このオプションは選択したままにしておくことをお勧めします。この機能を選択していることによるスキャン時間の増加はわずかです。 この設定は PC エンドポイントにのみ適用されます。
Windows エクスプローラーでの "右クリック" スキャンを有効にする	Windows エクスプローラーでファイルやフォルダを右クリックすると表示されるメニューから個々にスキャンを実行するオプションを有効にします。 このオプションは、ユーザーがダウンロード済みファイルをすばやくスキャンする場合に役立ちます。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
スキャンした個々のファイル名をスキャン時に表示する	各ファイルがスキャンされる度に表示されるファイル一覧がアップデートされます。 スキャンのパフォーマンスを少しでも向上させるには、このオプションの選択を解除すると、パネル上で 1 秒に 1 回のみファイル名がアップデートされるようになります。このオプションの選択を解除しても SecureAnywhere はすべてのファイルをスキャンしますが、各ファイルを画面に表示するための時間をかけずに済みます。 この設定は PC エンドポイントにのみ適用されます。
高速スキャンよりも低メモリ使用量を優先する	スキャン中に使用するメモリを減らすことにより、バックグラウンドでの RAM の使用量を削減します。ただし、スキャンの速度も若干遅くなります。 このオプションの選択を解除すると、スキャンの速度が上がり、より多くのメモリが使用されます。 この設定は PC エンドポイントにのみ適用されます。
高速スキャンよりも低 CPU 使用量を優先する	スキャン中の CPU 使用量を抑えます。ただし、スキャンの実行速度も若干遅くなります。 このオプションの選択を解除すると、スキャンの速度が上がります。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
非実行可能ファイルの詳細をスキャンログに保存する	スキャン ログにすべてのファイル データを保存します。結果としてログ ファイルのサイズが大幅に増加します。 実行可能ファイルの詳細のみをログに保存するには、このオプションの選択を解除したままにしてください。 この設定は PC エンドポイントにのみ適用されます。
新しいファイルを実行時にスキャンするときに [ファイルの認証中] ポップアップを表示する	ユーザーがプログラムを初めて実行するときに、小さなダイアログを表示します。ユーザーがこのダイアログを確認する必要がない場合は、このオプションの選択を解除したままにしてください。 この設定は PC エンドポイントにのみ適用されます。
アーカイブ ファイルをスキャンする	zip、rar、cab、7-zip のアーカイブ中にある圧縮されたファイルをスキャンします。 この設定は PC および Mac エンドポイントの両方に適用されます。
クリーンアップ中にプロンプトで通知することなく自動的に再起動する	マルウェアファイルの痕跡を完全に削除するためのクリーンアップを実行した後に、コンピュータを再起動します。 この設定は PC エンドポイントにのみ適用されます。
マルウェアのクリーンアップ中に再起動しない	マルウェア ファイルの痕跡を完全に削除するためのクリーンアップを実行中に、エンドポイントが再起動しないようにします。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
バックグラウンドのスキャン中に検出された脅威を自動的に削除する	エンドポイントのバックグラウンドで実行されているスキャン中に脅威を削除して、隔離先に移動します。 この設定は PC エンドポイントにのみ適用されます。
学習スキャンで検出された脅威を自動的に削除する	エンドポイントで実行されている最初のスキャン中に脅威を削除して、隔離先に移動します。 この設定は PC エンドポイントにのみ適用されます。
高度なサポートを有効にする	ウェブルート カスタマー サポートへのログの送信を許可します。 この設定は PC エンドポイントにのみ適用されます。
感染しているスキャン結果を表示する	スキャン結果を表示します。有効でない場合、マルウェアが検出されてもエンドポイントにスキャン結果が表示されません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
好ましくない動作をする可能性のあるアプリケーション (PUA) を悪意のあるものとして検知する	PUA を検出し、そのインストールをブロックします。 望ましくない可能性のあるアプリケーション (PUA) とは、必ずしも悪意があるわけではないものの、アドウェアやツールバー、その他の望ましくないツールなどをシステムに追加するプログラムを指します。一般的に PUA は悪意があるものではありませんが、ビジネス環境での使用には不適切な場合があり、セキュリティ上の問題を引き起こす可能性があります。 システム上に PUA がすでにインストールされている場合、Webroot SecureAnywhere はそのメインプログラムを検出しますが、すべてを完全に削除できない可能性があります。 この設定は PC エンドポイントにのみ適用されます。
ファイルを脅威リサーチに送信することを許可する	ウェブルートのシステムがまだ分類していない、悪意のある可能性があるファイルを自動的にウェブルートにアップロードすることを許可します。 この設定は PC エンドポイントにのみ適用されます。

自己保護の設定

自己保護は、悪意のあるソフトウェアが SecureAnywhere プログラムの設定やプロセスを変更できないようにします。別の製品が SecureAnywhere の機能に干渉しようとしていることが検出された場合、保護のためのスキャンを開始して脅威を探します。また、他のソフトウェアとの競合を避けるために、内部の自己保護の状態をアップデートします。

注意: SecureAnywhere に加えて別のセキュリティソフトウェアを使用する場合を除いて、自己保護の設定は [最大] にしておくことをお勧めします。他のセキュリティソフトウェアを併用する場合は、自己保

護の設定を [中] または [最小] に調整してください。[最大] の設定では、他のセキュリティソフトウェアに干渉する場合があります。

設定	説明
自己保護応答のクローキングを有効にする	自己保護をオンおよびオフにします。 この設定は PC エンドポイントにのみ適用されます。
自己保護のレベル	以下の検出レベルに設定することができます。 • **最小** - SecureAnywhere の設定とデータベースの整合性を保護します。エンドポイントが他のセキュリティ製品を複数インストールしている場合にお勧めします。 • **中** - 他のプログラムが保護を無効にできないようにします。他のセキュリティソフトウェアとの互換性を可能な限り最大にします。 • **最大** - SecureAnywhere のプロセスに対する保護を最高レベルにします。この設定を使用することをお勧めします。 この設定は PC エンドポイントにのみ適用されます。

ヒューリスティック

ヒューリスティック設定では、管理されているエンドポイントのスキャン時に SecureAnywhere が実行する脅威分析のレベルを調整できます。SecureAnywhere には、高度なヒューリスティック、経時ヒューリスティック、頻度ヒューリスティックの 3 種類があります。

これらのヒューリスティックは、次のようなさまざまなエリアに対して設定できます。

- **ローカルヒューリスティック** - ローカルドライブ
- **USB ヒューリスティック** - USB ドライブ
- **インターネットヒューリスティック** - インターネット

- **ネットワークヒューリスティック** - ネットワーク
- **CD/DVD ヒューリスティック**- CD/DVD
- **オフラインヒューリスティック** - オフライン時

各エリアに対して、以下のオプション設定が可能です。

- **ヒューリスティックを無効化** - ローカルドライブ、USB ドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時の動作に対するヒューリスティック分析をオフにします。推奨しません。
- **継時/頻度ヒューリスティックの前に高度なヒューリスティックを適用する** - ローカルドライブ、USB ドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時に疑わしい動作がみられる場合に、新しいプログラムと古いプログラムに関して警告を発します。
- **継時/頻度ヒューリスティックの後に高度なヒューリスティックを適用する** - ローカルドライブ、USB ドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時の動作に対する経時/頻度ヒューリスティックの結果に基づいて、疑わしいプログラムに対して高度なヒューリスティックを適用します。
- **正当と見なされていない新規プログラムを実行する場合に警告する** - ローカルドライブ、USB ドライブ、インターネット、ネットワーク、CD/DVD、あるいはオフライン時に悪意のあるまたは不審なプログラム、あるいは未知のプログラムの実行が試みられると警告を発します。この設定では、誤検出が発生する場合がありますので注意してください。

設定	説明
高度なヒューリスティック	新しいプログラムに関して、マルウェアによく見られる疑わしい動作がないか分析します。 • **無効** - 高度なヒューリスティックがオフになり、新しい脅威に対して脆弱な状態となります。ただし、既知の脅威に対しては保護されます。 • **低** - 非常に悪意のあるアクティビティを伴うプログラムを検出します。この設定は一部の疑わしい動作を無視し、ほとんどのプログラムの実行を許可します。 • **中** - 情報を集約したコミュニティデータベースを元に微調整されたヒューリスティックを使用して、検出と誤検知のバランスをとります。 • **高** - さまざまなレベルの新しい脅威から保護します。システムが感染している可能性や、非常に高いリスクにさらされているおそれがある場合は、この設定を使用してください。この設定では、誤検出が発生する場合があります。 • **最大** - 新しい脅威に対して最高レベルの保護を行います。システムが感染している可能性や、非常に高いリスクにさらされているおそれがある場合は、この設定を使用してください。この設定では、誤検出が発生する場合があります。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
経時ヒューリスティック	コミュニティ内で使用された時間の長さに基づいて、新しいプログラムを分析します。正当なプログラムは、通常長期にわたってコミュニティで使用されますが、マルウェアの存在期間は短期である場合が一般的です。 • **無効** - 経時ヒューリスティックがオフになり、新しい脅威に対して脆弱な状態となります。ただし、既知の脅威に対しては保護されます。 • **低** - ごく最近に作成または変更されたプログラムを検出します。 • **中** - 比較的新しい信頼されていないプログラムを検出し、ゼロデイ攻撃やゼロアワー攻撃を防止します。管理されているエンドポイントに一般的でないプログラムをインストールすることを許可せず、変異する脅威を防ぐために追加のセキュリティを必要とする場合に、この設定を使用することをお勧めします。 • **高** - 比較的短期間のうちに作成または変更された、信頼されていないプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムがインストールされることがほとんどなく、システムが比較的安定していると感じる場合にのみお勧めします。この設定では、不明瞭または一般的でないプログラムに対して、誤検検出が多くなることがあります。 • **最大** - ここ最近作成または変更された、信頼できないすべてのプログラムを検出します。この設定は、管理されているエンドポイントがリスクの高い状況にあるか、現在感染していると考えられる場合にのみ使用してください。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
頻度ヒューリスティック	コミュニティでの使用頻度や変更の頻度の統計に基づいて、新しいプログラムを分析します。正当なプログラムはすぐに変わることはありませんが、マルウェアは通常早いペースで変異します。マルウェアはそれぞれのコンピュータに固有のコピーとしてインストールされ、統計上は「非一般的」となることがあります。 • **低** - 初めて確認されたプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムまたはベータプログラムが頻繁にインストールされる場合や、エンドポイントのユーザーが新しいプログラムを頻繁に作成するソフトウェア開発者である場合にお勧めします。 • **中** - 変異している一般的でないプログラムを検出し、ゼロデイ攻撃やゼロアワー攻撃を防止します。この設定は、管理されているエンドポイントに新しいプログラムを頻繁にインストールすることを許可せず、標準の設定よりもセキュリティを強化する必要がある場合に使用することをお勧めします。 • **高** - コミュニティの一定数で確認されたプログラムを検出します。この設定は、管理されているエンドポイントに新しいプログラムをインストールすることを許可せず、現在感染していると疑われる場合にお勧めします。 • **最大** - コミュニティの大多数で確認されたプログラムを検出します。この設定は、管理されているエンドポイントが非常に高いリスクにあると考えられ、厳格なヒューリスティック規則のために誤検出を受信する可能性があることを受け入れる場合にお勧めします。 この設定は PC エンドポイントにのみ適用されます。

リアルタイムシールドの設定

リアルタイムシールドは、ウェブルートの脅威の定義とコミュニティのデータベースにある既知の脅威をブロックします。シールドが疑わしいファイルを検出した場合、警告を発して、そのアイテムをブロックまたは許可するようプロンプトを表示します。既知の脅威が検出された場合、エンドポイントに被害が及んだり情報が盗まれたりする前に、そのアイテムをただちにブロックして隔離します。

設定	説明
リアルタイム シールド有効	リアルタイムシールドをオンまたはオフにします。 この設定は PC および Mac エンドポイントの両方に適用されます。
SecureAnywhere の中央データベースに基づくオフライン保護を有効にする	管理されているエンドポイントに小規模な脅威定義ファイルをダウンロードし、エンドポイントがオフラインのときにも保護します。 この設定はオンのままにしておくことをお勧めします。 この設定は PC エンドポイントにのみ適用されます。
ブロックされたファイルに対するアクションを記憶する	ユーザーが警告に対してどのように対応したか (ファイルを許可したかブロックしたか) を記憶し、次回からは同じファイルを発見した場合にプロンプトを表示しません。 この設定の選択が解除されると、それ以降は、同じファイルが発見されるたびに警告が表示されます。 この設定は PC エンドポイントにのみ適用されます。
以前にブロックされたファイルを自動的に隔離する	脅威が発見された場合に警告を開き、ブロックし隔離先に移動するかの選択をユーザーに求めます。 この設定がオフの場合、ユーザーは手動でスキャンを実行して脅威を削除する必要があります。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
実行時に検出された場合ファイルを自動的にブロックする	脅威をブロックして、隔離先に移動します。 この設定がオフの場合、ユーザーは検出された脅威に関する警告に対応する必要があります。 この設定は PC および Mac エンドポイントの両方に適用されます。
書き込みまたは変更時にファイルをスキャンする	ディスクに保存された新しいファイルまたは変更されたファイルをすべてスキャンします。 この設定がオフの場合、新しいファイルのインストールは無視されます。ただし、脅威が実行されようとしている場合はユーザーに警告が発せられます。 この設定は PC および Mac エンドポイントの両方に適用されます。
ログインしているユーザーがいない場合に自動的に脅威をブロックする	管理されているエンドポイントがログオフしているときでも、脅威が実行されないようにします。脅威は通知なしに隔離先に移動させられます。 この設定は PC および Mac エンドポイントの両方に適用されます。
リアルタイムイベントの警告を表示する	疑わしい動作があった場合に警告を発します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
リアルタイム ブロックの警告を表示する	ヒューリスティックがマルウェアを検出したときに警告を表示し、アクションを許可またはブロックするようユーザーに指示を求めます。 ヒューリスティックが [正当と見なされていない新規プログラムを実行する場合に警告する] に設定されている場合は、この設定を [オン] にする必要があります。この設定を行わないと、ユーザーは警告を見ることができません。 この設定は PC エンドポイントにのみ適用されます。
リアルタイム ブロックのお知らせを表示する	リアルタイムシールドがマルウェアを検出した場合、トレイに通知を表示します。この設定がオフの場合、トレイに通知は表示されませんが、マルウェアはブロックされ、脅威が検出されたことがホーム ページに示されます。 この設定は PC エンドポイントにのみ適用されます。

動作シールドの設定

動作シールドは、管理されているエンドポイント上で実行されるアプリケーションとプロセスを分析します。シールドが疑わしいファイルを検出した場合、警告を発して、そのアイテムをブロックまたは許可するようプロンプトを表示します。既知の脅威が検出された場合、管理対象のエンドポイントに被害が及んだり情報が盗まれたりする前に、そのアイテムをただちにブロックして隔離します。

設定	説明
動作シールド有効	動作シールドをオンまたはオフにします。 この設定は PC エンドポイントにのみ適用されます。
新しいプログラムの実行を許可する前に意図を評価する	プログラムの実行を許可する前に、そのアクティビティを観察します。問題がないようであれば、SecureAnywhere は実行を許可し、動作を監視し続けます。 この設定は PC エンドポイントにのみ適用されます。
複合的な脅威を特定するための高度な動作解釈を有効にする	プログラムを分析し、その目的を調べます。マルウェア プログラムの疑わしいアクティビティの例として、レジストリエントリを変更して電子メールを送信するなどの動作があります。 この設定は PC エンドポイントにのみ適用されます。
高度な脅威の削除を行うため、信頼できないプログラムの動作を追跡する	正当なソフトウェアまたはマルウェアどちらにも分類されていないプログラムの動作を監視します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
警告メッセージを表示するのではなく推奨アクションを自動的に実行	潜在的な脅威の許可またはブロックの選択について尋ねるプロンプトをユーザーに表示しません。SecureAnywhere が、アイテムの管理方法を決定します。 この設定は PC エンドポイントにのみ適用されます。
オフライン時、信頼できないプログラムが低レベルのシステム変更を試行した場合に警告する	管理対象のエンドポイントがオフラインの場合に、未分類のプログラムが変更を加えようとすると、警告が表示されます。エンドポイントがインターネットに接続していないと、SecureAnywhere はオンラインの脅威データベースをチェックできません。 この設定は PC エンドポイントにのみ適用されます。

コアシステムシールド

コアシステムシールドは、管理対象のエンドポイントのシステム構成を監視し、マルウェアによって改ざんされていないか確認します。シールドが変更を試みようとする疑わしいファイルを検出した場合、警告を発してそのアイテムをブロックまたは許可するようプロンプトを表示します。既知の脅威が検出された場合、被害が及んだり情報が盗まれたりする前に、そのアイテムをただちにブロックして隔離します。

設定	説明
コア システム シールド有効	コアシステムシールドをオンまたはオフにします。 この設定は PC エンドポイントにのみ適用されます。
システム変更を実行する前にシステム変更を評価する	新しいサービスのインストールなど、管理対象のエンドポイントに対してシステムの変更を試みる、あらゆるアクティビティを阻止します。 この設定は PC エンドポイントにのみ適用されます。
破損したシステムコンポーネントを検出して修復する	壊れたレイヤード サービスプロバイダー (LSP) のチェーンやウイルスに感染したファイルなど、破損したコンポーネントを検出し、コンポーネントやファイルを元の状態に復元します。 この設定は PC エンドポイントにのみ適用されます。
信頼できないプログラムがカーネル メモリを変更できないようにする	未分類のプログラムがカーネルのメモリを変更しないように阻止します。 この設定は PC エンドポイントにのみ適用されます。
信頼できないプログラムがシステム プロセスを変更できないようにする	未分類のプログラムがシステムのプロセスを変更しないように阻止します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
LSP チェーンと他のシステム構造の整合性を検証する	レイヤード サービス プロバイダー (LSP) のチェーンおよび他のシステム構造がマルウェアの被害を受けないよう監視します。 この設定は PC エンドポイントにのみ適用されます。
どのプログラムも HOSTS ファイルを変更できないようにする	HOSTS ファイルの Web サイトの IP アドレスを追加または変更しようとするスパイウェアを阻止し、変更をブロックまたは許可するようユーザーに警告を表示します。 この設定は PC および Mac エンドポイントの両方に適用されます。

Web 脅威シールド

Web 脅威シールドは、ユーザーがインターネットネットを閲覧中にエンドポイントを保護します。脅威となりうる Web サイトが検出された場合、警告が開き、そのサイトをブロックするか、あるいは警告を無視して続行するかをユーザーが決定できます。ユーザーが検索エンジンを利用するときに、検索結果ページのすべてのリンクを分析し、信頼できるサイトであれば緑のチェックマークを、リスクとなり得るサイトであれば赤い X のマークをそれぞれのリンクの横に表示します。

設定	説明
Web シールドを有効化	Web 脅威シールドをオンまたはオフにします。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
ブラウザのエクステンションをアクティブ化	ブラウザエクステンションを使って、悪意のある Web サイトに対するブロック保護、リアルタイムのフィッシング対策保護、検索エンジンを使用する際の安全評価を行います。各機能に対し、この表で説明する個別のコントロールを使用することにより、各機能を別々に有効化または無効化することができます。 エクステンションを完全に無効化し、サポートされる各ブラウザから削除するには、この設定をオフに変更してください。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC エンドポイントにのみ適用されます。
悪意のある Web サイトをブロック	ブラウザに入力したすべての URL および IP はチェックされ、既知の悪意があるサイトについてはブロック ページが表示されます。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。

設定	説明
リアルタイム アンチフィッシングを有効にする	ゼロデイフィッシングサイトから保護します。ゼロデイ フィッシング サイトとは、これまで検出されたことがなく、関連のウイルスに定義がまだないサイトです。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
検索エンジンを使用する際に安全評価を表示する	検索結果にはアイコンとツールヒントの注釈が付き、悪意のあるサイトである確率が示されます。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
Web フィルタリング ドライバを有効化	悪意のある接続に対してさらなる保護を提供し、場合によってはブラウザのエクステンションを無効化します。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
ブロックされた Web サイトをユーザーが回避する機能を無効化	悪意のある Web サイトが検出された場合に表示されるブロックページを、ユーザーが回避できないようにします。この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。
ユーザーが Web サイトの評価をリクエストする機能を無効化	悪意のある Web サイトが検出された場合に、ブロックページからユーザーが Web サイトの評価を送信できないようにします。 この設定はデフォルトで選択されており、これが推奨設定です。 この設定は PC および Mac エンドポイントの両方に適用されます。

ID シールド

ID シールドは、オンライントランザクションを実行中に脅威にさらされる可能性のある重要なデータを保護します。ID シールドの動作を変更したり、ブロックする対象を制御したりできます。

設定	説明
ID シールド有効	ID シールドをオンまたはオフにします。 この設定は PC および Mac エンドポイントの両方に適用されます。 **注意:** Mac では、セキュアキーボード入力モードの設定を制御します。
オンライン上の個人情報に対する脅威を探す	ユーザーがインターネットを閲覧したり、リンクを開いたりする際に、Web サイトを分析します。シールドが悪意のあるコンテンツを検出した場合、そのサイトはブロックされ、警告が発せられます。 この設定は PC エンドポイントにのみ適用されます。
アクセス時に Web サイトを検証して正当性を判別する	それぞれの Web サイトの IP アドレスを分析して、リダイレクトされたか、ブラックリストに記載されているかを判断します。シールドが違法な Web サイトを検出した場合、サイトをブロックして警告を発します。 この設定は PC エンドポイントにのみ適用されます。
Web サイトの DNS/IP 解決を検証して中間者攻撃を検出する	ユーザーを悪意のある Web サイトにリダイレクト (中間者攻撃など) する可能性のあるサーバーを検索します。シールドが中間者攻撃を検出した場合、脅威をブロックして警告を発します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
Web サイトが危険度の高い追跡情報を作成しないようブロックする	サードパーティの Cookie が悪意のある追跡型 Web サイトからのものである場合、それらが管理対象のエンドポイントにインストールされるのをブロックします。 この設定は PC エンドポイントにのみ適用されます。
保護された認証情報にプログラムがアクセスできないようにする	プログラムがユーザーのログイン資格情報にアクセスしないようブロックします。たとえば、ユーザーが名前やパスワードを入力したり、Web サイトでそのような情報を記憶するよう指定したりする際にブロックします。 この設定は PC エンドポイントにのみ適用されます。
信頼できないプログラムが保護されたデータにアクセスするのをブロックする前に警告する	マルウェアがデータにアクセスしようとしたときに、既知のマルウェアを自動的にブロックすることはせず、必ず警告を発します。 この設定は PC エンドポイントにのみ適用されます。
信頼された画面キャプチャ プログラムが保護された画面の内容にアクセスすることを許可	画面に表示されているコンテンツに関係なく、正当なスクリーン キャプチャ プログラムを使用できるようにします。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
ID シールド対応モードを有効にする	通常処理で ID シールドがブロックする可能性のある特定のアプリケーションの実行を許可します。このオプションは、SecureAnywhere がエンドポイントにインストールされた後でアプリケーションの機能に問題がある場合に有効化することができます。この対応モードが有効化されていても、エンドポイントは ID シールドのコア機能により保護されています。 この設定は PC エンドポイントにのみ適用されます。
非ラテン語のシステム上でキーロギング保護機能を有効にする	日本語や中国語など非ラテン語のシステムを使用するエンドポイントを、キーロガーから保護します。 この設定は PC エンドポイントにのみ適用されます。

ファイアウォール

ウェブルートのファイアウォールは、エンドポイントのポートから出ていくデータトラフィックを監視します。インターネットに接続して個人情報を盗もうとする、信頼できないプロセスを探します。一方で、Windows ファイアウォールは、管理対象のエンドポイントに入力されるデータトラフィックを監視します。ウェブルートと Windows のファイアウォールをどちらも有効にしておけば、ネットワークデータの出入口を完全に保護することができます。

ウェブルートのファイアウォールは、管理対象のエンドポイント上のトラフィックをフィルタリングするよう設定されています。通常のアクティビティを中断することなく、バックグラウンドで動作します。ファイアウォールが判別できないトラフィックを検出した場合には、警告を発します。その際には、そのトラフィックをブロックするか許可するかを決定します。

設定	説明
有効	ファイアウォールのオン / オフを切り替えます。 この設定は PC エンドポイントにのみ適用されます。
ファイアウォールのレベル	• **デフォルトで許可** - 明示的にブロックされている場合を除き、すべてのプロセスにインターネットへの接続を許可します。 • **不明および感染している場合に警告** - 新しい信頼できないプロセスがインターネットに接続する場合やエンドポイントが感染している場合に警告します。 • **不明の場合に警告** - 新しい信頼できないプロセスがインターネットに接続する場合に警告します。 • **デフォルトでブロック** - 明示的にブロックされている場合を除き、すべてのプロセスがインターネットに接続する際に警告します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
ファイアウォール管理の警告を表示する	Windows ファイアウォールがオフになっている場合に SecureAnywhere により表示される警告を制御します。 • **オン** - SecureAnywhere によって Windows ファイアウォールがオフであることが検出されると警告が表示されます。 • **オフ** - Windows ファイアウォールがオフになっていても警告は表示されません。 この設定は PC エンドポイントにのみ適用されます。
ファイアウォールプロセスの警告を表示する	ファイアウォールの警告を制御します。この設定がオフの場合、ファイアウォールの警告は表示されません。このオプションはファイアウォールのレベルの設定と連携して機能します。 例: • [ファイアウォールプロセスの警告を表示する] と [デフォルトでブロック] のオプションが両方ともオンに設定されている場合、新しいプロセスが接続を試みると、エンドポイントのユーザーに警告が表示されます。 • [ファイアウォールプロセスの警告を表示する] がオフに設定されている場合は、エンドポイントのユーザーに警告は表示されず、プロセスは許可されます。 この設定は PC エンドポイントにのみ適用されます。

ユーザーインターフェイス

このポリシーを使用するエンドポイント上で、SecureAnywhere のインターフェイスを管理制御できます。

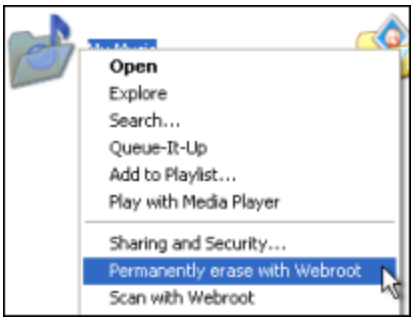
設定	説明
GUI	エンドポイントのユーザーによる SecureAnywhere メインインターフェイスへのアクセスをブロックまたは許可します。 このオプションが [非表示] に設定されている場合にユーザーが SecureAnywhere を開こうとすると、インターフェイスにアクセスするには管理者に問い合わせるよう案内するメッセージが表示されます。 この設定は PC および Mac エンドポイントの両方に適用されます。 **注意:** このオプションでも PC のシステムトレイのウェブルートのアイコンは非表示になりません。ただし、Mac ではこのアイコンが非表示になります。

システム最適化ツール

システム最適化ツールは、エンドユーザーのウェブの閲覧履歴、コンピュータ使用状況についてのファイル、貴重なディスク容量を消費する不要なファイル (ごみ箱内のファイルや Windows の一時ファイルなど) を削除します。システム最適化ツールは自動的には実行されません。最適化をスケジュールし、削除するアイテムを選択する必要があります。

注意: 最適化によって削除されるのは不要なファイルと痕跡です。マルウェアの脅威は除去されません。マルウェアはスキャン中に削除されます。システム最適化ツールはコンピュータの掃除係、スキャンは警備係であると考えることができます。

設定	説明
システム最適化ツールを集中管理	管理者はシステム最適化ツールの設定を以下のように変更することができます。 • **オン** - システム最適化ツールの設定はパネルに表示され、設定の変更が可能です。 • **オフ** - このパネルに設定は表示されません。 この設定は PC エンドポイントにのみ適用されます。
スケジュール	
曜日での設定	システム最適化ツールを自動的に実行する曜日を 1 から 7 までで設定します。 この設定は PC エンドポイントにのみ適用されます。
指定時間での実行 - 時	エンドポイントでシステム最適化ツールを実行する時刻を設定します。 この設定は PC エンドポイントにのみ適用されます。
指定時間での実行 - 分	エンドポイントでシステム最適化ツールを実行する時刻を 15 分単位で設定します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
スケジュールされた時刻にコンピュータの電源がオフの場合は、起動時にスキャンする	エンドポイントを起動した際に、スケジュールどおりに実行されなかったクリーンアップを実行します。これは、クリーンアップをスケジュールした時刻にエンドポイントがオフであった場合にのみ実行されます。これを設定しない場合、実行されなかったクリーンアップはスキップされます。 この設定は PC エンドポイントにのみ適用されます。
Windows エクスプローラーの右クリックで安全なファイル消去を有効にする	エンドポイントで、ファイルまたはフォルダを完全に削除するオプションを Windows エクスプローラーに追加します。ファイルまたはフォルダを右クリックすると、次のメニューアイテムが表示されます。  この設定は PC エンドポイントにのみ適用されます。
Windows デスクトップ	
ごみ箱	Windows エクスプローラーのごみ箱からすべてのファイルを削除します。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
最近使ったドキュメント履歴	Windows の [スタート] メニューからアクセス可能な、最近開いたファイルの履歴をクリアします。クリーンアップでは実際のファイルは削除されません。 この設定は PC エンドポイントにのみ適用されます。
スタート メニューのクリック履歴	エンドユーザーが [スタート] メニューを使用して最近開いたプログラムのショートカットの履歴をクリアします。 この設定は PC エンドポイントにのみ適用されます。
実行履歴	[スタート] メニューからアクセス可能な [ファイル名を指定して実行] ダイアログに最近入力したコマンドの履歴をクリアします。 [ファイル名を指定して実行] ダイアログからアイテムを完全に削除するには、クリーンアップ後にコンピュータを再起動しなければならない場合があります。 この設定は PC エンドポイントにのみ適用されます。
検索履歴	エンドユーザーがコンピュータで検索したファイルやその他の情報の履歴をクリアします。 検索履歴が保存されていると、エンド ユーザーが新しい検索の入力を開始した際に、同じ文字で始まる最近の検索が表示されます。クリーンアップでは実際のファイルは削除されません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
スタート メニューの並べ替え履歴	[スタート] メニューのプログラムとドキュメントのリストを、デフォルトの設定であるアルファベット順に戻します。 クリーンアップの実行後、システムを再起動すると、一覧がアルファベット順に戻ります。 この設定は PC エンドポイントにのみ適用されます。
Windows システム	
クリップボードの内容	Windows のすべてのプログラムでは、コピーまたは切り取りの機能を使用するとデータがクリップボードに保管されます。このクリップボードの内容をクリアします。 この設定は PC エンドポイントにのみ適用されます。
Windows 一時フォルダ	Windows 一時フォルダにあるすべてのファイルとフォルダを削除します (現在開いているプログラムで使用中のファイルは削除されません)。 通常このフォルダは C:\Windows\Temp です。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
システム一時フォルダ	システム一時フォルダにあるすべてのファイルとフォルダを削除します (現在開いているプログラムで使用中のファイルは削除されません)。 通常このフォルダは C:\Documents and Settings\[username]\Local Settings\Temp にあります。 この設定は PC エンドポイントにのみ適用されます。
Windows Update 一時フォルダ	このフォルダにあるすべてのファイルとフォルダを削除します (現在開いているプログラムで使用中のファイルは削除されません)。 これらのファイルは、Windows Update の実行時に Windows によって使用されます。これらのファイルは通常 C:\Windows\Software\Distribution\Download にあります。 この設定は PC エンドポイントにのみ適用されます。
Windows レジストリストリーム	Windows レジストリに対して最近行った変更の履歴をクリアします。 このオプションは、レジストリへの変更そのものを削除するものではありません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
デフォルト ログオン ユーザー履歴	コンピュータへの前回のログオンで使用された名前を保存する Windows レジストリエントリを削除します。 このレジストリエントリを削除すると、コンピュータの電源を入れたとき、またはコンピュータを再起動したときに、毎回ユーザー名を入力する必要があります。このクリーンアップ オプションは、デフォルトの "ようこそ" 画面を使用するコンピュータには影響しません。 この設定は PC エンドポイントにのみ適用されます。
メモリダンプ ファイル	特定の Windows エラーが発生した際に作成されるメモリダンプファイル (memory.dmp) を削除します。このファイルには、エラーの発生時に起きた事柄に関する情報が保存されています。 この設定は PC エンドポイントにのみ適用されます。

CD 書き込みストレージ フォルダ	Windows に内蔵の機能を使用して CD にファイルをコピーした際に作成される Windows プロジェクトファイルを削除します。通常、これらのプロジェクトファイルは次のいずれかのディレクトリに保存されています。
	
	`C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning`
	
	または
	
	`C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn`
	
	この設定は PC エンドポイントにのみ適用されます。

設定	説明
Flash cookie	Adobe Flash によって作成されたデータを削除します。これらのデータはユーザー設定などを追跡しているため、プライバシーの問題につながる可能性があります。 Flash Cookie は実際には Cookie ではなく、ブラウザの Cookie のプライバシー制御では制御されません。 この設定は PC エンドポイントにのみ適用されます。
Internet Explorer	
アドレスバー履歴	Internet Explorer のオートコンプリート機能の一部として保管される、最近表示した Web サイトのリストを削除します。 このリストは、Internet Explorer ブラウザの上部にあるアドレスバーの右側の矢印をクリックすると、ドロップダウンリストとして表示されます。 この設定は PC エンドポイントにのみ適用されます。
Cookie	エンドポイントからすべての Cookie を削除します。すべての Cookie ファイルを削除した場合、エンドユーザーは Cookie に保存されているパスワードやショッピングカートの内容などを再入力しなければならない点に注意してください。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
一時インターネット ファイル	エンド ユーザーが最近閲覧した Web ページのキャッシュされたコピーを削除します。 Web ページをキャッシュするとページを素早く表示できるためパフォーマンスが向上しますが、ハードドライブで大量の領域が消費されることもあります。 この設定は PC エンドポイントにのみ適用されます。
URL 履歴	Internet Explorer のツールバーで表示される最近訪問した Web サイトの履歴のリストを削除します。 この設定は PC エンドポイントにのみ適用されます。
ログの設定	Internet Explorer のアップデート中に作成されたログファイルを削除します。 この設定は PC エンドポイントにのみ適用されます。
Microsoft ダウンロード フォルダ	Internet Explorer を使用して前回のダウンロード済みファイルを保存しているフォルダのコンテンツを削除します。 この設定は PC エンドポイントにのみ適用されます。
MediaPlayer バー履歴	Internet Explorer でメディアプレーヤーを使用して最近開いたオーディオファイルとビデオファイルの一覧を削除します。クリーンアップでは、ファイルのそのものは削除されません。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
オートコンプリート フォーム情報	エンド ユーザーが Web サイトのフィールドに情報を入力した際に Internet Explorer によって保存されたデータを削除します。 これは Internet Explorer のオートコンプリート機能の一部です。 この設定は PC エンドポイントにのみ適用されます。
Index.dat の消去 (再起動時に消去)	index.dat ファイル内のファイルを削除対象としてマークし、システムの再起動後にこれらのファイルをクリアします。 index.dat ファイルは、Web アドレス、検索クエリ、および最近開いたファイルを記録する Windows リポジトリで、随時情報が追加されていきます。このオプションは、Cookie、一時インターネットファイル、URL 履歴のうち 1 つ以上を選択している場合に機能します。Index.dat はアクティブなデータベースのように機能します。このファイルがクリーンアップされるのは Windows を再起動した後のみです。 この設定は PC エンドポイントにのみ適用されます。

設定	説明
安全なファイル削除	
ファイルの削除時に適用するセキュリティのレベルを制御する	ファイルをランダムな文字で上書きする "ワイププロセス" を使用して、ファイルを完全に削除します。このワイプ プロセスを利用すれば、誰かが復元ツールを使用してエンドポイントのファイルの内容を見るおそれもありません。 デフォルトでは、ファイル削除は [標準] に設定されており、アイテムはごみ箱には入らず永久に削除されます。ただし、この [標準] 設定で削除されたファイルは、データ復元ユーティリティにより復元できる場合があります。 ファイルを確実に復元できないようにするには、[最大] を選択します。[中] ではファイルが 3 回上書きされ、[最大] では 7 回上書きされて、ファイルの周辺の領域がクリーンアップされます。なお、[中] または [最大] を選択すると、クリーンアップにかかる時間が長くなることに注意してください。 この設定は PC エンドポイントにのみ適用されます。

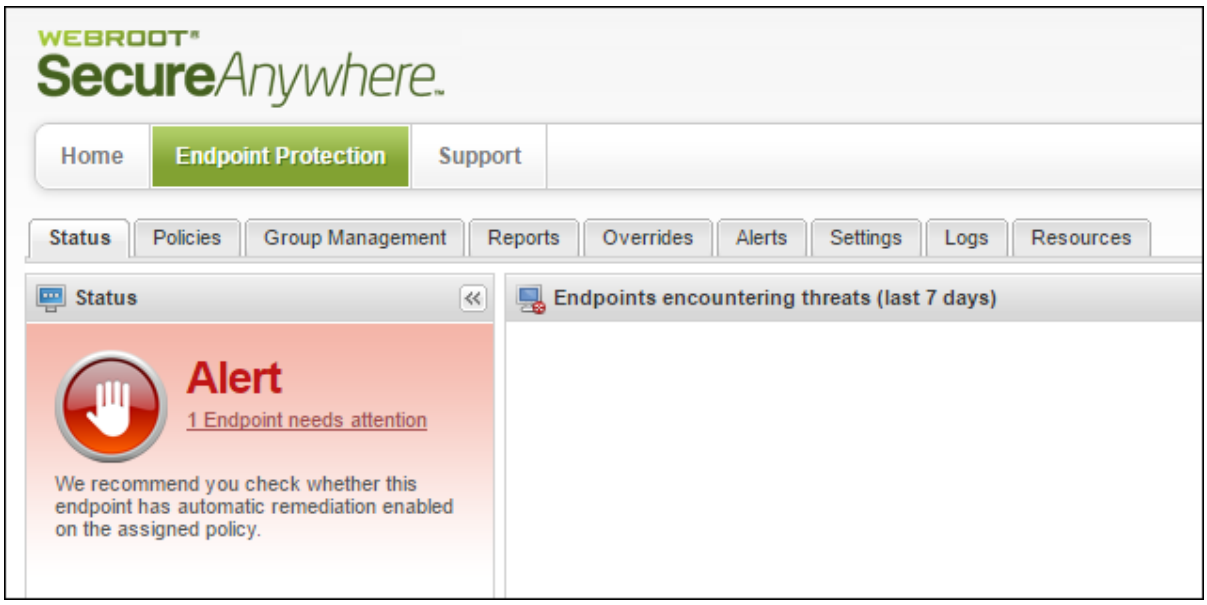
ポリシーに割り当てられたエンドポイントの表示

[ポリシー] タブで、ポリシーに割り当てられたエンドポイントを簡単に確認できます。

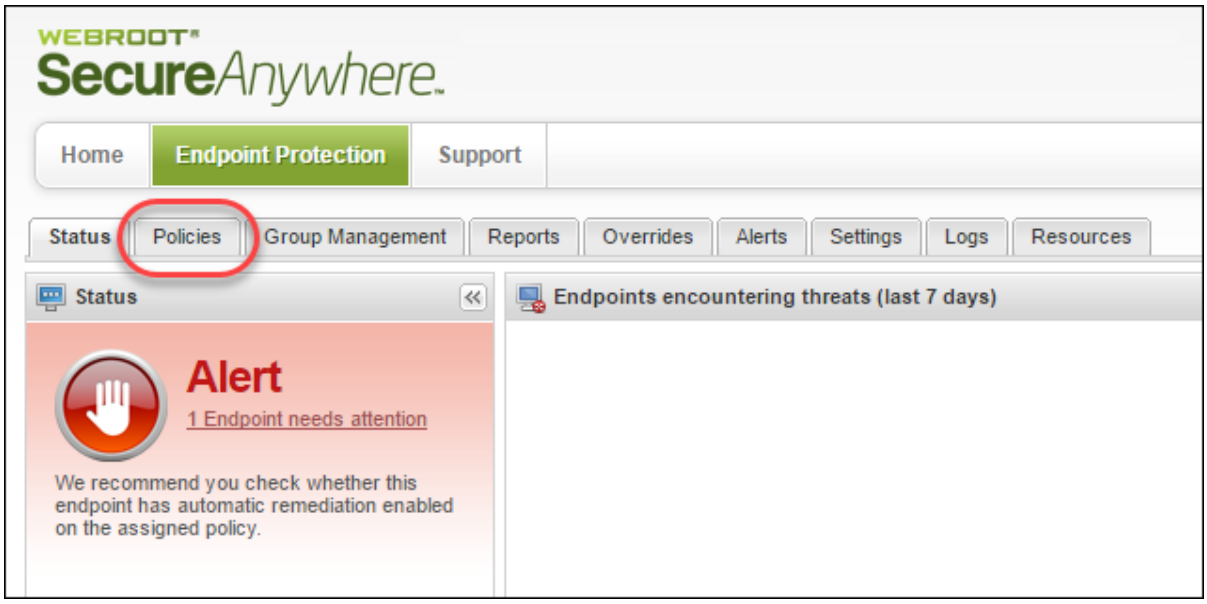
ポリシーに割り当てられたエンドポイントを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

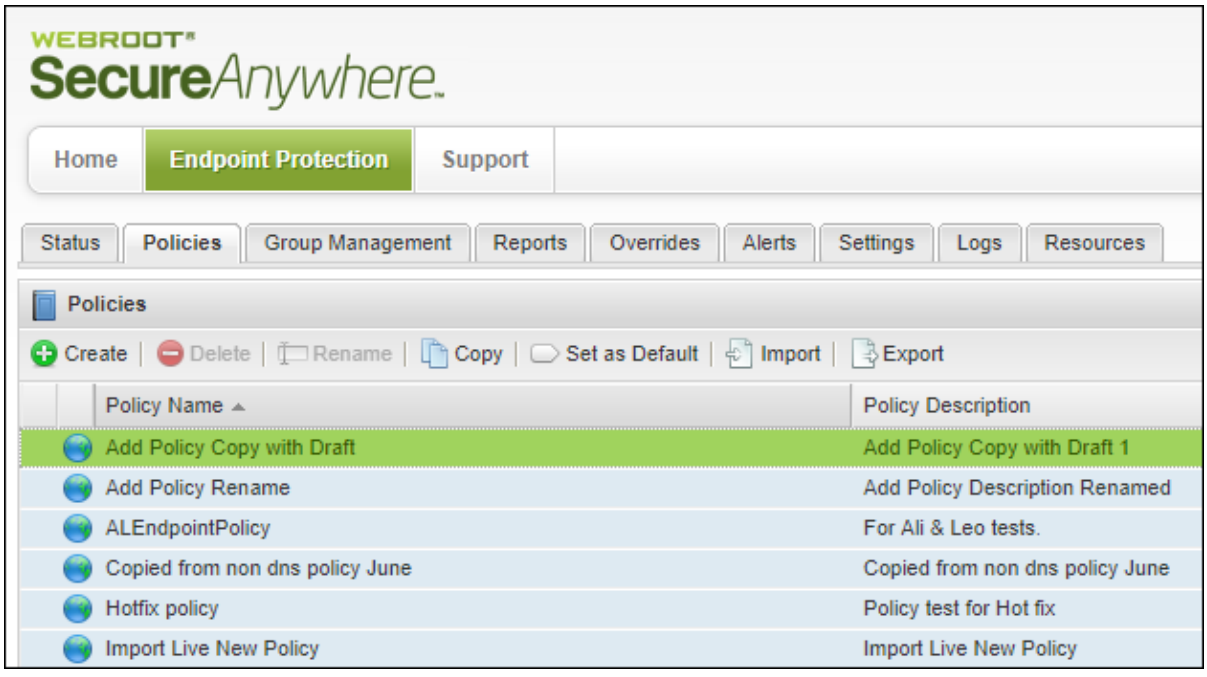
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



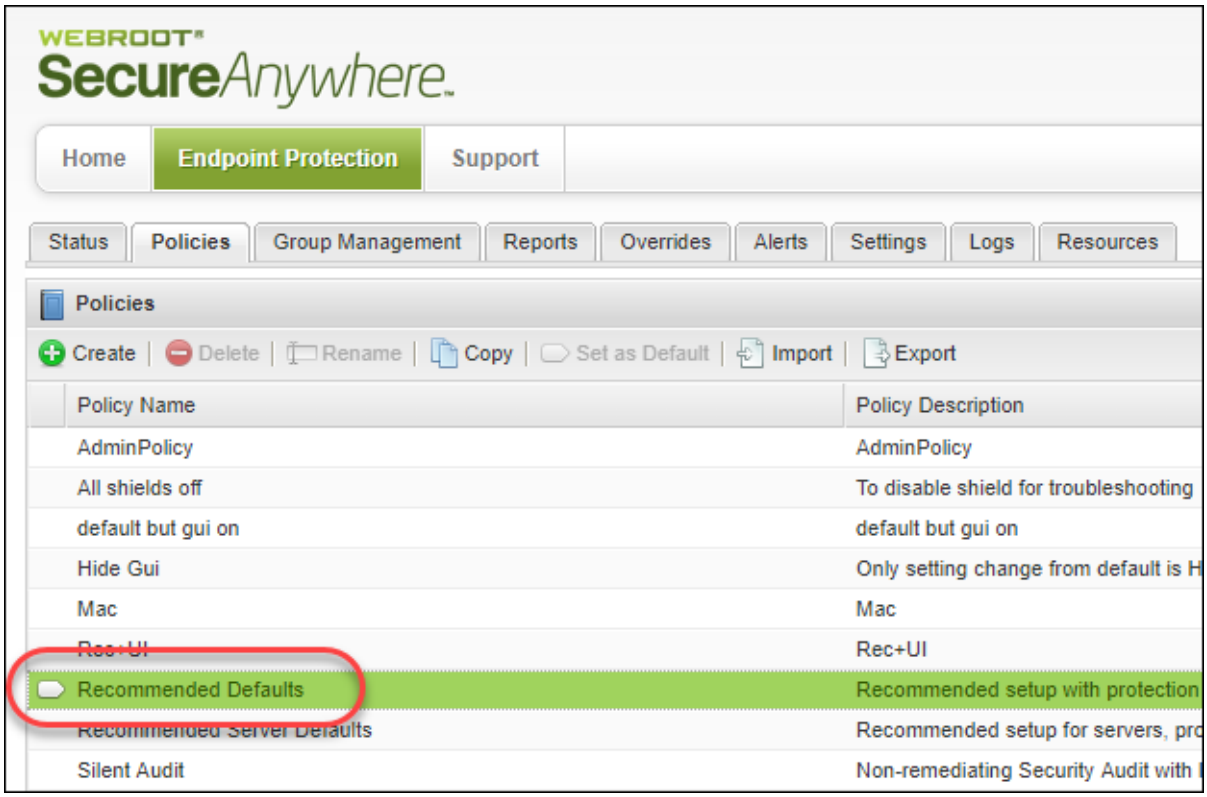
2. [**ポリシー**] タブをクリックします。



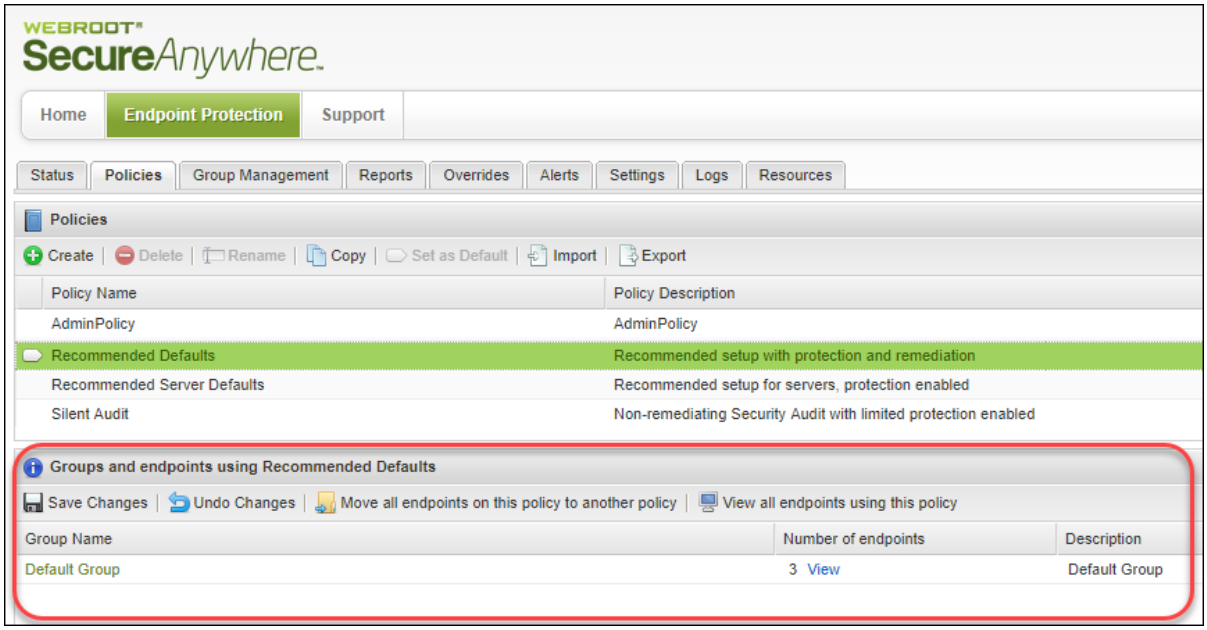
[ポリシー] タブが表示されます。



3. [ポリシー名] カラムで、エンドポイントの情報を表示するポリシーを選択します。



グループとエンドポイントのエリアに、選択したポリシーを使用するグループが表示されます。

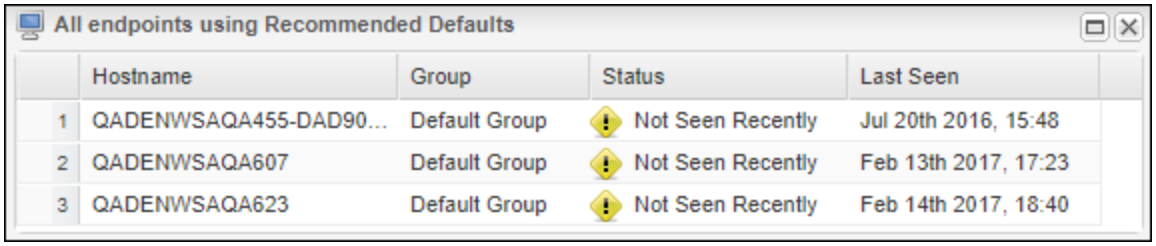


4. エンドポイントに関する情報を表示するには、次のいずれかの操作を行います。

- コマンドバーの [**このポリシーを使用するすべてのエンドポイントを表示**] をクリックします。

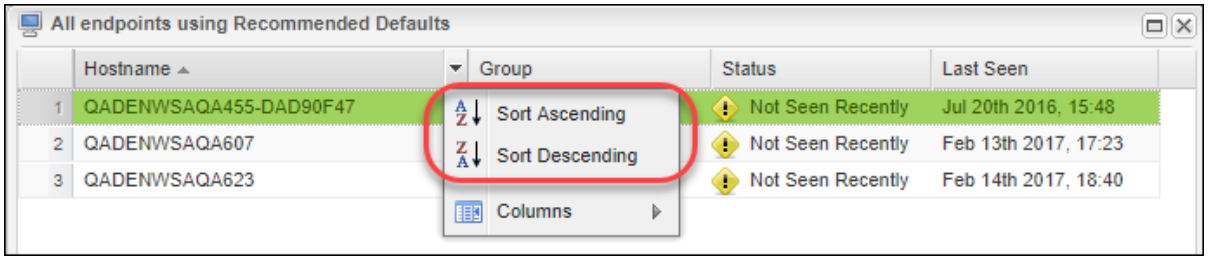
- グループの行で [**表示**] リンクを選択します。

[推奨デフォルト設定を使用するすべてのエンドポイント] ウィンドウが表示されます。



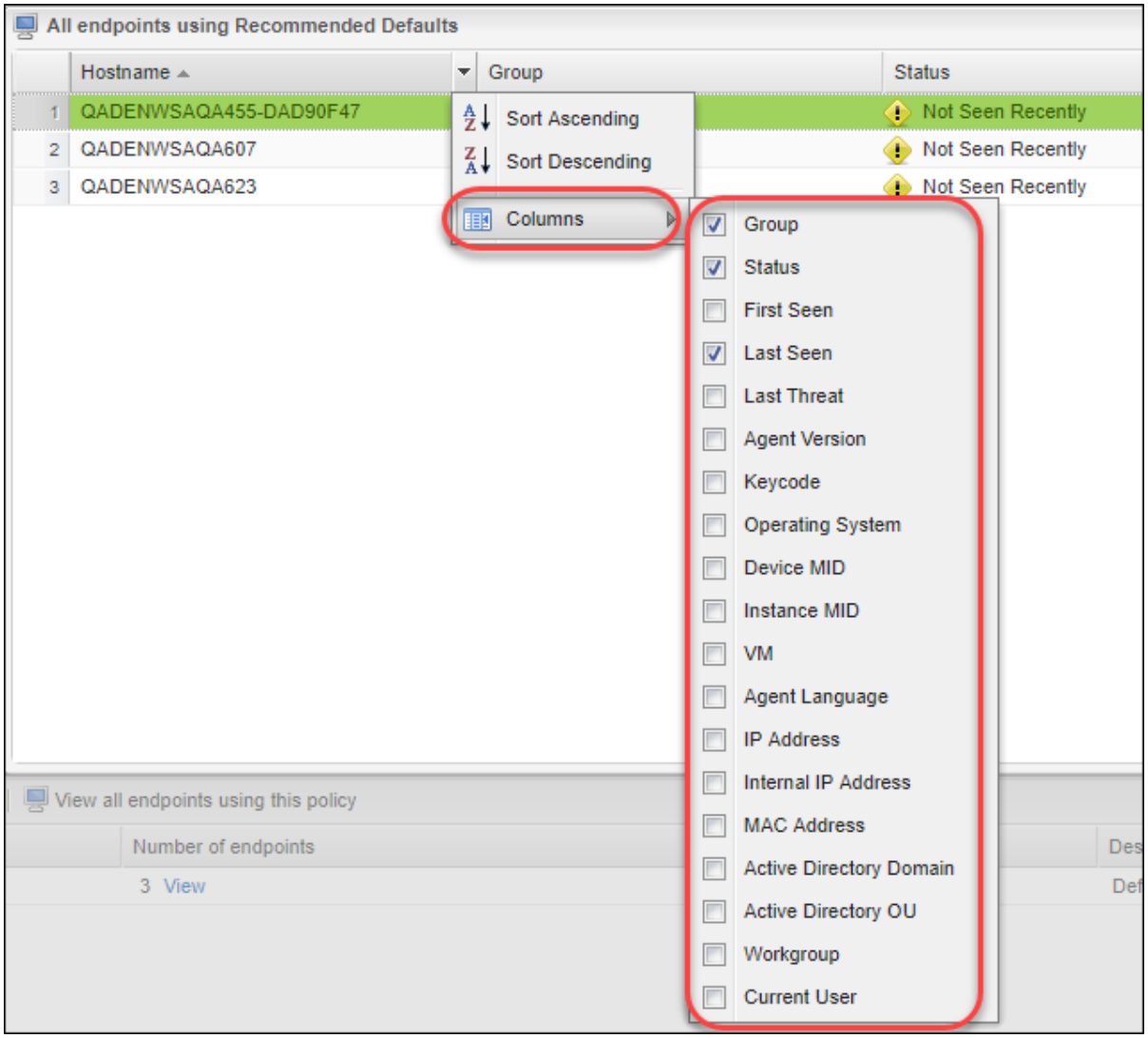
5. 必要に応じて、任意のカラム見出しをクリックし、次のいずれか、または両方の操作を行います。

- 次のいずれかを選択し、カラムを並べ替えます。
  - **昇順に並べ替え**
  - **降順に並べ替え**



- [**カラム**] を選択し、次のいずれかの操作を行います。
  - 表示するカラムのチェックボックスを選択する。

- 非表示にするカラムのチェックボックスの選択を解除する。



カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

ポリシー間でのエンドポイントの移動

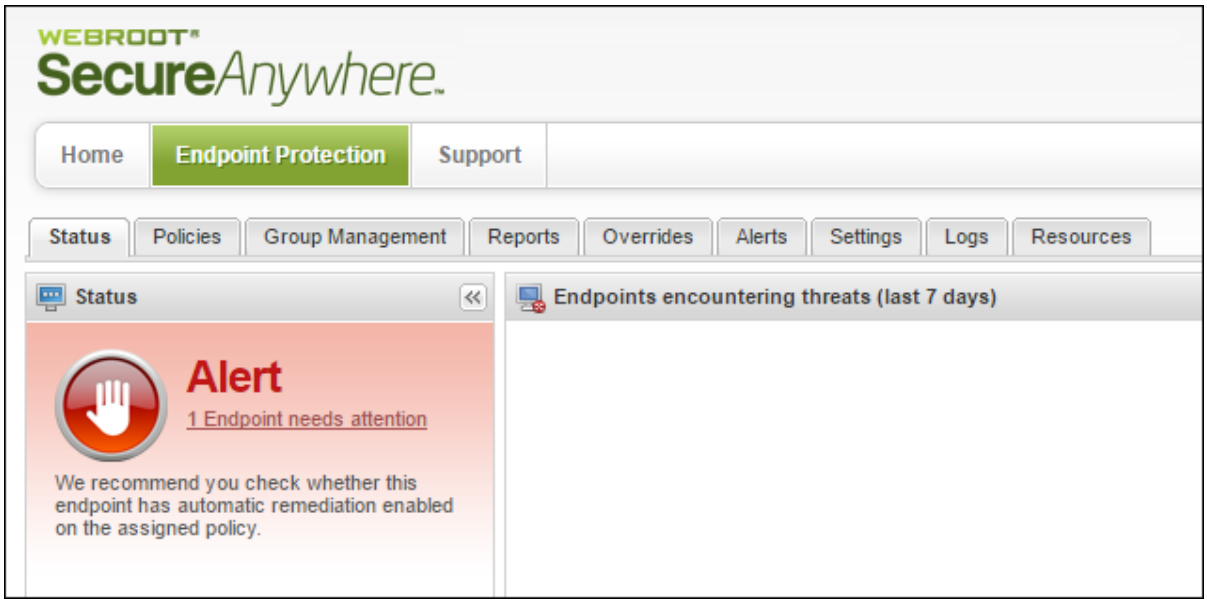
[ポリシー] タブで、1 つのポリシーに割り当てられたエンドポイントをすべて別のポリシーに移動することができます。

注意: 個々のエンドポイントをポリシーに移動する手順については、「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

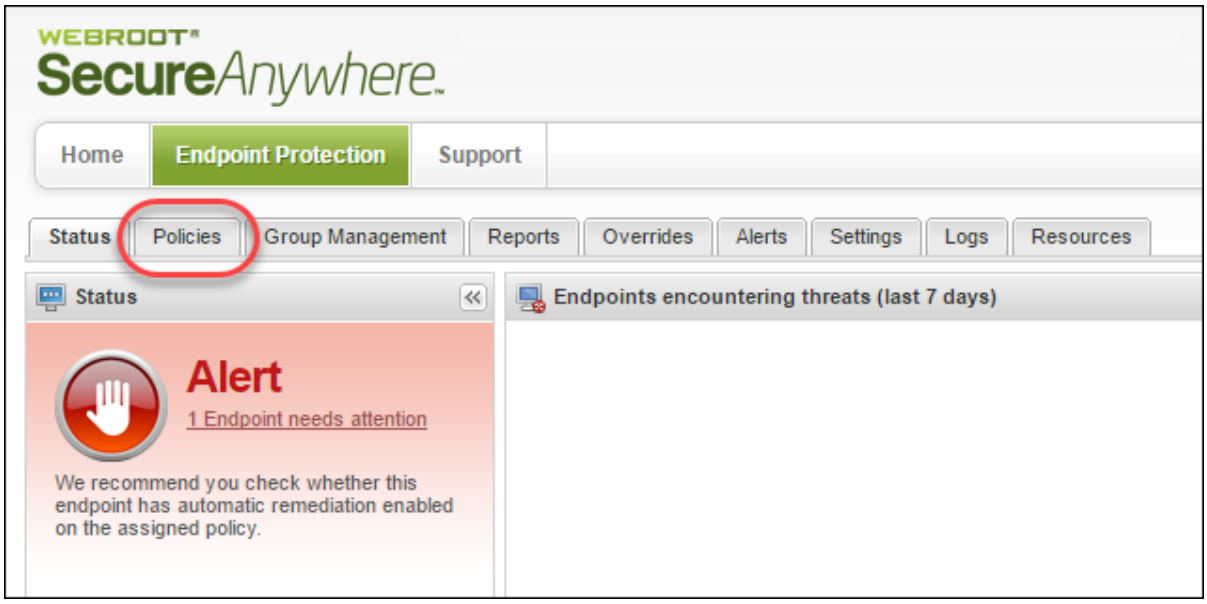
エンドポイントをポリシー間で移動するには

1. エンドポイントプロテクションのコンソールにログインします。

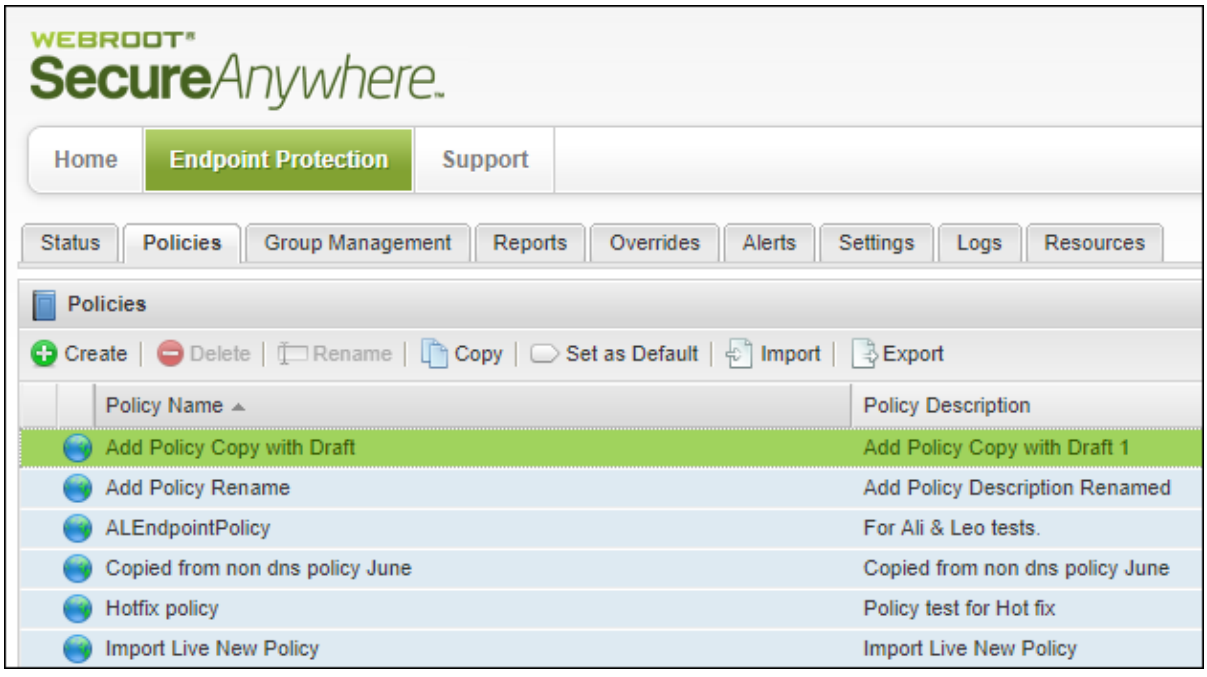
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



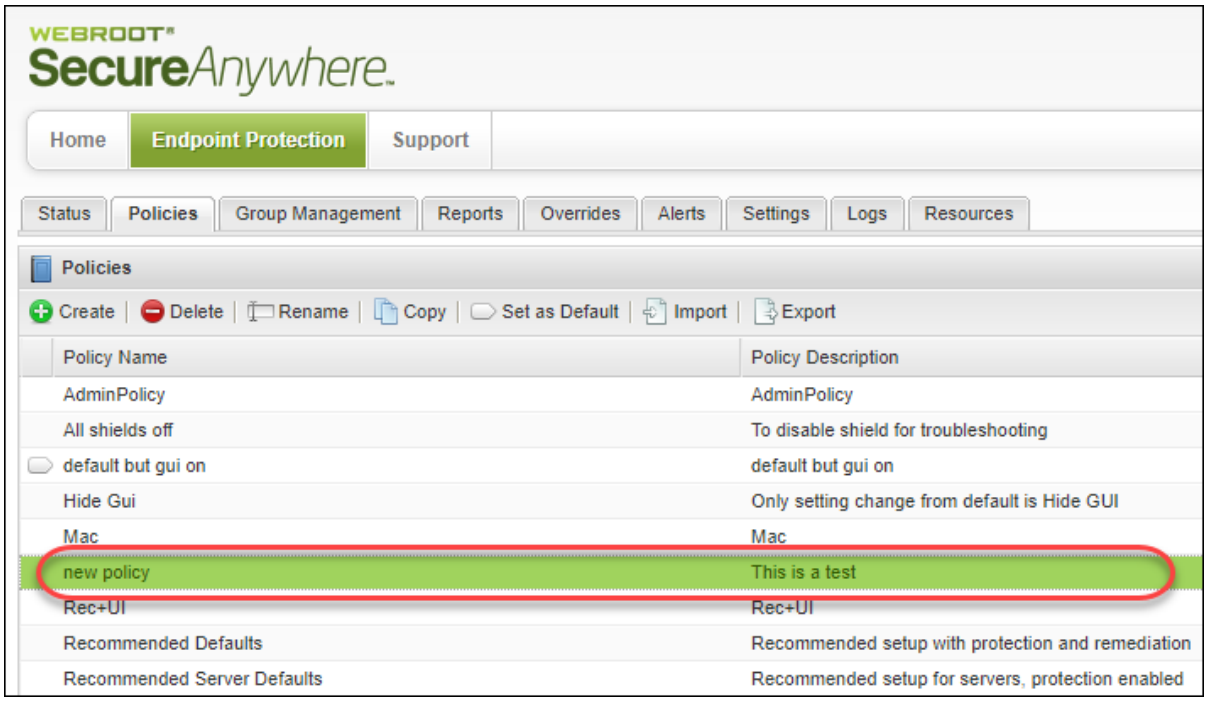
2. [**ポリシー**] タブをクリックします。



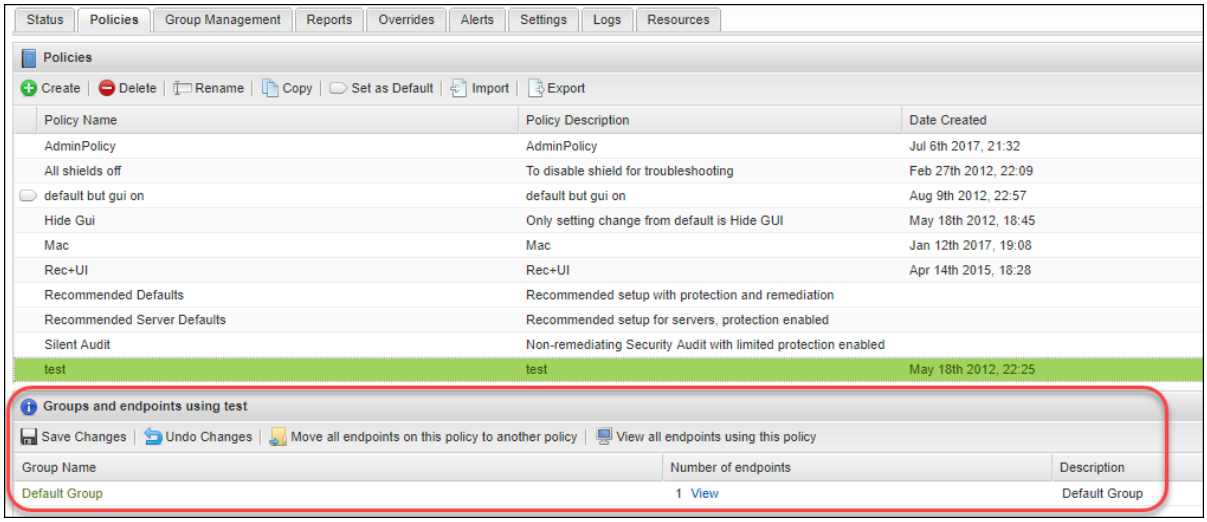
[ポリシー] タブが表示されます。



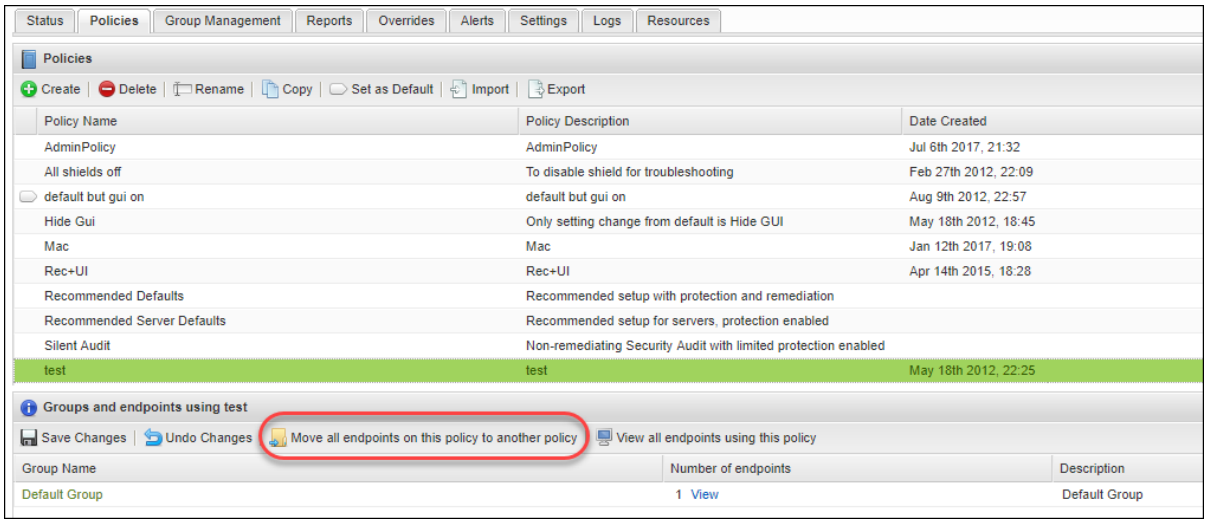
3. [ポリシー名] カラムから移動するポリシーを選択します。



下のパネルに、このポリシーを使用するグループが一覧表示されます。

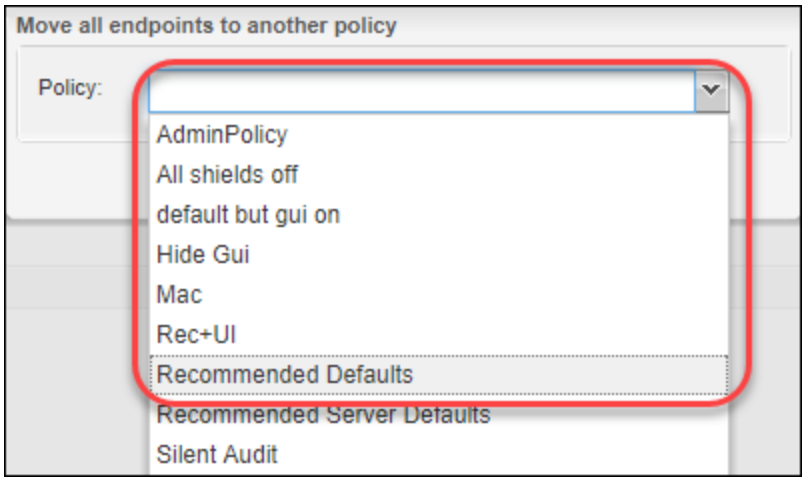


4. [**このポリシーのすべてのエンドポイントを別のポリシーに移動**] ボタンをクリックします。

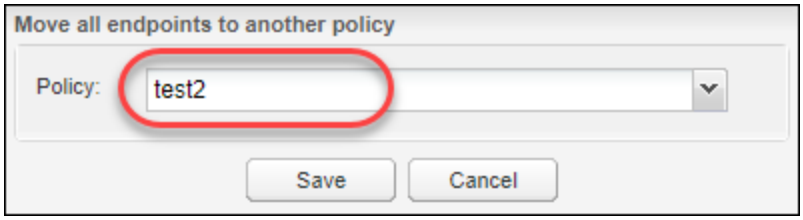


[すべてのエンドポイントを別のポリシーに移動] ウィンドウが表示されます。

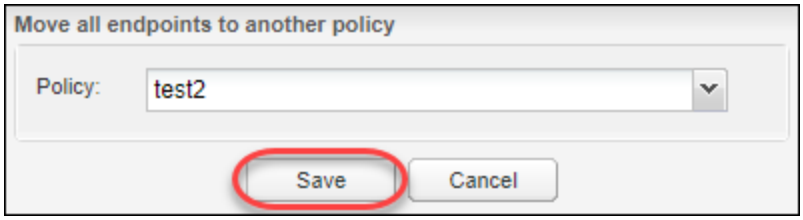
5. [**ポリシー**] ドロップダウンメニューのポリシーの一覧から、エンドポイントの移動先ポリシーを選択します。



[ポリシー名] フィールドに、選択したポリシーの名前が反映されます。



6. **保存**] ボタンをクリックします。



7. ポリシーのリストで、新しいエンドポイントが変更した割り当てに表示されていることを確認します。

詳細については、「*ポリシーに割り当てられたエンドポイントの表示 ページ301*」を参照してください。

ポリシーの削除

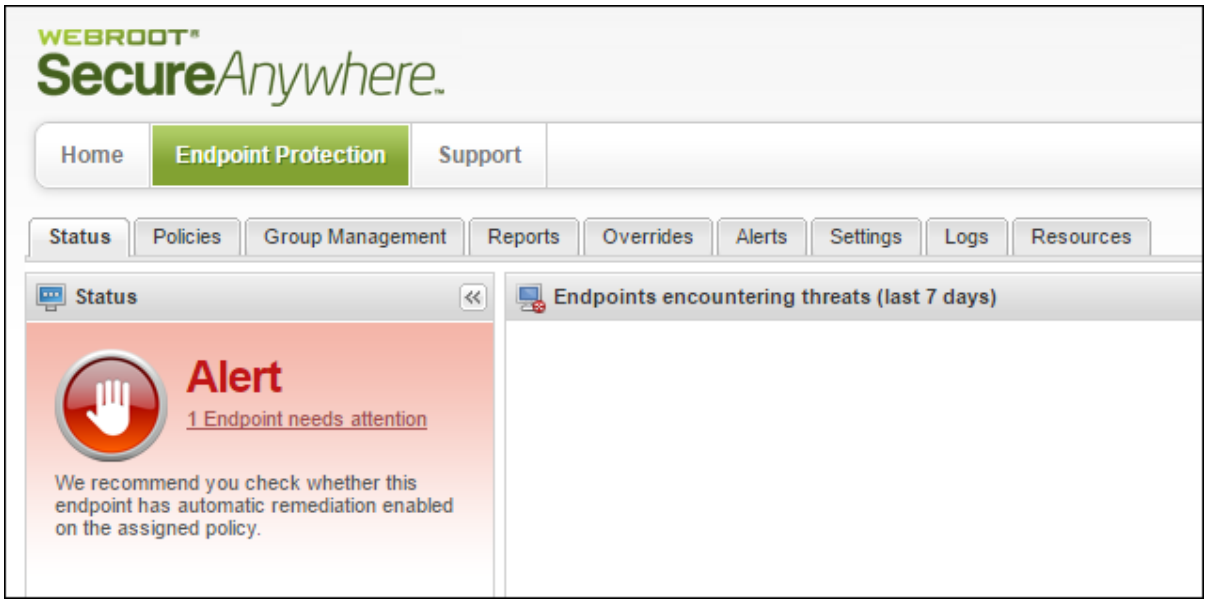
デフォルトのポリシーを除くすべてのポリシーを削除することができます。ポリシーを削除するとアクティブなポリシーのリストから削除され、削除したポリシーのリストに移されます。削除したポリシーはレポートログで確認できます。

注意: ポリシーを削除した場合、同じポリシー名を再び使用することはできません。また、削除したポリシーを復元することはできません。ただし、コピーして名前を変更することは可能です。

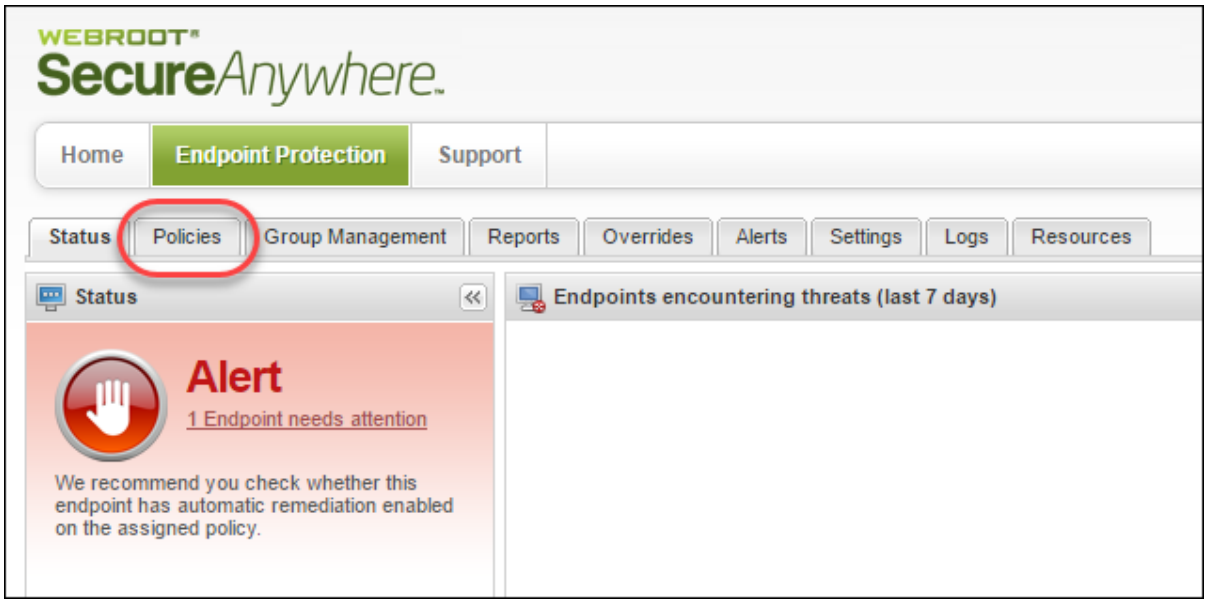
ポリシーを削除するには

1. エンドポイント プロテクションのコンソールにログインします。

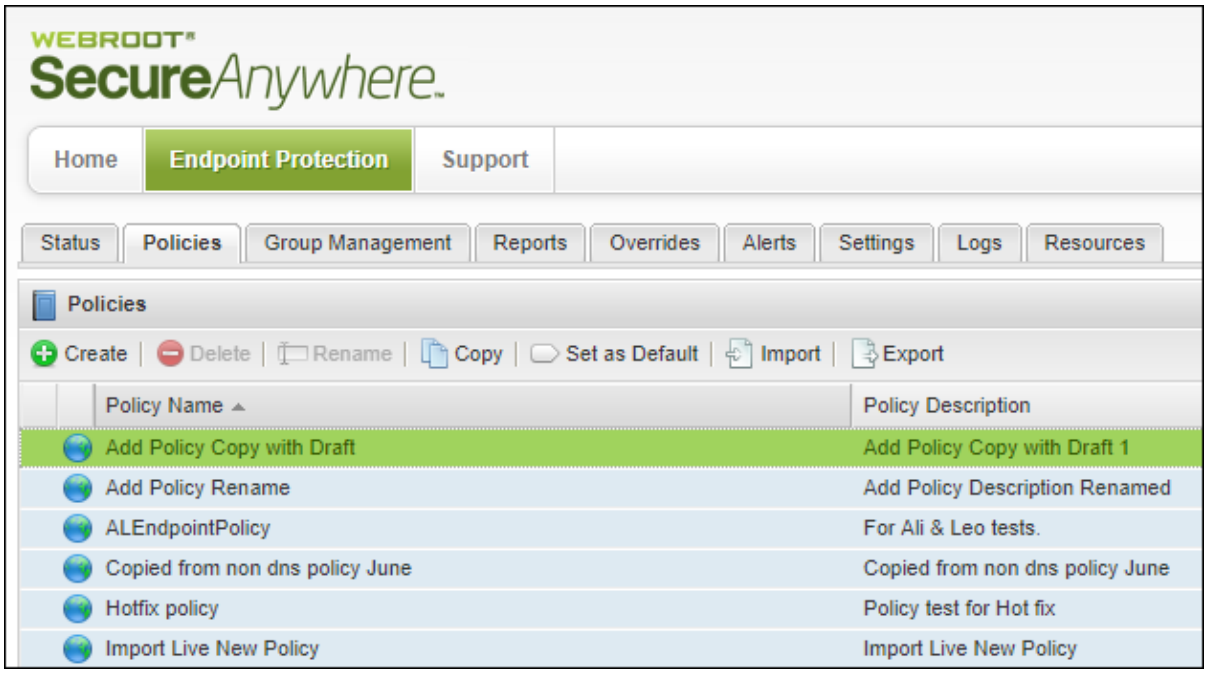
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



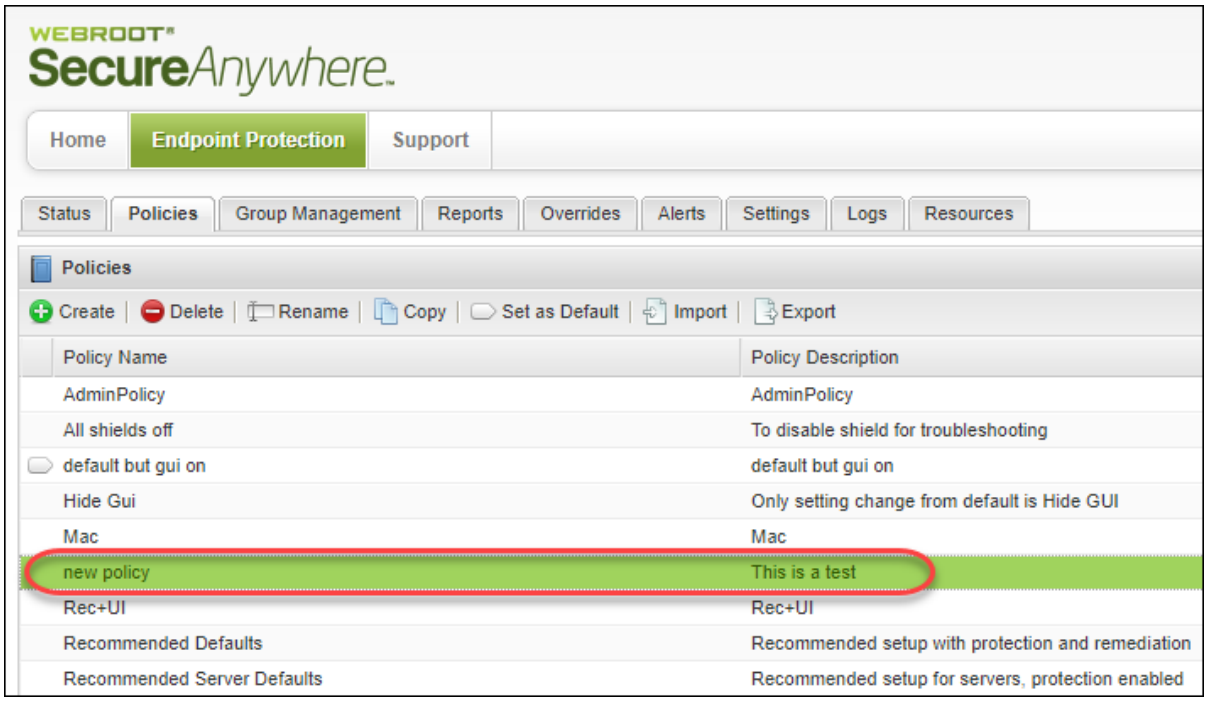
2. [**ポリシー**] タブをクリックします。.



[ポリシー] タブが表 示されます。

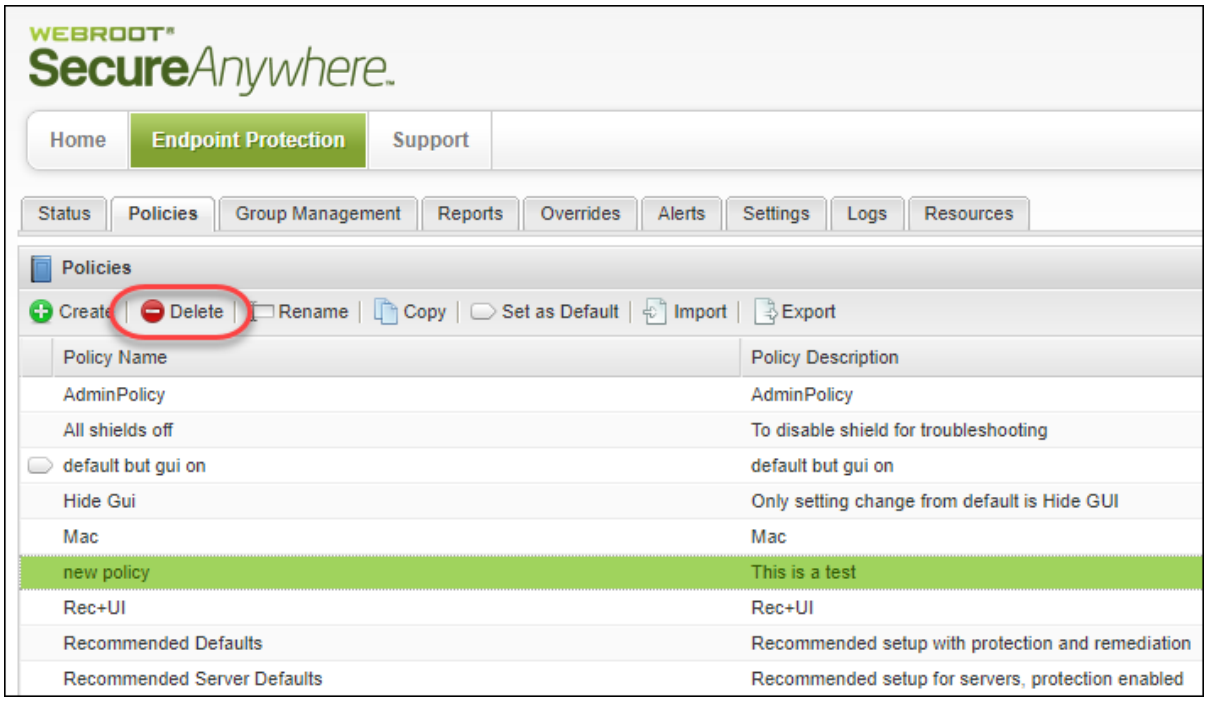


3. [ポリシー名] カラムから削除するポリシーを選択します。

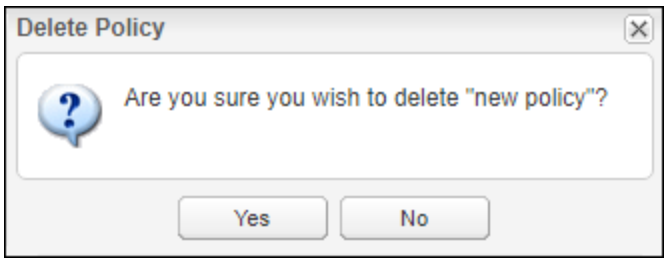


[削除] ボタンがアクティブになります。

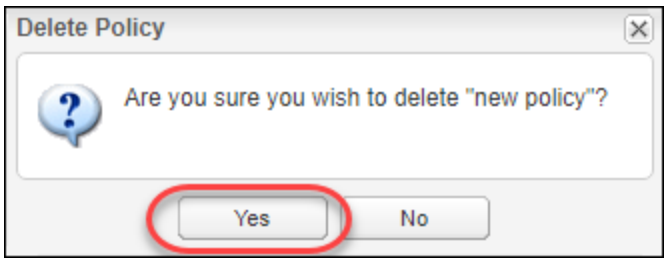
4. [**削除**] ボタンをクリックします。



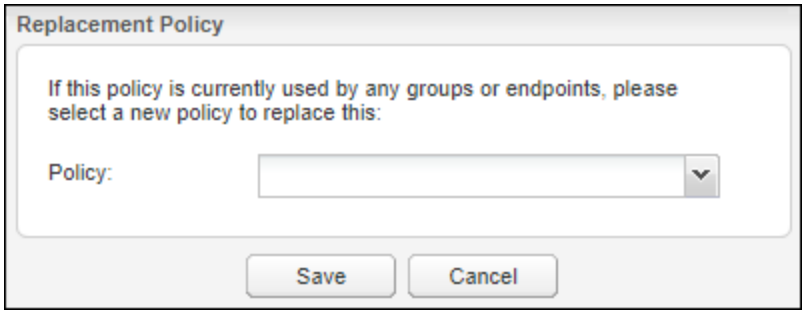
[ポリシーを削除] ウィンドウが表示されます。



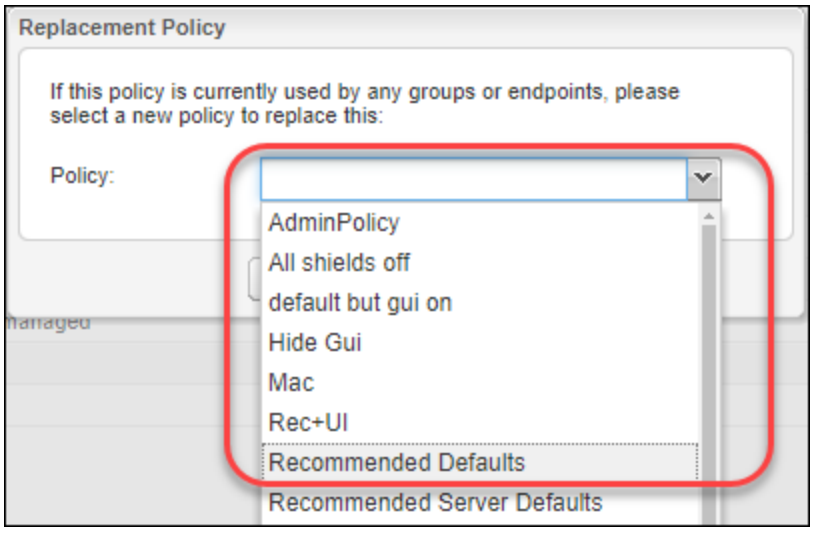
5. [**はい**] ボタンをクリックします。



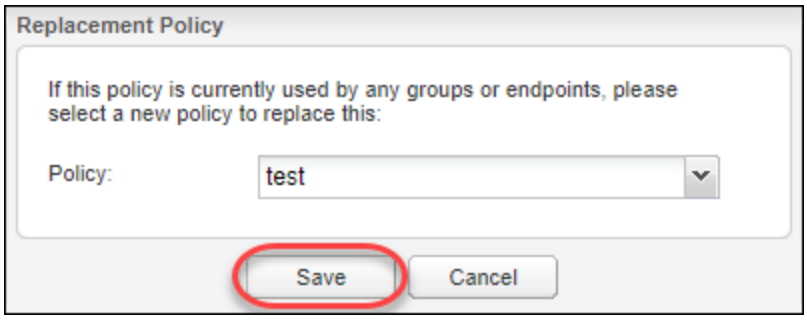
[代替ポリシー] ウィンドウが表示されます。



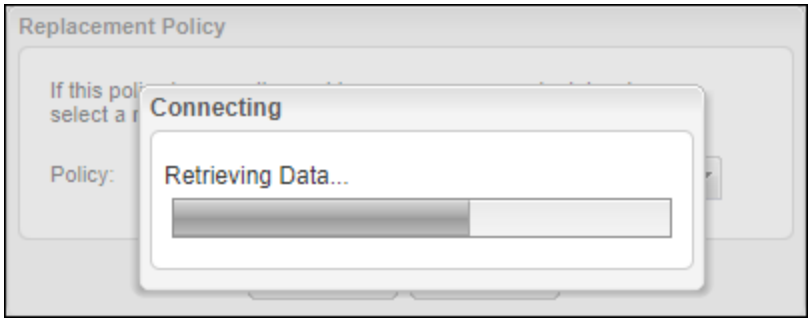
6. [ポリシー] ドロップダウンメニューから、前のポリシーが関連付けられていたグループまたはエンドポイントと関連付ける新しいポリシーを選択します。



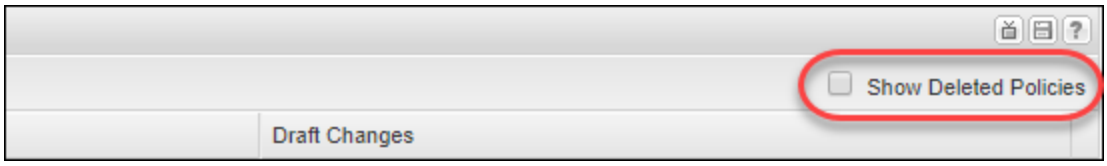
7. [**保存**] ボタンをクリックします。



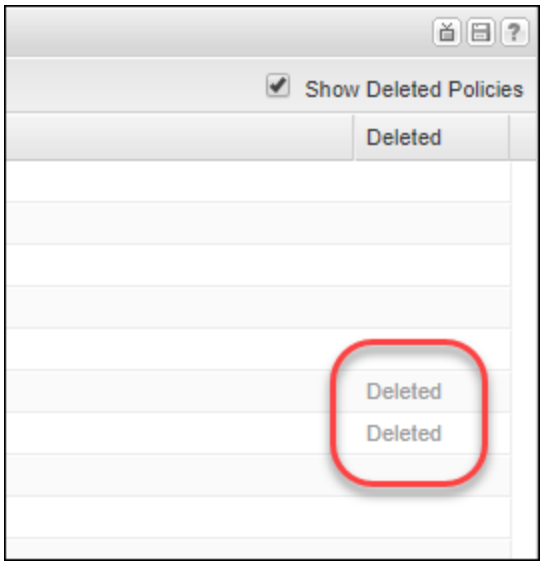
削除したポリシーは、削除したポリシーのリストに移動されます。



8. 削除されたポリシーを表示するには、[ポリシー] タブの右上隅にある [**削除したポリシーを表示**] チェックボックスを選択します。



削除したポリシーはグレー表示されます。



第 7 章: グループの管理

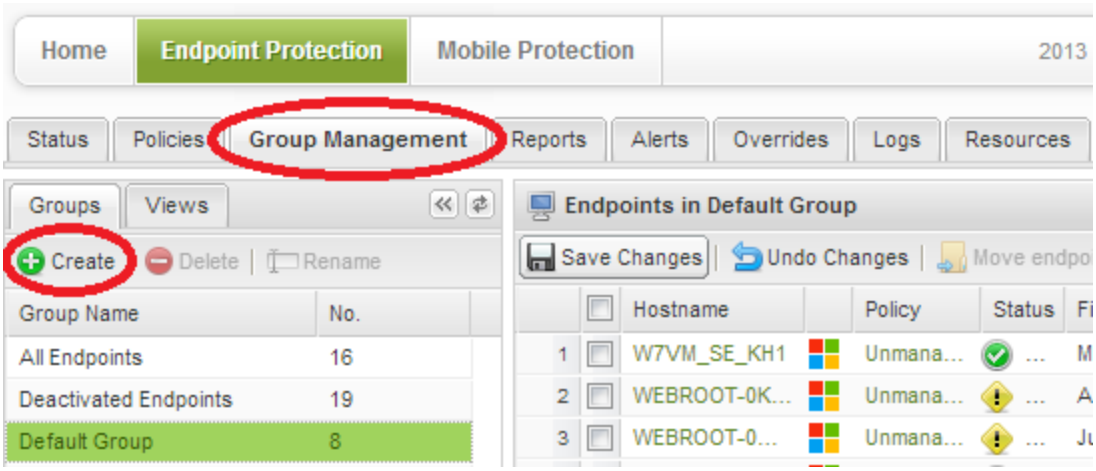
グループの管理方法については、以下のトピックを参照してください。

新規グループの追加

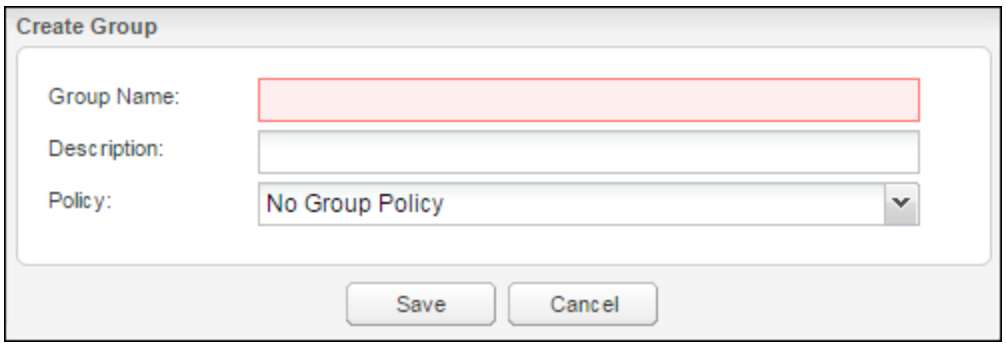
初めてエンドポイントに SecureAnywhere を配備する際は、エンドポイントプロテクションによってすべてデフォルトのグループに割り当てられます。必要な場合は、異なる管理目的ごとにグループを追加し、この新しく追加されたグループにエンドポイントを再割り当てすることもできます。

グループを作成するには

1. [**グループの管理**] タブをクリックします。
2. コマンドバーの [**作成**] アイコンをクリックします。



3. 表示される [グループを作成] ダイアログで、グループ名と説明を入力し、[**グループを作成**] ボタンをクリックします。

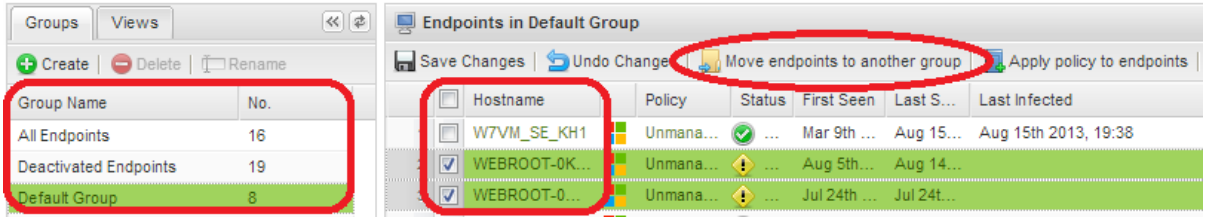


左側の [グループ] パネルに新しいグループが表示されます。

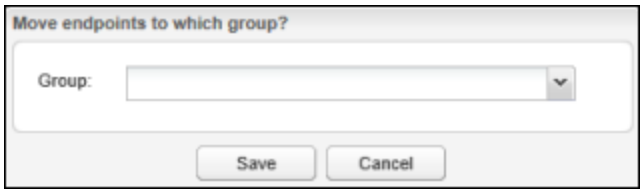
4. この新しいグループにエンドポイントを移動するには、エンドポイントが現在割り当てられているグループをクリックします。
5. 右側の [エンドポイント] パネルで 1 つ以上のエンドポイントを選択します。

> **注意:** リストの一番上にある [**ホスト名**] チェックボックスをクリックすると、指定したグループ内のすべてのエンドポイントを選択することができます。

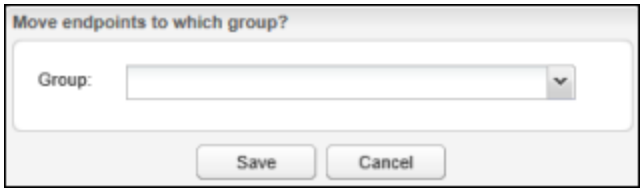
6. コマンド バーの [**エンドポイントを別のグループに移動**] ボタンをクリックします。



[エンドポイントをどのグループに移動しますか?]ウィンドウが表示されます。



7. [グループ] ドロップダウンメニューで新しいグループを選択し、[**保存**] ボタンをクリックします。



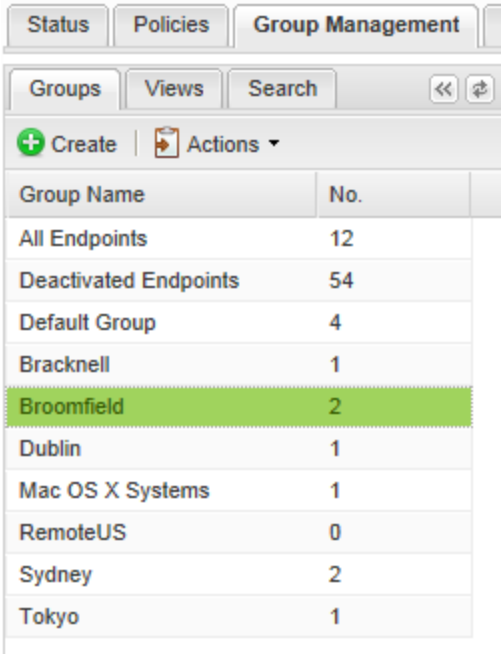
8. これで、ポリシーをグループ全体または個々のエンドポイントに適用できるようになりました。詳細については、「*エンドポイントのグループへのポリシーの適用 ページ324エンドポイントのグループへのポリシーの適用*」を参照してください。

グループの名前の変更

[グループの管理] タブでは、リストにあるグループの名前を簡単に変更できます。名前を変更したグループのエンドポイントはそのままグループ内に残ります。エンドポイントを移動する必要はありません。

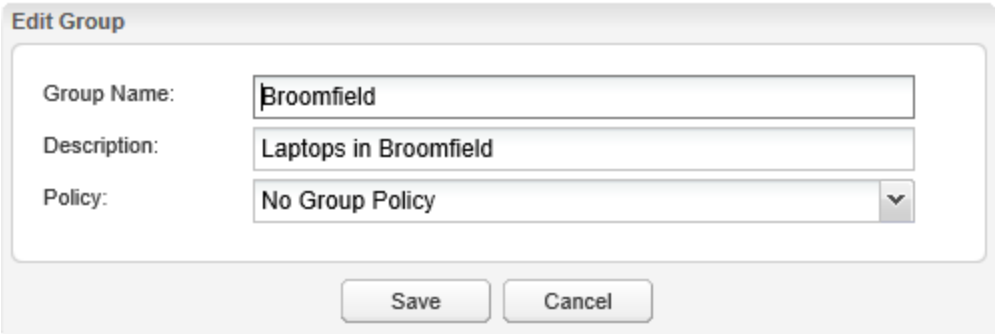
グループの名前を変更するには

1. エンドポイントのコンソールで [**グループの管理**] タブをクリックします。
2. 左のパネルで、名前を変更するグループを選択します。

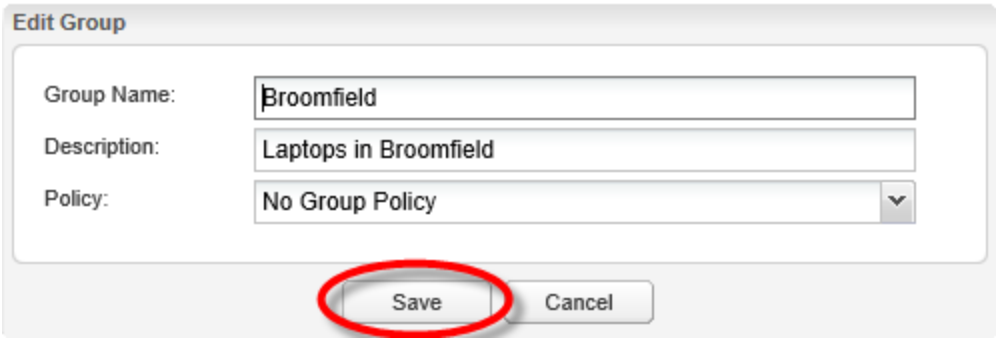


3. [アクション] ドロップダウンメニューの [**グループの編集**] を選択します。

[グループの編集] ウィンドウが表示されます。



4. [グループ名] フィールドに新しいグループ名を入力します。
5. 設定が完了したら [**保存**] ボタンをクリックします。



エンドポイントのグループへのポリシーの適用

すべてのエンドポイントはまず、デフォルトのポリシーに割り当てられます。ポリシーの割り当てを変更するには、新しいポリシーを定義してから、以下の手順に従ってそのポリシーをグループに適用する必要があります。詳細については、「*ポリシーの導入 ページ222*」を参照してください。

このトピックでは、次の手順について説明します。

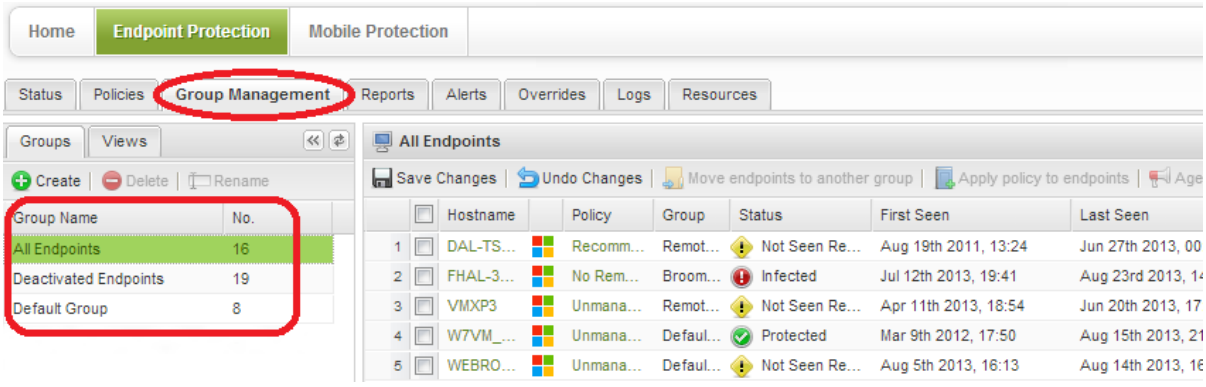
- エンドポイントのグループへのポリシーの適用
- 単一のエンドポイントへのポリシーの適用

エンドポイントのグループへのポリシーの適用

[グループの管理] タブで、複数のエンドポイントにポリシーを適用することができます。

エンドポイントのグループにポリシーを適用するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、必要なエンドポイントを含むグループを選択します。

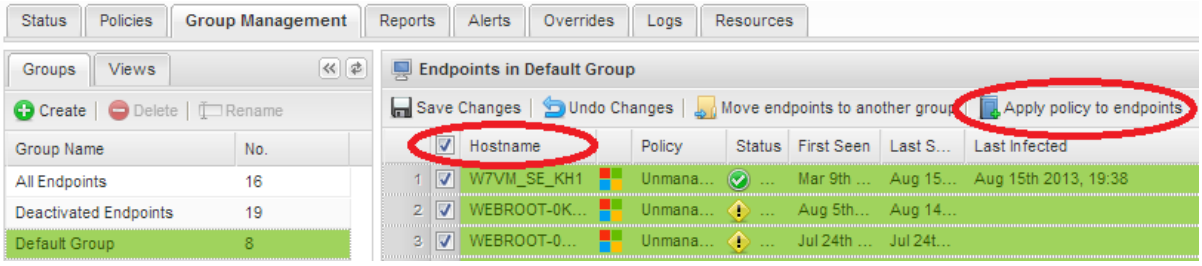


3. 右側の [エンドポイント] パネルで 1 つ以上のエンドポイントを選択します。

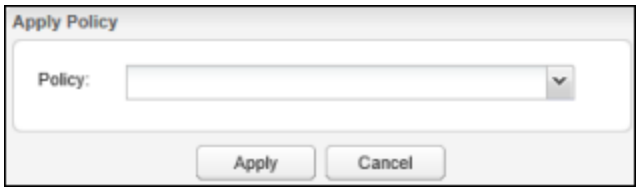
> **注意:** リストの一番上にある [ホスト名] チェックボックスをクリックすると、指定したグループ内のすべてのエンドポイントを選択することができます。

4. コマンド バーの [**ポリシーをエンドポイントに適用**] ボタンをクリックします。

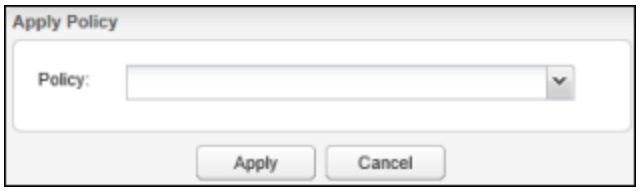
> **注意:** グループのエンドポイントが 1 ページ以上ある場合は、ポリシーの適用対象が現在のページのエンドポイントか、全ページのエンドポイントかを、ダイアログで尋ねられます。



[ポリシーを適用] ウィンドウが表示されます。



5. [ポリシー] ドロップダウンメニューでグループの新しいポリシーを選択し、[**適用** button.



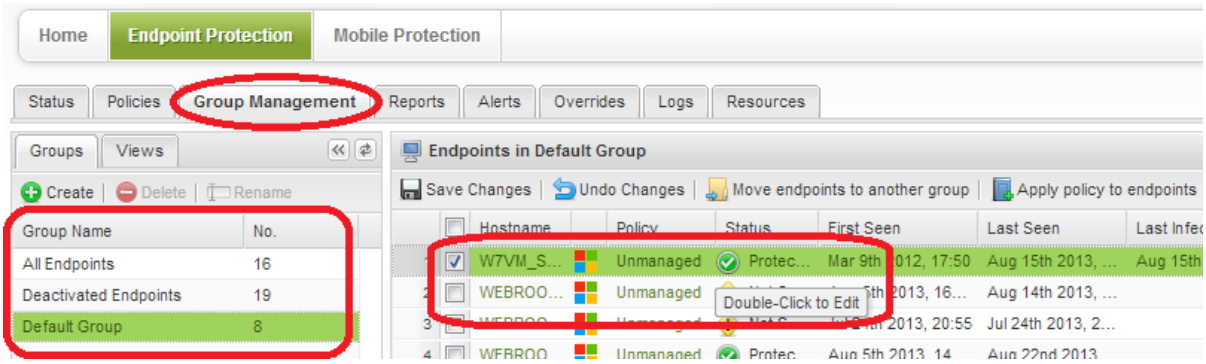
6. [ポリシー] カラムで、新しいポリシーが選択したエンドポイントに適用されていることを確認します。

単一のエンドポイントへのポリシーの適用

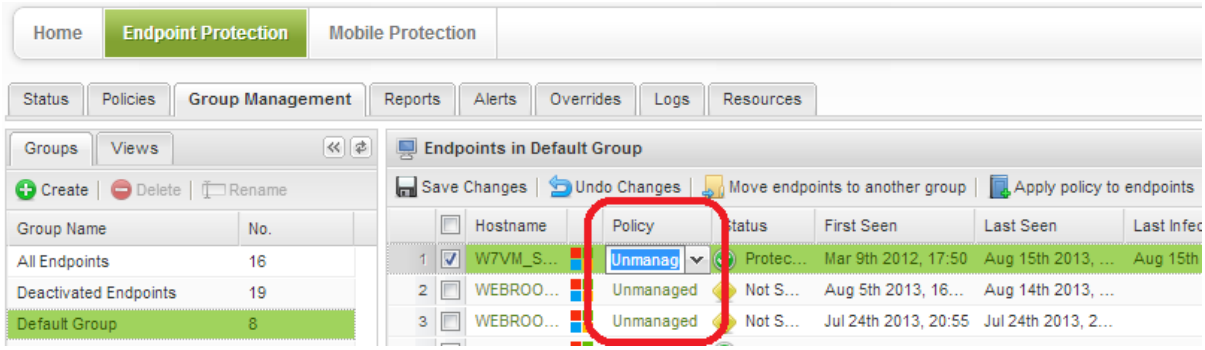
1 つのエンドポイントだけにポリシーを適用するには、[ポリシー] カラムをダブルクリックして変更を加える方法が最も簡単です。

個々のエンドポイントにポリシーを適用するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、該当するエンドポイントを含むグループを選択します。
3. 右側の [エンドポイント] パネルでエンドポイントを選択します。



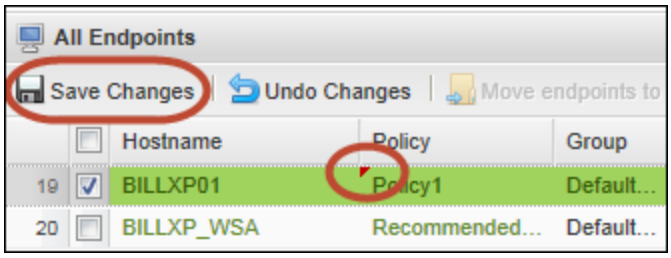
4. 選択されたエンドポイントの [ポリシー] カラムでポリシー名をダブルクリックすると、使用可能なポリシーのドロップダウンが表示されます。



5. ポリシーを選択して **Enter**キーを押します。

</bpt>1新しいポリシー名が、左上隅に赤いフラグがついたカラムに表示されます。これは変更が下書きの状態にあることを示し、この時点では [**変更を取り消す**] を選択して前の設定に戻すこともできます。必要に応じて、このパネルで引き続き他の変更を加えます。

6. 変更を適用するには、[**変更を保存**] ボタンをクリックします。



行の赤いフラグが消えます。

グループ間でのエンドポイントの移動

このセクションの説明に従うと、エンドポイントを別のグループに移動することができます。個々のエンドポイントまたはエンドポイントのグループ全体の移動が可能です。

グループ間でエンドポイントを移動するには

1. [**グループの管理**] タブをクリックします。
2. 左側の [グループ] パネルで、移動するエンドポイントを含むグループを選択します。

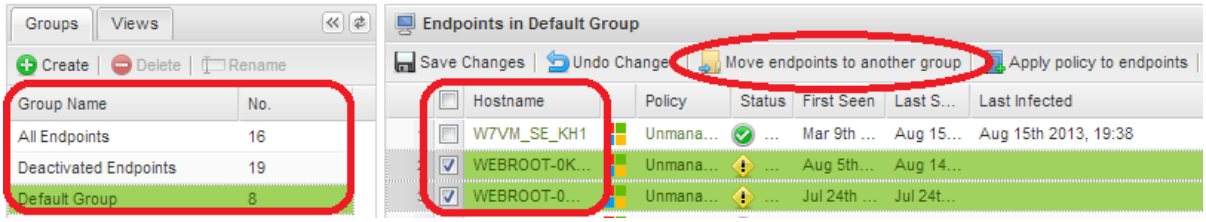
> **注意：** この手順では、[すべてのエンドポイント] ではなく特定のグループを選択する必要があります。

3. 右側の [エンドポイント] パネルで 1 つ以上のエンドポイントを選択します。

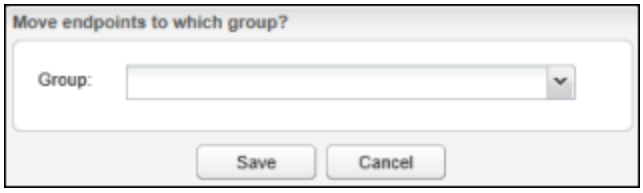
> **注意：** リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したグループ内のすべてのエンドポイントを選択することができます。

4. コマンドバーの [**エンドポイントを別のグループに移動**] アイコンをクリックします。

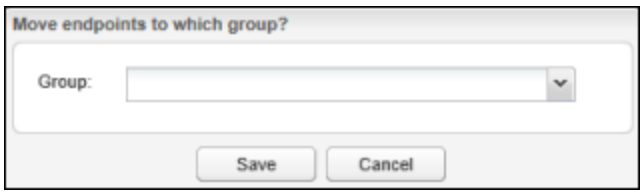
> **注意：** グループのエンドポイントが 1 ページ以上ある場合は、ポリシーの適用対象が現在のページのエンドポイントか、全ページのエンドポイントかを、ダイアログで尋ねられます。



[エンドポイントをどのグループに移動しますか？]ウィンドウが表示されます。



5. [グループ] ドロップダウン矢印でグループを選択し、[**保存**] ボタンをクリックします。



6. 左側のパネルで選択したグループをクリックします。エンドポイントがすべて、右側の [エンドポイント] パネルに表示されることを確認してください。

エンドポイントをグループに整理

エンドポイントに SecureAnywhere をインストールする際、対象のエンドポイントは自動的にデフォルトのポリシーとグループに割り当てられます。グループはエンドポイントをひとまとめにした単位であり、デバイスを整理しやすくして管理を助けるものです。

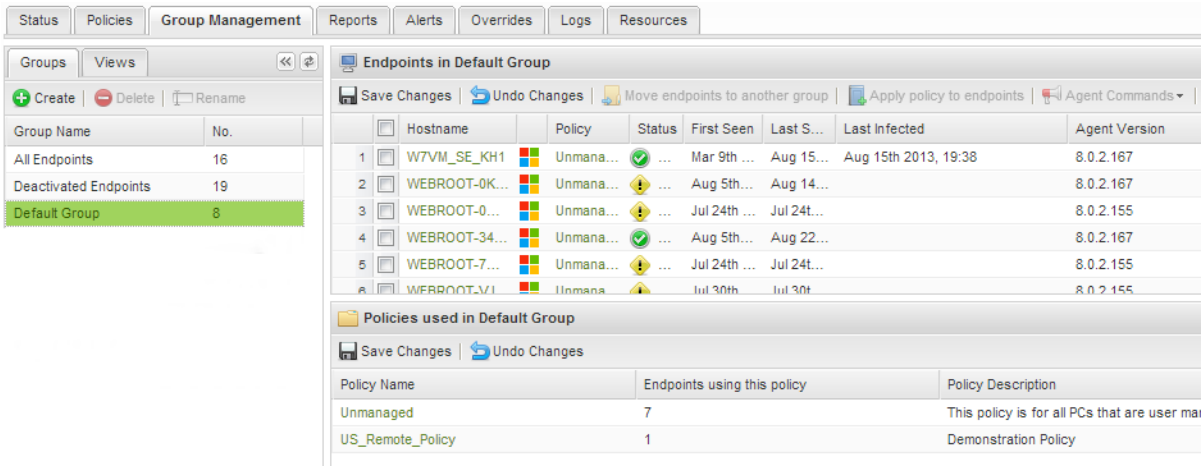
エンドポイントが最初のスキャンの実行後に管理ポータルへの報告を行ったら、それらのエンドポイントを別のグループに移動することができます。たとえば、スキャン時間のスケジュールを統一して指定できるよう、タイムゾーン別にエンドポイントを整理することも可能です。

注意: グループを完全に管理するには、[グループ] の [作成・編集]、[グループ] の [エンドポイントの非アクティブ化 / 再アクティブ化]、[グループ] の [グループへのエンドポイントの割り当て] へのアクセス権限が必要です。詳細については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

エンドポイントをグループに整理するには

1. [グループの管理] タブですべてのグループを表示できます。
2. 左側の [グループ] パネルでグループを選択すると、関連するエンドポイントとポリシーが右側に表示されます。

   エンドポイントは上に、ポリシーは下に表示されます。



注意: サイレントインストール中にコマンドラインで /groupname スイッチを使用していない限り、エンドポイントはすべてデフォルトのグループに割り当てられます。詳細については、「*エンドポイントへの SecureAnywhere の配備 ページ112*」を参照してください。

グループの追加作成とエンドポイントの移動の手順

1. 1 つ以上の新規グループの追加 -「*新規グループの追加 ページ319*」を参照してください。
2. 新しく作成した別のグループへのエンドポイントの移動 -「*グループ間でのエンドポイントの移動 ページ328*」を参照してください。
3. 新しいエンドポイントのグループへのポリシーの割り当て -「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

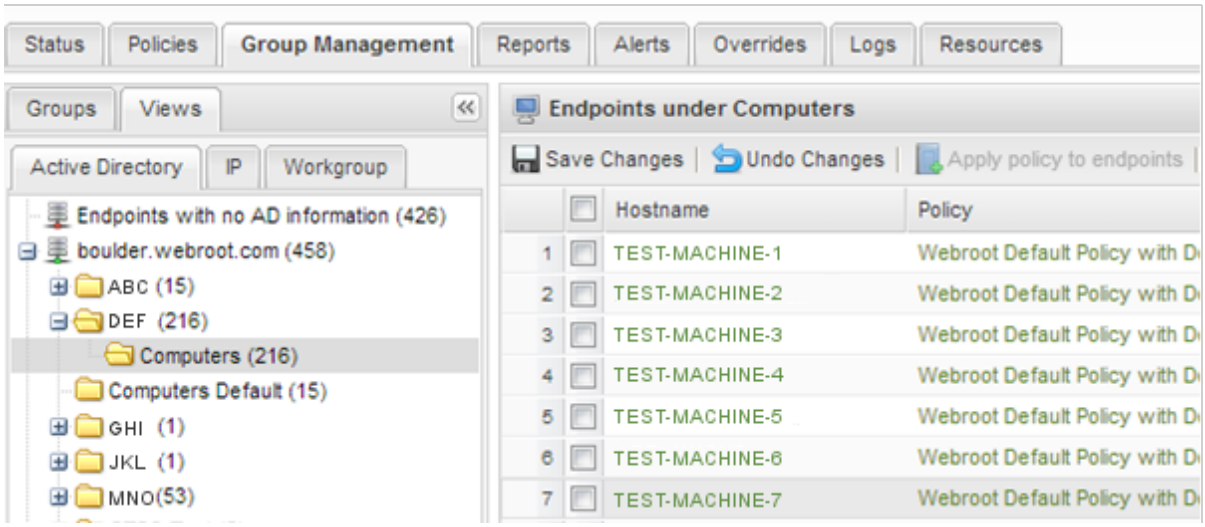
ビュー内の [アクティブディレクトリ] タブの使用

SecureAnywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが [グループの管理] の [ビュー] タブに表示されるようになります。

詳細については、「*ビュー内の [IP 範囲] タブの使用 ページ334*」および「*ビュー内の [ワークグループ] タブの使用 ページ336*」を参照してください。

管理ポータルで Active Directory のリストを表示するには

1. [**グループの管理**] タブをクリックします。
2. 左側のパネルで [**ビュー**] タブをクリックし、[**アクティブディレクトリ**] タブをクリックします。



3. このタブで、Active Directory 別にエンドポイントを確認できます。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

> **注意：** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデータをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出されると、この情報は変わります。

4. また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできませ

ん。

注意: リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできません。この場合は、[グループ] タブを使用します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」および「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

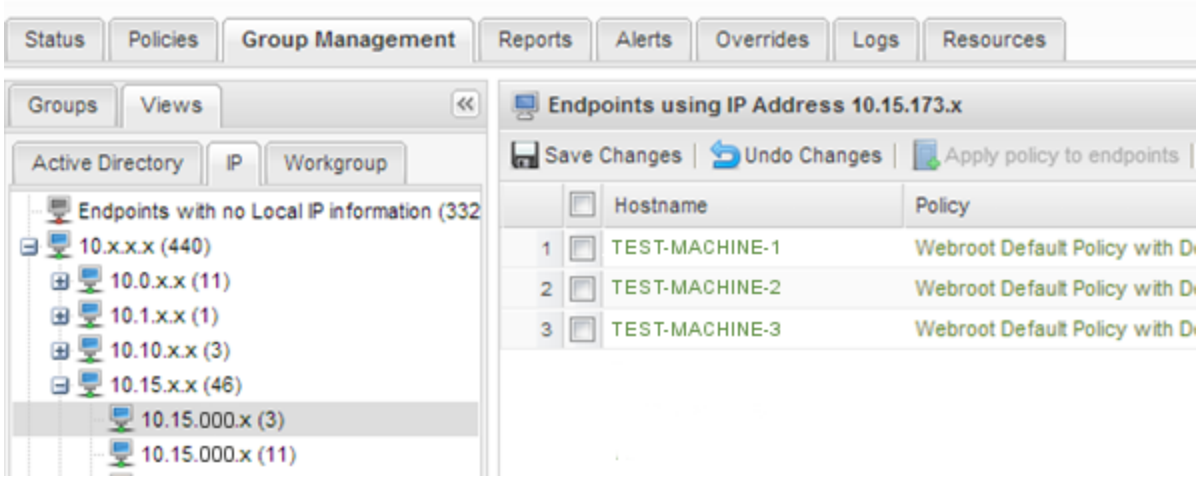
ビュー内の [IP 範囲] タブの使用

SecureAnywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが [グループの管理] の [ビュー] タブに表示されるようになります。

詳細については、「*ビュー内の [アクティブディレクトリ] タブの使用 ページ332*」および「*ビュー内の [ワークグループ] タブの使用 ページ336*」を参照してください。

管理ポータルで IP 範囲リストを表示するには

1. [**グループの管理**] タブをクリックします。
2. 左側のパネルで [**ビュー**] タブをクリックし、[**IP 範囲**] タブをクリックします。



3. このタブで、IP 範囲別にエンドポイントを確認できます。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

> **注意:** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデータをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出されると、この情報は変わります。

4. また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできません。

注意: リストの一番上にある [**ホスト名**] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできません。この場合は、[グループ] タブを使用します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」および「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

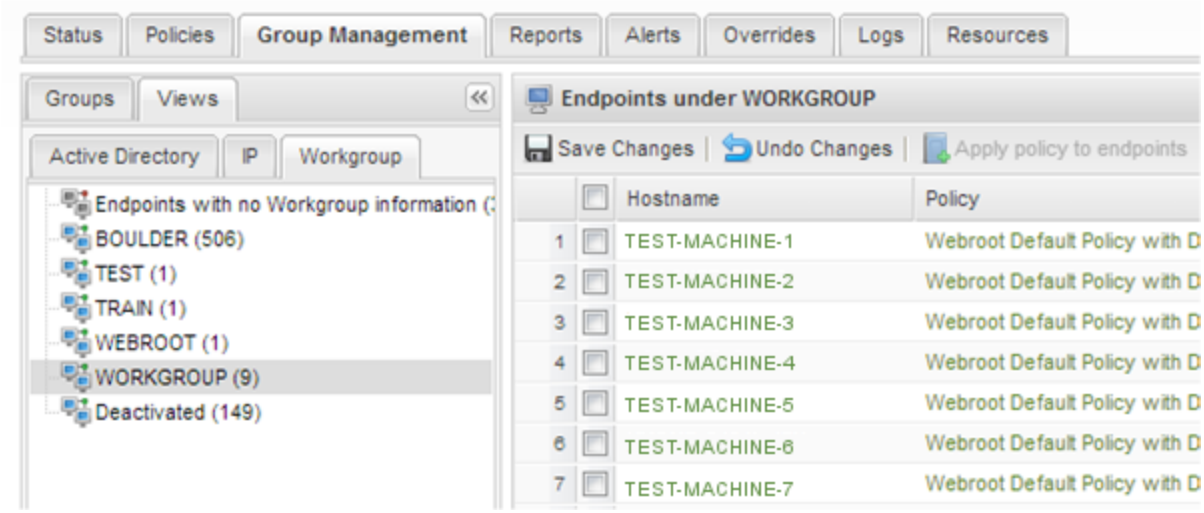
ビュー内の [ワークグループ] タブの使用

SecureAnywhere をエンドポイントにインストールする際、エージェントは初回のスキャンを実行してエンドポイントの状態の報告と情報の収集を行い、管理ポータルで識別できるようにします。エンドポイントから管理コンソールに報告が返されると、エージェントによって収集されたデータが [グループの管理] の [ビュー] タブに表示されるようになります。

詳細については、「*ビュー内の [IP 範囲] タブの使用 ページ334*」および「*ビュー内の [ワークグループ] タブの使用*」を参照してください。

管理ポータルでワークグループのリストを表示するには

1. [**グループの管理**] タブをクリックします。
2. 左側のパネルで [**ビュー**] タブをクリックし、[**ワークグループ**] タブをクリックします。



3. このタブで、ワークグループ別にエンドポイントを確認できます。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

> **注意：** このリストに含まれているエンドポイントは、エージェントが最新のスキャンで収集したデータをもとに整理されているため、移動できません。以後のスキャンで異なるデータが検出されると、この情報は変わります。

4. また、一覧のエンドポイントに対してコマンドを送信してポリシーを変更することも可能です。これらの変更は、個々のエンドポイントまたはページにのみ送ることができ、ビュー全体に適用することはできませ

ん。

注意: リストの一番上にある [ホスト名] チェックボックスを選択すると、指定したビュー内のページ上にあるすべてのエンドポイントを選択することができます。

[ビュー] タブでは、グループに対してコマンドを送信して割り当てられたポリシーを変更することはできません。この場合は、[グループ] タブを使用します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」および「*エンドポイントのグループへのポリシーの適用 ページ324*」を参照してください。

グループの削除

[グループの管理] タブでは、リストにあるグループを簡単に削除したり、エンドポイントを別のグループに移動したりできます。

削除したグループを復元することはできません。ただし、削除されたグループの名前を再利用することは可能です。

グループを削除するには

1. [**グループの管理**] タブをクリックします。
2. [グループ名] カラムで、削除するグループを選択します。
3. コマンドバーの [**削除** icon.

4. プロンプトが表示されたら [**はい**] ボタンをクリックします。

   エンドポイントがこのグループに割り当てられている場合は、別のウィンドウが表示され、エンドポイントの移動先のグループを選択するよう求められます。

5. 移動先のグループを選択し、[**保存**] ボタンをクリックします。

第 8 章: レポートの操作

レポートの操作方法については、以下のトピックを参照してください。

エンドポイント プロテクションのレポートの生成

エンドポイント プロテクションでは、SecureAnywhere のバージョンとエンドポイントにおける脅威のアクティビティに関する詳細なレポートを表示できます。次の表に、ビジネス上のニーズ別に生成が推奨されるレポートの種類を示します。

目的	使用するレポート
異なる SecureAnywhere のバージョンがインストールされているエンドポイントを特定する	*[エージェントのバージョンの使用状況] レポートの生成 ページ 390*
SecureAnywhere ソフトウェアが新しくインストールされたエンドポイントを特定する	*[インストールされたエージェント] レポートの生成 ページ395*
検出された脅威を特定して管理する	*[確認されたすべての脅威] レポートの生成 ページ342* または *[最新のスキャンで脅威が存在したエンドポイント] レポートの生成 ページ361*
未判定と分類されたファイルを特定する	*[確認されたすべての未判定のソフトウェア] レポートの生成 ページ349* または *[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成 ページ365*

目的	使用するレポート
検出された脅威の概要を表示する	[脅威の履歴 (内訳)] レポートの生成 ページ377
検出された脅威の概要を日単位で表示する	[脅威の履歴 (日単位)] レポートの生成 ページ369

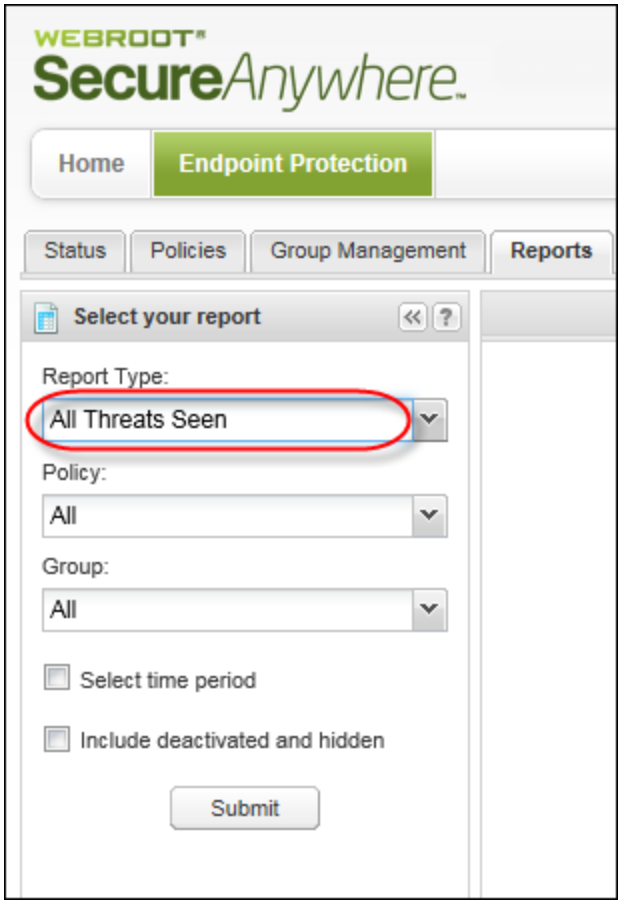
[確認されたすべての脅威] レポートの生成

検出された脅威を特定して管理するには、[確認されたすべての脅威] レポートを生成します。このレポートには脅威がファイル名で一覧表示され、SecureAnywhere がその脅威を検出した時刻と場所が表示されます。脅威が繰り返し検出された場合、または複数の場所で検出された場合は、エントリが重複して表示されることがあります。このレポートから、ファイルのオーバーライドの作成や、隔離されたファイルの復元を実行できます。レポートのデータは次の手順で変更できます。

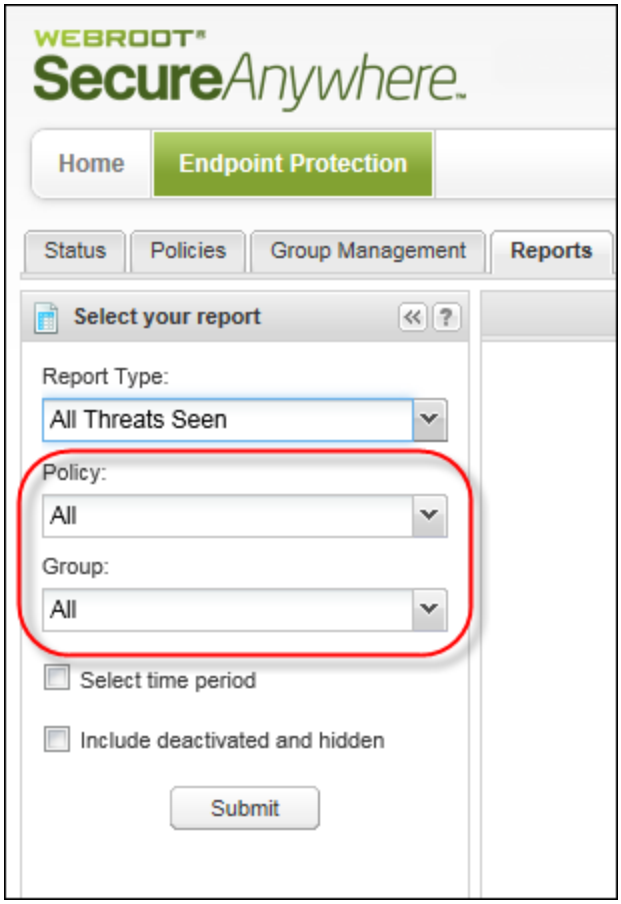
- 選択したポリシーまたはグループ内で検出された脅威をすべて表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に便利です。

[確認されたすべての脅威] レポートを生成するには

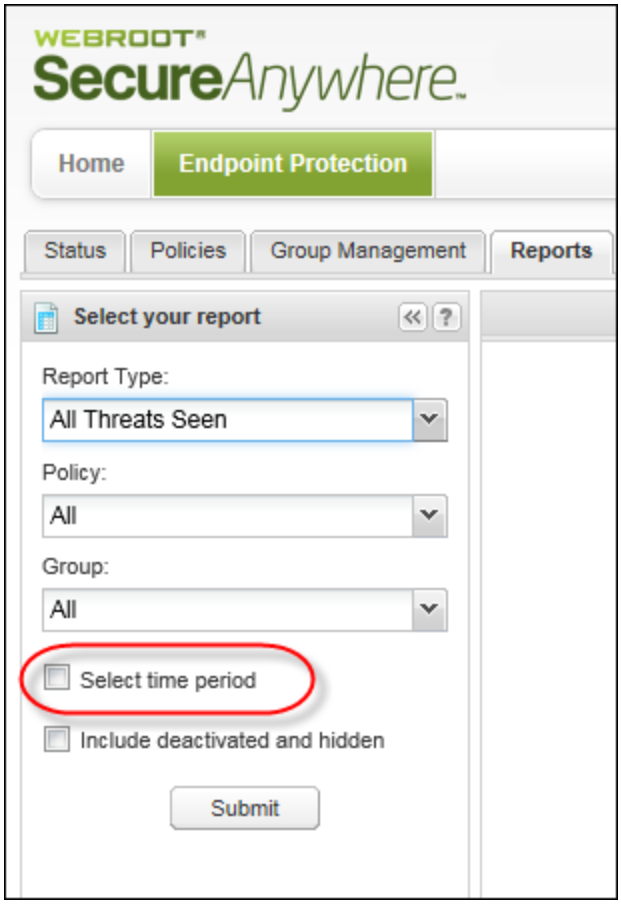
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**確認されたすべての脅威**] を選択します。



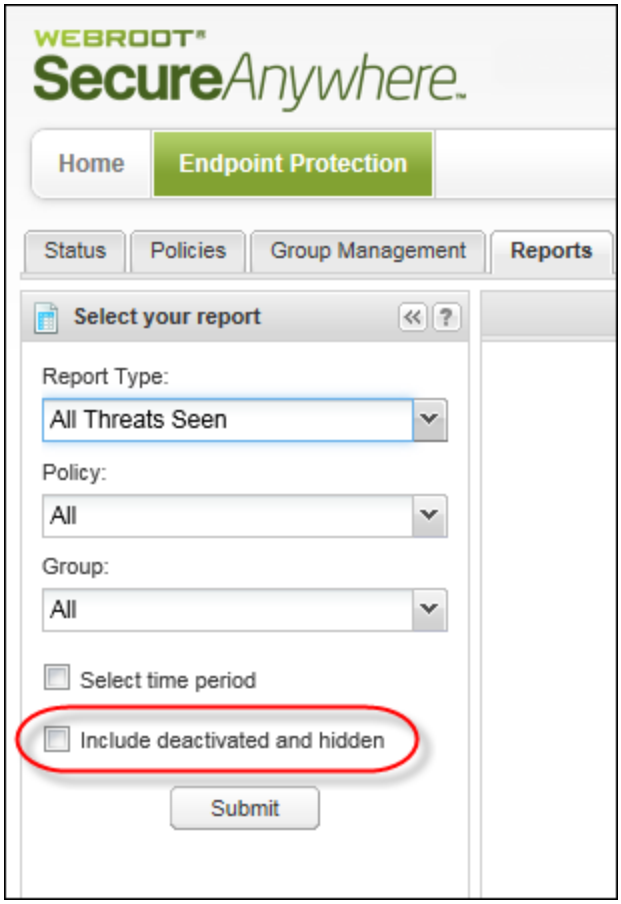
3. 必要に応じて、特定のポリシーとグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。



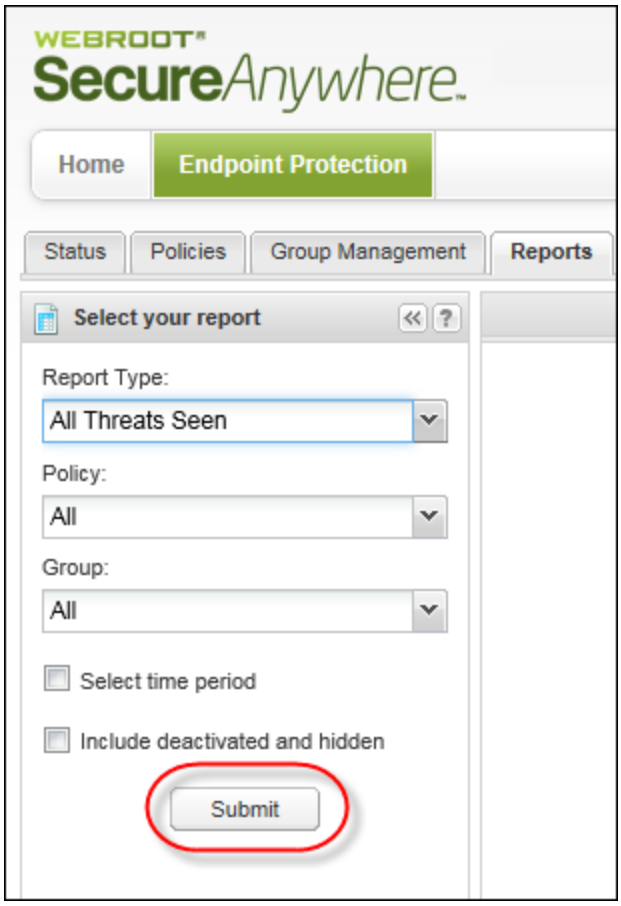
4. データの期間を入力するには、[**期間を選択**] チェックボックスを選択します。この手順はオプションです。



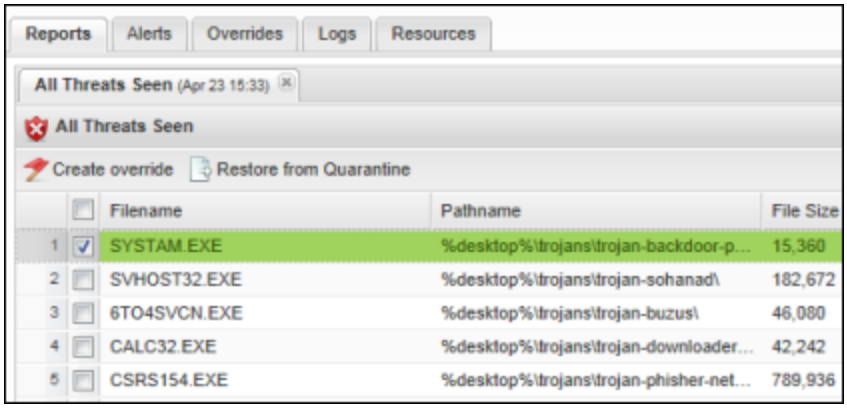
5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[非アクティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
All Threats Seen
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit

6. [**送信**] ボタンをクリックします。



右側のパネルにレポートが開きます。各脅威がファイル名で一覧表示され、SecureAnywhere がその脅威を検出し削除した場所と時刻が表示されます。



7. このパネルで、必要に応じて次のいずれかの操作を行います。

   - **オーバーライドの作成** - エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [**オーバーライドの作成**] アイコンをクリックします。詳細については、「*レポートからのファイルへのオーバーライドの適用*」を*参照してください*。

   - **隔離先から復元する** - ファイルが安全で、エンドポイントの元の場所に復元する場合は、コマンドバーの [隔離先から復元する] をクリックします。

8. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。
9. レポートのスプレッドシートをダウンロードするには、「*レポートのスプレッドシートのダウンロード ページ402*」を参照してください。

[確認されたすべての未判定のソフトウェア] レポートの生成

SecureAnywhere は、正当なファイルのように見えても動作が疑わしいファイルを検出することがあります。この場合、そのファイルは [*未判定*] に分類されます。

SecureAnywhere が [*未判定*] と分類したファイルを特定するには、[確認されたすべての未判定のソフトウェア] レポートを生成します。[確認されたすべての未判定のソフトウェア] レポートには、SecureAnywhere が安全であるかマルウェアであるかを判定できないすべての未判定のソフトウェア (一般的に実行可能ファイル) が表示されます。

このレポートにはアイテムがファイル名で一覧表示され、SecureAnywhere がその脅威を検出した時刻と場所が表示されます。未判定のソフトウェアが繰り返し検出された場合、または複数の場所で検出された場合は、レポートにエントリが重複して表示されることがあります。また、このレポートを使用してオーバーライドを作成し、ファイルに [正当] または [不正] のタグを付け、SecureAnywhere に今後の分類方法を指定することができます。

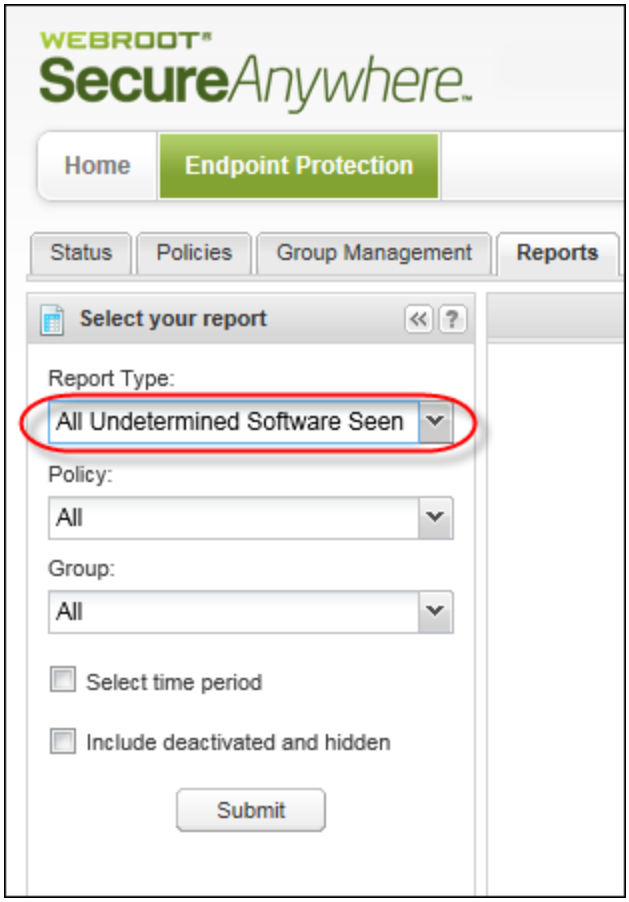
注意: 未判定のソフトウェアが最後に検出されたエンドポイントを表示する方法の詳細については、「*[最新のスキャンで脅威が存在したエンドポイント] レポートの生成 ページ361*」を参照してください。

このレポートでは、レポートデータを次のように変更できます。

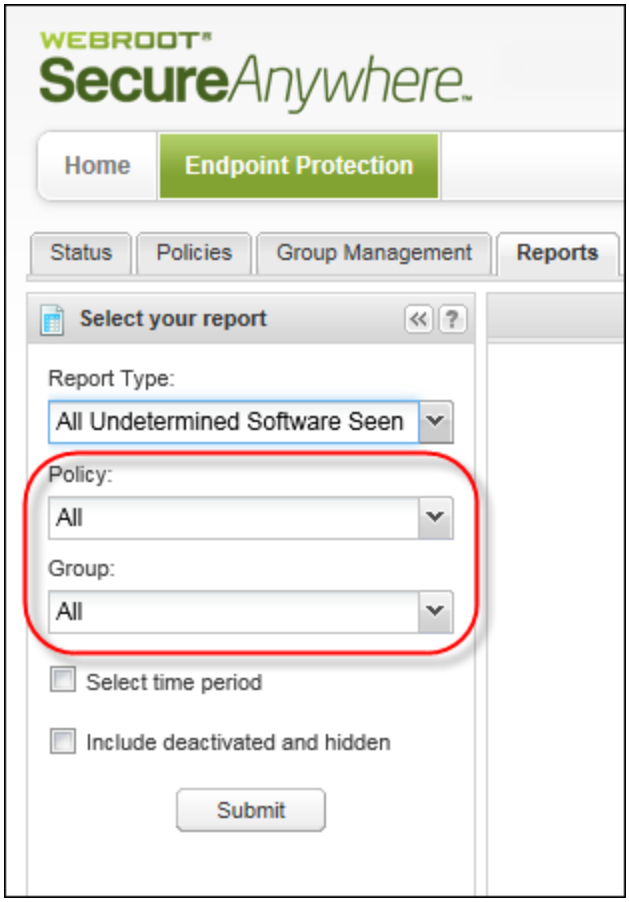
- 選択したポリシーやグループ内のすべての未判定のソフトウェアを表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして特定の期間内に検出されたファイルを確認する。特定の期間に検索結果を絞り込む場合に便利です。

[確認されたすべての未判定のソフトウェア] レポートを生成するには

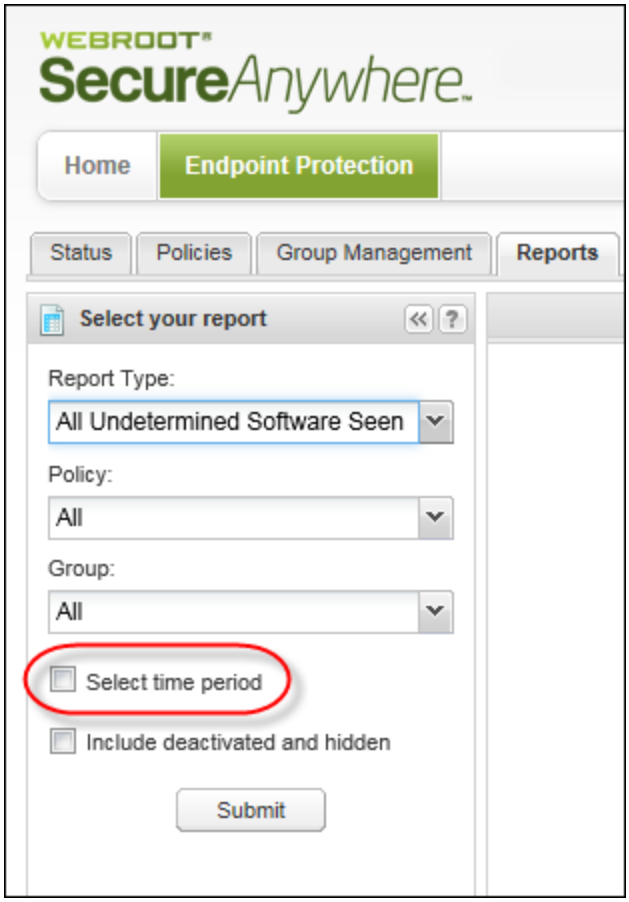
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**確認されたすべての未判定のソフトウェア**] を選択します。



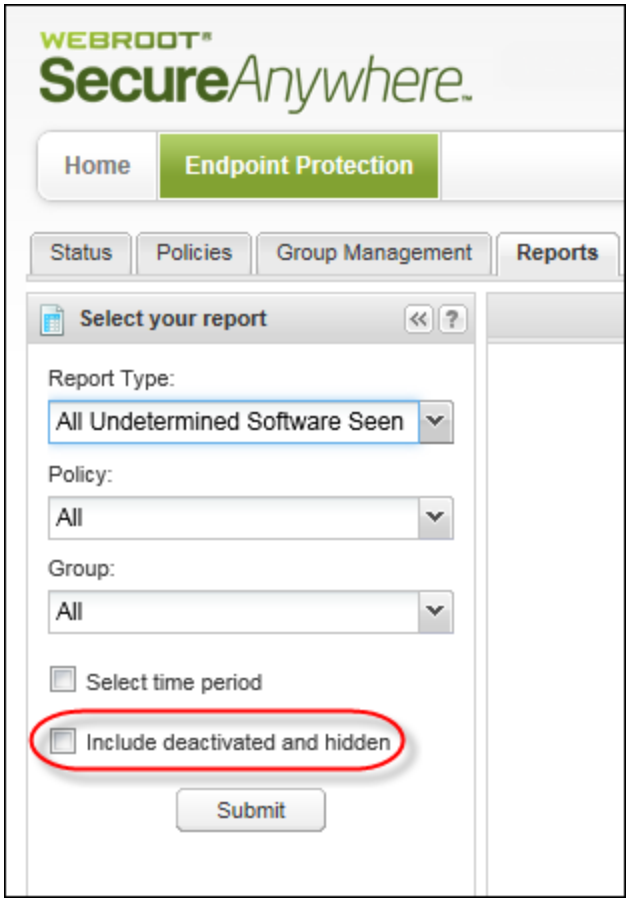
3. 必要に応じて、特定のポリシーとグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。



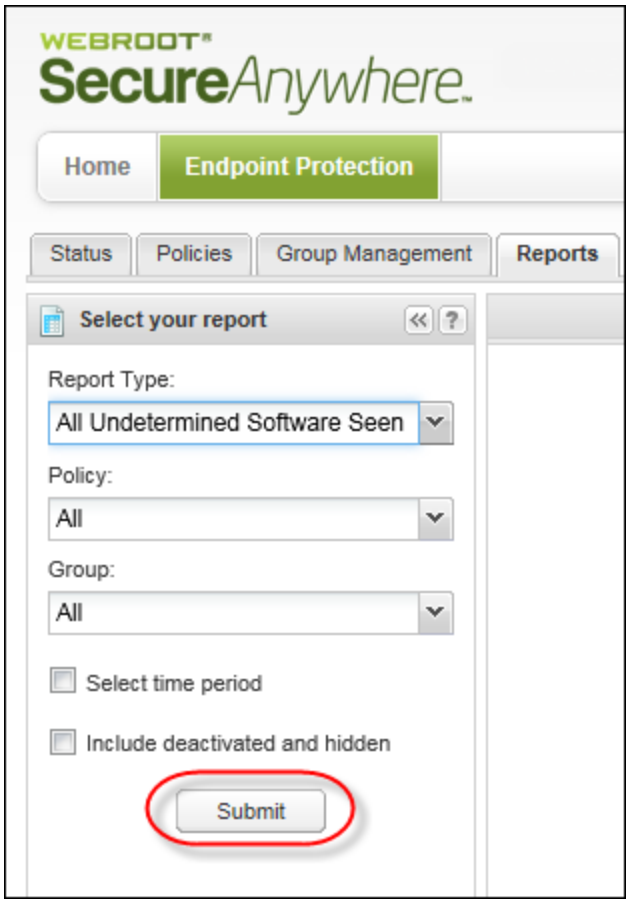
4. データの期間を入力するには、[**期間を選択**] チェックボックスを選択します。この手順はオプションです。



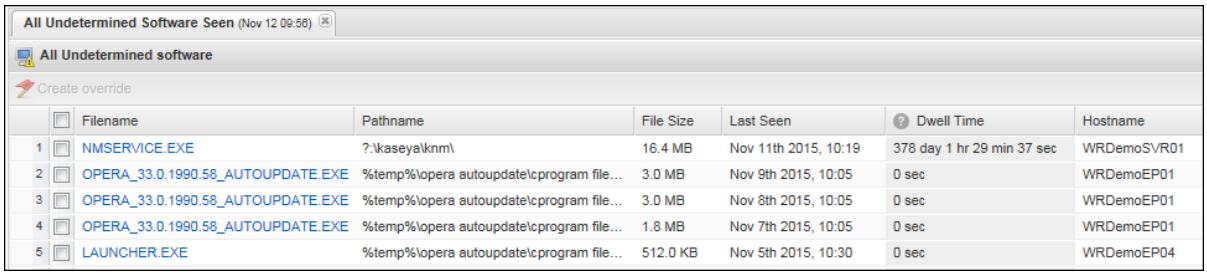
5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
All Undetermined Software Seen
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit

6. [**送信**] ボタンをクリックします。



右側のペインにレポートが表示されます。



7. ファイルを選択して [**オーバーライドの作成**] ボタンをクリックすると、次のようにファイルを再分類することができます。

- **正当** - エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、隔離も行いません。[正当] を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて正当] と表示されますが、クラウド判定は未判定のままになります。

- **不正** - スキャン中に検出された場合、常にファイルを隔離します。[不正] を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて不正] と表示されますが、クラウド判定は未判定のままになります。

また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

8. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。
9. レポートのスプレッドシートをダウンロードするには、「*レポートのスプレッドシートのダウンロード ページ402*」を参照してください。

[ブロックされたすべての URL] レポートの生成

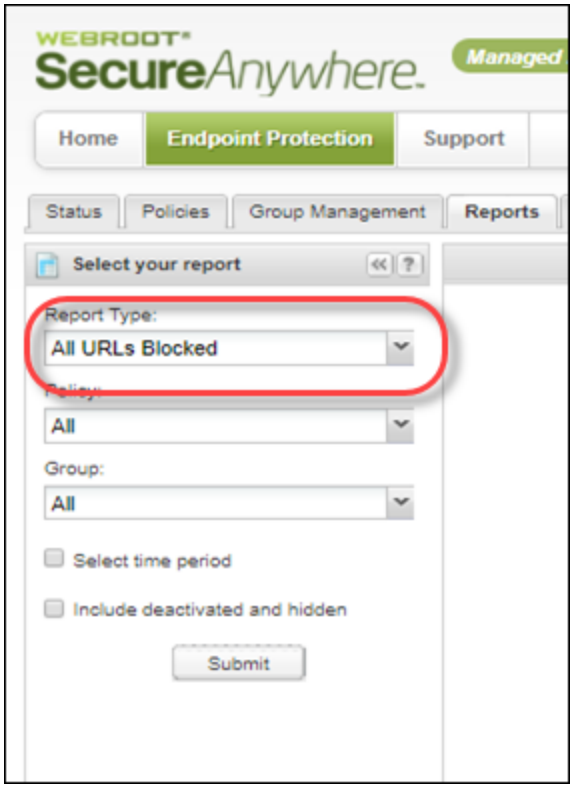
Webroot の SecureAnywhere の Web 脅威シールドによってブロックされたすべての URL を表示するには、[ブロックされたすべての URL] レポートを生成します。また、このレポートを生成すると、不正な URL として分類されブロックされたサイトにアクセスしたエンドポイントを確認することもできます。

レポートのデータは次の手順で変更できます。

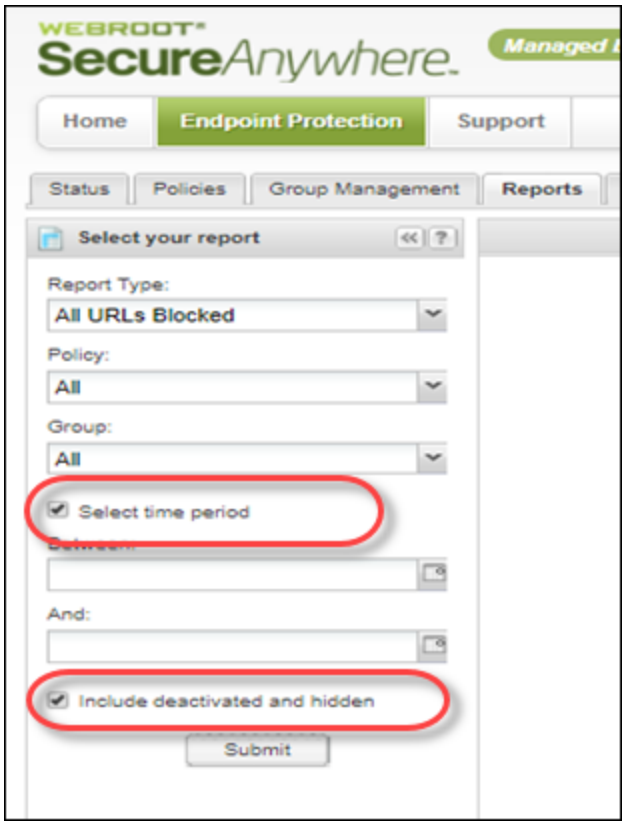
- 選択したグループ内のブロックされたすべての URL を表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- 選択したポリシー内のブロックされたすべての URL を表示する。これにより、修正が必要なポリシー設定を確認できます。

[ブロックされたすべての URL] レポートを生成するには

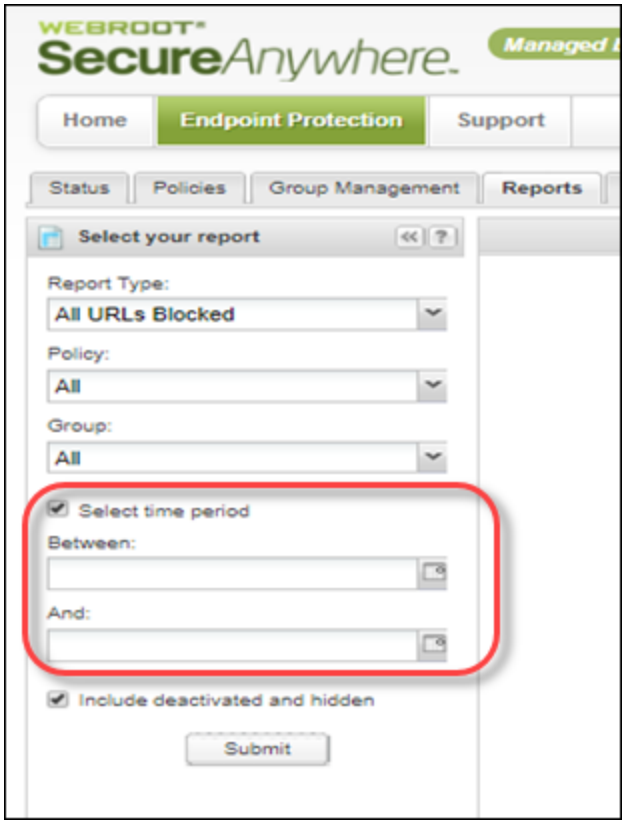
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**ブロックされたすべての URL**] を選択します。



3. 特定の期間を含める場合、または非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**期間を選択**] および [**非アクティブ化および非表示を含む**] チェックボックスを選択します。

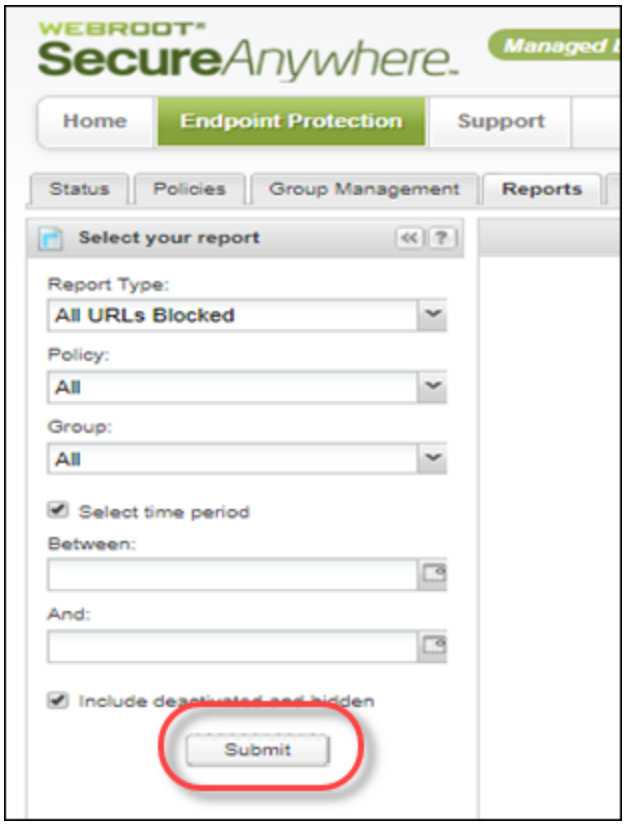


4. 期間を選択した場合は、レポートの対象期間を特定の日付で指定します。この手順はオプションです。



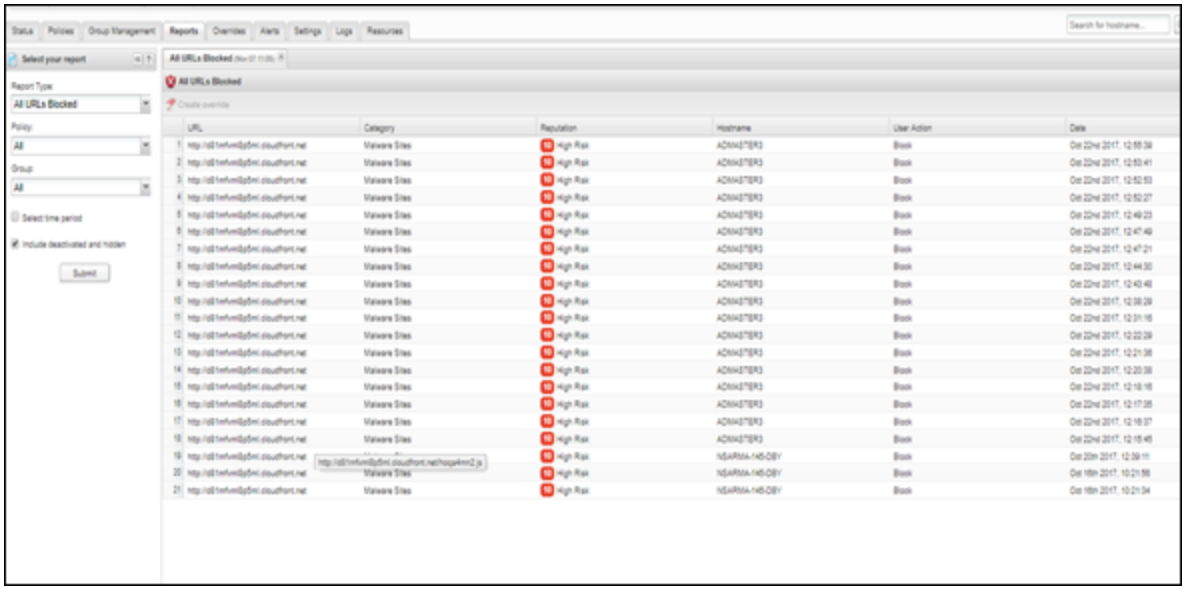
注意: レポートの対象期間を最長 90 日間まで指定できるようになりました。

5. 設定が完了したら、[**送信**] ボタンをクリックしてレポートを生成します。



次の情報を含むレポートの結果が右側に表示されます。

- ブロックされた URL
- ブロックのカテゴリー
- 評価
- ホスト名
- ユーザーアクション
- ブロックの日時


Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Select your report
All URLs Blocked
Report Type:
All URLs Blocked
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit
All URLs Blocked
URL
Category
Reputation
Hostname
User Action
Date

[最新のスキャンで脅威が存在したエンドポイント] レポートの生成

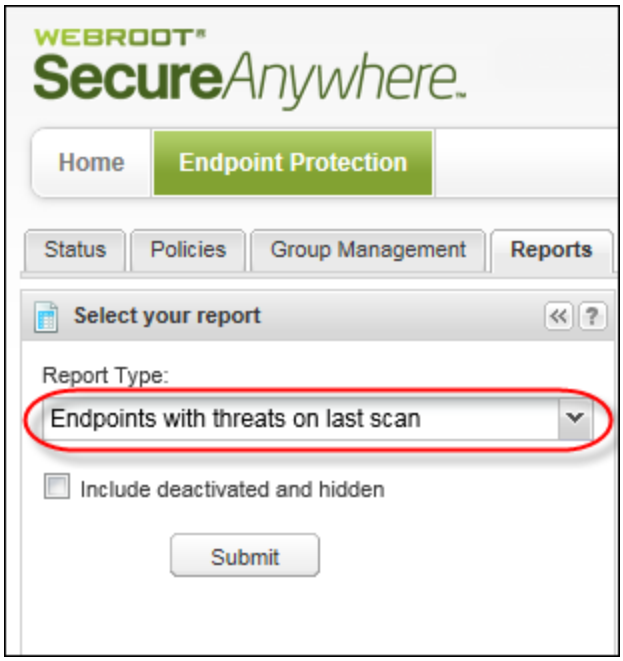
最新のスキャンで検出された脅威を特定し管理するには、[最新のスキャンで脅威が存在したエンドポイント] レポートを生成します。このレポートは、脅威をエンドポイントのロケーション別に表示します。このレポートから、エンドポイントのポリシーの変更、スキャンの実行、ファイルのオーバーライドの作成、隔離されたファイルの復元を実行できます。

レポートのデータは次の手順で変更できます。

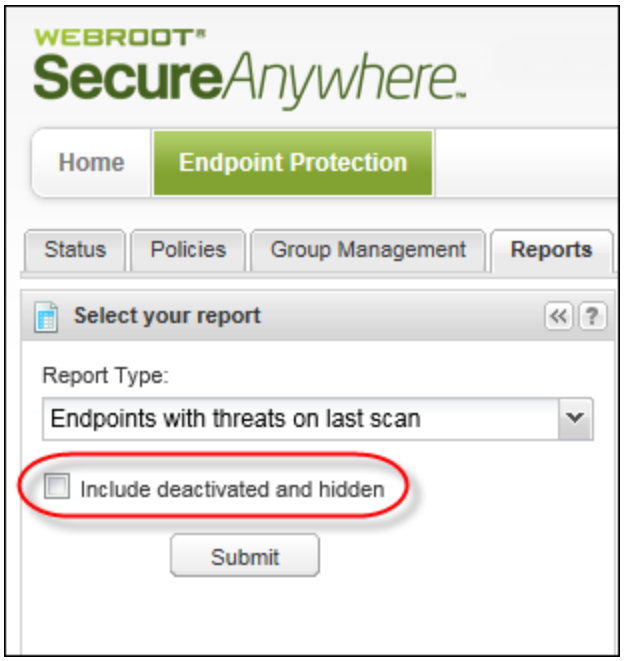
- 選択したポリシーまたはグループ内で検出された脅威をすべて表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に便利です。

[最新のスキャンで脅威が存在したエンドポイント] レポートを生成するには

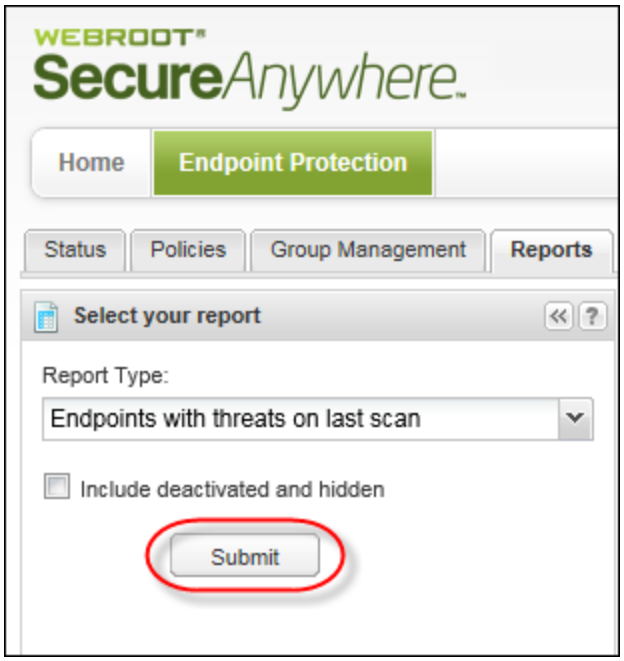
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**最新のスキャンで脅威が存在したエンドポイント**] を選択します。



3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。



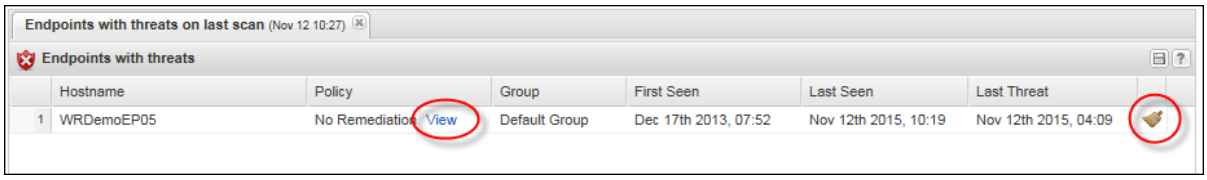
4. [**送信**] ボタンをクリックします。



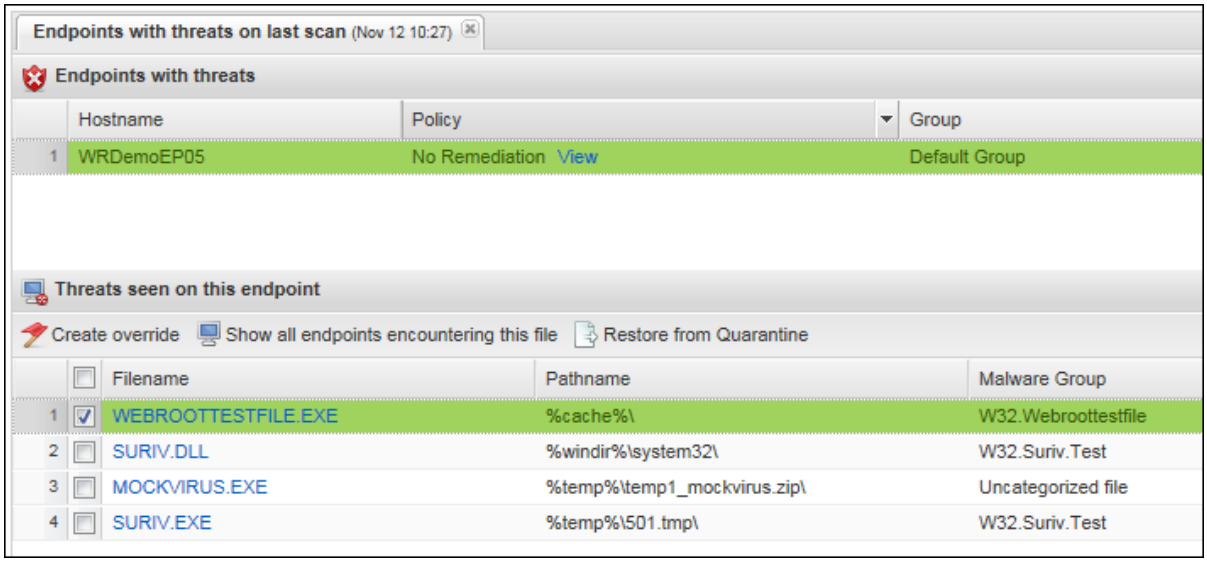
レポートと次のオプションが右側のパネルに表示されます。

- **ポリシーの表示と変更** - エンドポイントのポリシー設定を開き、設定を変更するには、[**表示**] リンクをクリックします。非管理ポリシーに割り当てられたエンドポイントに関しては、エンドポイントレベルで制御されているため [表示] リンクがありません。

- **スキャンを実行** - 右端にある**ほうき**のアイコンをクリックすると、スキャンを開始し、脅威の自働隔離を行うことができます。



5. エンドポイントで検出された脅威の詳細を確認するには、[ホスト名] カラムのアイテムをクリックします。詳細が下のパネルに表示されます。



6. 下のパネルから、選択した脅威に対して次のいずれかの操作を行うことができます。

   - **オーバーライドの作成** - エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [**オーバーライドの作成**] アイコンをクリックします。.詳細については、「*レポートからのファイルへのオーバーライドの適用 ページ454*」を参照してください。

   - **隔離先から復元する** - ファイルが安全である場合、エンドポイントの元の場所に復元するには、コマンドバーの [**隔離先から復元する**] アイコンをクリックします。

7. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラムの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

   レポートのスプレッドシートをダウンロードする場合の詳細については、「*レポートのスプレッドシートのダウンロード ページ402*」を参照してください。

[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成

SecureAnywhere は、正当なファイルのように見えても動作が疑わしいファイルを検出することがあります。この場合、そのファイルは [*未判定*] に分類されます。

SecureAnywhere が最新のスキャンで [*未判定*] と分類したファイルを特定するには、[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートを生成します。エンドポイントを選択してドリルダウンすると、ファイルの詳細を確認できます。

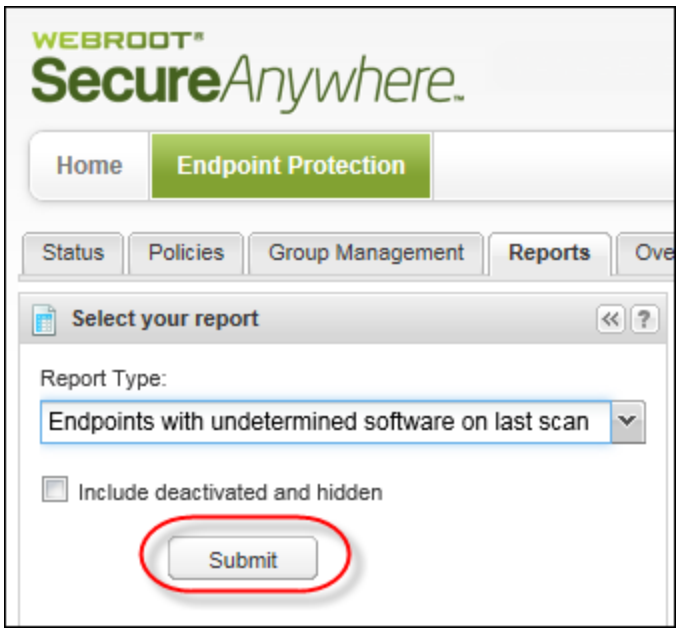
[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートを生成するには

1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**最新のスキャンで未判定のソフトウェアが検出されたエンドポイント**] を選択します。

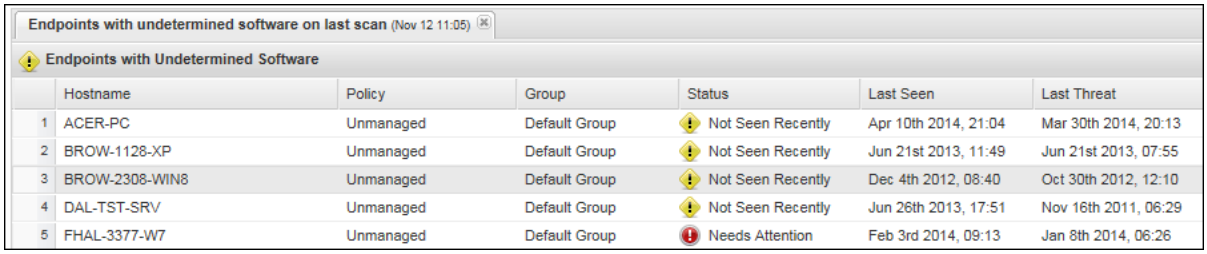
3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[非アク

ティブ化および非表示を含む] チェックボックスを選択します。この手順はオプションです。

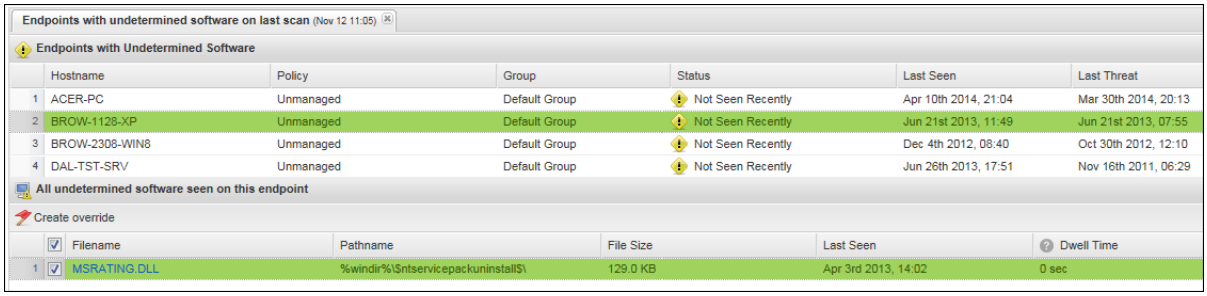
4. [**送信**] ボタンをクリックします。



右側のパネルでレポートが開き、すべてのエンドポイントが表示されます。



5. 検出された未判定のソフトウェアの詳細を確認する場合は、エンドポイントの行をクリックすると、下に詳細が表示されます。



6. このパネルでファイルを選択して [**オーバーライドの作成**] をクリックすると、次のようにファイルを再分類することができます。

   - **正当** - エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、隔離も行いません。[正当] を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて正当] と表示されますが、クラウド判定は未判定のままになります。

   - **不正** - スキャン中に検出された場合、常にファイルを隔離します。[不正] を選択した後、ファイルは [オーバーライド] タブ内に [手動判定にて不正] と表示されますが、クラウド判定は未判定のままになります。

   また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

7. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラムの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

   レポートのスプレッドシートをダウンロードする方法の詳細については、「*レポートのスプレッドシートのダウンロード ページ402*」を参照してください。

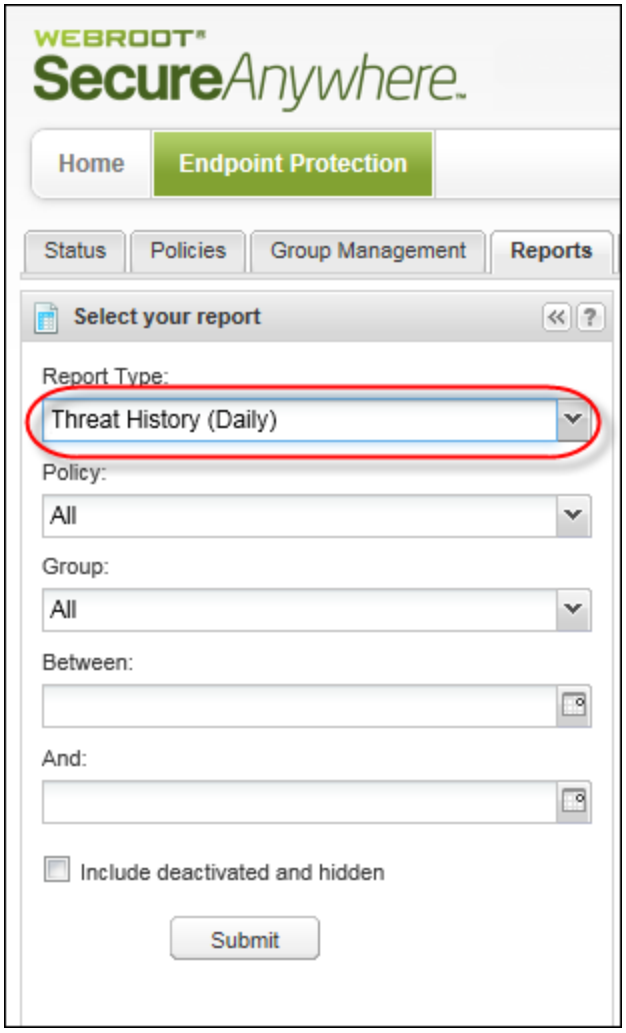
[脅威の履歴 (日単位)] レポートの生成

検出された脅威の概要を日単位で表示するには、[脅威の履歴 (日単位)] レポートを生成します。このレポートには、SecureAnywhere によってエンドポイントで脅威が検出された場所が日単位で表示されます。レポートのデータは次の手順で変更できます。

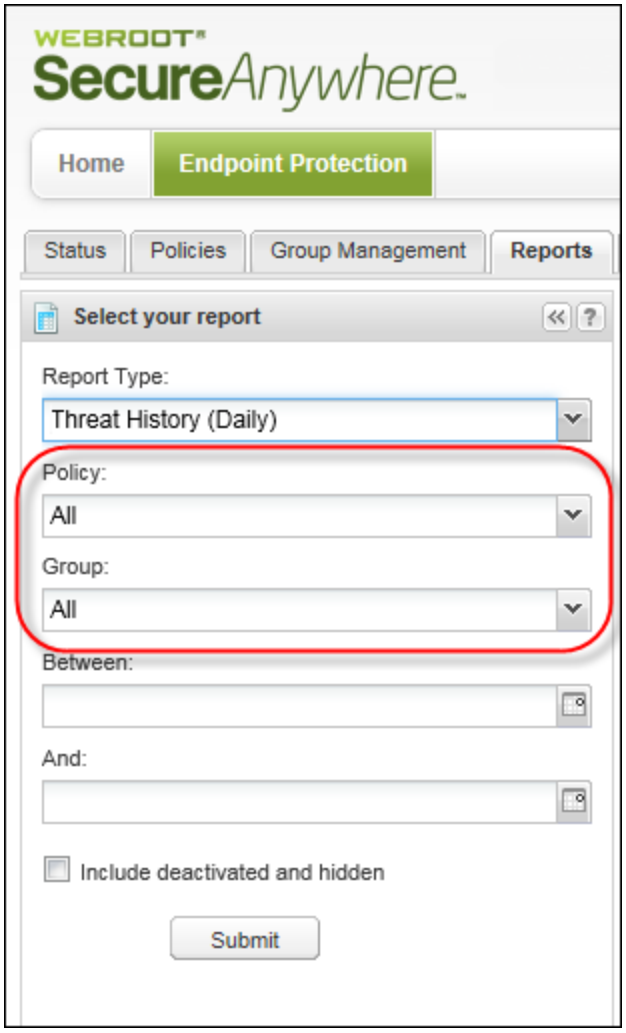
- 選択したポリシーまたはグループ内の脅威を日単位で表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に便利です。

[脅威の履歴 (日単位)] レポートを生成するには

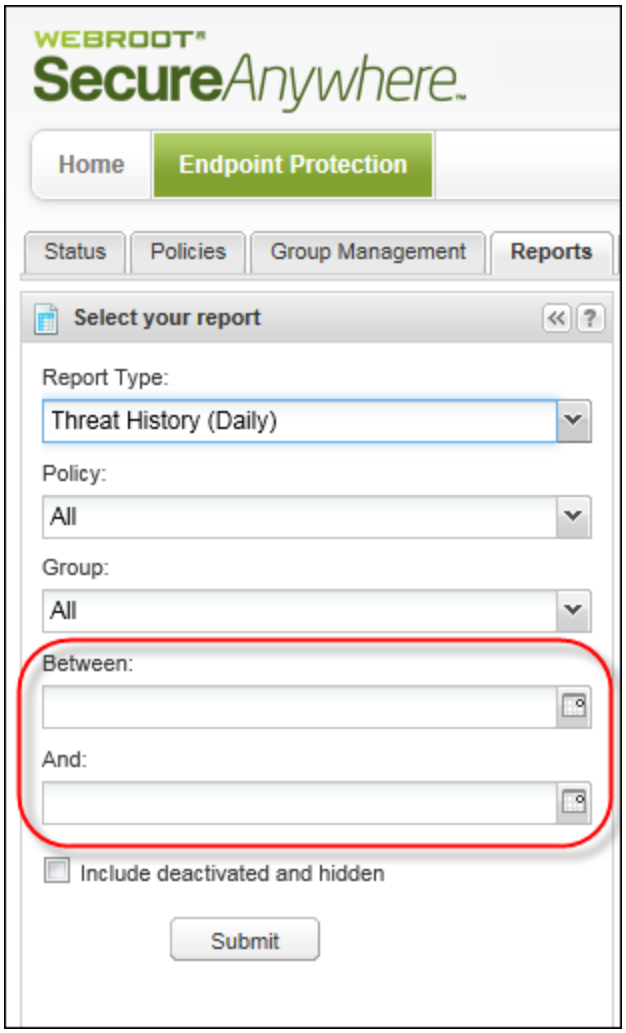
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**脅威の履歴 (日単位)**] を選択します。



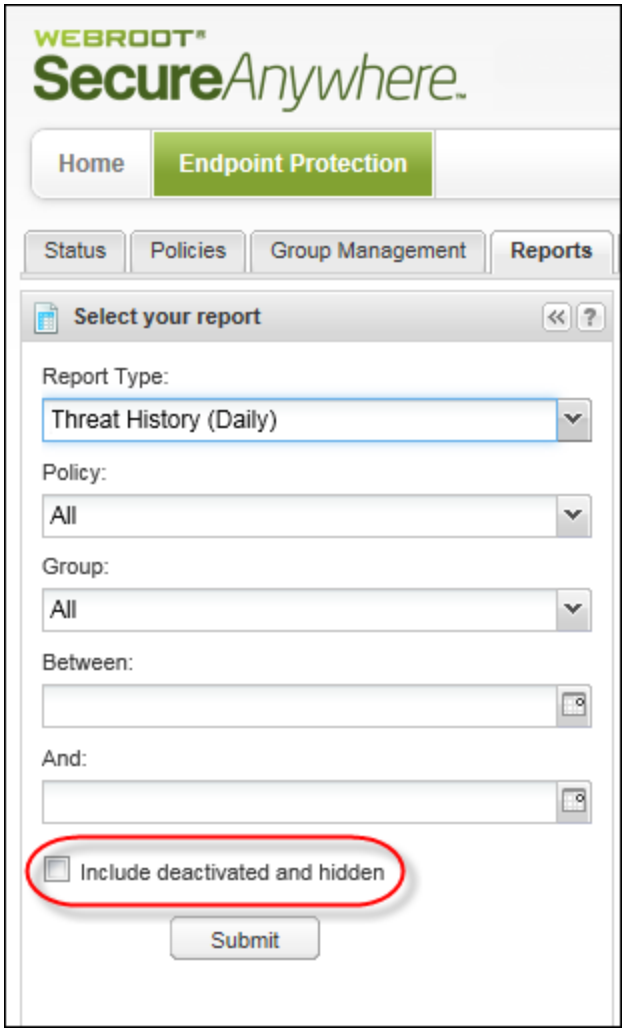
3. 必要に応じて、特定のポリシーやグループを選択します。ポリシーやグループを選択しない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Threat History (Daily)
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

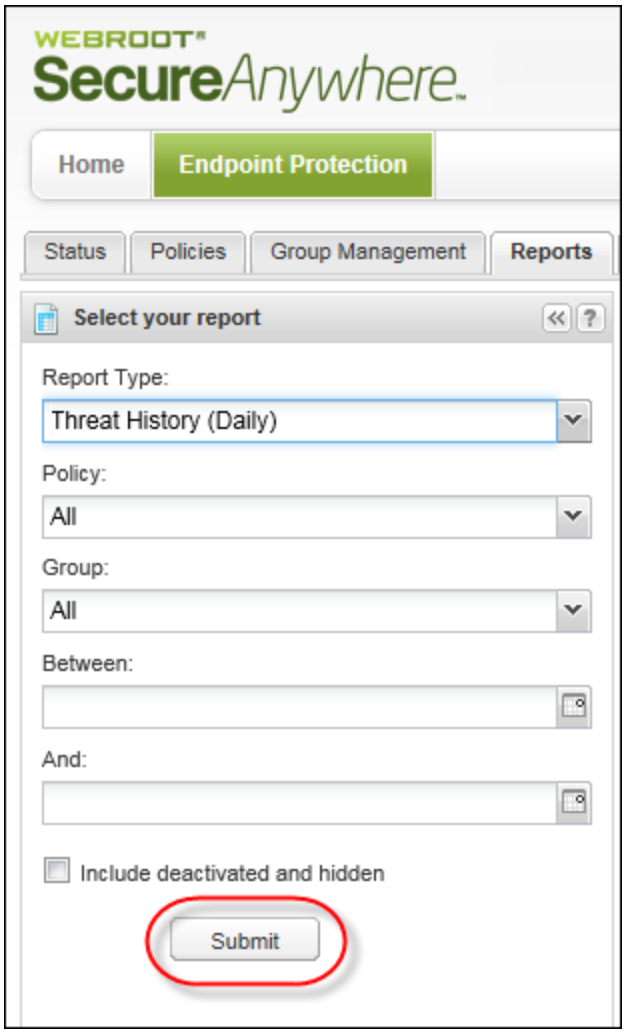
4. [開始日] と [終了日] のフィールドに、レポートデータの期間の開始日と終了日を入力します。



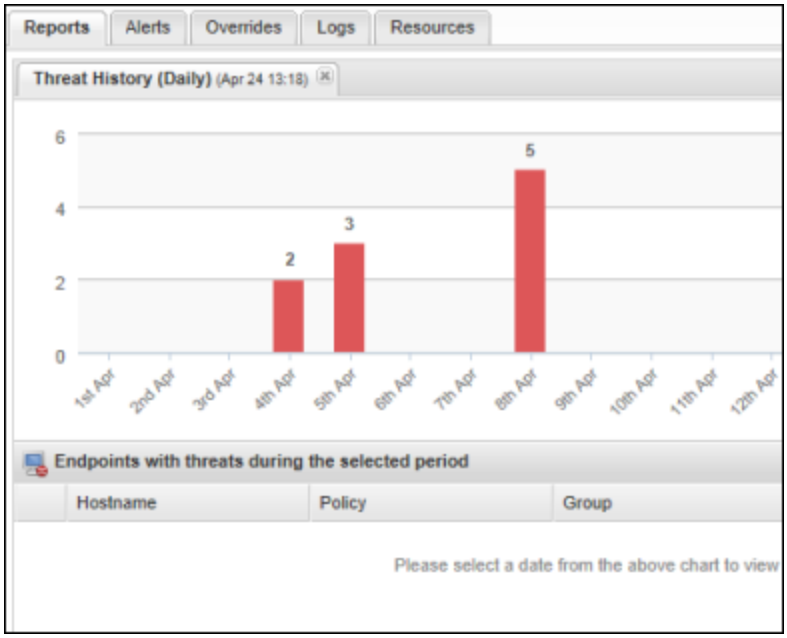
5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Threat History (Daily)
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

6. [**送信**] ボタンをクリックします。

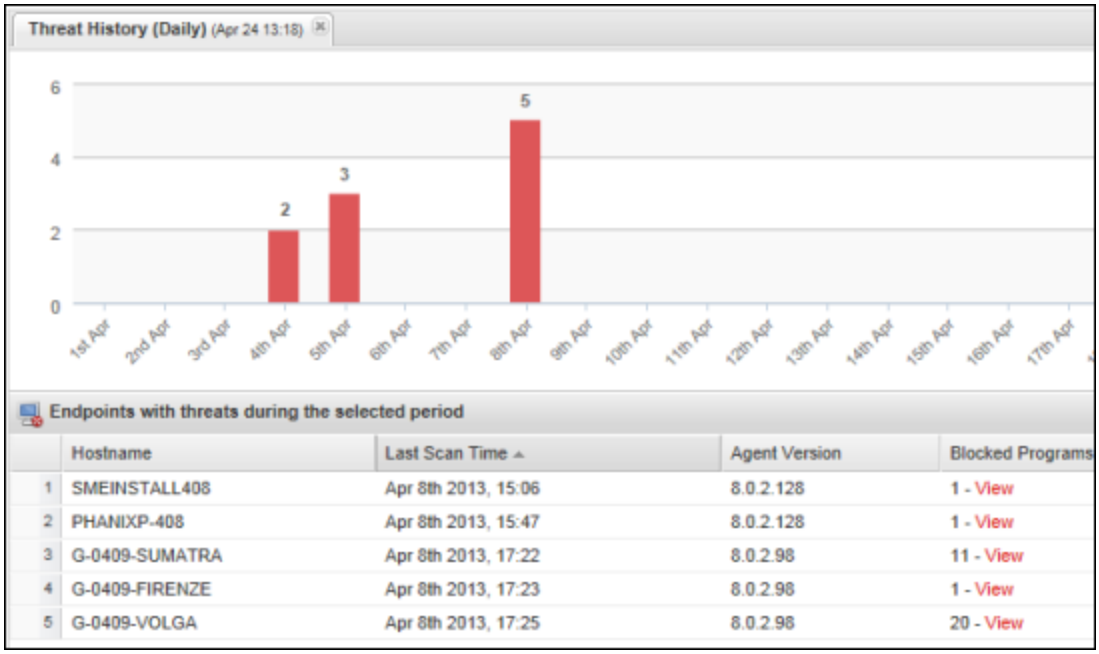


右側のペインにレポートが表示されます。



7. 脅威の詳細を表示するには、棒グラフをクリックします。その日付の詳細が表示されます。

   脅威が検出されたエンドポイントの詳細が下のパネルに表示されます。



	Hostname	Last Scan Time	Agent Version	Blocked Programs
1	SMEINSTALL408	Apr 8th 2013, 15:06	8.0.2.128	1 - View
2	PHANIXP-408	Apr 8th 2013, 15:47	8.0.2.128	1 - View
3	G-0409-SUMATRA	Apr 8th 2013, 17:22	8.0.2.98	11 - View
4	G-0409-FIRENZE	Apr 8th 2013, 17:23	8.0.2.98	1 - View
5	G-0409-VOLGA	Apr 8th 2013, 17:25	8.0.2.98	20 - View

8. ブロックされたプログラムの詳細を表示するには、[ブロックされたプログラム] カラムの [**表示**] リンクをクリックします。
9. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

[脅威の履歴 (内訳)] レポートの生成

検出された脅威の概要を表示するには、[脅威の履歴 (内訳)] レポートを生成します。このレポートには、脅威が検出されたエンドポイントとプログラムがブロックされたエンドポイントの棒グラフが表示されます。このレポートから、ブロックされたプログラムのオーバーライドを作成したり、隔離されたファイルを復元したりできます。

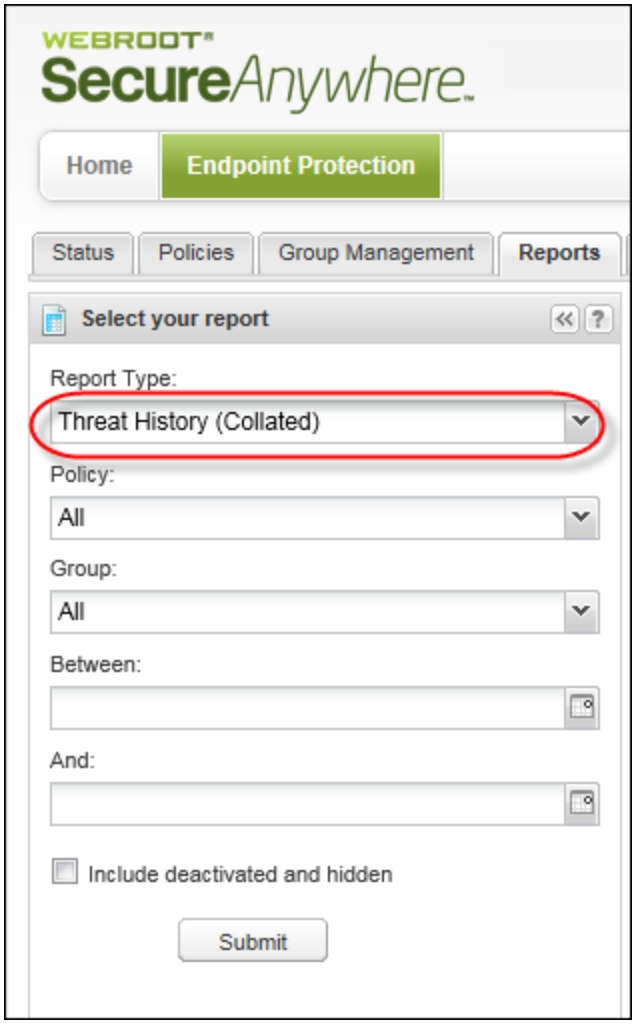
注意: 脅威の概要を表示するには、「*[脅威の履歴 (日単位)] レポートの生成 ページ369*」を参照してください。[脅威の履歴 (日単位)] レポートは概要を確認するためのものであり、このレポートから脅威を管理することはできません。

レポートのデータは次の手順で変更できます。

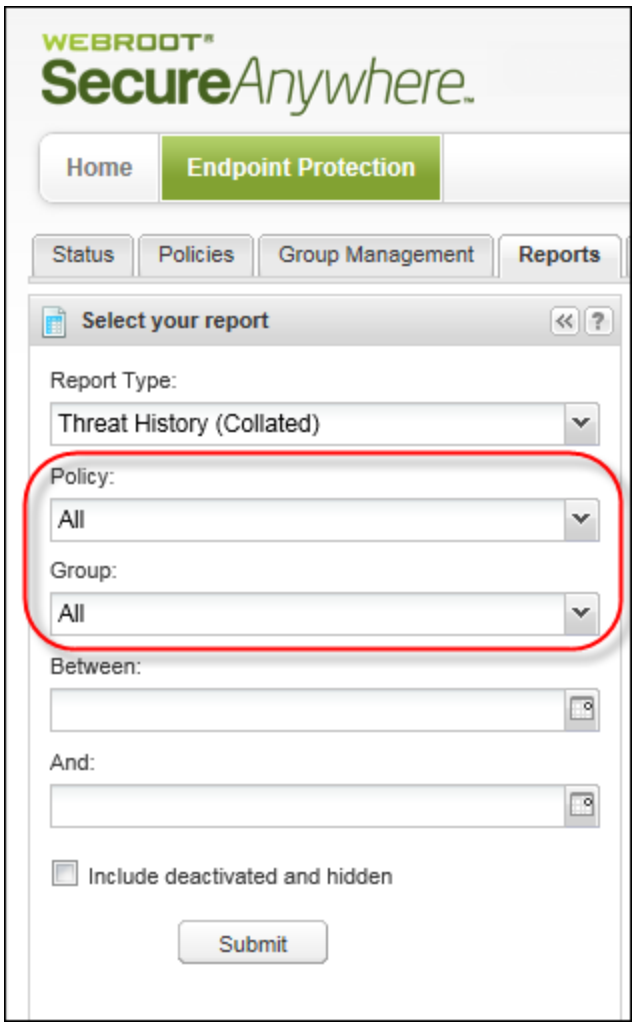
- 選択したポリシーまたはグループ内の脅威をすべて表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして日付範囲内で検出された脅威を確認する。特定の期間に検索結果を絞り込む場合に便利です。

[脅威の履歴 (内訳)] レポートを生成するには

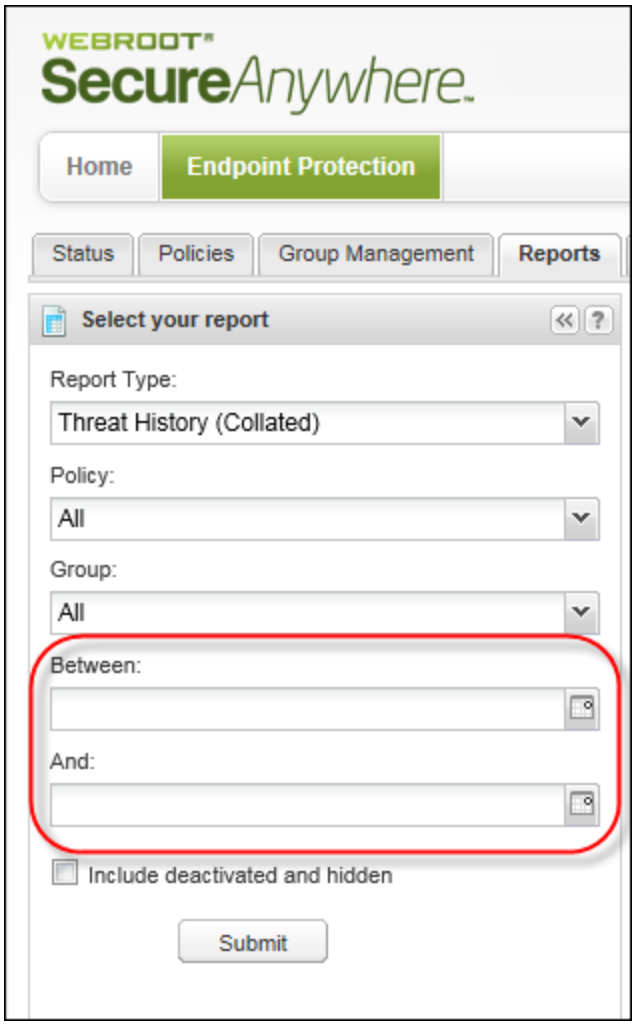
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**脅威の履歴 (内訳)**] を選択します。



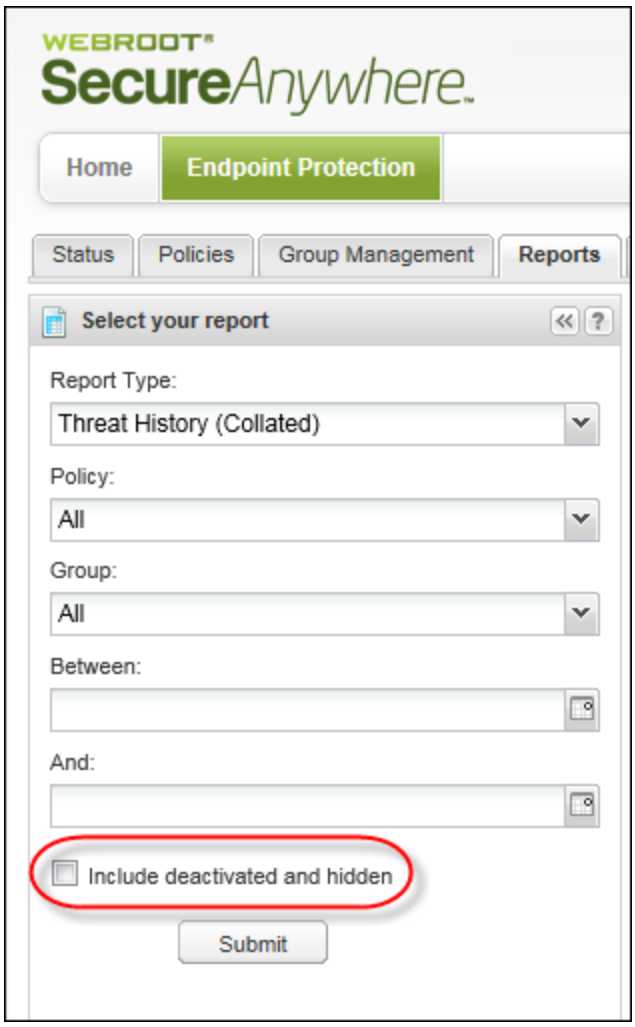
3. 必要に応じて、特定のポリシーやグループを選択します。この選択を行わない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Threat History (Collated)
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

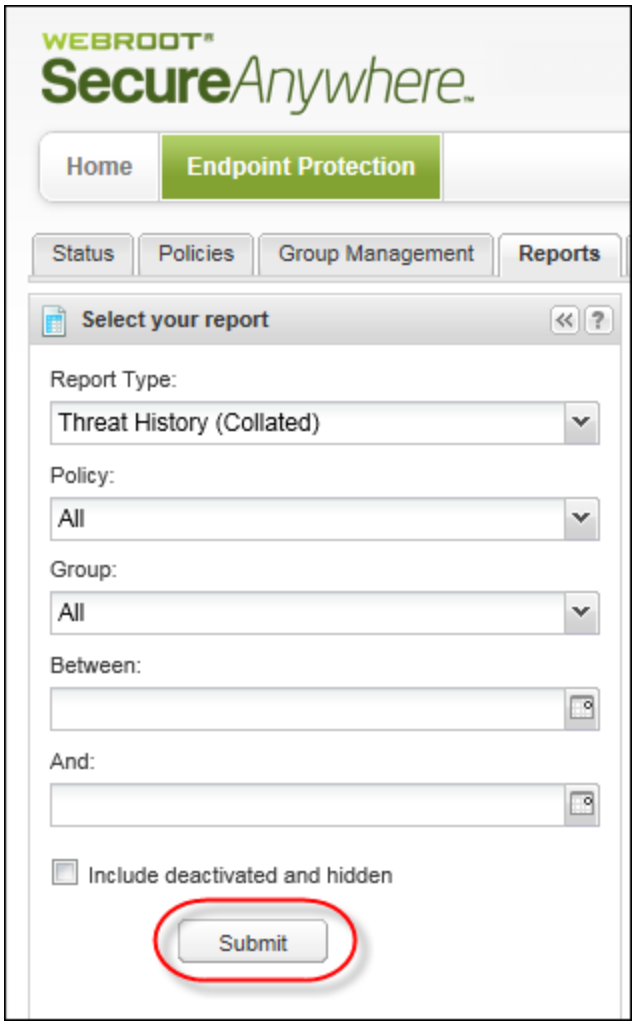
4. [開始日] と [終了日] のフィールドに、レポートデータの期間の開始日と終了日を入力します。



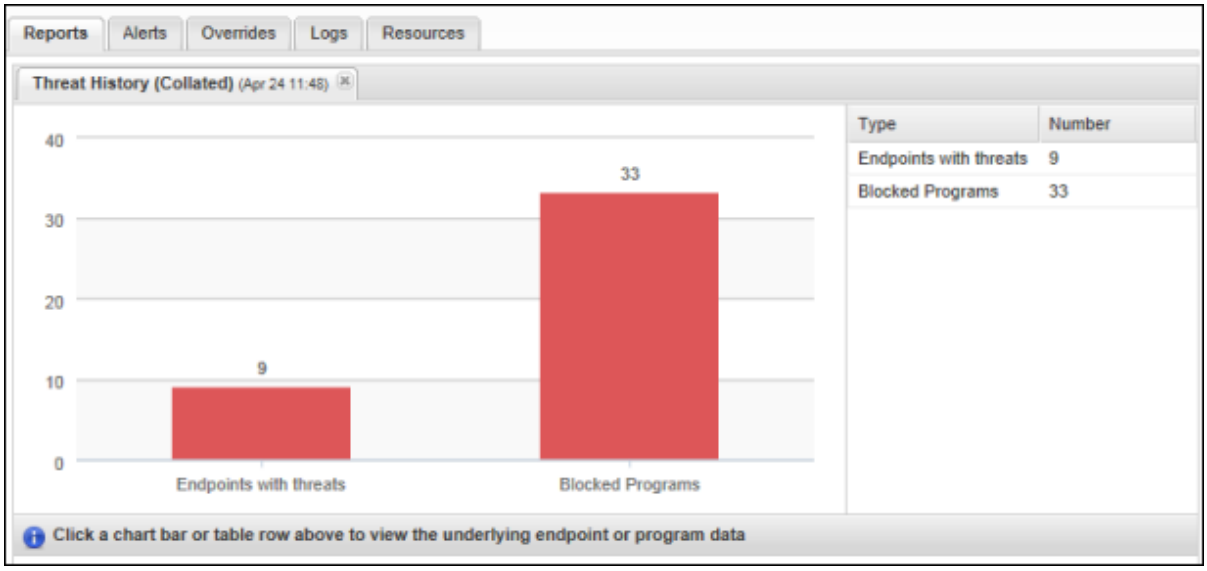
5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Threat History (Collated)
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

6. [**送信**] ボタンをクリックします。

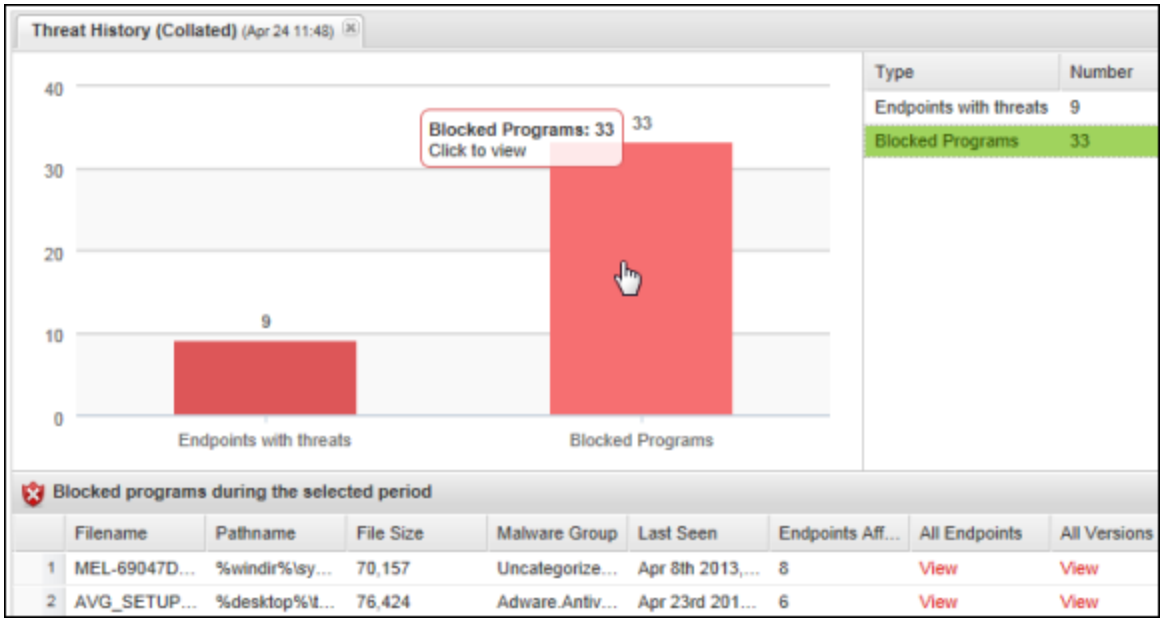


右側のペインにレポートが表示されます。



7. このパネルでいずれかの棒グラフをクリックすると、[脅威が存在したエンドポイント] または [ブロックされたプログラム] の詳細を確認できます。

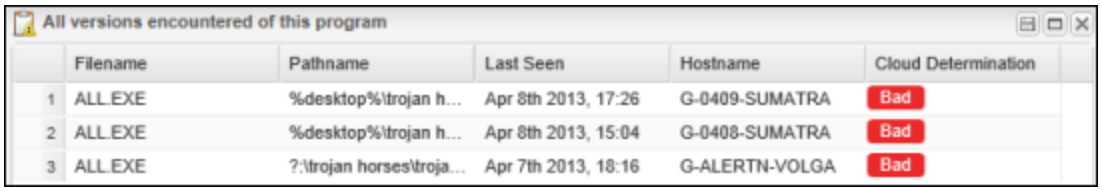
   [ブロックされたプログラム] の棒グラフをクリックすると、プログラムの詳細が下のパネルに表示されます。



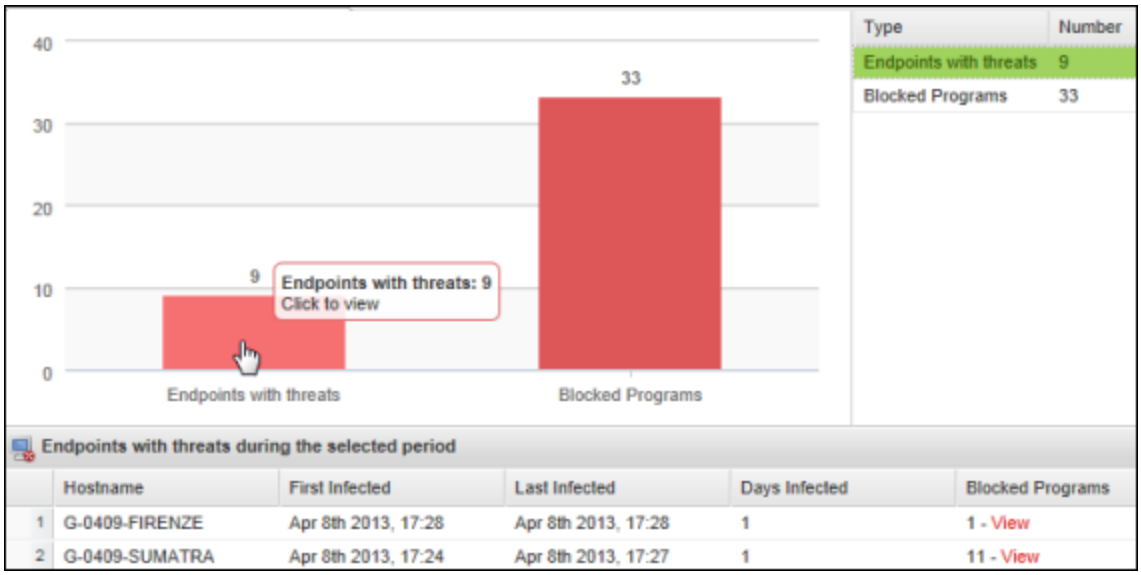
8. 下のパネルで [すべてのエンドポイント] および [すべてのバージョン] カラムの [**表示**] リンクをクリックすると、それぞれの詳細が表示されます。

[すべてのエンドポイント] の [表示] リンクをクリックすると、このパネルが表示されます。

[すべてのバージョン] の [表示] リンクをクリックすると、このパネルが表示されます。

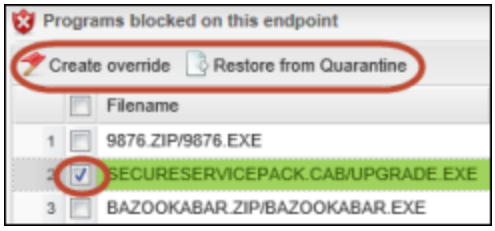


9. ファイルに対するオーバーライドを設定する、またはファイルを隔離先から復元するには、[**脅威が存在したエンドポイント**] の棒グラフを選択すると、詳細が下のパネルに表示されます。



10. ブロックされたプログラムが確認されたエンドポイントの行を探し、[ブロックされたプログラム] カラムの [**表示**] リンクを選択します。

次のウィンドウが表示されます。



11. このウィンドウで、次のいずれかの操作を行います。

    - **オーバーライドの作成** - エンドポイントプロテクションを回避してファイルを [正当] (ファイルの実行を許可) または [不正] (ファイルを検出して隔離) に指定するには、コマンドバーの [オーバーライドの作成] をクリックします。詳細については、「*レポートからのファイルへのオーバーライドの適用 ページ454*」を参照してください。

    - **隔離先から復元する** - ファイルが安全である場合、エンドポイントの元の場所に復元するには、コマンドバーの [隔離先から復元する] をクリックします。

    また、このオーバーライドをすべてのポリシーに適用するか、選択したポリシーのみに適用するかを選ぶことができ、他のエンドポイントのためにオーバーライドを何度も作成する必要がありません。

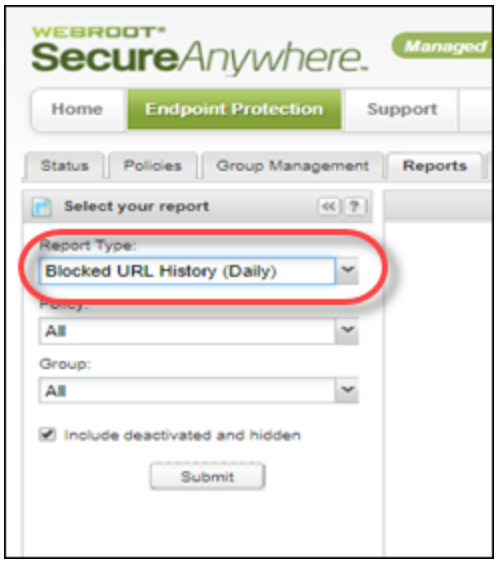
12. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

[ブロックされた URL の履歴 (日単位)] レポートの生成

Webroot の SecureAnywhere の Web 脅威シールドによってブロックされた URL の履歴を表示するには、[ブロックされた URL の履歴 (日単位)] レポートを生成します。

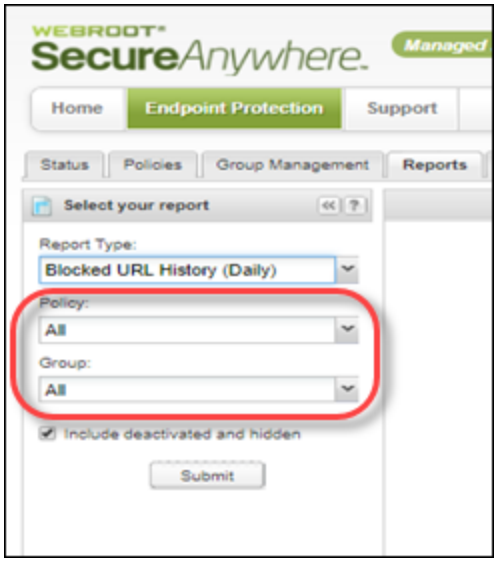
[ブロックされた URL の履歴 (日単位))] レポートを生成するには

1. エンドポイント プロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**ブロックされた URL の履歴 (日単位)**] を選択します。

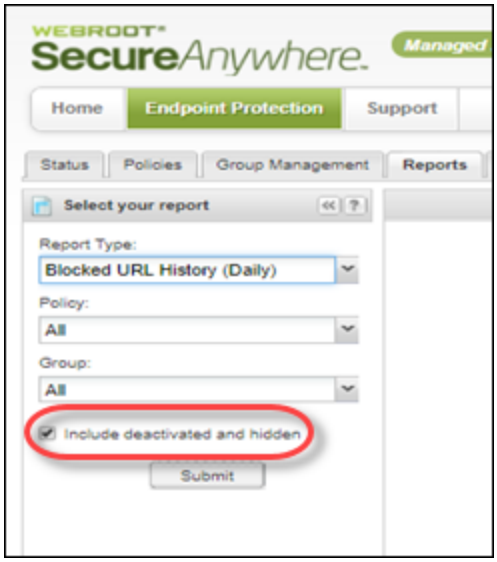


3. 以下のいずれかの操作を行います。

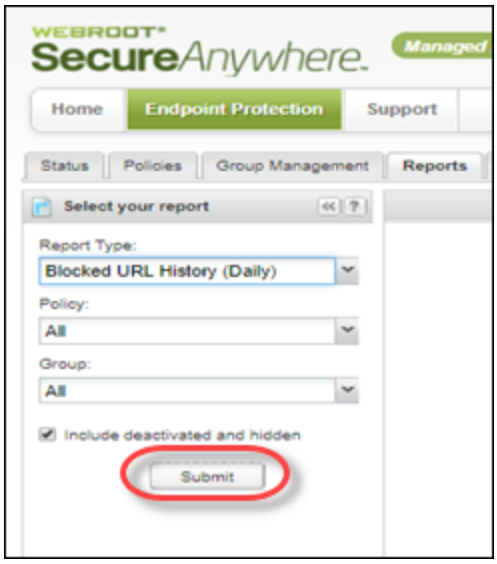
   - すべてのポリシーとグループの結果を表示するように選択する。
   - ブロックされた URL の表示元となるポリシーまたはグループを選択する。



4. ブロック済みの非アクティブ化された URL および非表示の URL を表示するには、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。

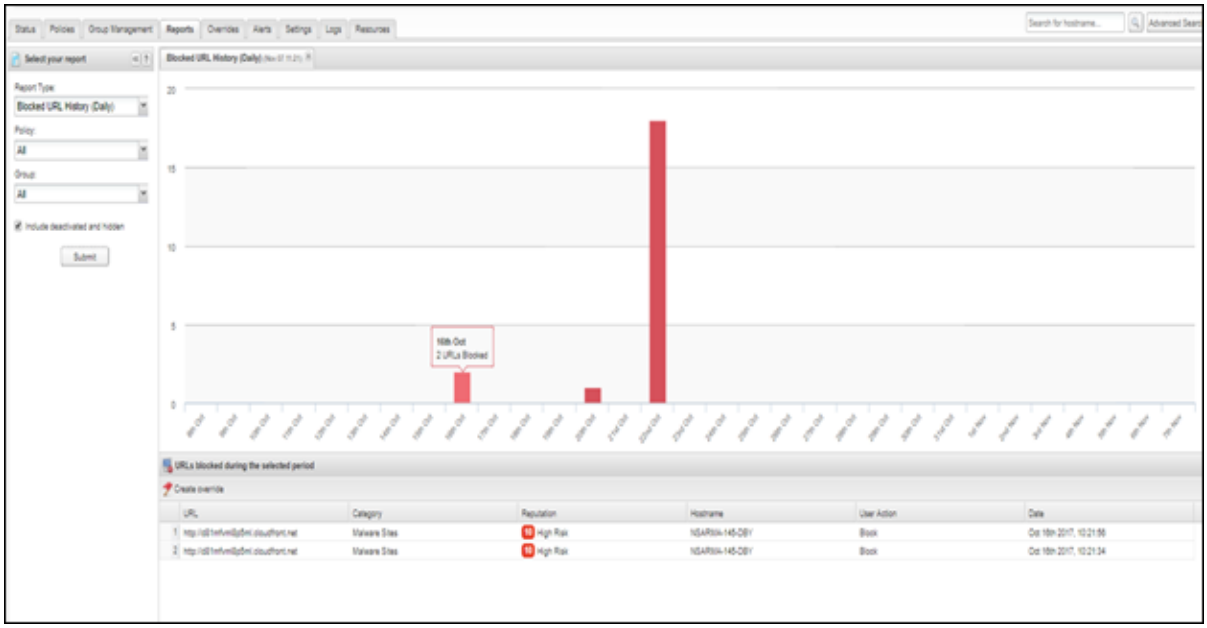


5. 設定が完了したら、[**送信**] をクリックしてレポートを生成します。



次の情報を含むレポートの結果が右側に表示されます。

- ブロックされた URL
- ブロックのカテゴリー
- 評価
- ホスト名
- ユーザーアクション
- ブロックの日時


Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Select your report
Report Type:
Blocked URL History (Daily)
Policy:
All
Group:
All
Include deactivated and hidden
Submit
Blocked URL History (Daily)
16th Oct
2 URLs Blocked
URLs blocked during the selected period
Create override
URL
Category
Reputation
Hostname
User Action
Date
Malware Sites
High Risk
Block

[エージェントのバージョンの使用状況] レポートの生成

異なる SecureAnywhere のバージョンがインストールされているエンドポイントを特定するには、[エージェントのバージョンの使用状況] レポートを生成します。エージェントとは、エンドポイントで実行されている SecureAnywhere ソフトウェアです。

このレポートを使用して、アップグレードが必要なエンドポイントを特定できます。このレポートには、ネットワーク内で使用されているバージョン番号と、各バージョンを使用しているエンドポイントを示す棒グラフが表示されます。

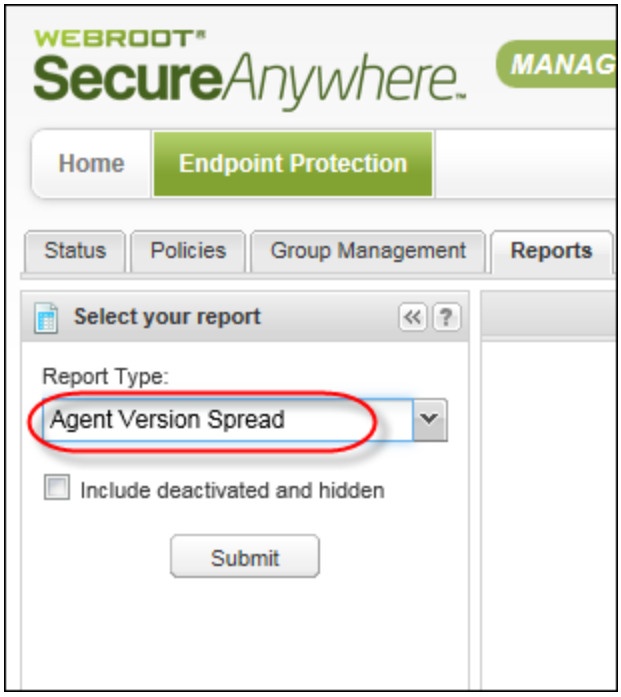
レポートのデータは次の手順で変更できます。

- 選択したグループ内のすべてのバージョンを表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして特定のバージョンを使用しているエンドポイントを確認する。アップグレードの必要なエンドポイントを判定する場合に便利です。

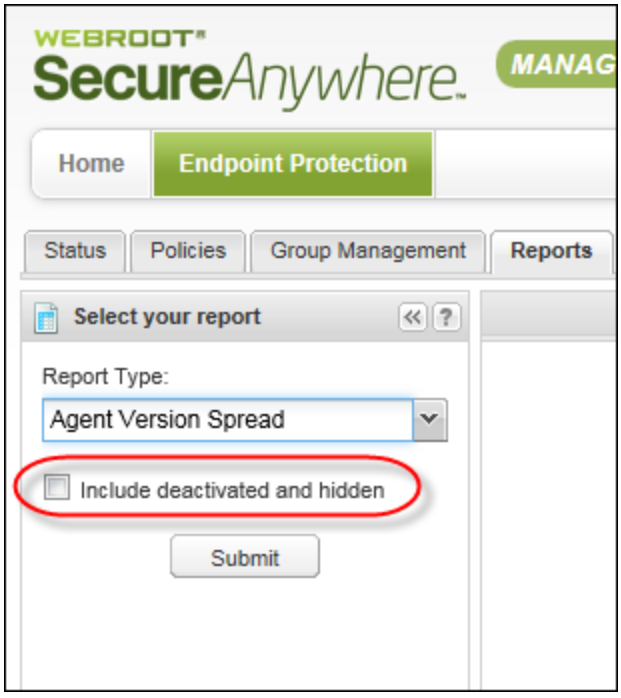
注意: [状態] パネルで、エージェントのバージョンの使用状況を示す円グラフを簡単に確認できます。ただし、この円グラフでは [エージェントのバージョンの使用状況] レポートほど詳細な情報は提供されません。詳細については、「*エージェントのバージョンの概要表示 ページ212*」を参照してください。

[エージェントのバージョンの使用状況] レポートを生成するには

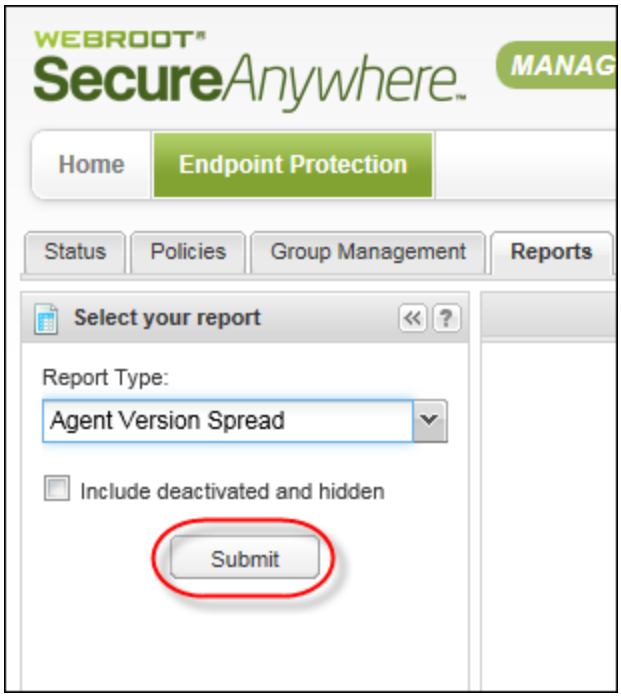
1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**エージェントのバージョンの使用状況**] を選択します。



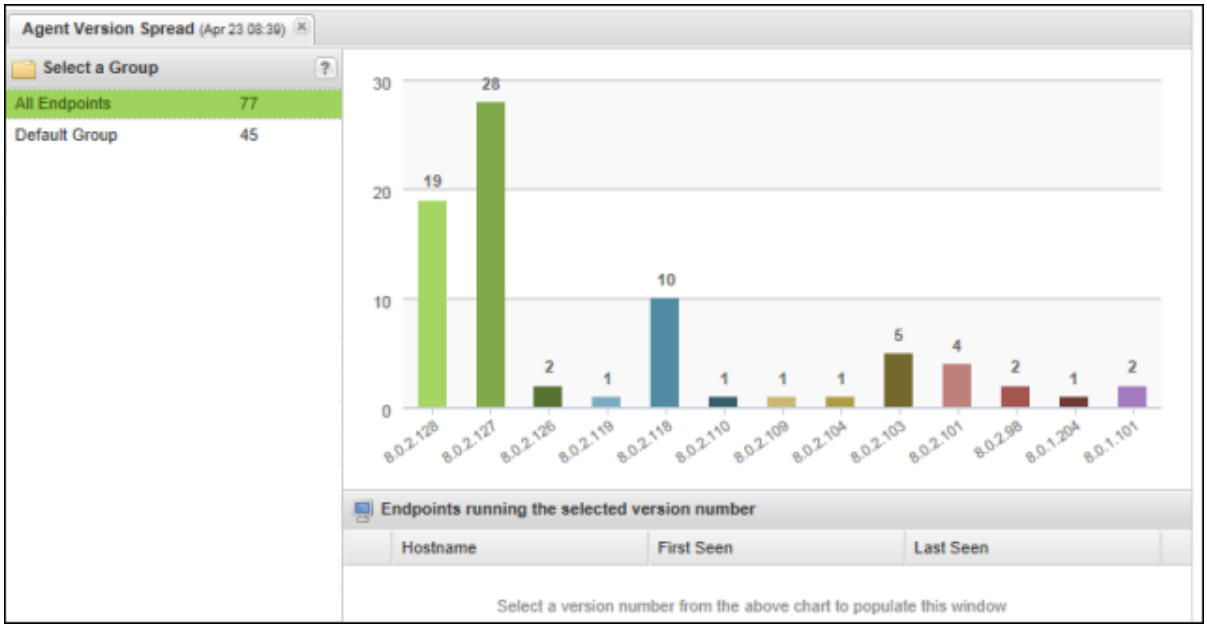
3. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。



4. [**送信**] ボタンをクリックします。



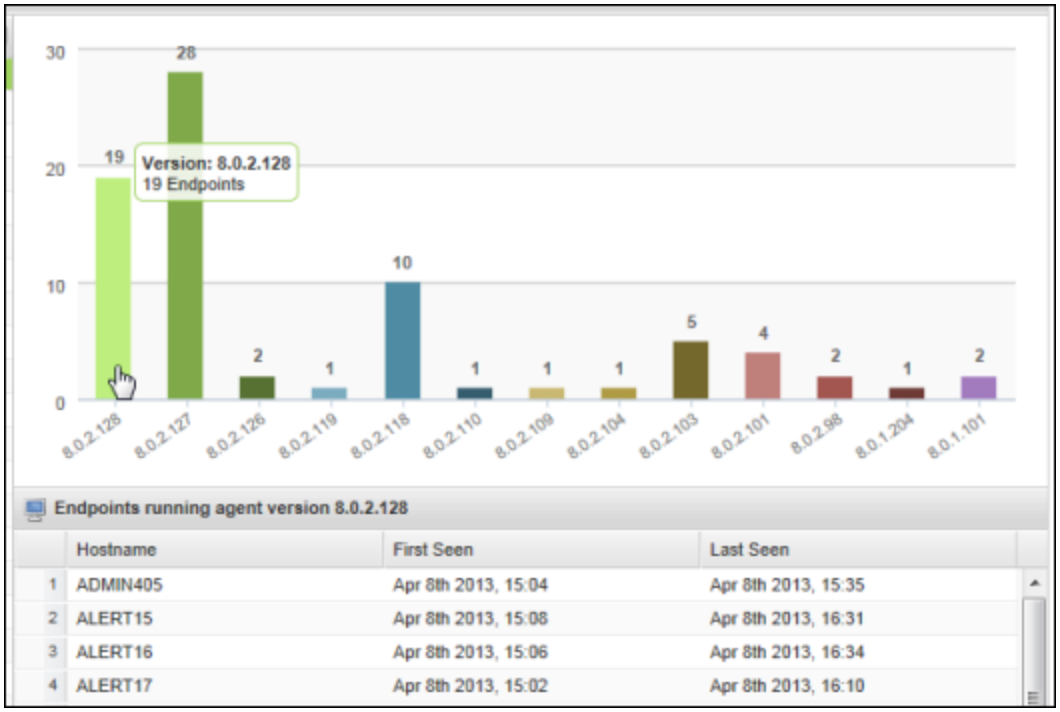
[エージェントのバージョンの使用状況] レポートと、グループのリストが表示されます。



5. 次のいずれか、または両方の操作を行います。

   - 特定のグループのデータを表示するには、左側でグループ名をクリックします。棒グラフに選択したグループのみのデータが表示されます。

   - 特定のバージョンを使用しているエンドポイントを確認するには、棒グラフの棒をクリックして詳細を表示します。下のパネルに各エンドポイントに関するデータが表示されます。



6. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。

   カラム内のデータの詳細については、「*表とレポートのデータの並べ替え ページ45*」を参照してください。

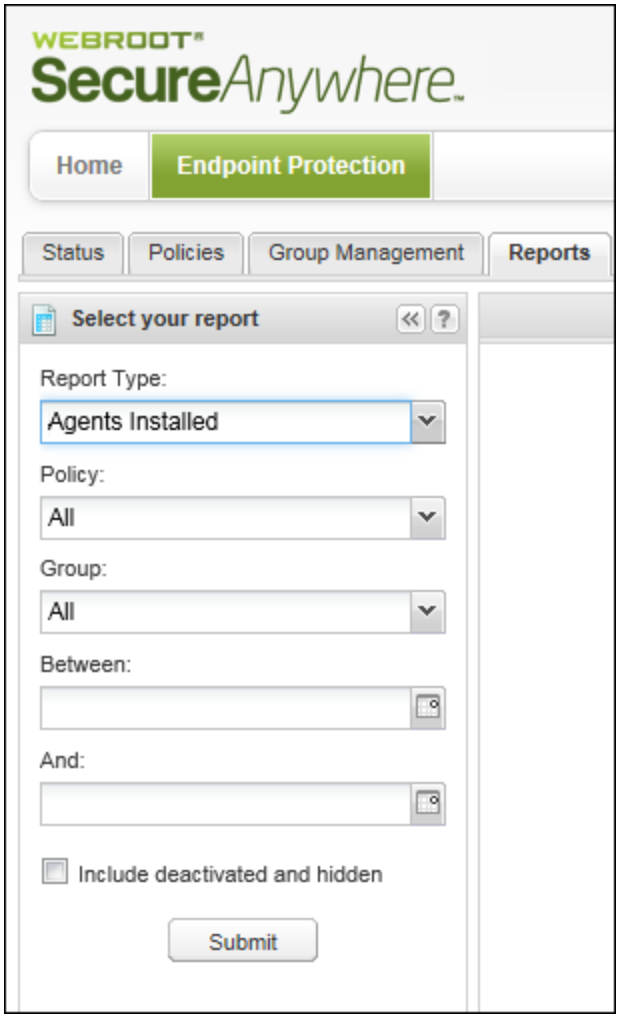
[インストールされたエージェント] レポートの生成

インストールされている SecureAnywhere のグラフを表示するには、[インストールされたエージェント] レポートを作成します。エージェントとは、エンドポイントで実行されている SecureAnywhere ソフトウェアです。このレポートには、SecureAnywhere がエンドポイントにインストールされた日付と、インストールが行われたエンドポイントの数を示す棒グラフが表示されます。レポートのデータは次の手順で変更できます。

- 選択したポリシーやグループ内のすべての SecureAnywhere のインストールを表示する。特定のエンドポイントのセットに検索結果を絞り込む場合に便利です。
- ドリルダウンして同じ日に SecureAnywhere がインストールされたエンドポイントを確認する。特定の期間に検索結果を絞り込む場合や、特定の日にインストールされたエンドポイントのセットにポリシーを割り当てなければならない場合に便利です。

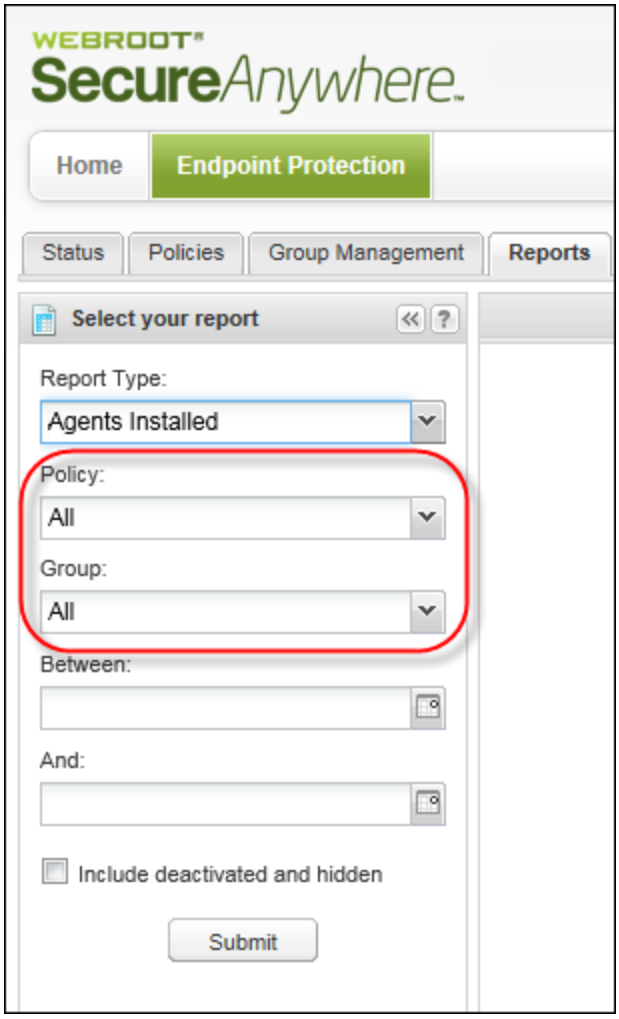
[インストールされたエージェント] レポートを生成するには

1. エンドポイントプロテクションのコンソールで [**レポート**] タブをクリックします。
2. [レポートの種類] ドロップダウンメニューで [**インストールされたエージェント**] を選択します。

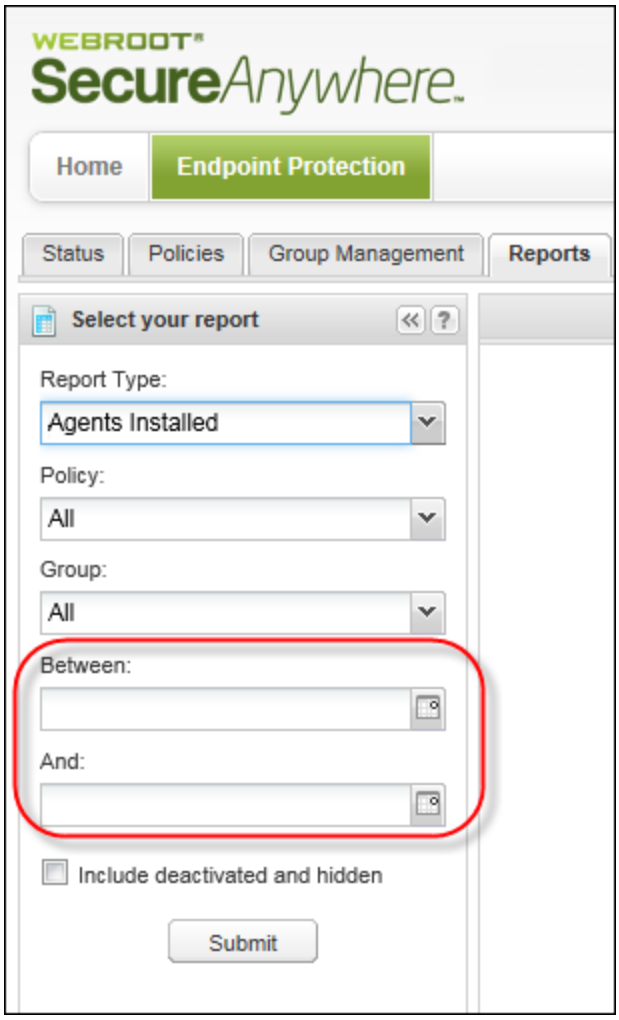


3. 必要に応じて、特定のポリシーやグループを選択します。

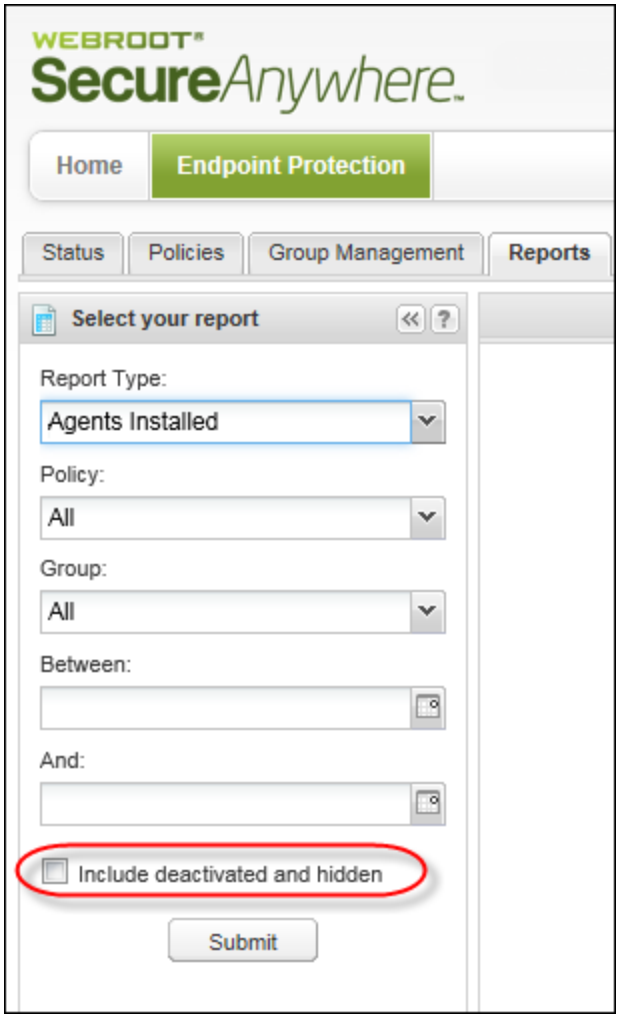
   ポリシーやグループを選択しない場合、レポートにはすべてのポリシーとグループが表示され、使用する環境によっては生成に時間がかかることがあります。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Agents Installed
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

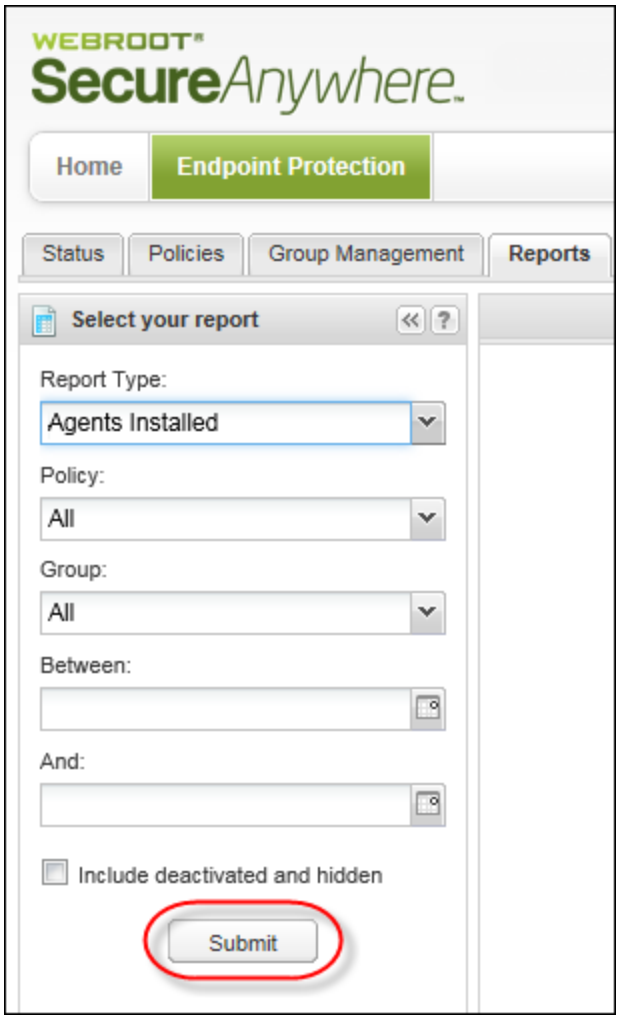
4. [開始日] と [終了日] のフィールドに、レポートデータの期間の開始日と終了日を入力します。



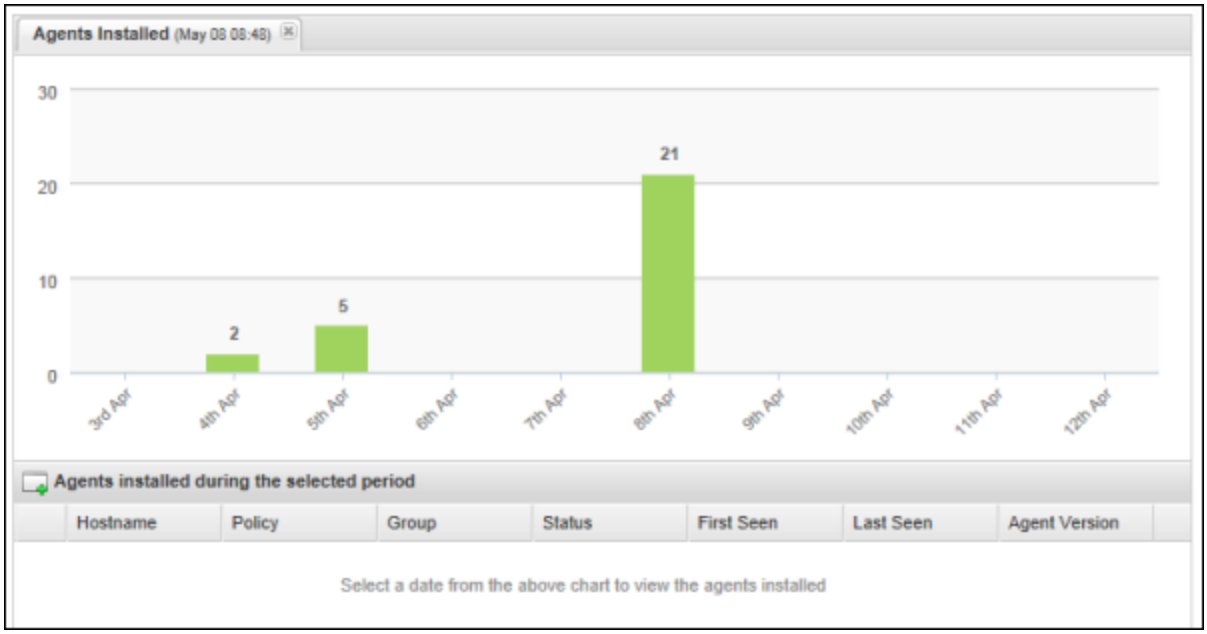
5. 非アクティブ化されたエンドポイントおよび非表示のエンドポイントをレポートに含める場合は、[**非アクティブ化および非表示を含む**] チェックボックスを選択します。この手順はオプションです。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Select your report
Report Type:
Agents Installed
Policy:
All
Group:
All
Between:
And:
Include deactivated and hidden
Submit

6. [**送信**] ボタンをクリックします。

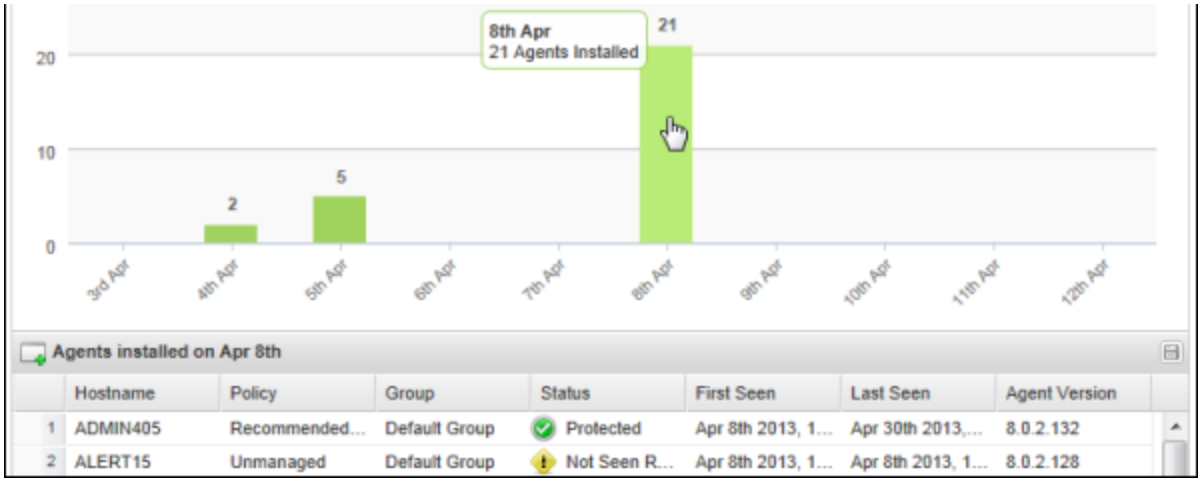


右側のペインにレポートが表示されます。



7. 特定の日付に SecureAnywhere がインストールされたエンドポイントを確認するには、棒グラフの棒をクリックして詳細を表示します。

   下のパネルに各エンドポイントに関するデータが表示されます。



8. レポートの追加データを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加するにはチェックボックスを選択し、カラムを削除するには選択解除します。詳細については、「 *表とレポートのデータの並べ替え ページ45* 」を参照してください。

レポートのスプレッドシートのダウンロード

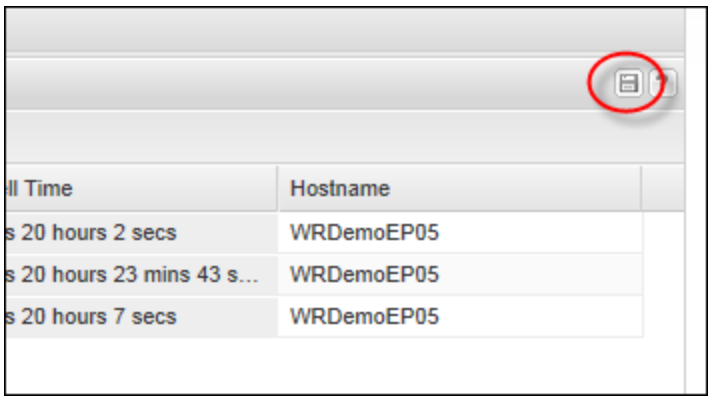
レポートの実行後、電子メールで送信したり保存したりするために、レポートのスプレッドシート (CSV ファイル) が必要になることがあります。必要に応じてレポートのスプレッドシートをダウンロードするには、次の手順に従ってください。

以下のレポートのスプレッドシートをダウンロードできます。

- 確認されたすべての脅威
- 確認されたすべての未判定のソフトウェア
- 最新のスキャンで脅威が存在したエンドポイント
- 未判定のソフトウェアが検出されたエンドポイント

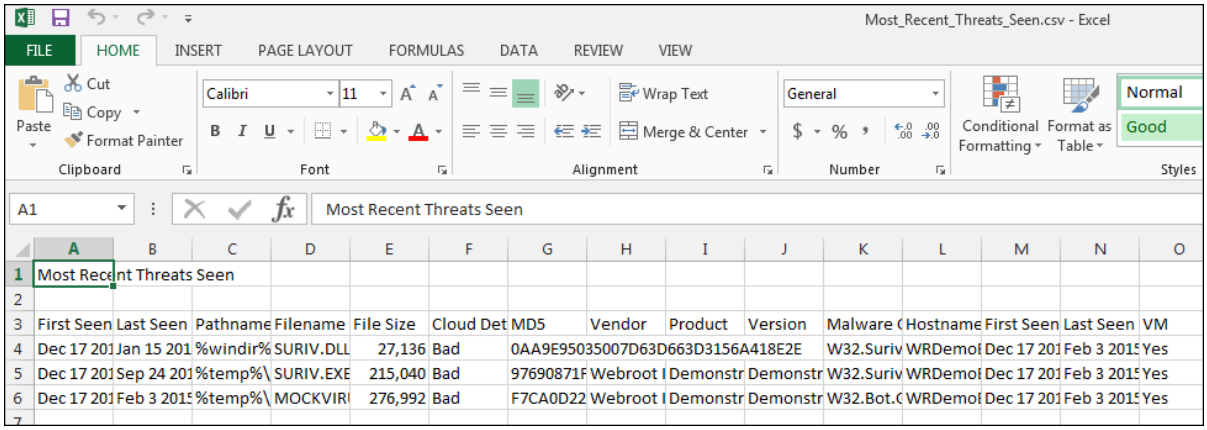
レポートのスプレッドシートをダウンロードするには

1. レポートの実行後、レポートの右上隅にある **CSV** のアイコンをクリックします。.



2. メッセージがウィンドウの下部に表示されたら、[**開く**] ボタンをクリックします。

レポートの設定に基づいてデータが入力された状態でスプレッドシートが表示されます。



3. 必要に応じてスプレッドシートのソートやフォーマット設定を行ってから、コンピュータに保存します。

第 9 章: 警告の管理

警告の管理方法については、以下のトピックを参照してください。

警告の導入

警告メッセージをカスタマイズして、次のイベントが発生した際に、配信先リストに送信することができます。

- エンドポイントによる感染の報告
- エンドポイントでの新しい SecureAnywhere のインストール

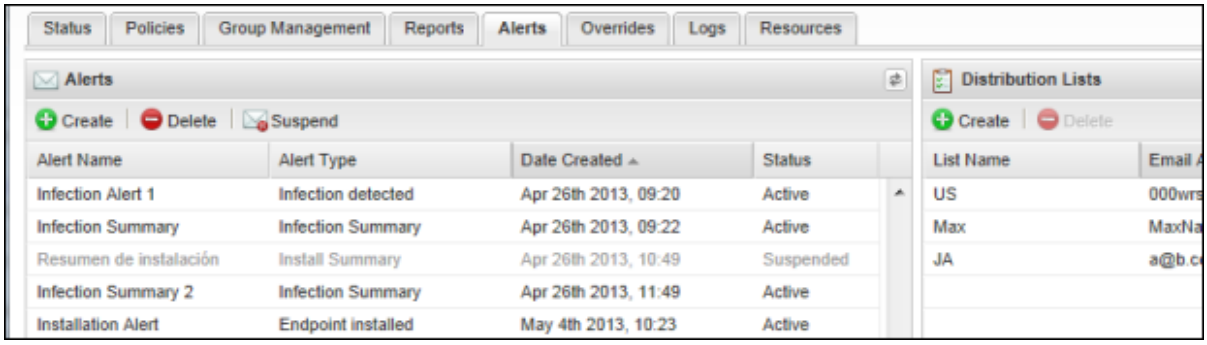
どちらの場合も、イベントが発生したらすぐに、またはスケジュール(毎日、毎週、毎月)に沿って、管理者にメッセージを送信するように警告の方法をカスタマイズできます。[警告] タブのセットアップウィザードを使用すると、メッセージの件名と本文をカスタマイズすることができます。また、変数を使用して、警告を動作させるエンドポイント、影響を受けたグループ、イベントに関するその他の詳細について情報を追加することも可能です。

注意: 警告をカスタマイズするには、[警告] の [作成・編集] へのアクセス権限が必要です。アクセス権限の変更に関する詳細と手順については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

警告を導入するには

1. 電子メールアドレスに基づいて配信先リストを作成します。管理ポータルの [ユーザーの管理] パネルでリストのメンバーを定義する必要はありません。詳細については、「*配信先リストの作成 ページ406*」を*参照してください*。
2. エンドポイントが感染を報告した場合やエンドポイントに SecureAnywhere がインストールされた場合に配信先リストに送信される警告メッセージを作成します。詳細については、「*カスタムの警告の作成 ページ408*」を*参照してください*。

   すべてのカスタムの警告が [警告] タブに表示されます。



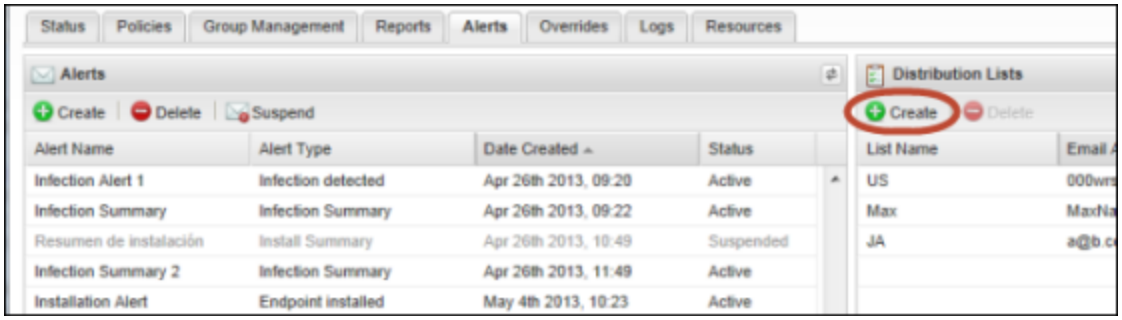
配信先リストの作成

[警告] タブでは、警告メッセージを送信するユーザーの配信先リストを簡単に作成することができます。たとえば、脅威が検出された際にリモートオフィスで対応する必要がある管理者の一覧などを作成できます。

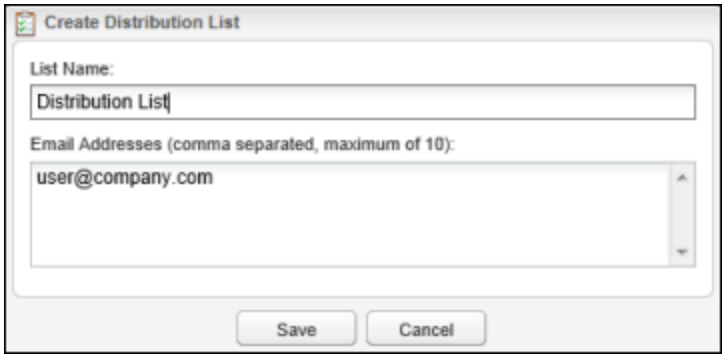
注意: [警告の作成] ウィザードでも配信先リストを作成できます。詳細については、「カスタムの警告の作成 ページ408」を参照してください。

配信先リストを作成するには

1. [**警告**] タブをクリックします。
2. [配信先リスト] カラムで、コマンドバーの [**作成**] をクリックします。



T[配信先リストの作成] ウィンドウが表示されます。



3. [リストの名前] フィールドにリストの名前を入力します。
4. [電子メールアドレス] フィールドに受信者の電子メールアドレスを入力します。各アドレスはコンマで区切ります。

5. 設定が完了したら [**保存**] ボタンをクリックします。

   [配信先リスト] パネルに新しいリストが追加されます。

   後でリストを削除するには、リストの名前を選択してコマンドバーの [**削除**] アイコンをクリックします。

カスタムの警告の作成

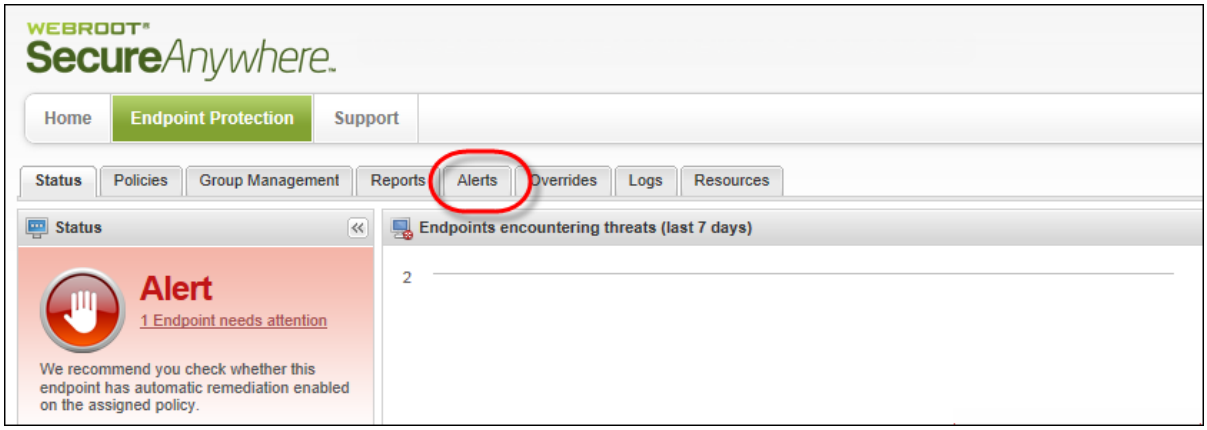
次のイベントについて、配信先リストに送信される警告メッセージをカスタマイズできます。

- **感染が検出されました** - エンドポイントが感染を報告するとただちに送信されるメッセージ。
- **エンドポイントがインストールされました** - SecureAnywhere がエンドポイントにインストールされ、管理ポータルに報告するとただちに送信されるメッセージ。
- **感染の概要** - エンドポイントで検出された脅威の概要を示すメッセージ。概要の配信頻度は、毎日、毎週、毎月のいずれかを設定できます。
- **インストールの概要** - SecureAnywhere のインストールの概要を示す概要メッセージ。概要の配信頻度は、毎日、毎週、毎月のいずれかを設定できます。

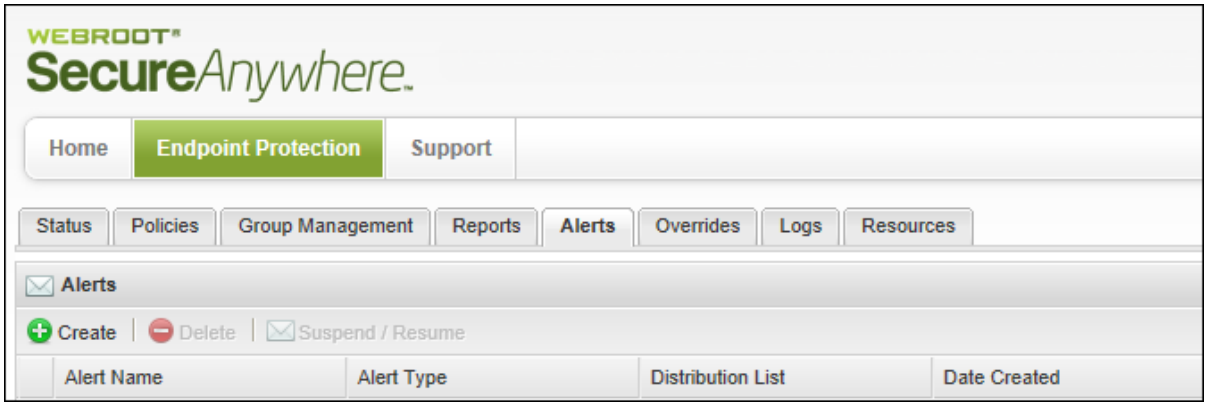
このトピックで説明するように、[警告の作成] ウィザードを使用してメッセージと配信先リストを定義することができます。また、配信先リストは個別に定義することもできます。詳細については、「*配信先リストの作成 ページ406*」を参照してください。

カスタムの警告を作成するには

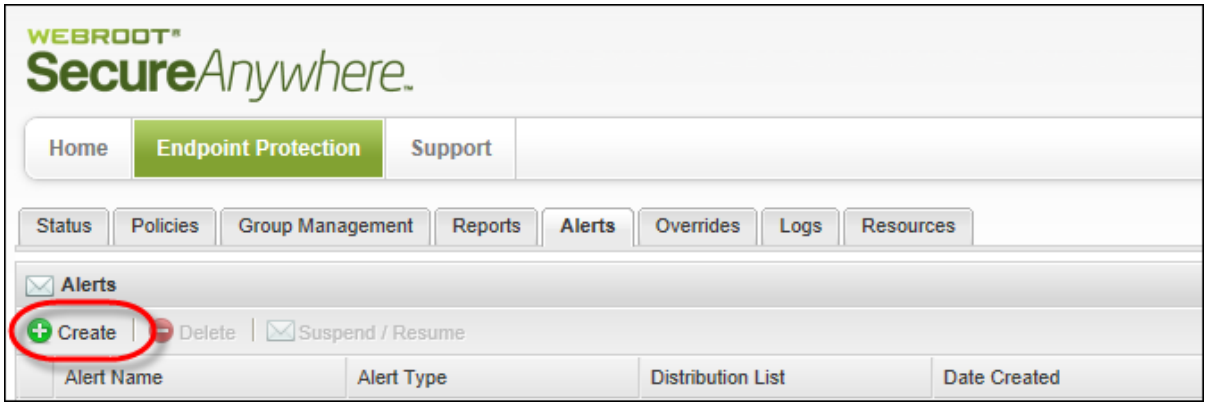
1. メインコンソールで [**警告**] タブをクリックします。



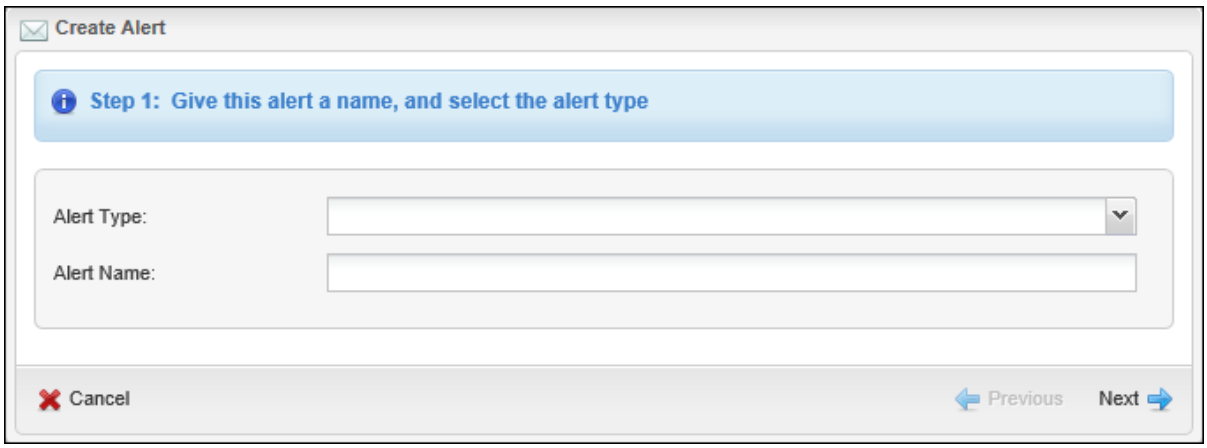
[警告] パネルが表示されます。



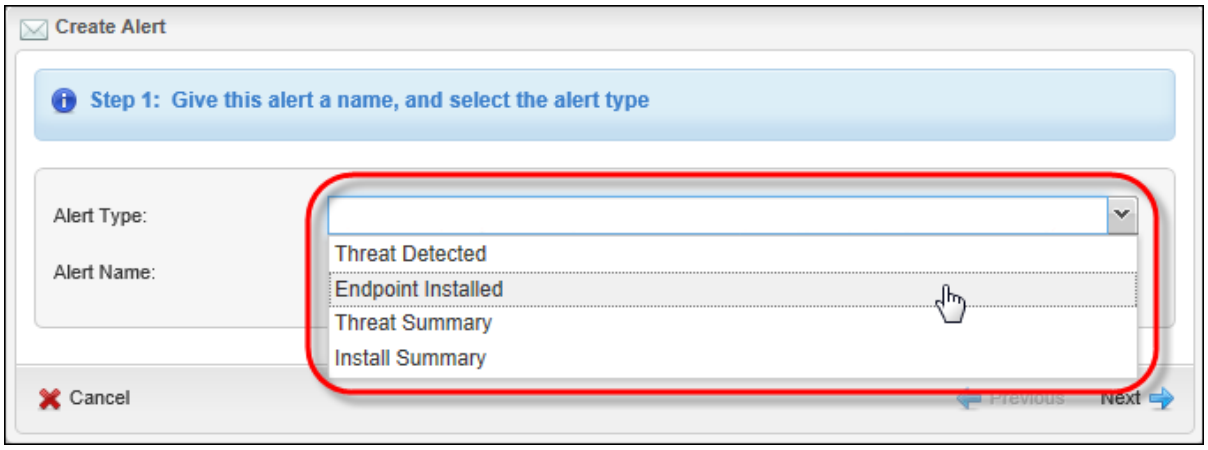
2. コマンド バーの [**作成**] アイコンをクリックします。



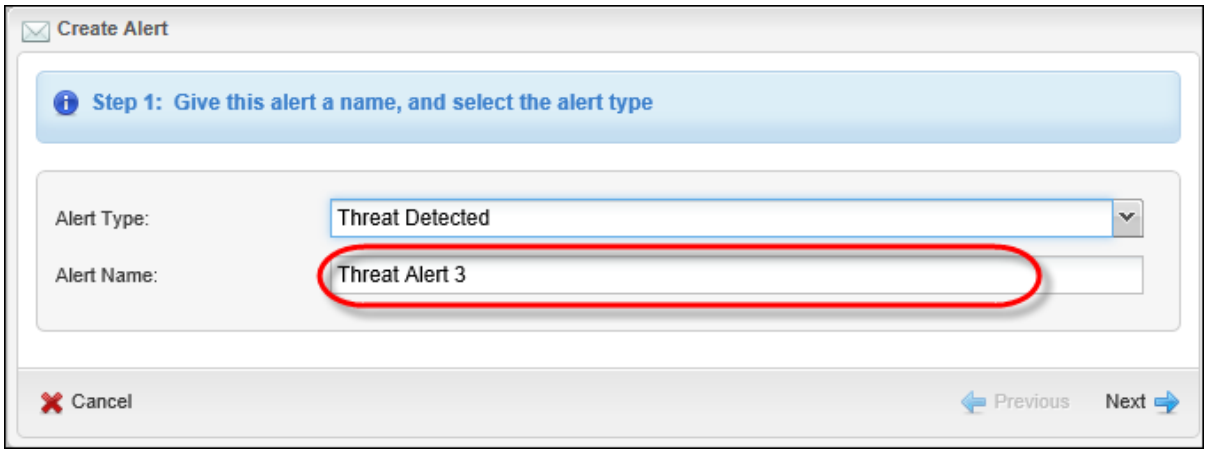
[警告の作成] ウィンドウが表示されます。



3. [警告のタイプ]ドロップダウンメニューで警告のタイプを選択します。



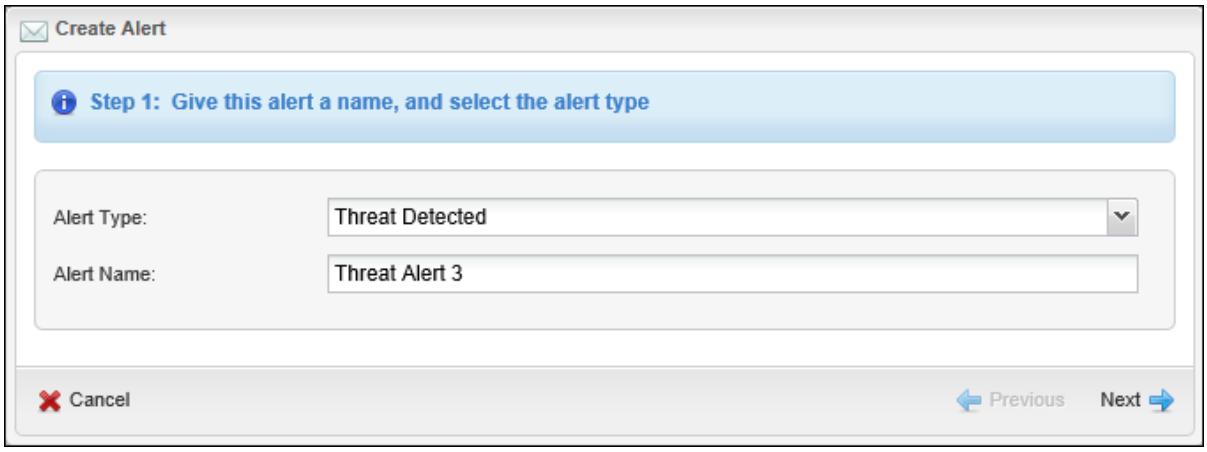
4. [警告の名前]フィールドに、この警告の名前を入力します。



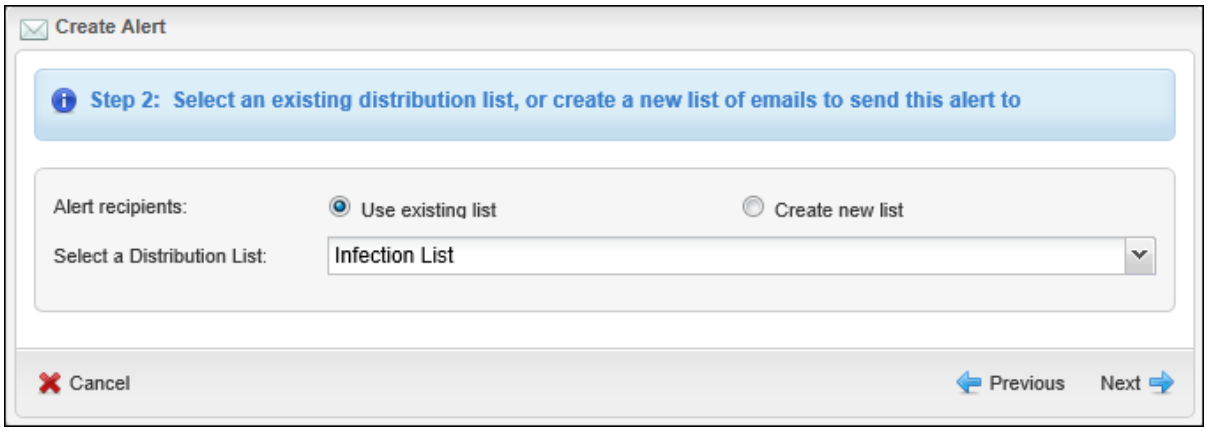
5. 警告のタイプとして[脅威の概要]または[インストールの概要]を選択した場合は、[頻度]フィールドが表示されます。希望する警告の送信頻度を選択します。

- **毎日**
- **毎週**
- **毎月**

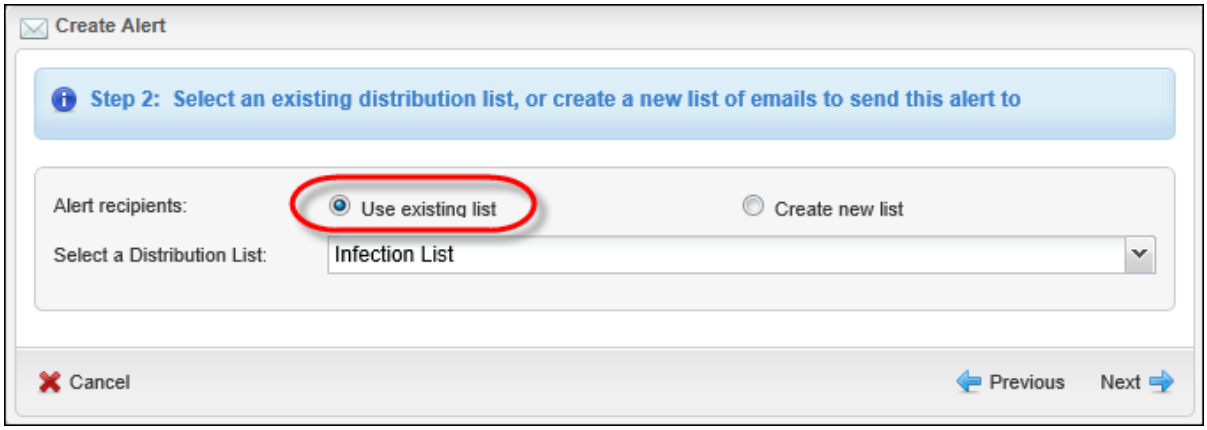
6. [**次へ**] ボタンをクリックします。



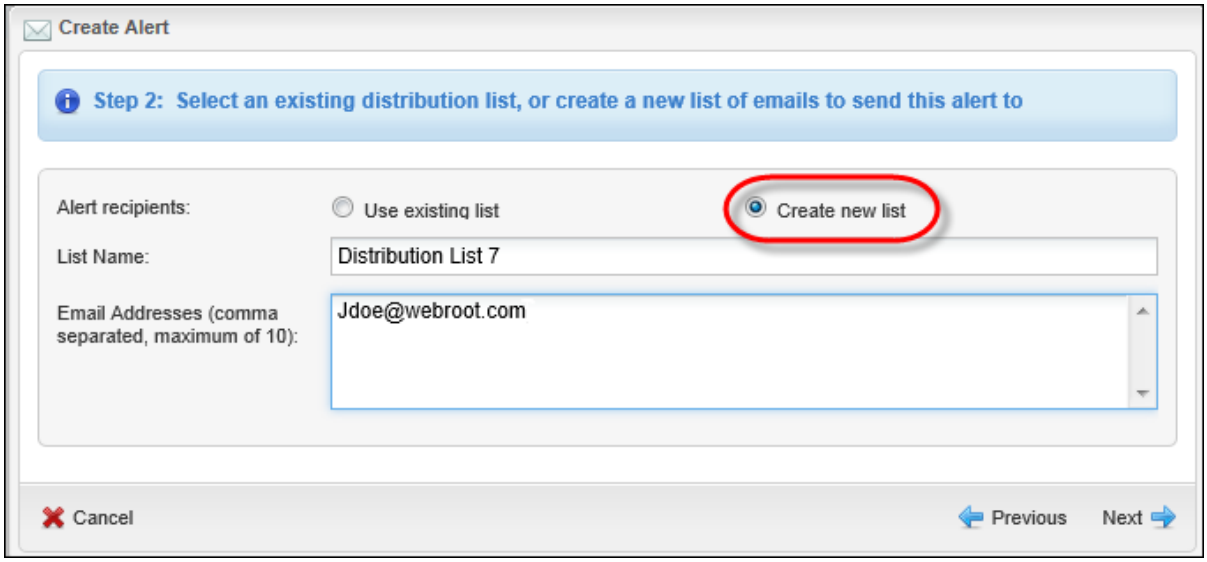
[ステップ 2] ウィンドウが表示されます。



7. 次のいずれかのラジオボタンを選択し、警告の受信者の一覧を決定します。
   - 配信先リストがすでに作成されている場合は、[**既存のリストを使用**] ラジオボタンを選択します。

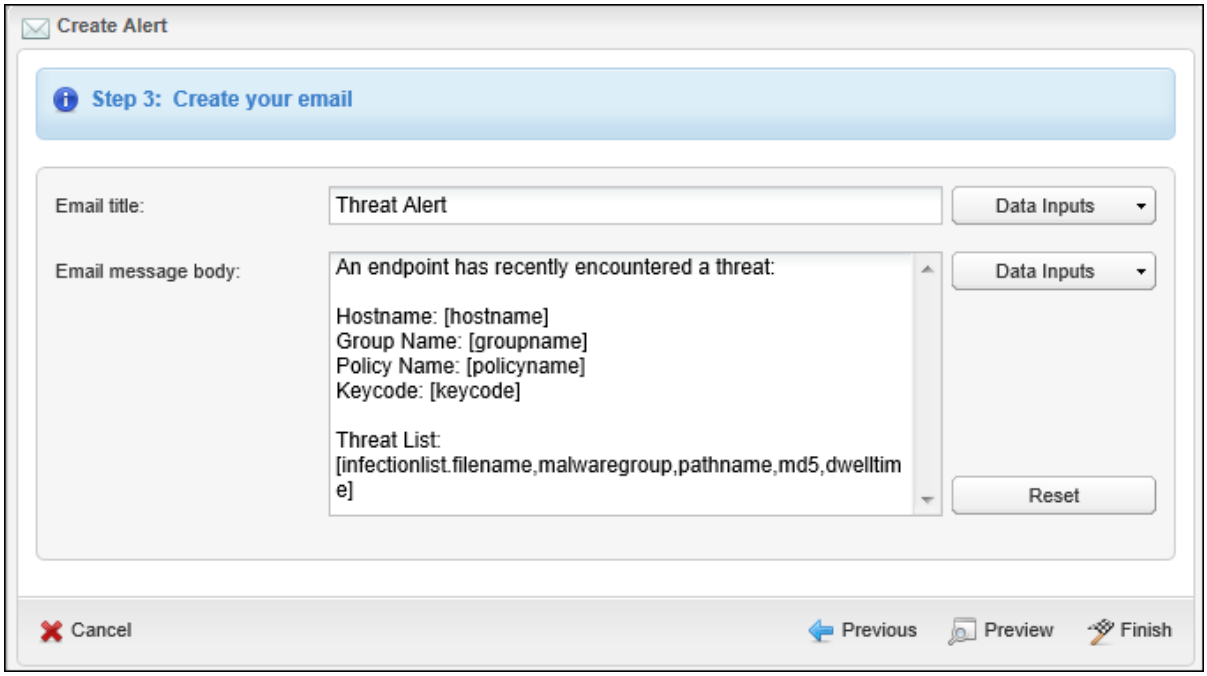


- 配信先リストをまだ作成していない場合は、[**新規リストの作成**] ラジオボタンをクリックしてリストの名前を入力し、電子メールアドレスを入力します。

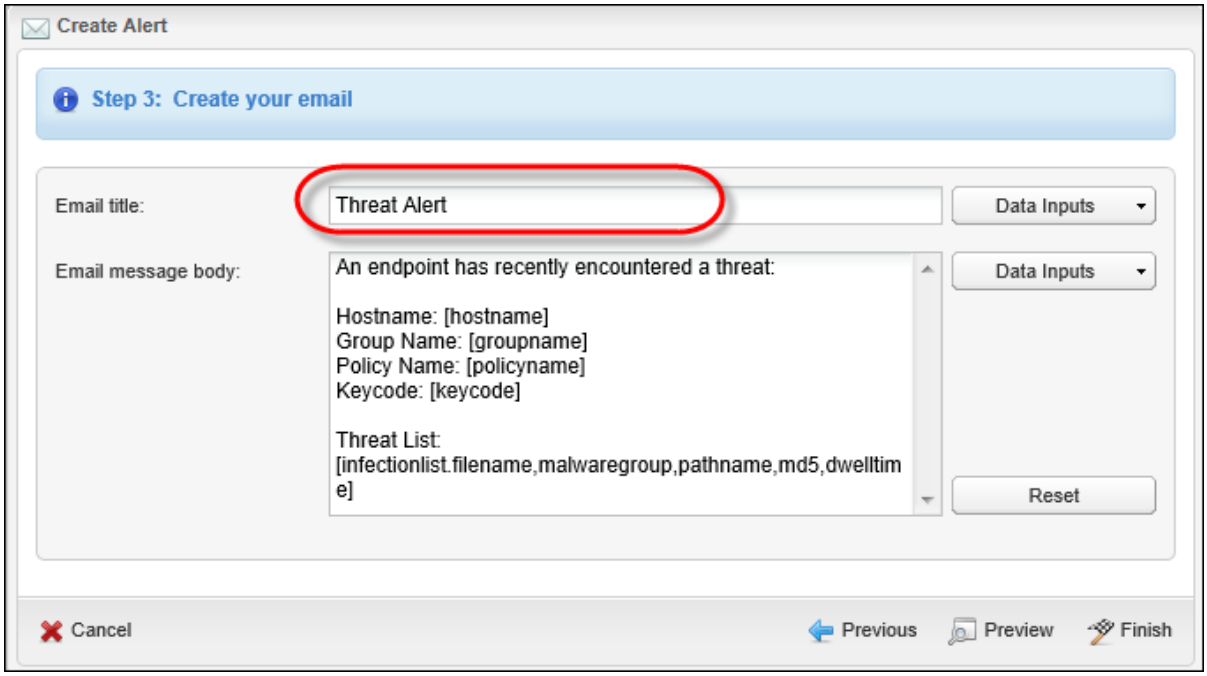


8. 終わったら [**次へ**] ボタンをクリックします。

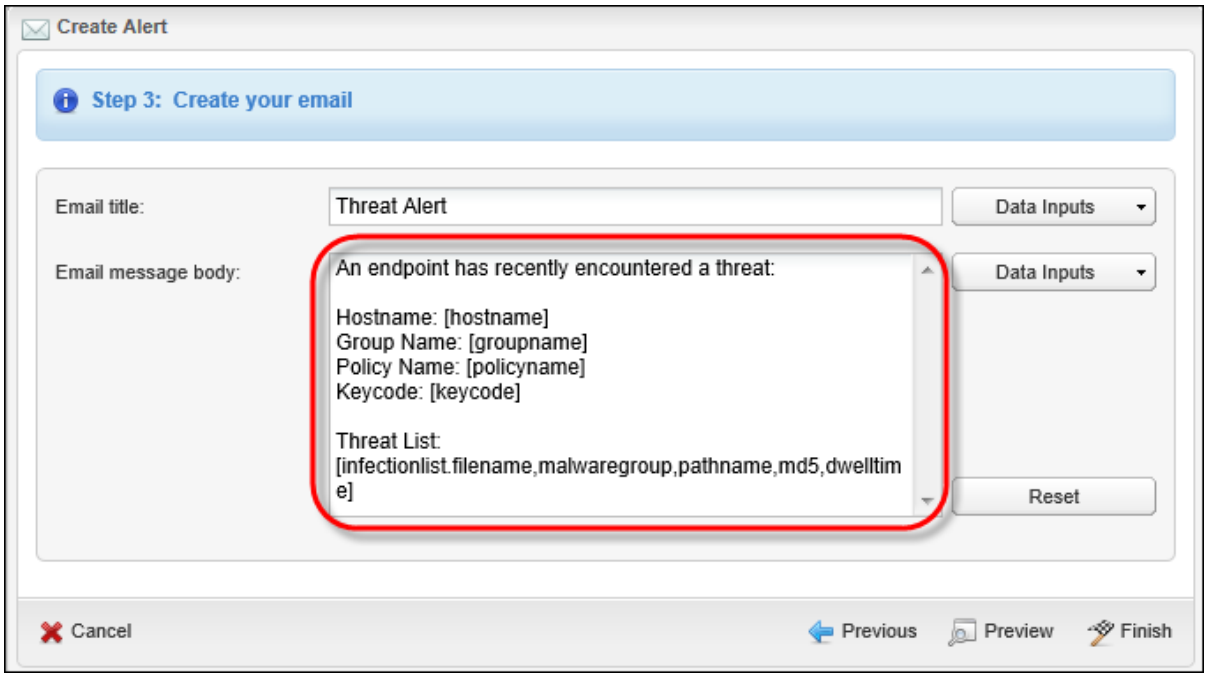
   [ステップ 3] ウィンドウが表示されます。



9. [電子メールの件名] フィールドにメッセージの件名を入力します。

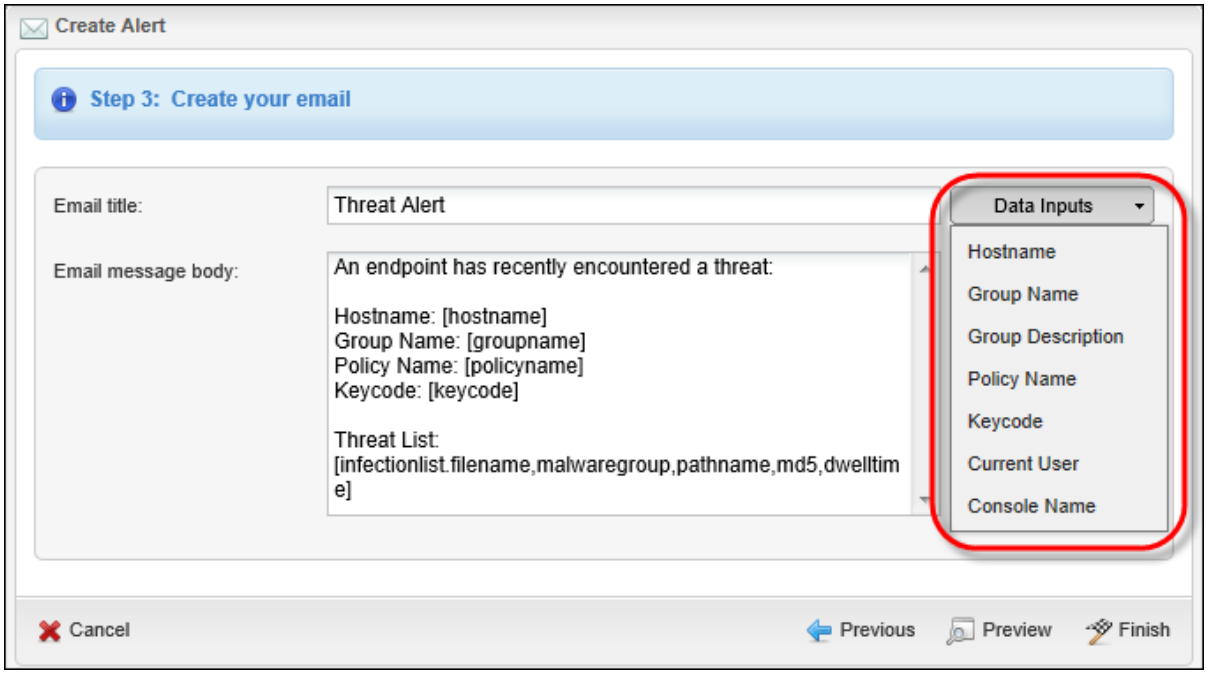


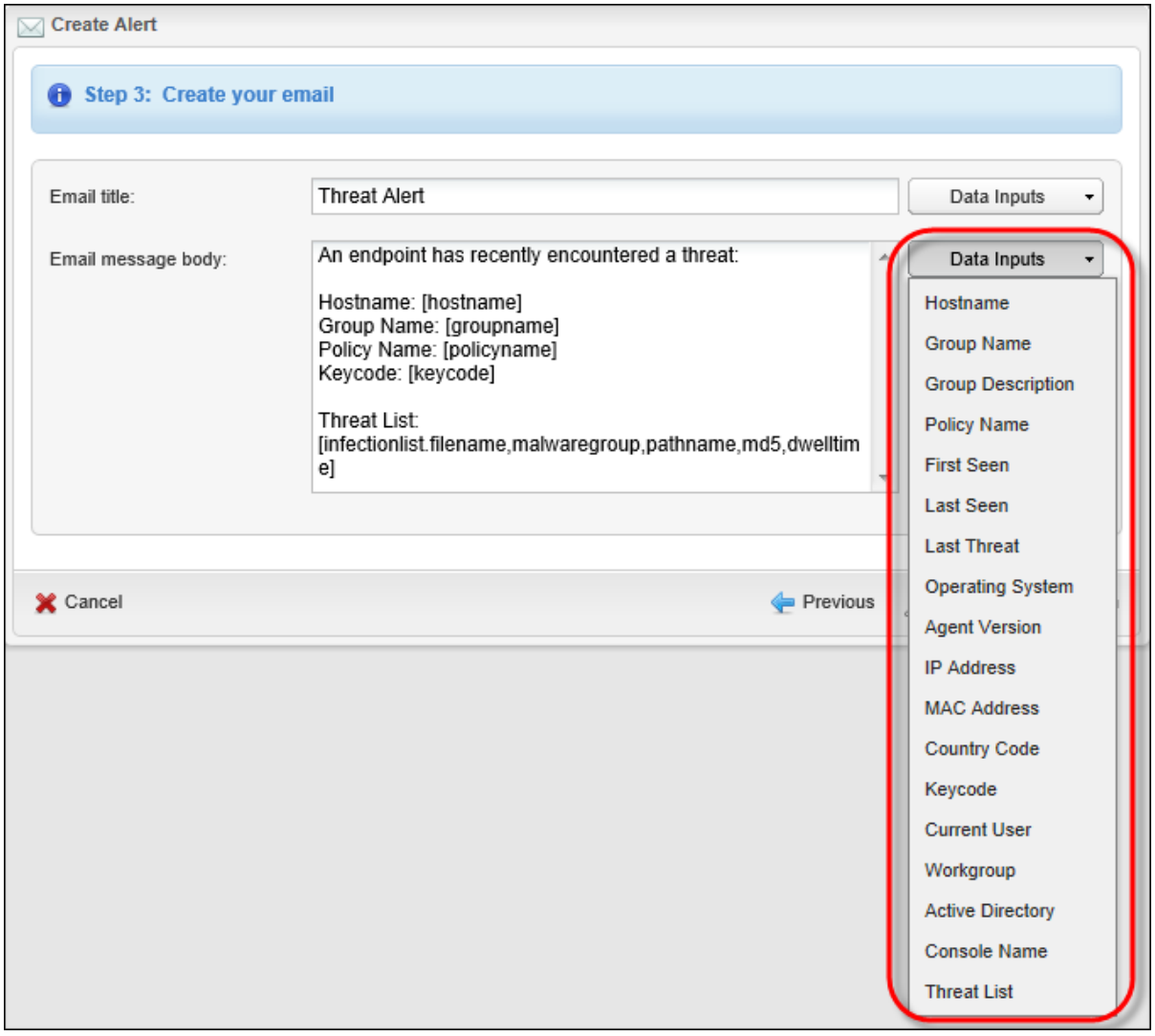
10. [電子メールメッセージの本文] フィールドにメッセージのテキストを入力します。



11. ウィザードでは、テキスト内へのデータ入力項目も表示されます。これは、エンドポイントのホスト名などの情報を自動的に挿入するための変数です。一部のデータ入力は、サンプルのテキストにすでに表示されています。データ入力は角括弧 ([ ]) で囲まれて表示されます。

    データ入力を追加するには、テキスト内で変数を表示する部分をクリックし、[データ入力] ボタンのドロップダウン矢印をクリックします。このボタンは、電子メールの件名と本文のそれぞれに 1 つずつあります。


Create Alert
Step 3: Create your email
Email title:
Threat Alert
Data Inputs
Email message body:
An endpoint has recently encountered a threat:
Hostname: [hostname]
Group Name: [groupname]
Policy Name: [policyname]
Keycode: [keycode]
Threat List:
[infectionlist.filename,malwaregroup,pathname,md5,dwelltime]
Hostname
Group Name
Group Description
Policy Name
Keycode
Current User
Console Name
Cancel
Previous
Preview
Finish



12. データ入力項目を選択します。それぞれの項目について以下の表で説明します。

注意： 定義する警告メッセージのタイプに応じて、該当するデータ入力項目のみがドロップダウンメニューに表示されます。

データ入力	説明
ホスト名	警告を発信するエンドポイントの名前。
グループ名	警告を発信するエンドポイントに割り当てられたグループ。
グループの説明	警告を発信するエンドポイントに割り当てられたグループの説明。
ポリシー名	警告を発信するエンドポイントに割り当てられたポリシー。
キーコード	警告を発信するエンドポイントで使用するキーコード。
現在のユーザー	警告を発信するエンドポイントのユーザー。
コンソール名	エンドポイントが含まれるコンソールの名前。
初回確認日時	このイベントが最初に検出された日時。
最終確認日時	このイベントが最後に検出された日時。
最近の感染	警告を発信するエンドポイントが最後に感染した日時。

データ入力	説明
OS	警告を発信するエンドポイントの OS のバージョン。
エージェントのバージョン	警告を発信するエンドポイントにインストールされている SecureAnywhere ソフトウェアのバージョン番号。
MAC アドレス	警告を発信するエンドポイントがインストールされているネットワークの Media Access Control (MAC) アドレス。
ワークグループ	エンドポイントがあるネットワークのワークグループ (該当する場合)。
Active Directory	Active Directory の名前。
感染リスト	感染の一覧。
感染の概要	感染の概要。
インストールの概要	SecureAnywhere のインストールの概要。

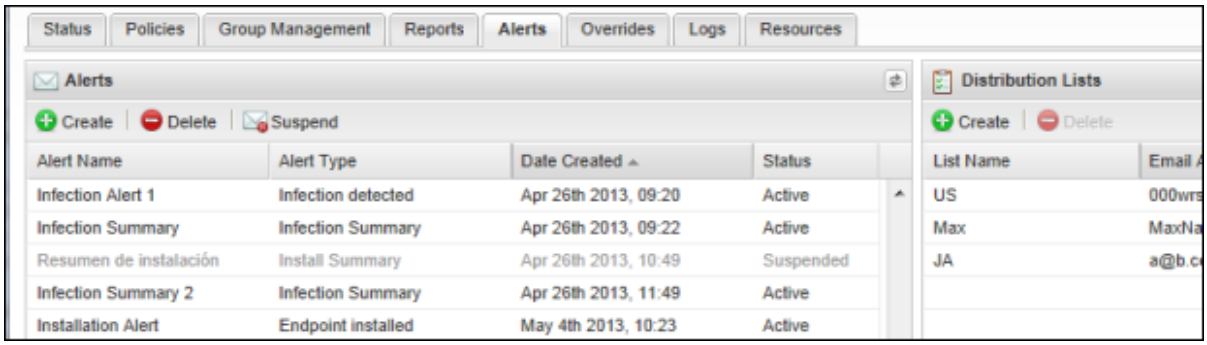
注意: ワークグループと Active Directory のデータポイントは共に、Mac エージェントでサポートされていません。

13. 電子メールメッセージを表示するには、[**プレビュー**] をクリックします。
14. メッセージの作成が完了したら、[**終了**] をクリックします。

定義済みの警告メッセージの表示

すべてのカスタムの警告は、[警告] タブに [アクティブ] の状態で表示されます。このタブで警告の行をダブルクリックすることで、その警告を編集することができます。

パネルの右側には、定義した配信先リストが表示されます。

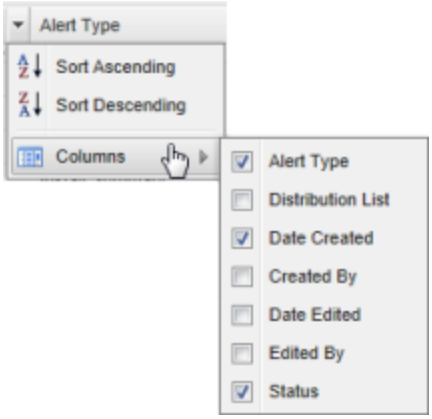


必要に応じて、警告メッセージに関する追加データの表示と非表示を切り替えることができます。

定義済みの警告メッセージを表示するには

1. カラム見出しをクリックしてドロップダウンメニューを開き、次のいずれかの操作を行います。

   - チェックボックスを選択してカラムを追加する。
   - チェックボックスの選択を解除してカラムを削除する。



カラム内の情報について、次の表で説明します。

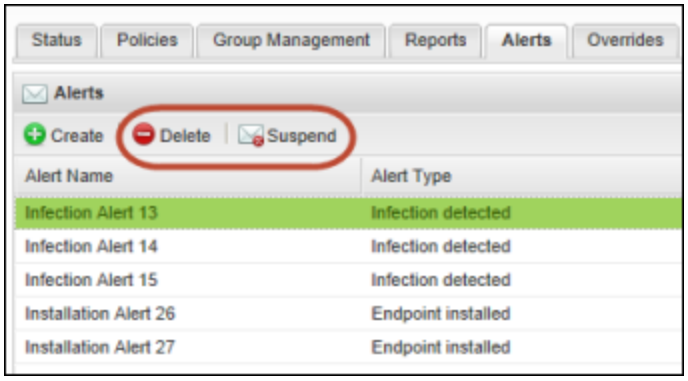
カラム	説明
警告の名前	[警告の作成] ウィザードで定義された名前。これは静的なデータで、非表示にはできません。
警告のタイプ	次のいずれかの警告タイプを表示します。 • 感染が検出されました • エンドポイントがインストールされました • 感染の概要 • インストールの概要
配信先リスト	この警告の電子メールの受信者。
作成日	警告メッセージが定義された日付。
作成者	警告メッセージを作成した管理者。
編集日	警告メッセージが変更された日付 (該当する場合)。
編集者	警告メッセージを変更した管理者 (該当する場合)。
状態	警告の状態 ([アクティブ] または [一時停止])。

警告の一時停止または削除

配信先リストの警告メッセージをカスタマイズした後に、警告が必要なくなることがあります。このような場合、警告を完全に削除することができます。将来的に再使用する可能性がある場合は、一時的に停止することも可能です。

警告を一時停止または削除するには

1. [**警告**] タブをクリックします。
2. [警告の名前] フィールドで警告を選択します。
3. コマンドメニューバーの [**削除**] または [**一時停止**] アイコンをクリックします。



- [一時停止] を選択すると、カラムの警告がグレー表示され、[状態] カラムに [一時停止] と表示されます。後で再使用する場合、警告を再度選択し、[**再開**] をクリックします。

- [削除] を選択した場合は、確認のメッセージが表示されたら [**はい**] をクリックします。警告はエンドポイントプロテクションから完全に削除されます。

第 10 章: オーバーライドの使用

オーバーライドの使用方法については、以下のトピックを参照してください。

オーバーライドの導入

オーバーライドにより、環境内のファイルとアプリケーションを管理し、ファイルが正当 (常に実行) または不正 (常に隔離) かを指定できます。例:

- 特定のビジネスの目的で使用する正当なファイルを隔離するよう設定することができます。たとえば、ユーザーに対し営業時間中の Skype 通話を許可しない場合、スキャン中に検出された Skype の実行可能ファイルを必ず隔離するようオーバーライドを設定することができます。
- 反対に、許可するファイルがエンドポイントプロテクションにより隔離されている場合は、スキャン中にそのファイルを無視するようオーバーライドを設定することが可能です。
- 1 つのオーバーライドにグローバルレベルとポリシーレベルで異なる設定を指定することができます。ポリシーの設定はグループの設定よりも優先されることに注意してください。

> **注意:** オーバーライドを完全に管理するには、[オーバーライド] の [MD5] と [オーバーライド] の [判定の範囲] のアクセス権限が必要です。権限の変更については、「*コンソールユーザーの権限設定 ページ75*」を参照してください。

ファイルの検出と管理の方法を変更するには、次のいずれかのオーバーライドを適用します。

- **正当** - エンドポイントでのファイルの実行を常に許可します。スキャン中にこのファイルを検出せず、隔離も行いません。
- **不正** - スキャン中に検出された場合、常にファイルを隔離します。

以下の複数の場所から、オーバーライドを追加できます。

- **[オーバーライド] タブ** - 任意の種類のファイルに対して [正当] または [不正] のオーバーライドを作成できます。このためには、まずエンドポイントをスキャンしてスキャンログを保存し、ファイルの MD5 値を特定する必要があります。MD5 (メッセージダイジェストアルゴリズム 5) とは、128 ビット値を生成し、指紋のように動作してファイルを一意に識別する暗号学的ハッシュ関数です。

  詳細については、「*[オーバーライド] タブからのオーバーライドの適用 ページ439*」を参照してください。

- **[グループの管理] タブ** - 脅威が検出されたエンドポイントを検索し、オーバーライドをすばやく適用することができます。ファイルの MD5 値はすでに特定されています。

  詳細については、「*グループからのファイルへのオーバーライドの適用 ページ446*」を参照してください。

- **[レポート] タブ** - 特定のレポートで脅威が検出されたエンドポイントを検索し、オーバーライドをすばやく適用することができます。ファイルの MD5 値はすでに特定されています。

詳細については、「レポートからのファイルへのオーバーライドの適用 ページ454」を参照してください。

- **滞留時間のポップアップ** - このポップアップ内で MD5 のオーバーライドを作成することができます。

  詳細については、「滞留時間のポップアップからのオーバーライドの適用 ページ459」を参照してください。

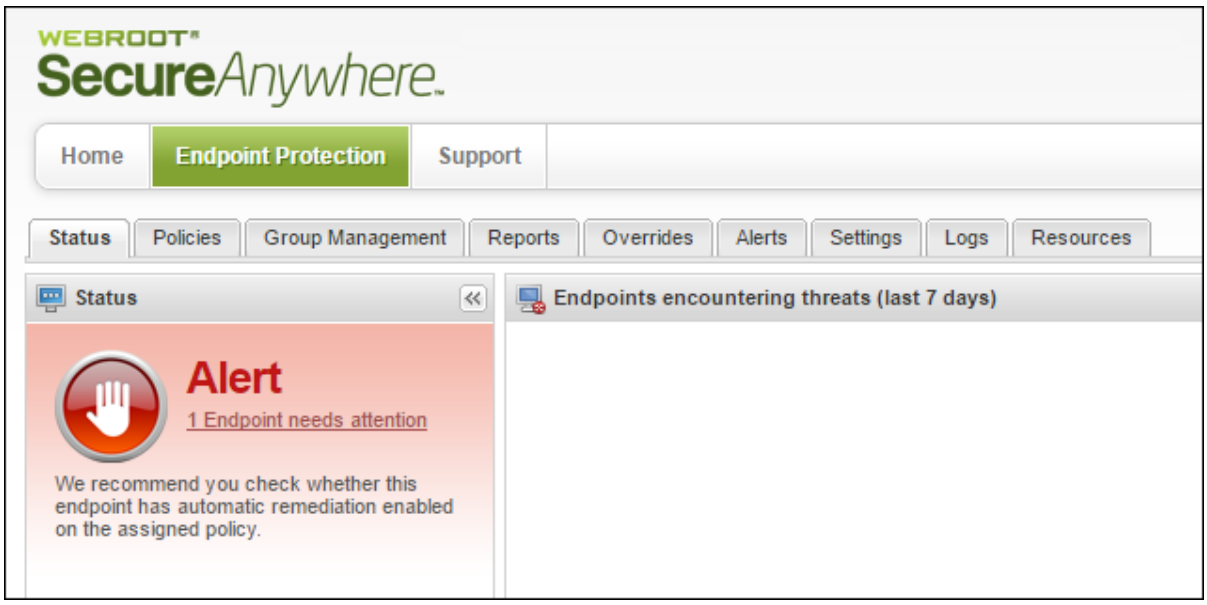
ブラックリストのオーバーライドの作成

エンドポイントプロテクションのコンソールの [オーバーライド] パネルで、ブラックリストのオーバーライドを作成することができます。

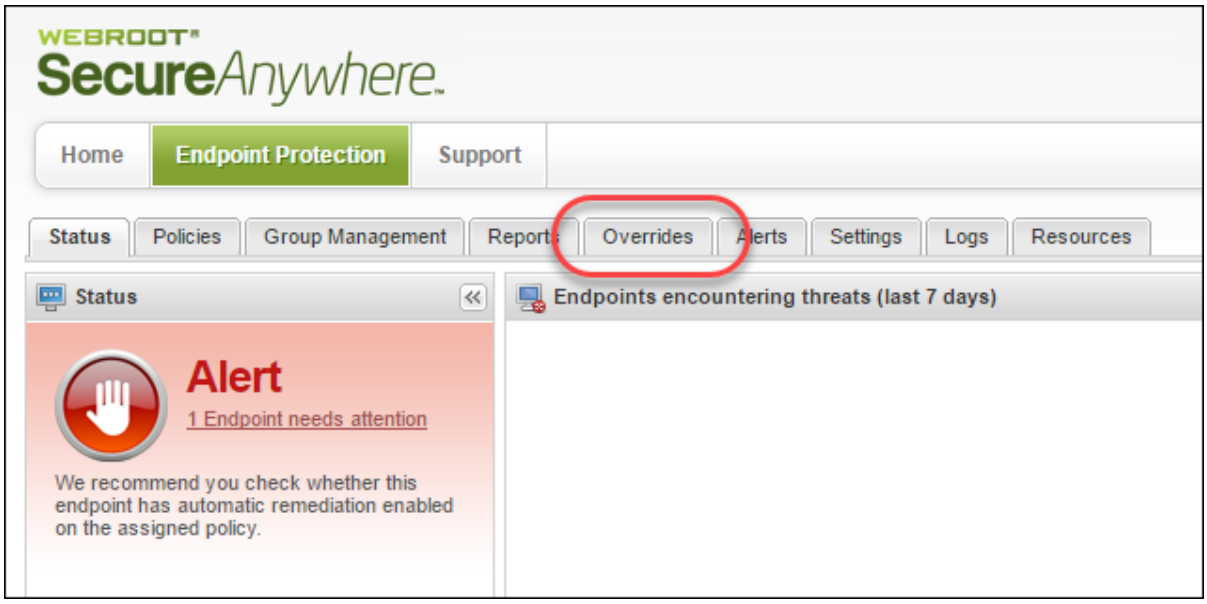
ブラックリストのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

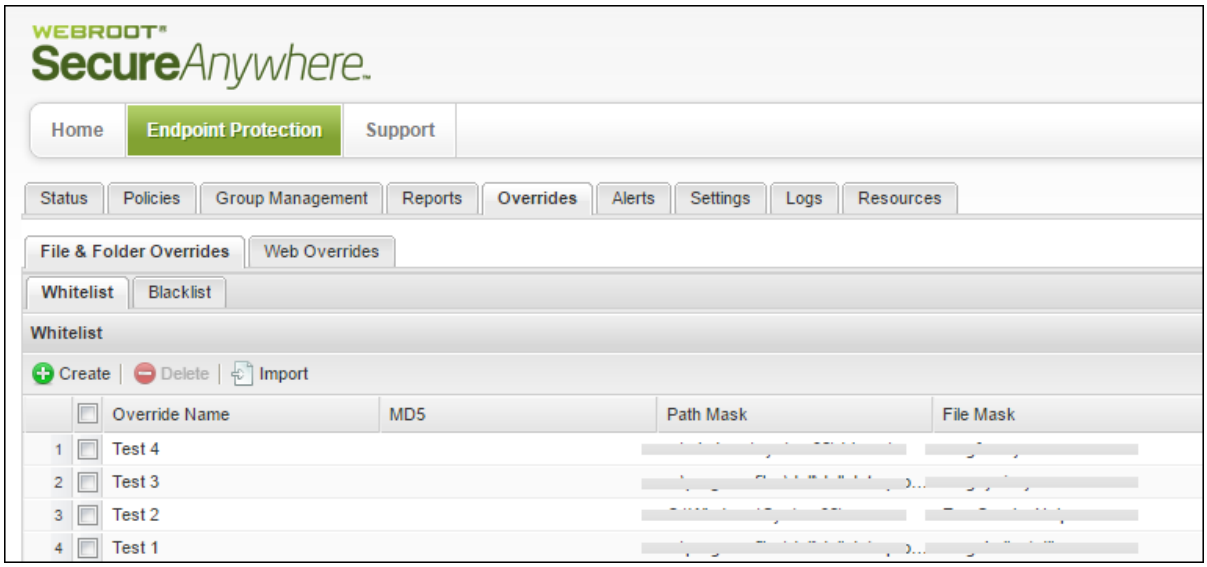
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



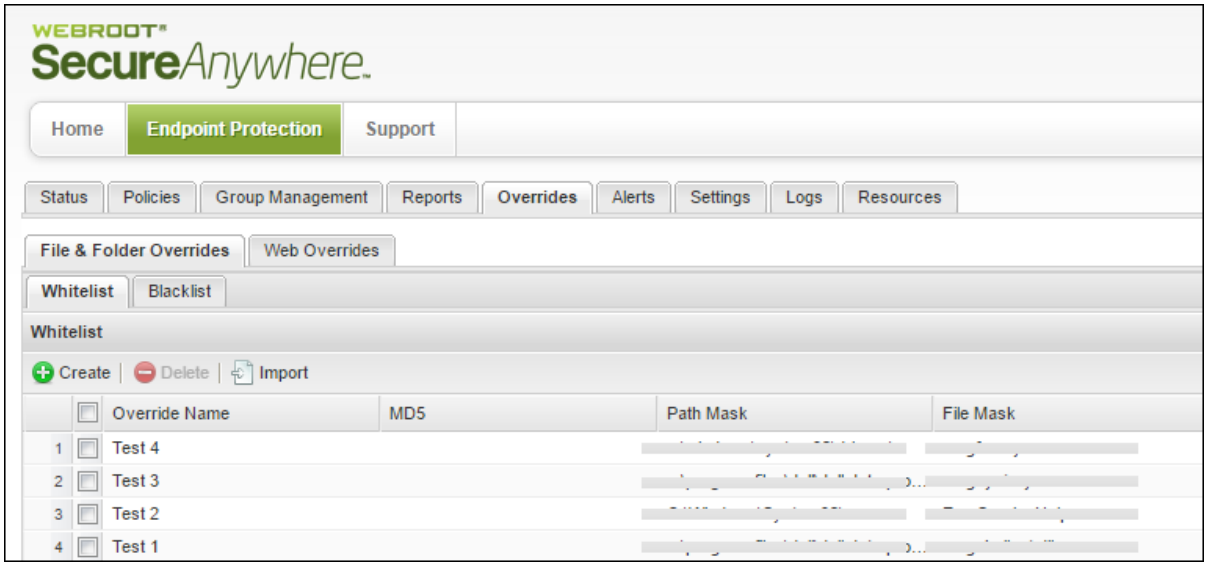
2. [**オーバーライド**] タブをクリックします。



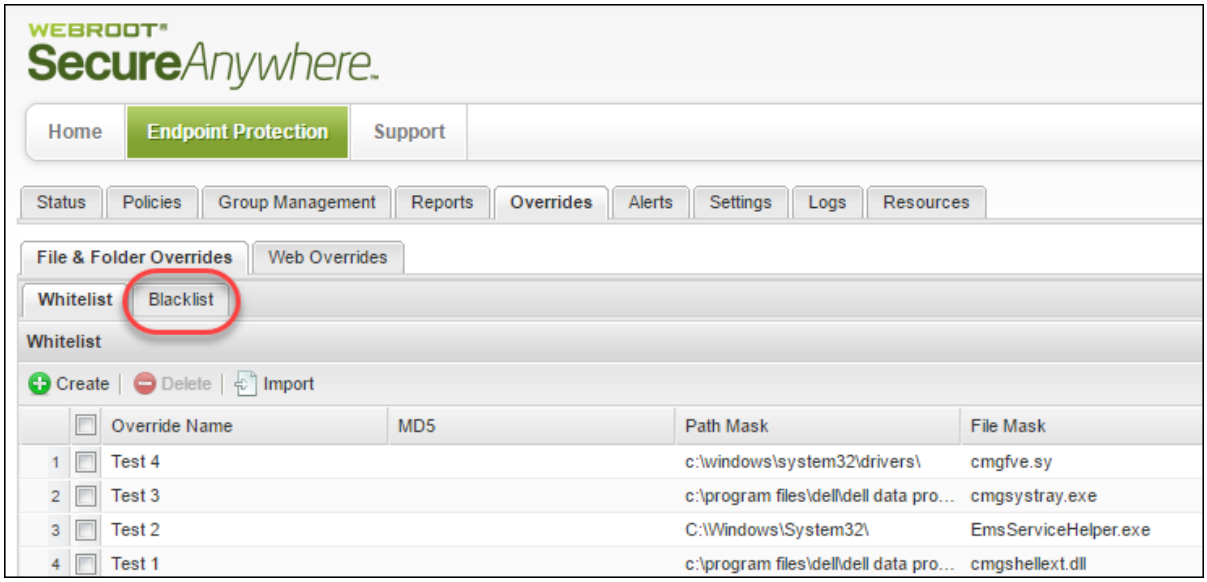
[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。



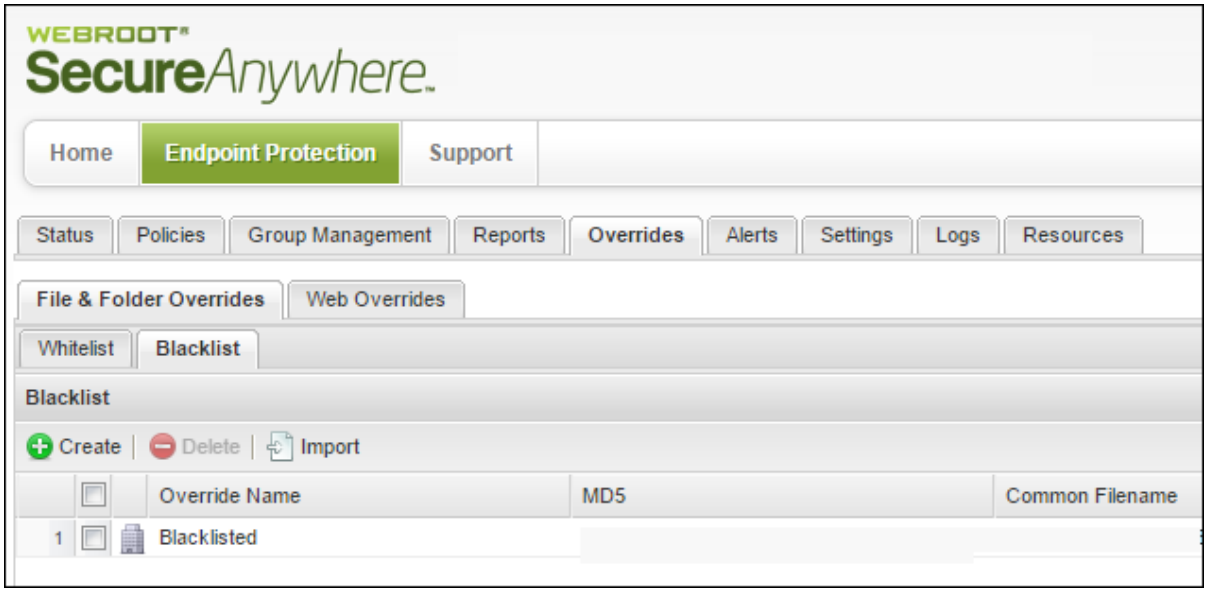
[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。



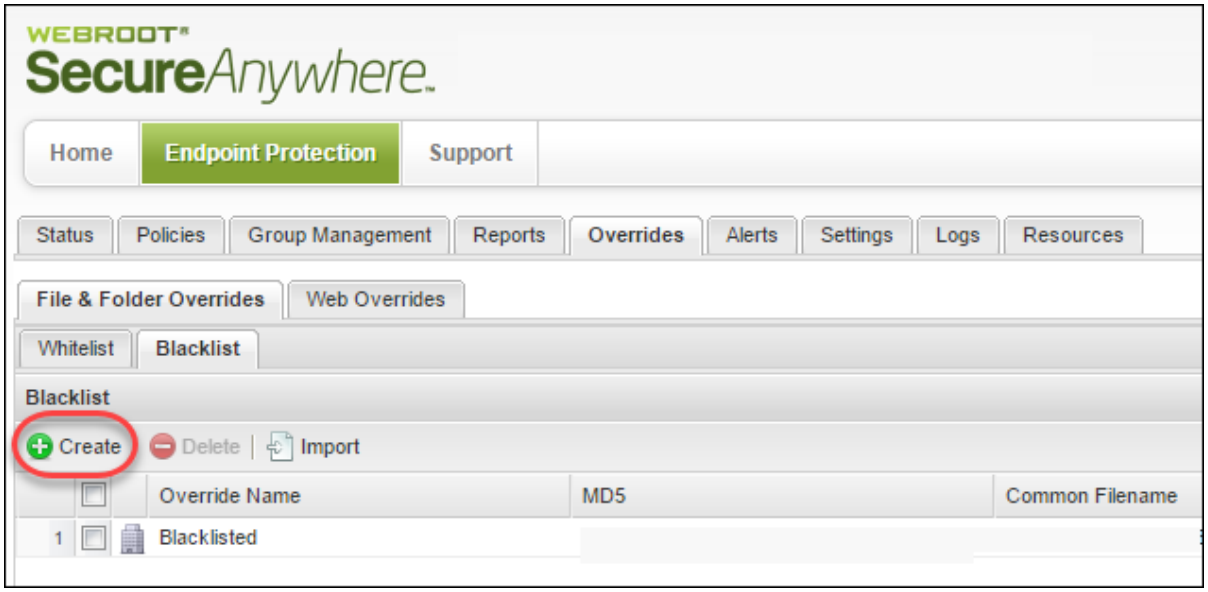
3. [**ブラックリスト**] タブをクリックします。



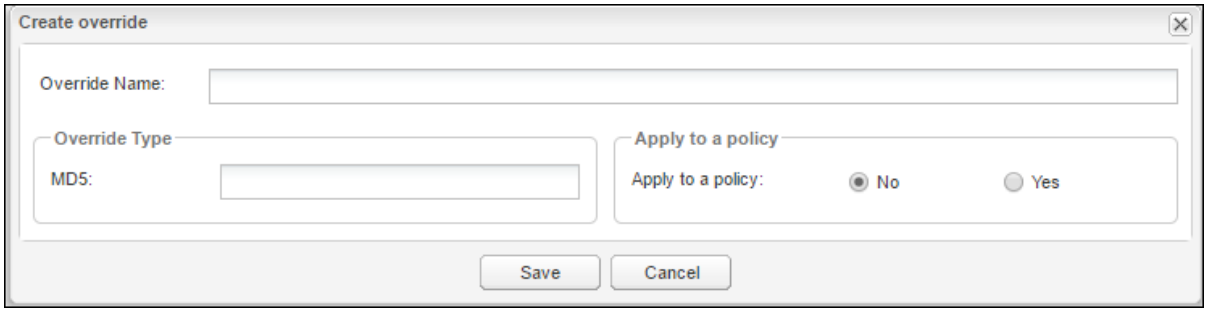
[ブラックリスト] タブが表示されます。



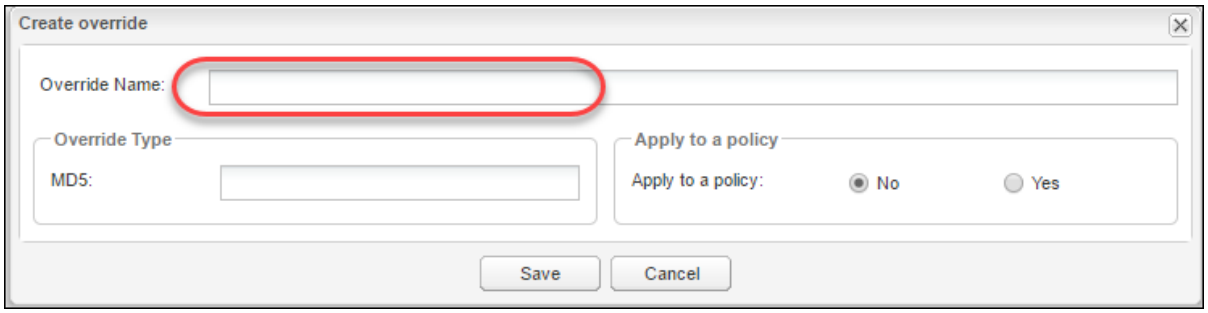
4. [**作成**] ボタンをクリックします。



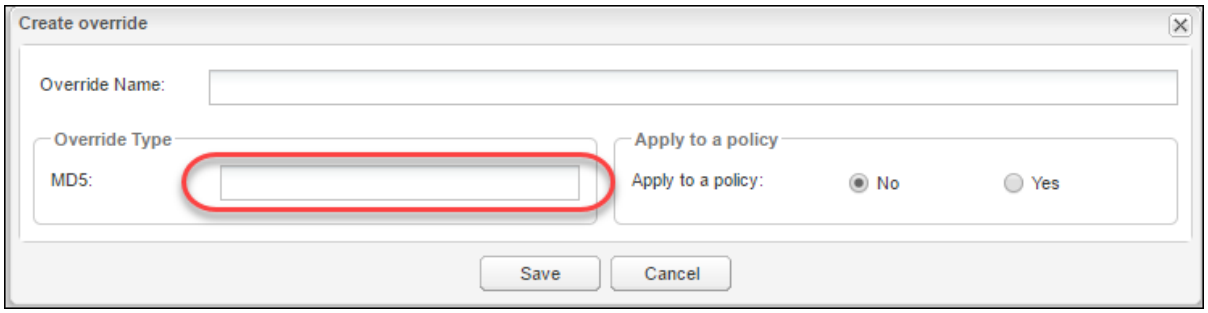
[オーバーライドの作成] ウィンドウが表示されます。



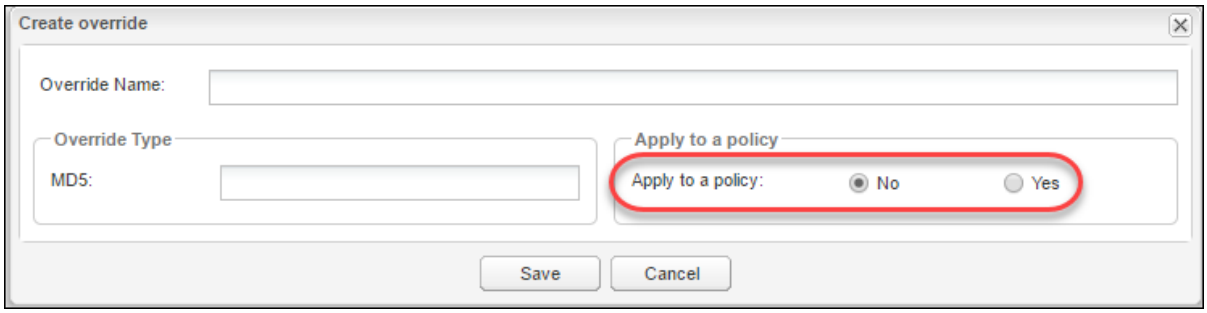
5. [オーバーライド名] フィールドにオーバーライドの名前を入力します。



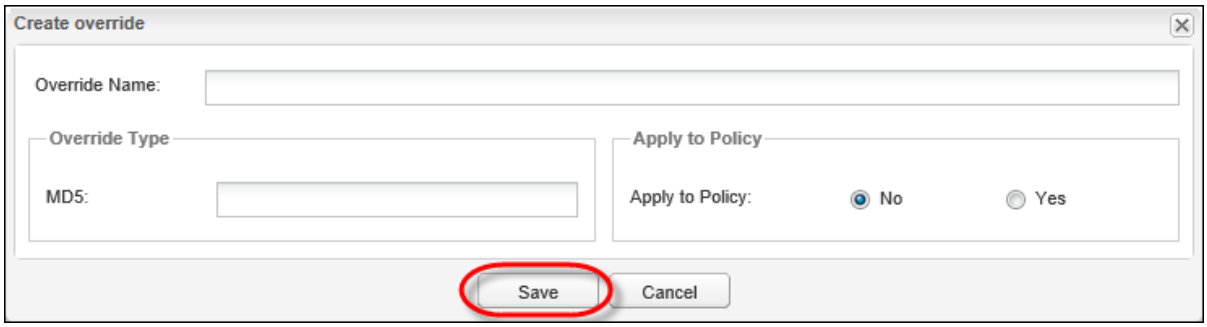
6. [MD5] フィールドに、32 文字の英数字から成るファイルの一意の識別子を入力します。



7. [**いいえ**] または [**はい**] の [1 つのポリシーに適用] ラジオボタンを選択します。



8. 設定が完了したら [**保存**] ボタンをクリックします。



ホワイトリストのオーバーライドの作成

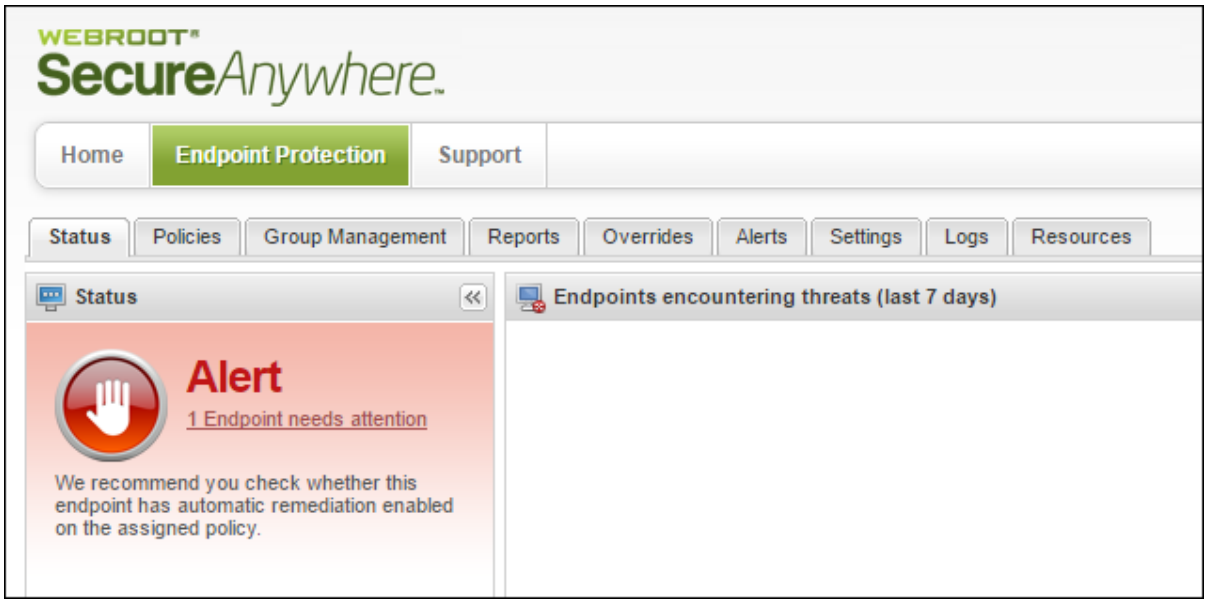
グローバル規模のホワイトリストのオーバーライドを、これまでのエンドポイントプロテクションの MD5 (メッセージダイジェストアルゴリズム 5) レベルだけでなく、ファイルやフォルダのレベルでも設定できるようになりました。このアップグレードによって、より柔軟にオーバーライドを配備できるようになりました。たとえば、複数の関連する MD5オーバーライドを個別にホワイトリスト化せずに、関連ディレクトリ全体を一括でホワイトリスト化することができます。

注意: 除外やオーバーライドを設定する前にファイルを検出または削除した場合は、アンインストールしてから再インストールするか、検出したファイルを隔離から復元しておく必要があります。ファイルがローカルで隔離されたままの状態、または [ブロック / 許可] タブ内にある状態では除外は適用されません。

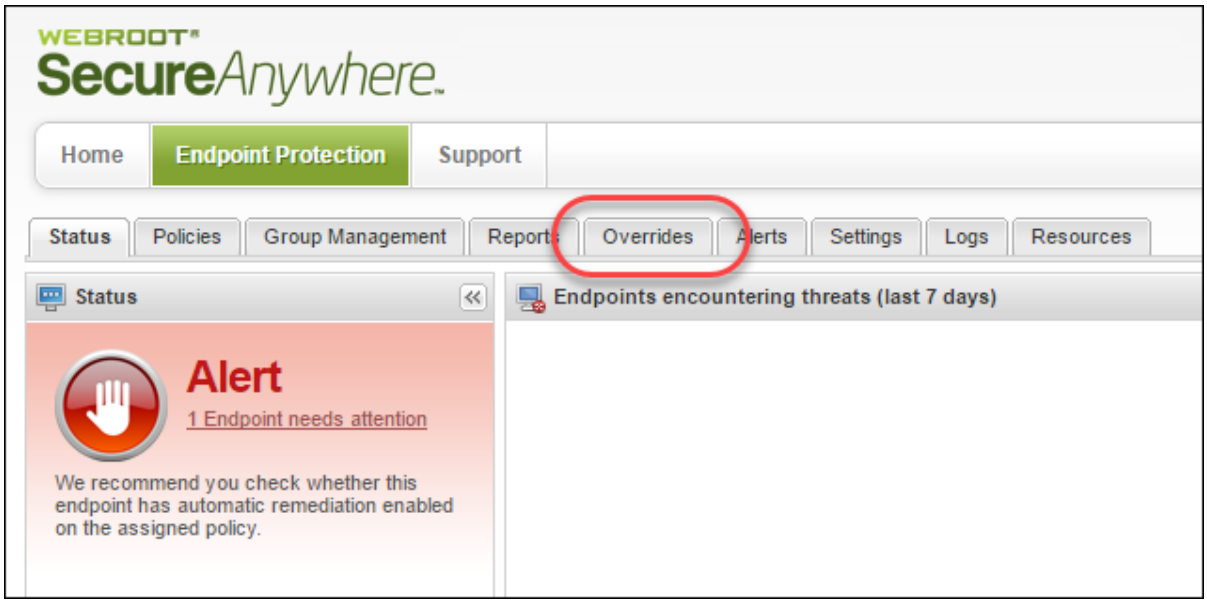
ホワイトリストのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

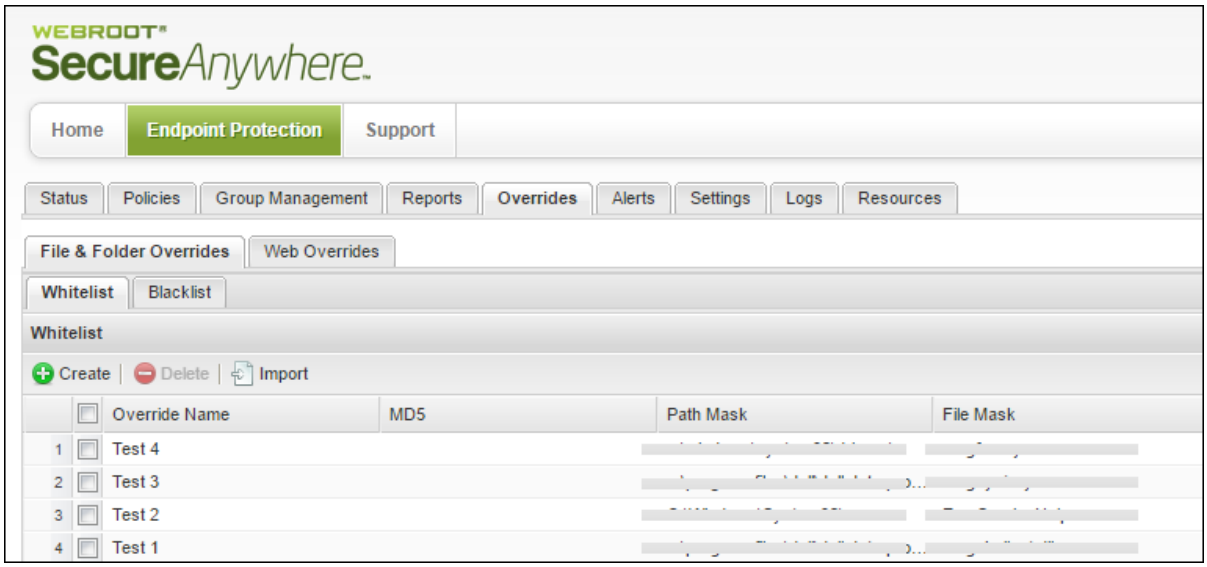
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



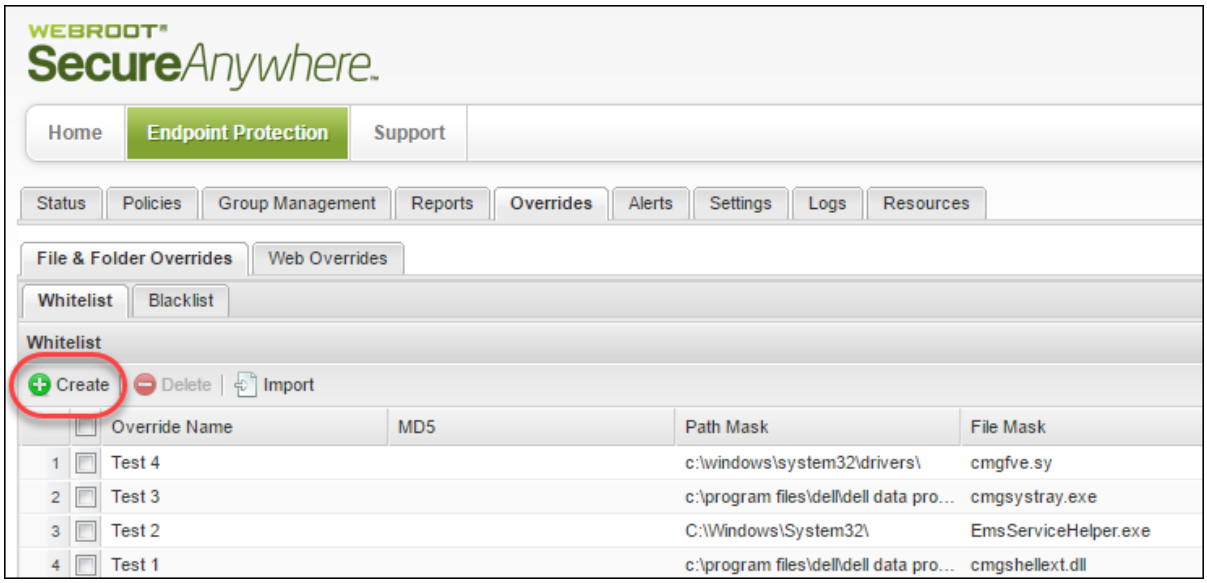
2. [**オーバーライド**] タブをクリックします。



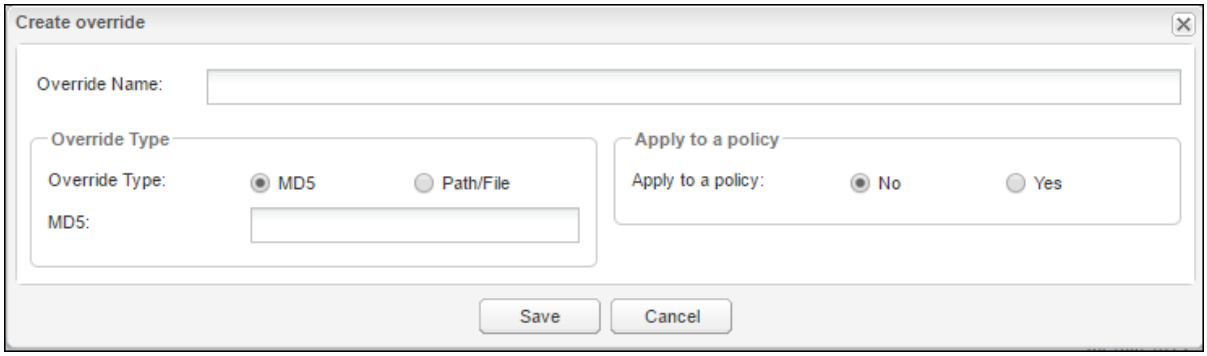
3. [ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。



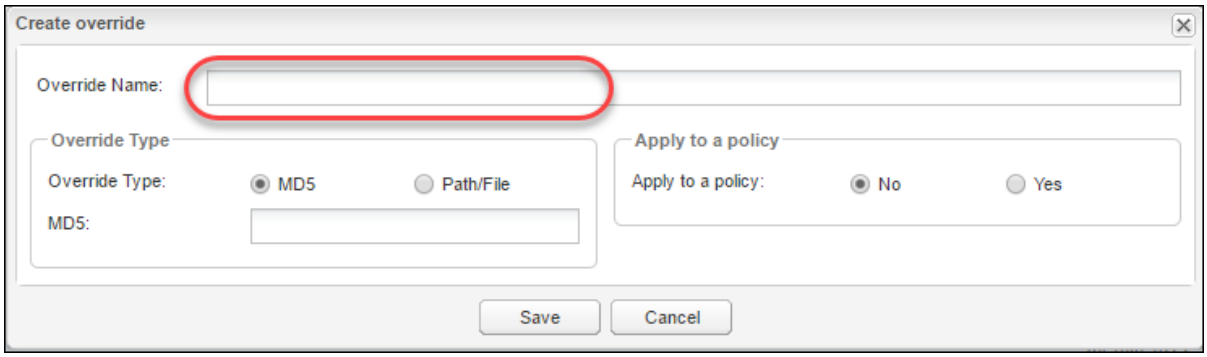
4. [**作成**] ボタンをクリックします。



[オーバーライドの作成] ウィンドウが表示されます。



5. [オーバーライド名] フィールドにオーバーライドの名前を入力します。



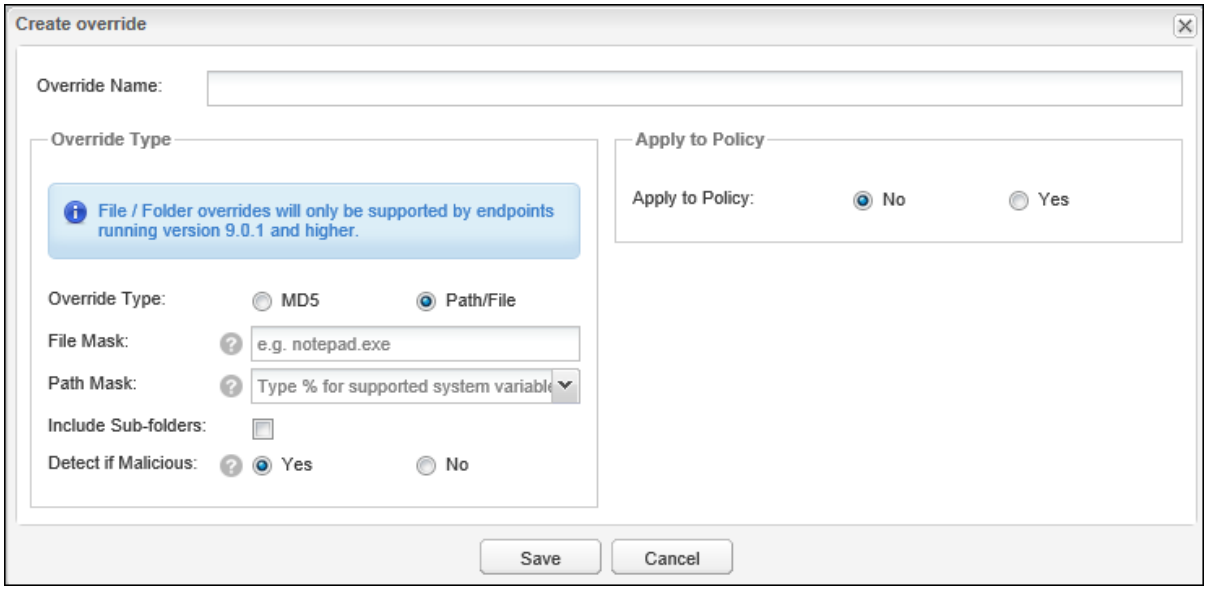
6. 以下のいずれかの操作を行います。

- 設定が完了したら [**保存**] ボタンをクリックします。
- フォルダ / ファイルのオーバーライドを作成するには、この手順を続行します。

> **注意:** ファイル / フォルダのオーバーライドを使用するには、エンドポイントが Webroot SecureAnywhere Endpoint Protection のバージョン 9.0.1 以降を使用していることを確認してください。それより前のバージョンでは MD5 のオーバーライドにしか対応していません。

7. [新規ホワイトリストエントリ] ウィンドウで、[**パス/ファイル**] ラジオボタンを選択します。

[オーバーライドの作成] ウィンドウに、関連するフィールドが表示されます。



8. 次の表を参照して各フィールドに情報を入力します。

フィールド	説明
オーバーライド名	オーバーライドの名前を入力します。
オーバーライドの種類	[パス/ファイル] ラジオボタンをすでに選択しています。
ファイルマスク	オプションのワイルドカードでファイルマスクを指定し、ファイルやファイルのグループを絞り込みます (例: 選択したフォルダ内のすべての実行可能ファイルを対象とする場合は *.exe)。指定がない場合はデフォルトとして、選択したフォルダ / パス内のすべてのファイルが対象になります。

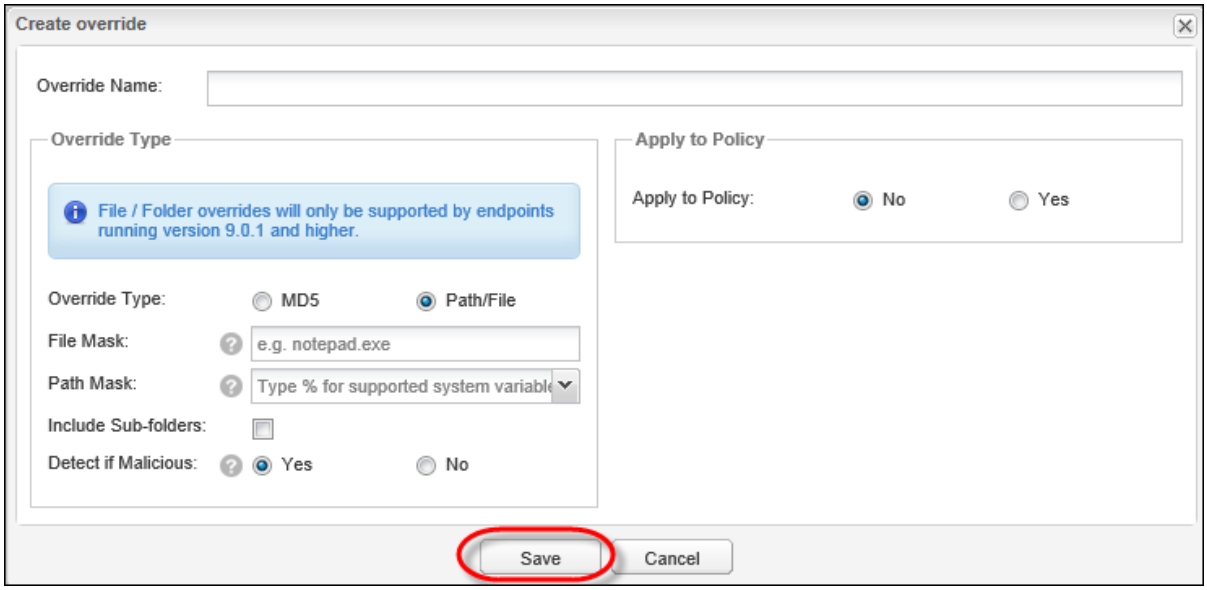
フィールド	説明

パス / フォルダマスク	オーバーライドの対象となるフォルダです。次のような絶対パスを指定することができます。
	
	`x:\myfolder\`
	
	または、次のようにシステム変数と任意のパスを指定できます。
	
	`%SystemDrive%\myfolder.`
	
	デフォルトでサポートされている環境変数は "%" (パーセント記号) を入力すると表示されます。対象のコンピュータ上で設定済みの変数もすべて使用できます。ただし、サポートされていないユーザー変数を除きます。たとえば、"%temp%" は特定のユーザーー時ディレクトリ (‘username/temp/’) であるため使用できません。ワイルドカードはサポートされていません。

サブフォルダを含める	対象フォルダ内のすべてのサブフォルダにオーバーライドを適用する場合に、このチェックボックスを選択します。
悪意のある場合は検出	この設定が有効になっている場合、ウェブルートは引き続き、指定のファイル / フォルダのホワイトリストのオーバーライドにより発生する脅威からユーザーを保護しますが、監視およびジャーナルは無効になります。この機能は主に、大量の未判定のファイルに監視とジャーナルを適用する際、パフォーマンスを向上するために使用します。この設定を無効にすると完全なホワイトリスト作成が可能になり、ウェブルートの保護なしでファイルを実行することができます。

フィールド	説明
グローバル (GSM) オーバーライド	これを選択すると、現在の GSM コンソールにあるすべてのサイトについてオーバーライドがグローバルに設定されます。
ポリシーに適用	以下のいずれかの操作を行います。 • グローバルポリシーを含む特定のポリシーにオーバーライドを適用する場合は [**はい**] を選択します。 • 選択したサイトにすべてのポリシーに適用する場合は [**いいえ**] を選択します。

9. 設定が完了したら [**保存**] ボタンをクリックします。



[オーバーライド] タブからのオーバーライドの適用

[オーバーライド] タブからオーバーライドを適用する際は、まずエンドポイントでスキャンを実行し、ファイルの MD5 値を特定する必要があります。SecureAnywhere がデバイスをスキャンすると、実行可能ファイルやプロセスを実行する他のタイプのファイルのパス名、ファイル名、MD5 値を保存したスキャンログが作成されます。オーバーライドを作成するには、その MD5 値が必要になります。

[*不正*] と指定されたファイルをオーバーライドする場合は、[グループ] タブまたは [レポート] タブを使用します。これらのタブには検出された脅威と関連する MD5 値が表示されるため、[不正] オーバーライドの作成の手間が省けます。

この手順には 2 つの段階があります。

- MD5 値の特定と保存
- MD5 値の追加

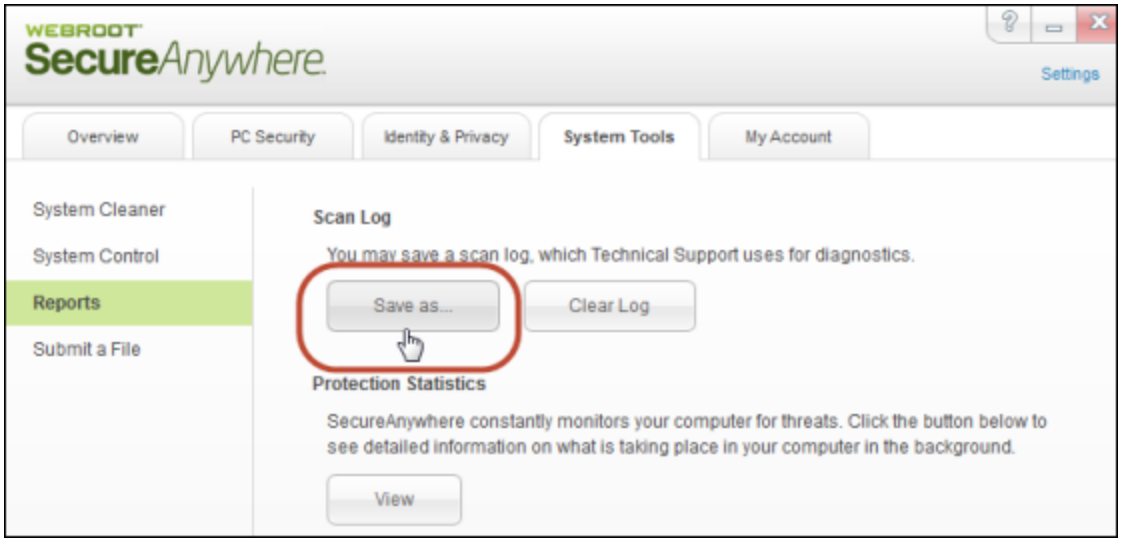
注意: この手順は Windows コンピュータでしか実行できません。

MD5 値を特定して保存するには

1. エンドポイントでスキャンを実行して MD5 値を取得します。

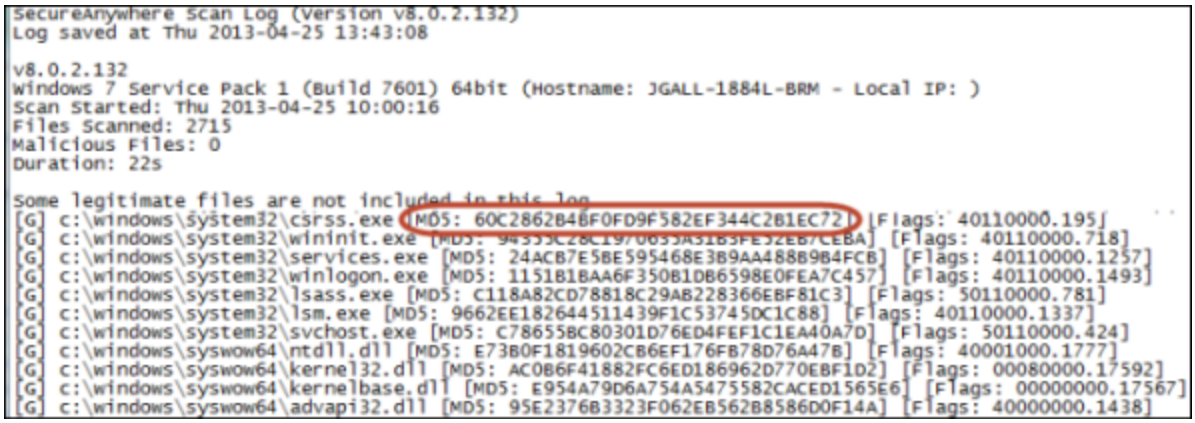
   [スキャン] コマンドを実行する場合は、エンドポイントそのものから実行するか、[グループ] タブの [スキャン] コマンドを使用します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

2. PC やその他のデバイスなどのエンドポイントで SecureAnywhere を開きます。
3. [**システムツール**] タブをクリックします。
4. 左側のペインで [**レポート**] を選択します。
5. 開かれたページの [スキャンログ] セクションで、**[名前を付けて保存]**ボタンをクリックし、ログのファイル名と場所を指定します。



6. スキャンログを開くと、ファイル名の右側に MD5 値が記載されています。

   以下に、"csrss.exe" という名前のファイルの MD5 値の例を示します。

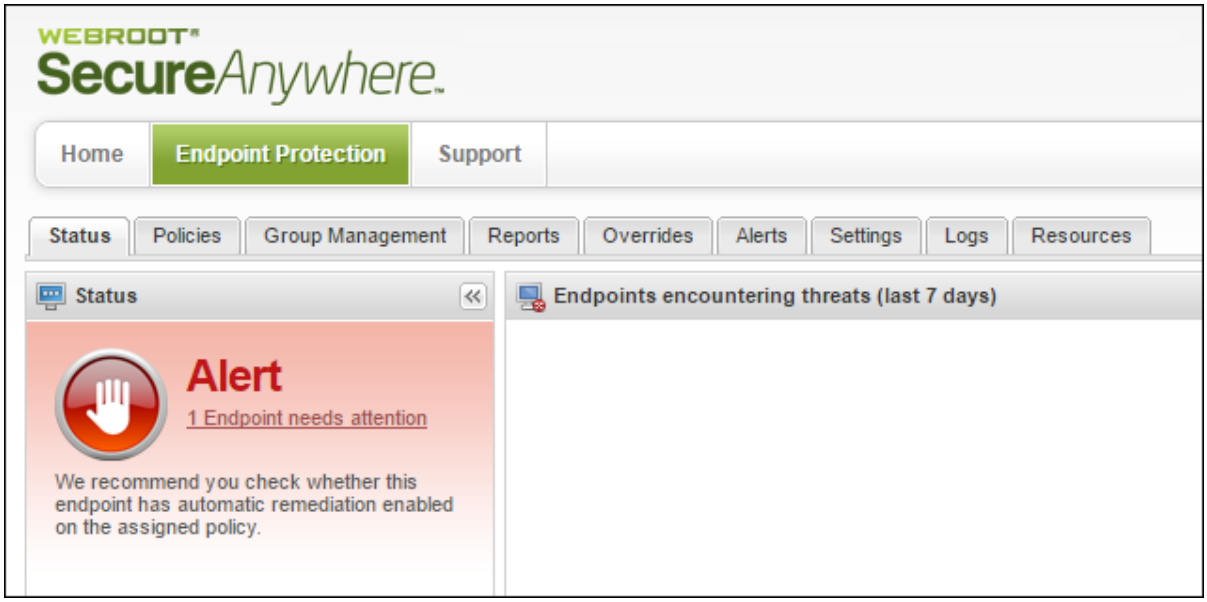


7. 値をコピーして管理ポータルに貼り付けます。

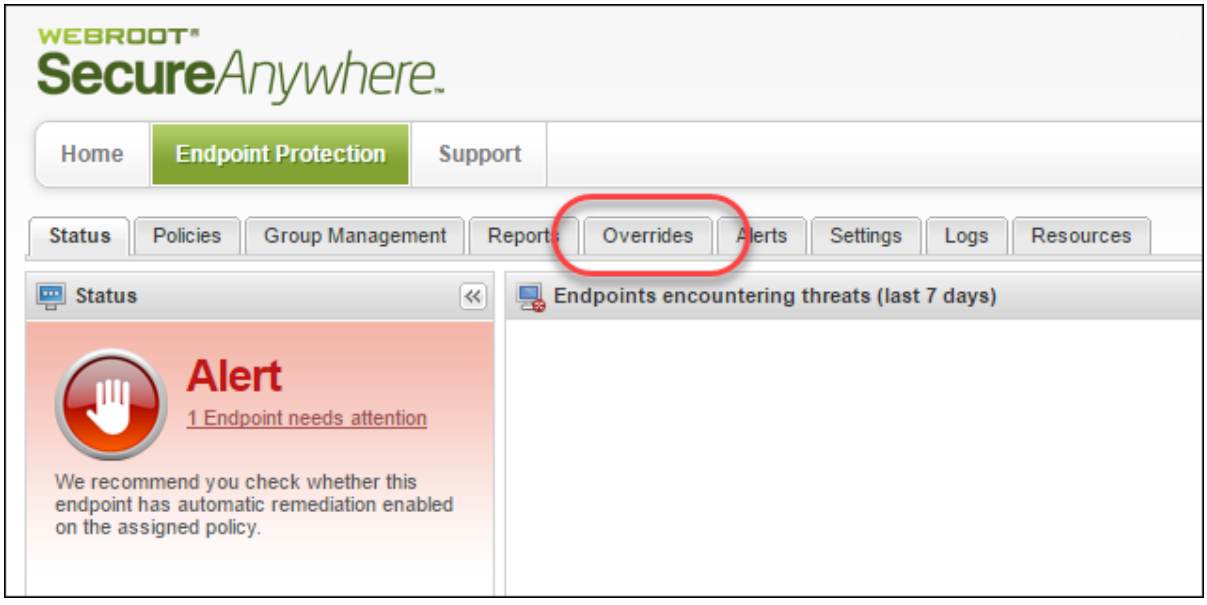
[オーバーライド] タブから MD5 オーバーライドを追加するには

1. エンドポイントプロテクションのコンソールにログインします。

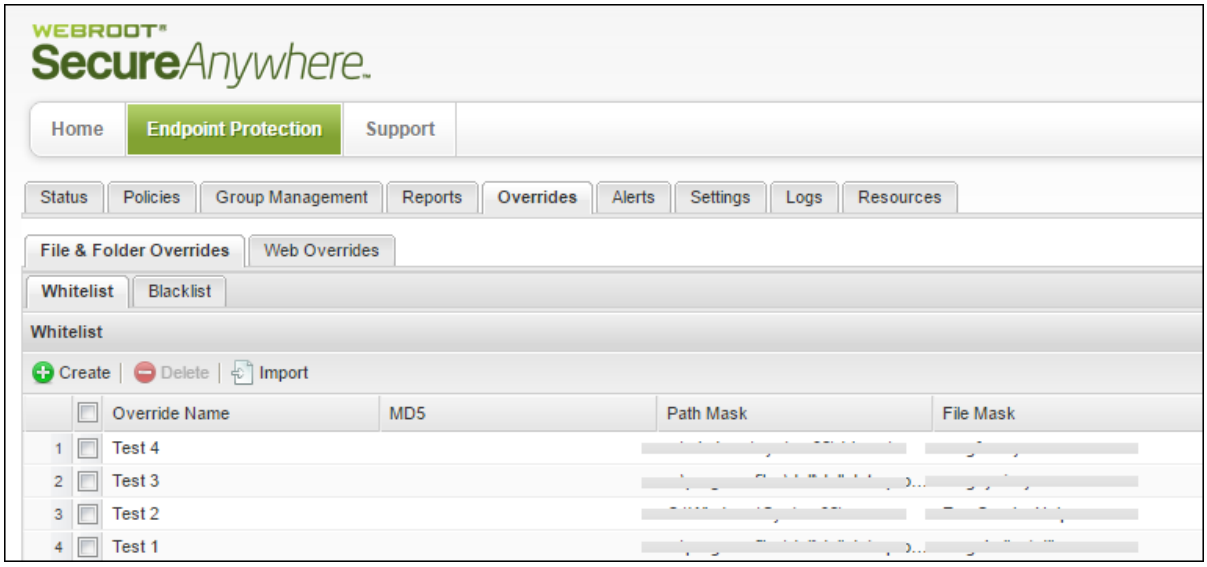
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



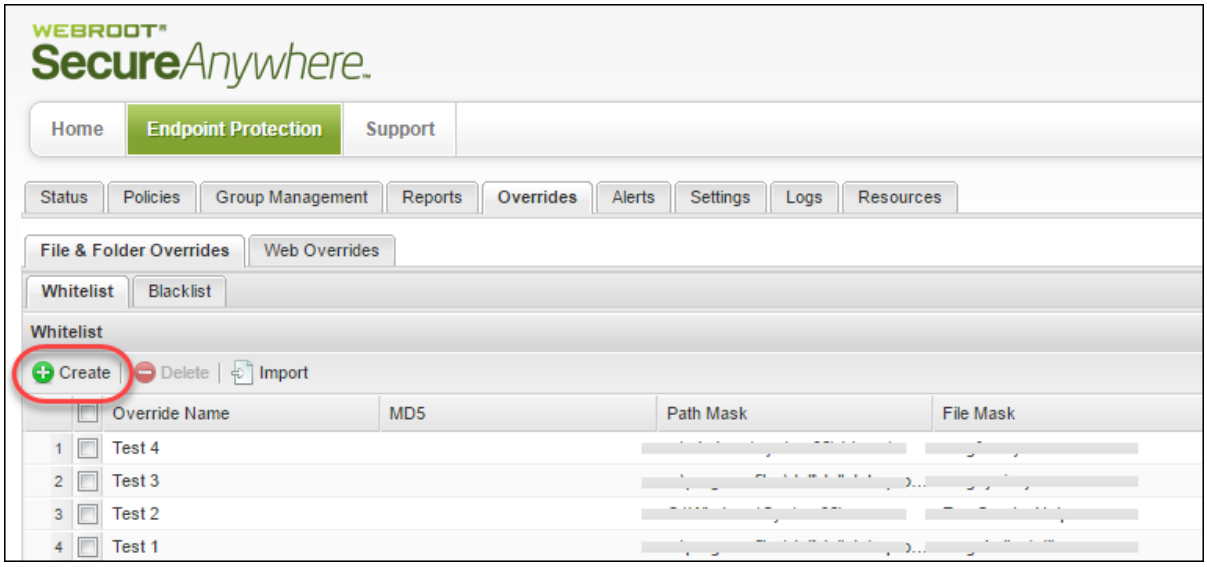
2. [**オーバーライド**] タブをクリックします。



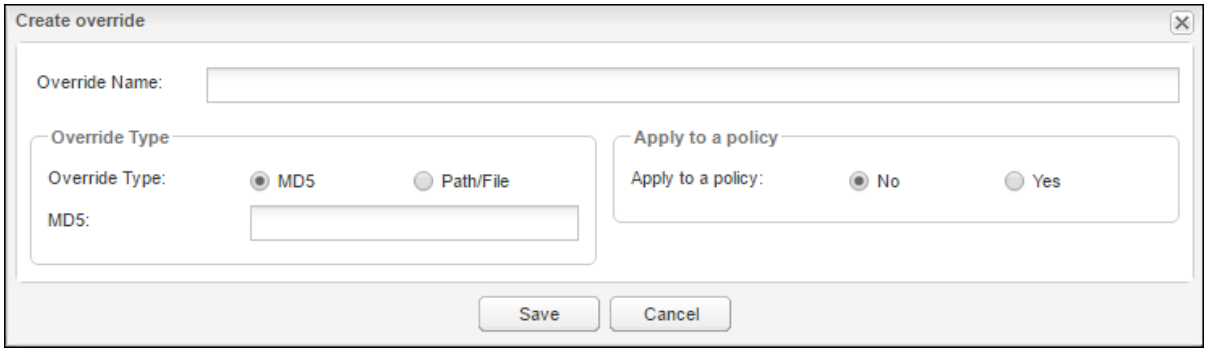
[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。



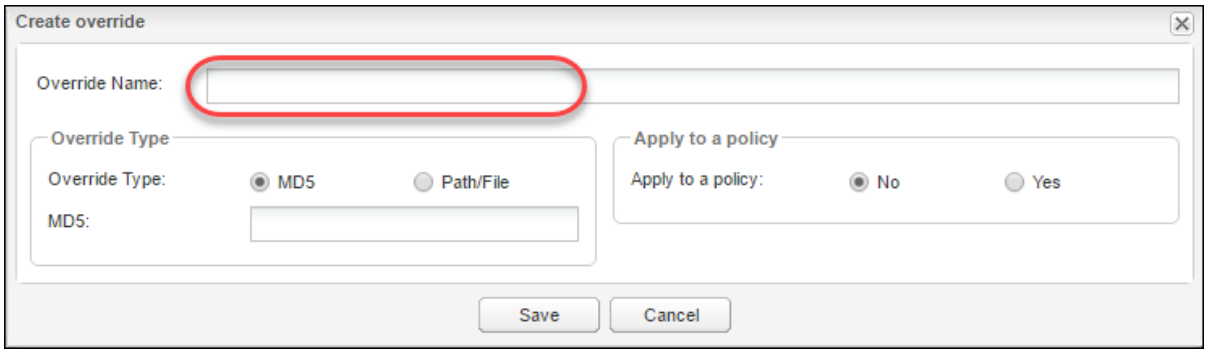
3. [**作成**] アイコンをクリックします。



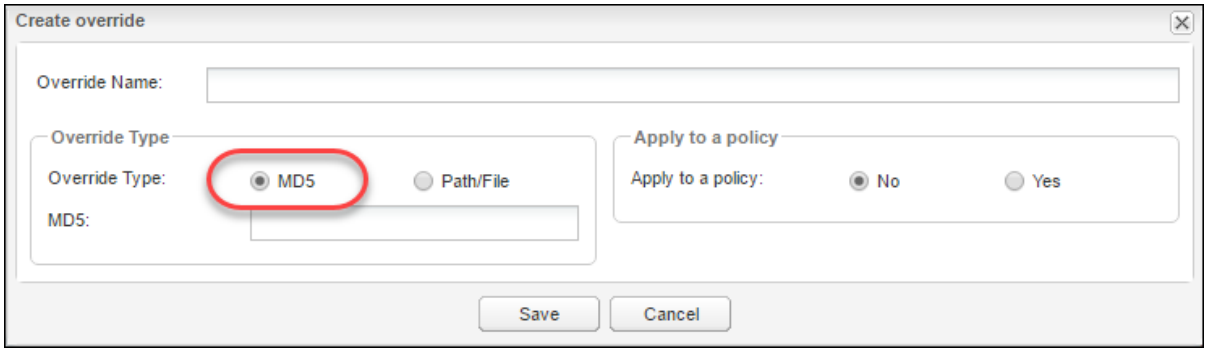
[オーバーライドの作成] ウィンドウが表示されます。



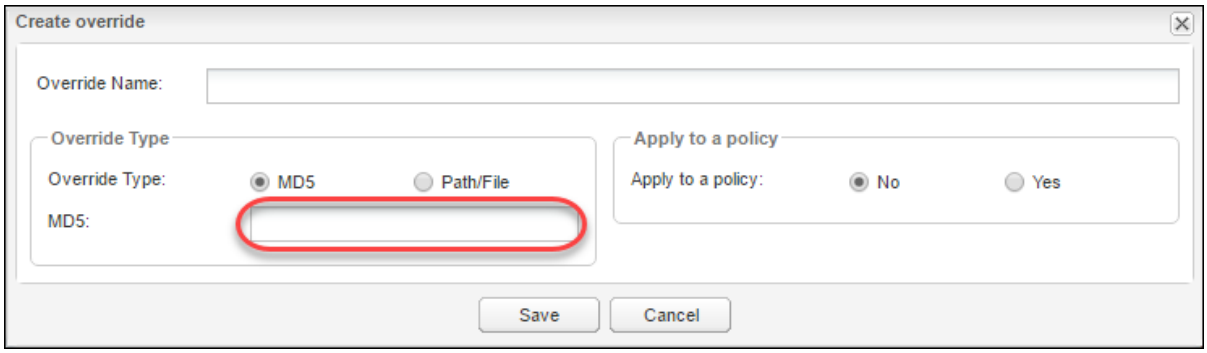
4. [オーバーライド名] フィールドにオーバーライドの名前を入力します。



5. [オーバーライドの種類] のエリアで、[**MD5**] ラジオボタンを選択します。

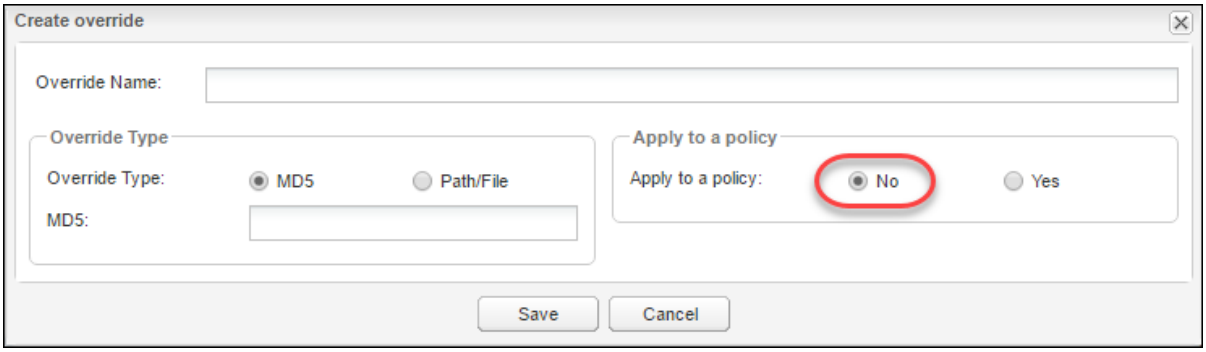


6. [MD5] フィールドで、コピーした **MD5 値**を貼り付けます。

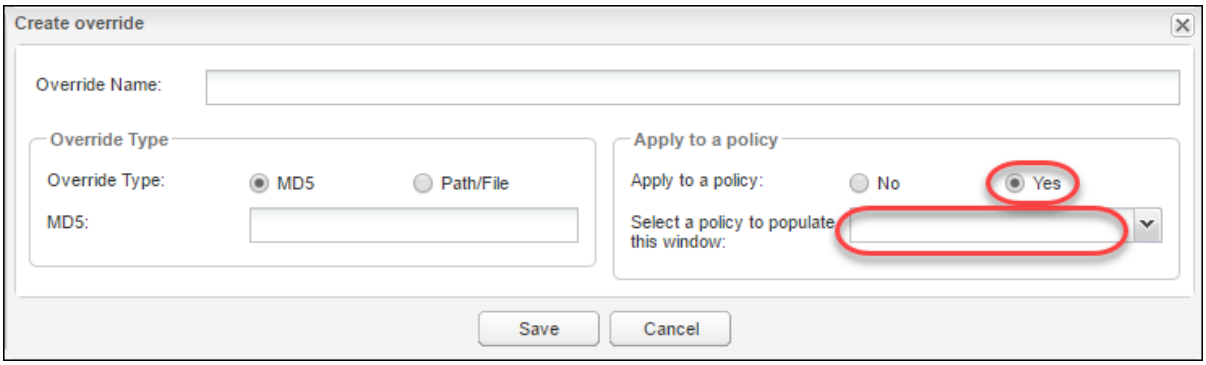


7. [1 つのポリシーに適用] エリアで、次のいずれかの操作を行います。

- ポリシーを適用しない場合は、[**いいえ**] ラジオボタンを選択します。

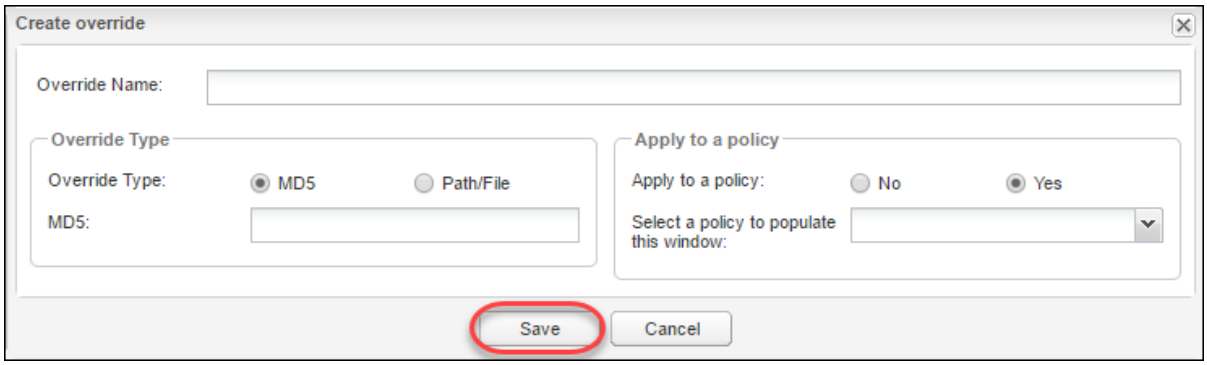


- 1 つのポリシーにオーバーライドを適用する場合は、[**はい**] ラジオボタンを選択します。続いて、ポリシー選択用のドロップダウンメニューで、オーバーライドを適用するポリシーを選択します。



注意: グローバルにオーバーライドを適用することも、単一のポリシーに適用することもできます。ただし、両方を行うことはできません。

8. 設定が完了したら [**保存**] ボタンをクリックします。



9. SecureAnywhere がファイルを検出する方法をテストするには、[**すべてのファイルとプロセスを再検証する**] コマンドをそのエンドポイントに送信します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

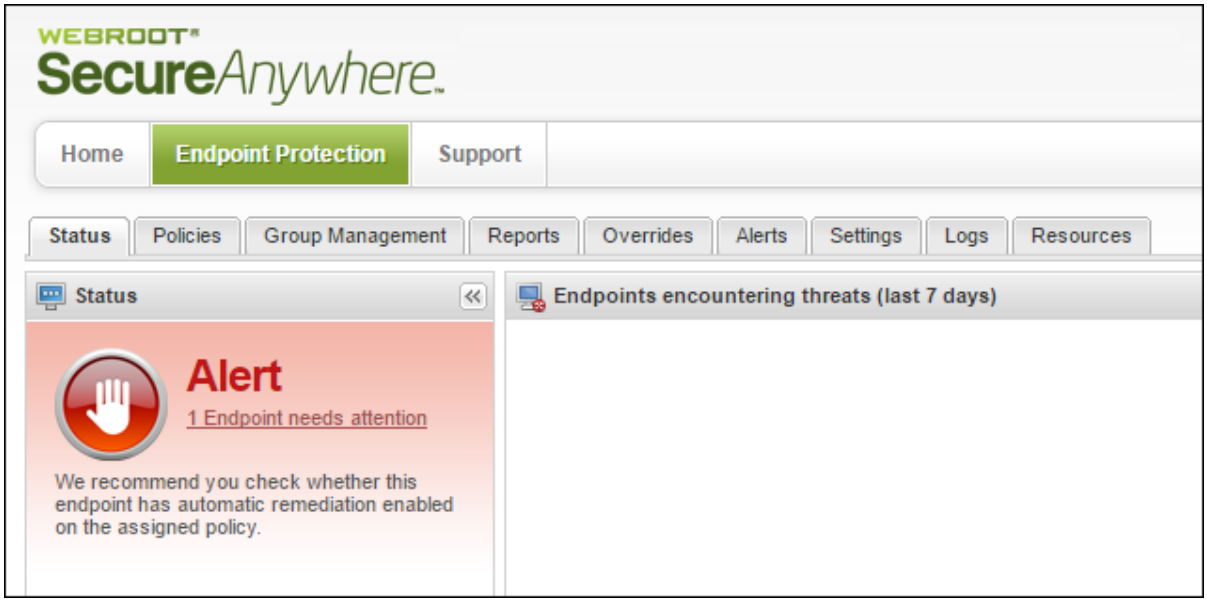
グループからのファイルへのオーバーライドの適用

グループのレベルから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、今後そのファイルが再び検出および隔離されることはなくなります。

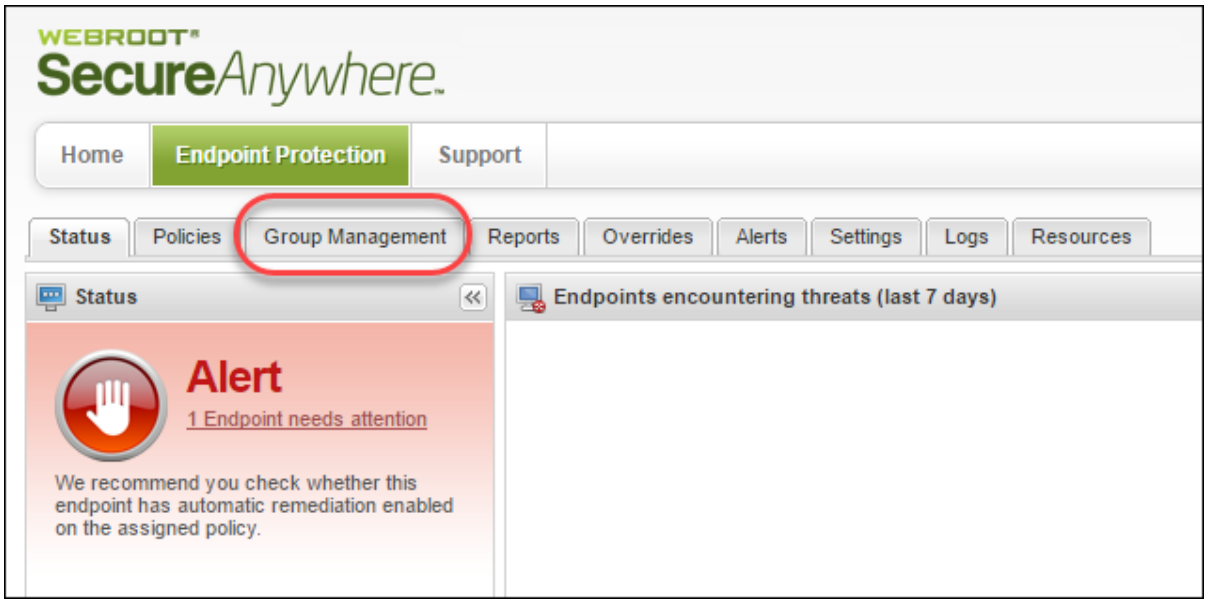
グループからオーバーライドを適用するには

1. エンドポイント プロテクションのコンソールにログインします。

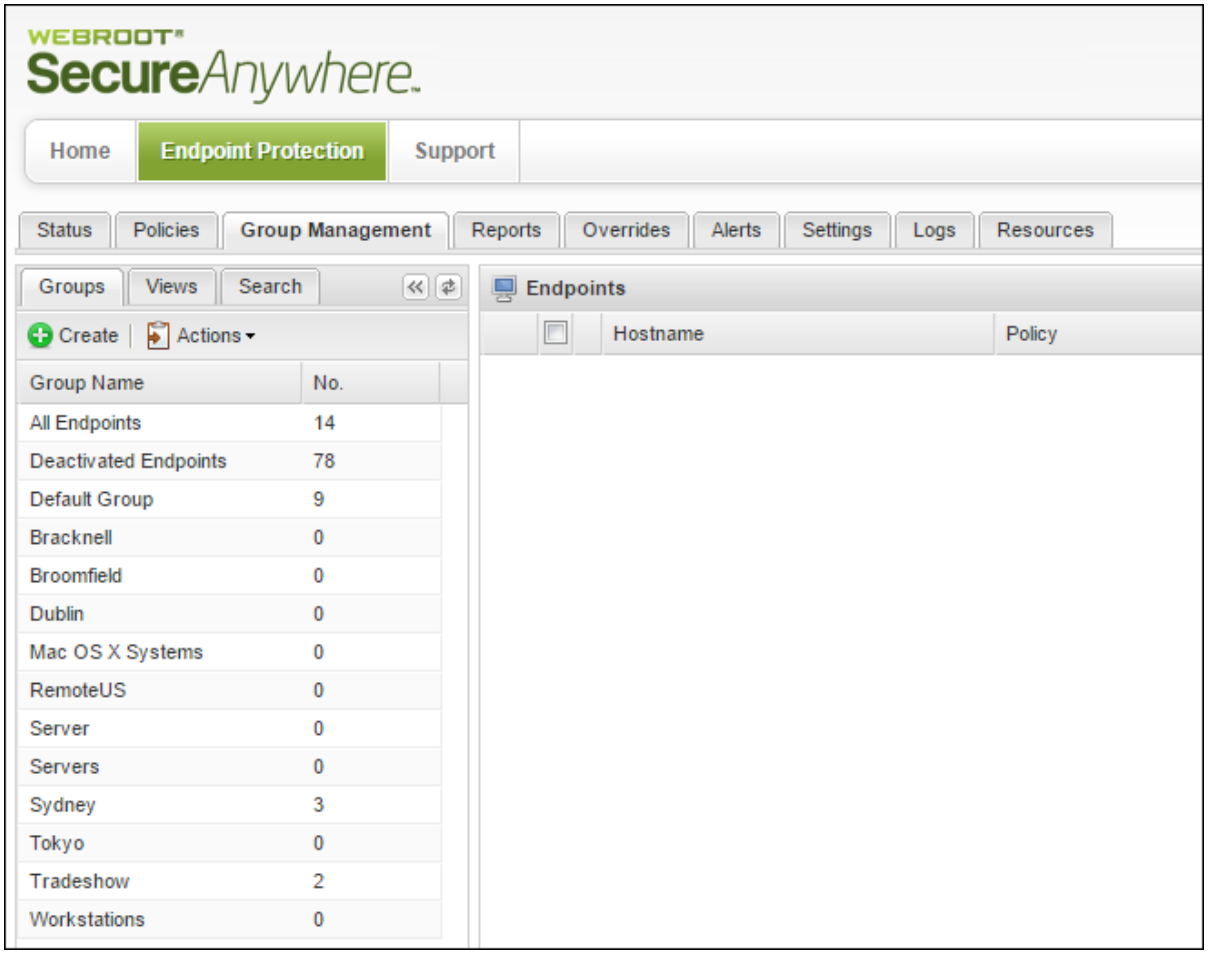
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



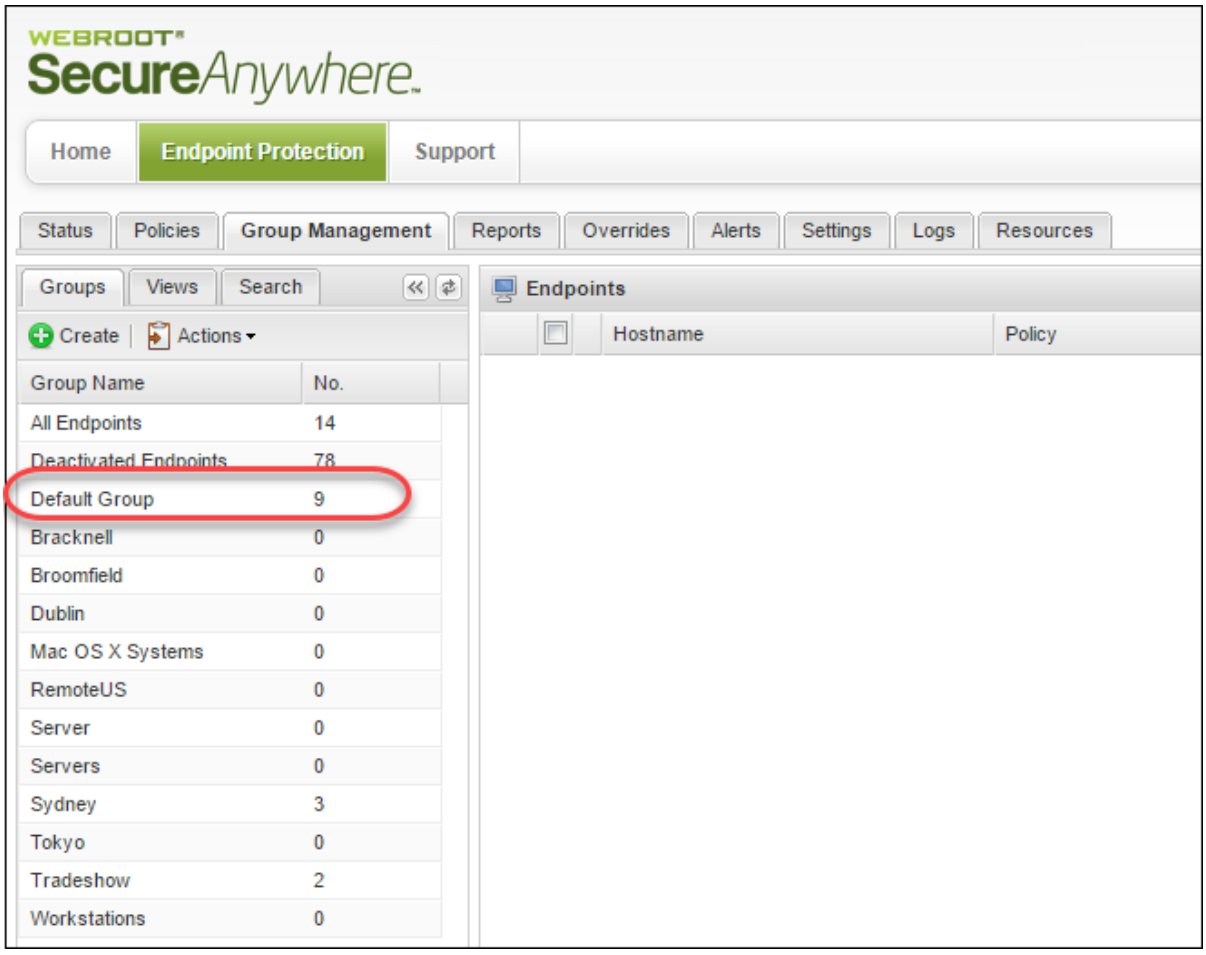
2. [**グループの管理**] タブをクリックします。



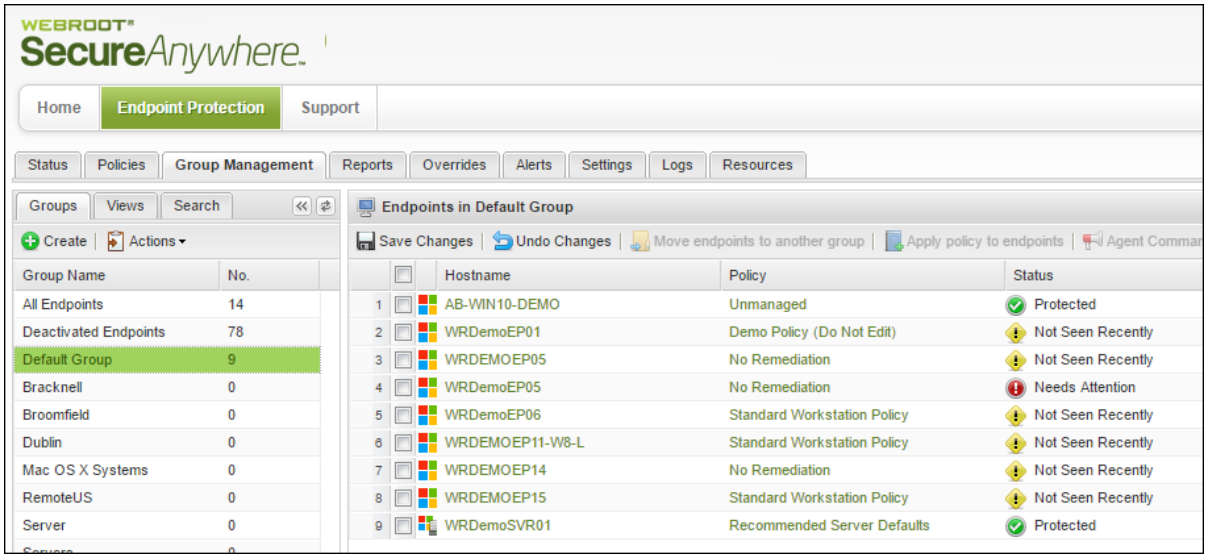
[グループ] タブがアクティブになった状態で [グループの管理] タブが表示されます。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Support
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Groups
Views
Search
Create
Actions
Group Name
No.
All Endpoints 14
Deactivated Endpoints 78
Default Group 9
Bracknell 0
Broomfield 0
Dublin 0
Mac OS X Systems 0
RemoteUS 0
Server 0
Servers 0
Sydney 3
Tokyo 0
Tradeshow 2
Workstations 0
Endpoints
Hostname
Policy

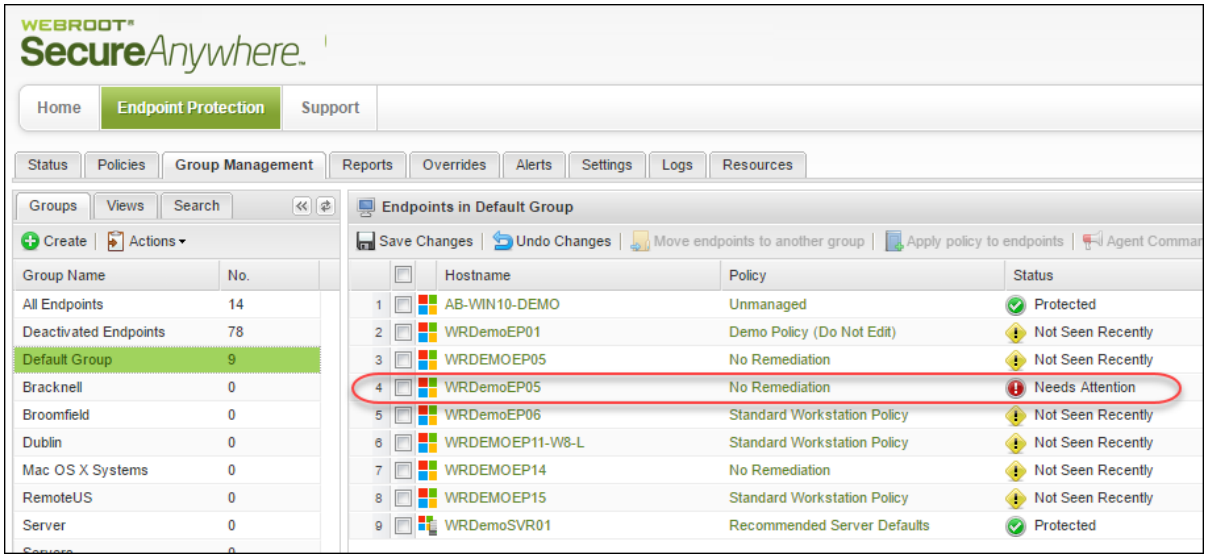
3. 左側のペインで、ファイルが検出されたエンドポイントのグループを選択します。



エンドポイントのリストが表示されます。

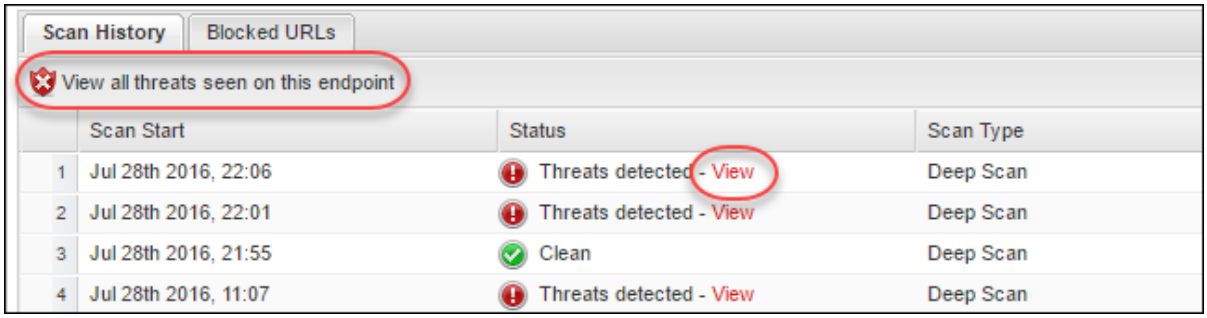


4. 右側のペインで、ファイルが検出されたエンドポイントを選択します。

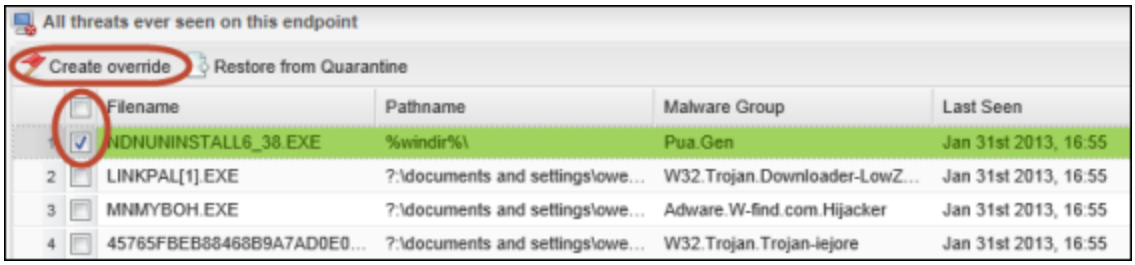


5. 下部の [スキャン履歴] リストで、次のいずれかの操作を行います。

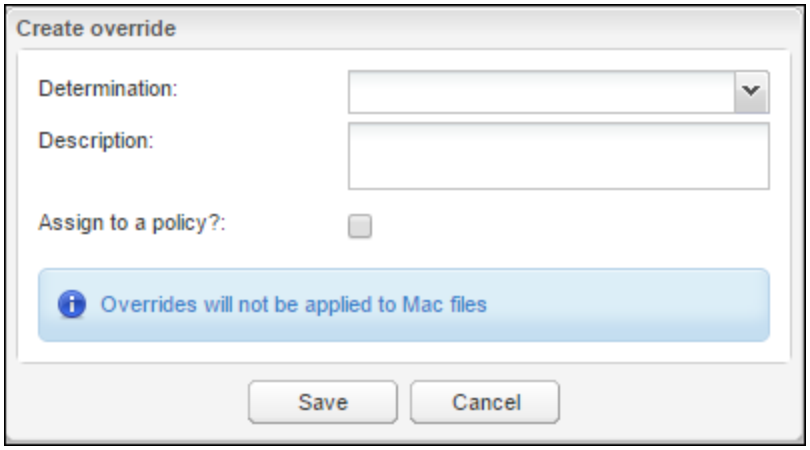
- [**このエンドポイントで確認されたすべての脅威を表示**] をクリックする
- [状態] カラムで [**表示**] をクリックして、脅威が検出された日付を確認する



6. このダイアログで、オーバーライドを作成するファイル名のチェックボックスを選択し、[オーバーライドの作成] アイコンをクリックします。



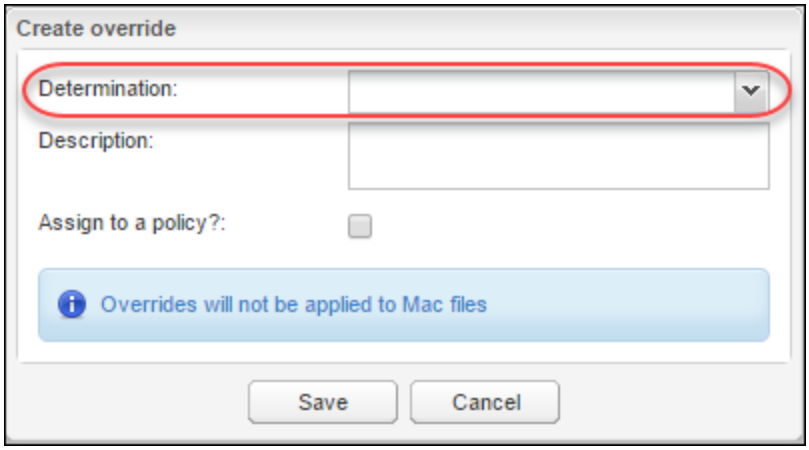
[オーバーライドの作成] ウィンドウが表示されます。



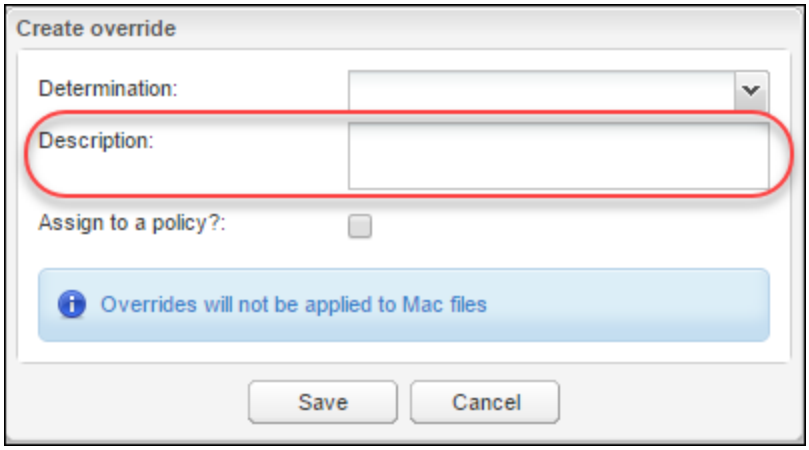
7. [判定] ドロップダウンメニューで、次のいずれかを選択します。

- **正当** - ファイルの実行を常に許可します。

- **不正** - 常にファイルを隔離します。



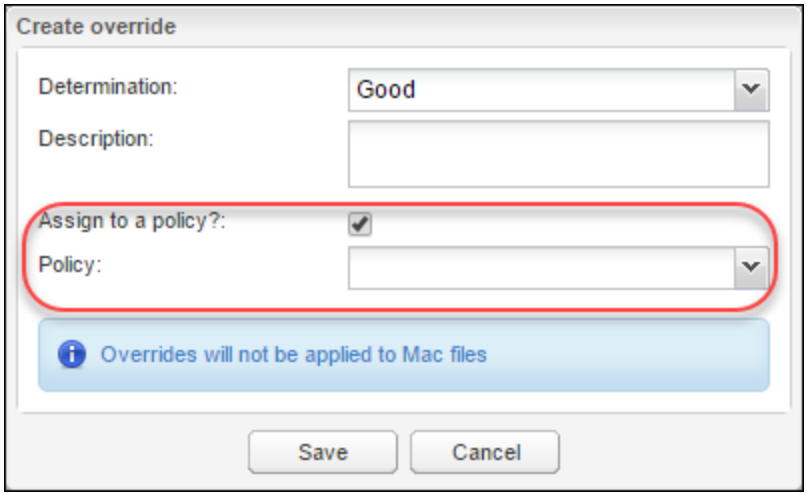
8. [説明] フィールドにオーバーライドについての説明を入力します。



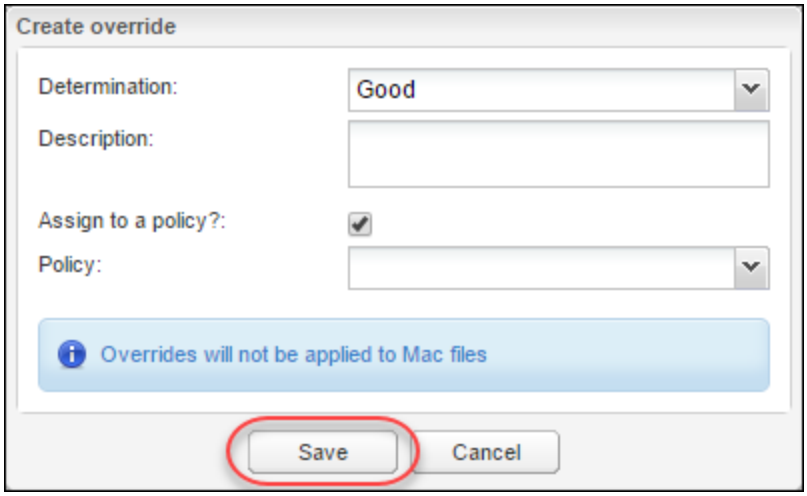
9. オーバーライドを適用するには、次のいずれかの操作を行います。

- すべてのポリシーにオーバーライドを適用するには、[**ポリシーに割り当てますか?**] チェックボックスを選択しません。

- 個別のポリシーにオーバーライドを適用するには、[**ポリシーに割り当てますか?**] チェックボックスを選択しません。[ポリシー] フィールドが表示されたら、ドロップダウンメニューでポリシーを選択します。



10. 設定が完了したら [**保存**] ボタンをクリックします。



11. ファイルの検出をテストするには、[すべてのファイルとプロセスを再検証する] コマンドをそのエンドポイントに送信します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

レポートからのファイルへのオーバーライドの適用

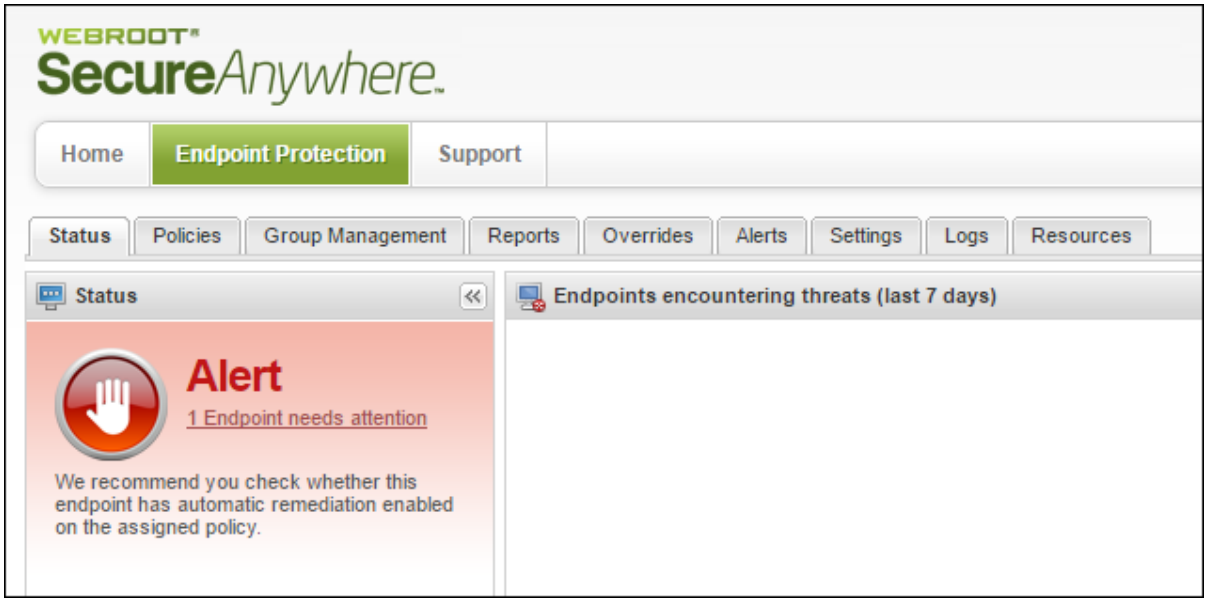
[レポート] タブから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、今後そのファイルが再び検出および隔離されることはなくなります。以下のレポートから、オーバーライドを追加できます。

- *[確認されたすべての脅威] レポートの生成 ページ342*
- *[確認されたすべての未判定のソフトウェア] レポートの生成 ページ349*
- *[最新のスキャンで脅威が存在したエンドポイント] レポートの生成 ページ361* - [このエンドポイントで確認された脅威] パネル内、個々のエンドポイントのみ。
- *[最新のスキャンで未判定のソフトウェアが検出されたエンドポイント] レポートの生成 ページ365* - [このエンドポイントで確認されたすべての未判定のソフトウェア] パネル内、個々のエンドポイントのみ。

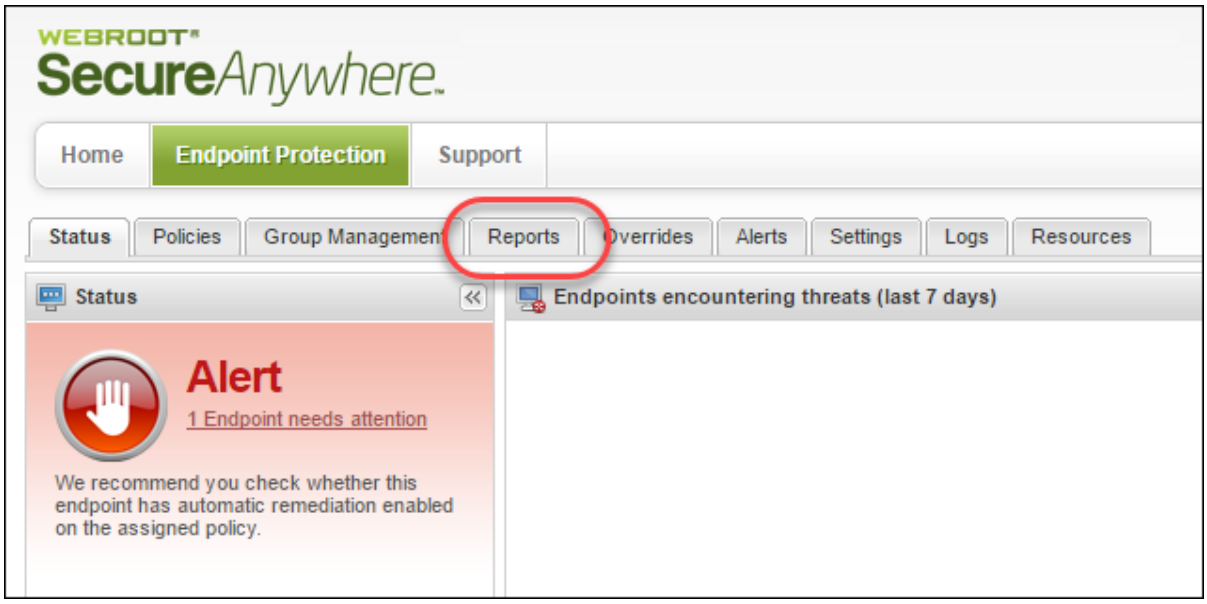
レポートからオーバーライドを適用するには

1. エンドポイントプロテクションのコンソールにログインします。

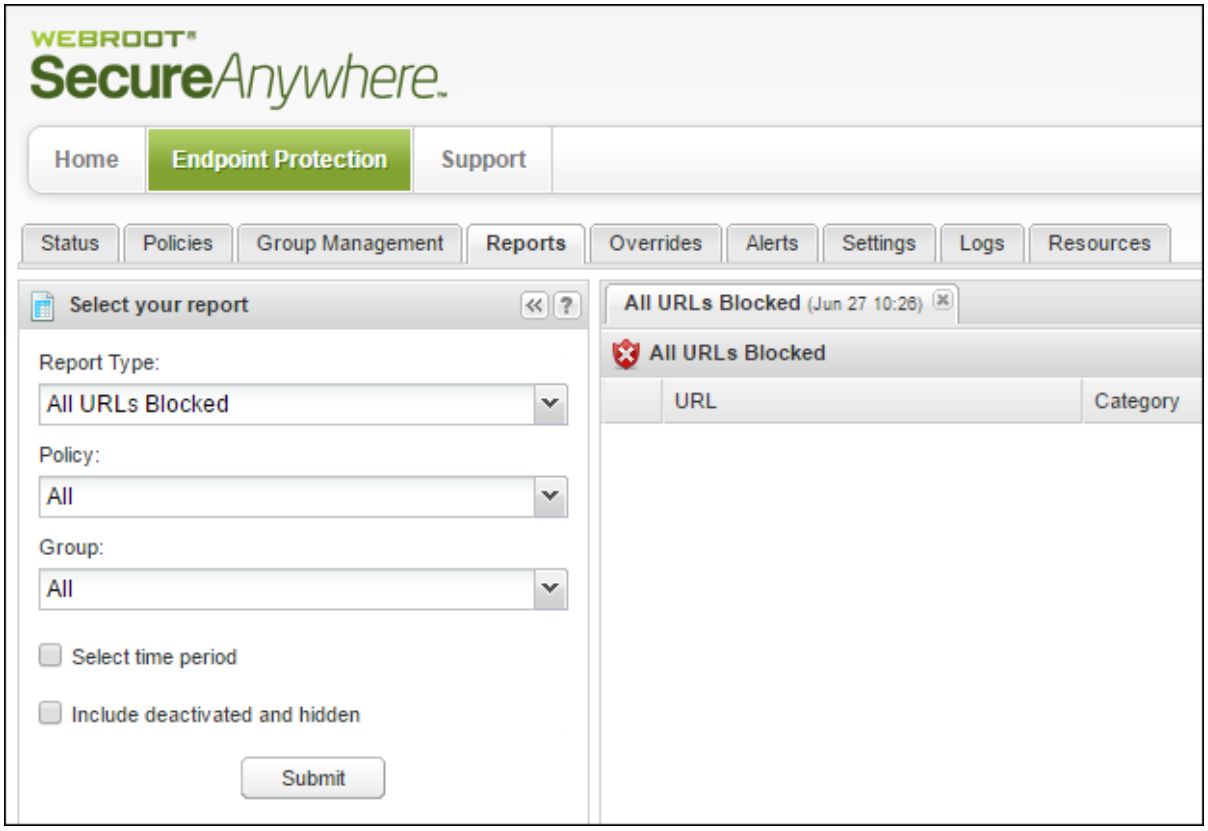
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



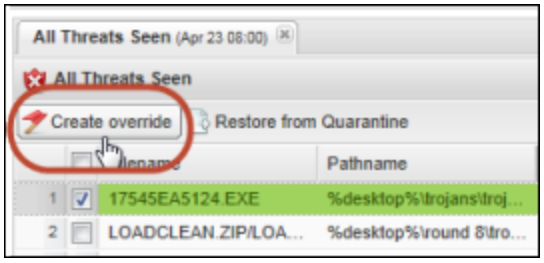
2. [**レポート**] タブをクリックします。



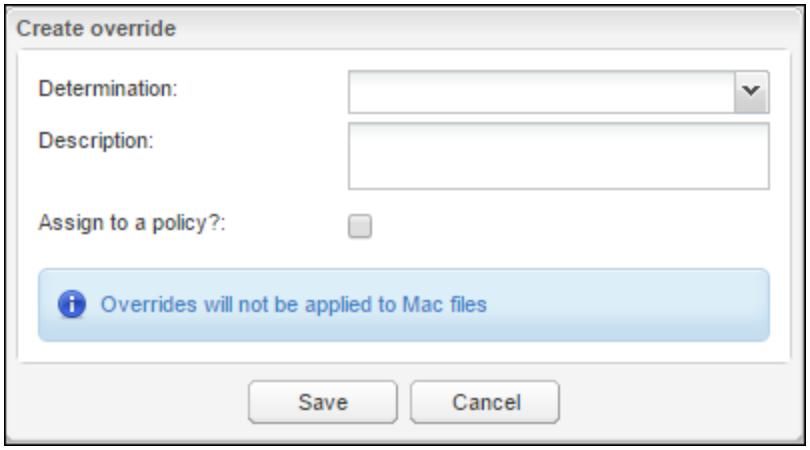
[レポート] タブが表示されます。



3. [**レポートの種類**] ドロップダウンメニューで前述したレポートのいずれかを選択し、[**送信**] ボタンをクリックしてレポートを生成します。
4. [確認されたすべての脅威] エリアでファイル名を選択し、コマンドバーの [**オーバーライドの作成**] アイコンをクリックします。

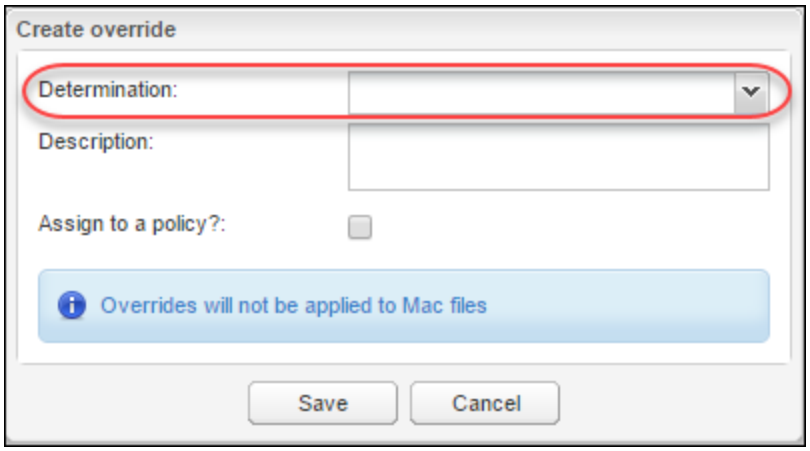


[オーバーライドの作成] ウィンドウが表示されます。



5. [判定]ドロップダウンメニューで、次のいずれかを選択します。

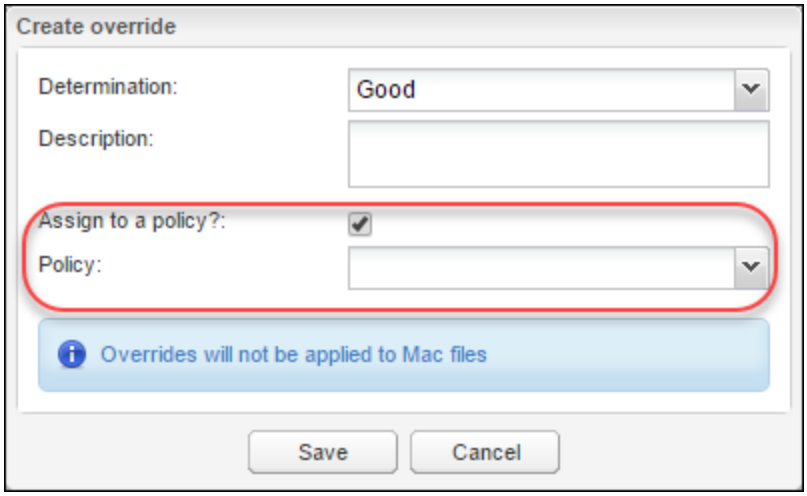
   - **正当** - ファイルの実行を常に許可します。
   - **不正** - 常にファイルを隔離します。



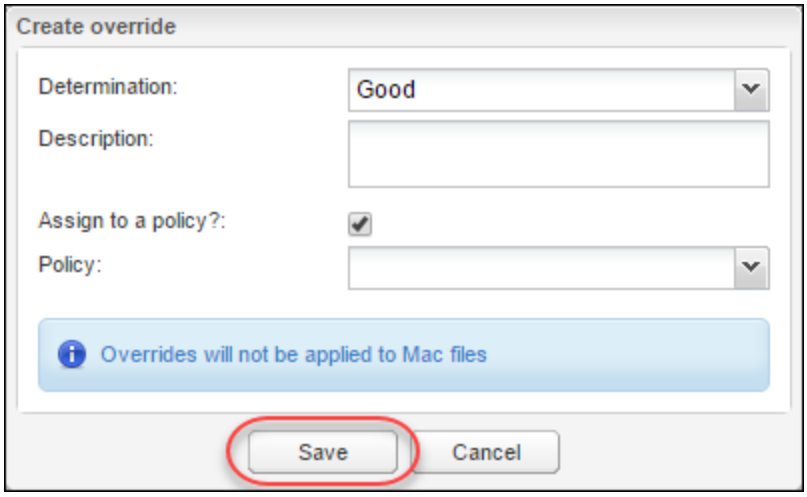
6. オーバーライドを適用するには、次のいずれかの操作を行います。

   - すべてのポリシーにオーバーライドを適用するには、[**ポリシーに割り当てますか?**] チェックボックスを選択しません。

- オーバーライド対象のポリシーを個別に選択するには、[**ポリシーに割り当てますか?**] チェックボックスを選択しません。[ポリシー] フィールドが表示されたら、[ポリシー] ドロップダウンメニューでポリシーを選択します。



7. 設定が完了したら [**保存**] ボタンをクリックします。



8. ファイルの検出をテストするには、[**すべてのファイルとプロセスを再検証する**] コマンドをそのエンドポイントに送信します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

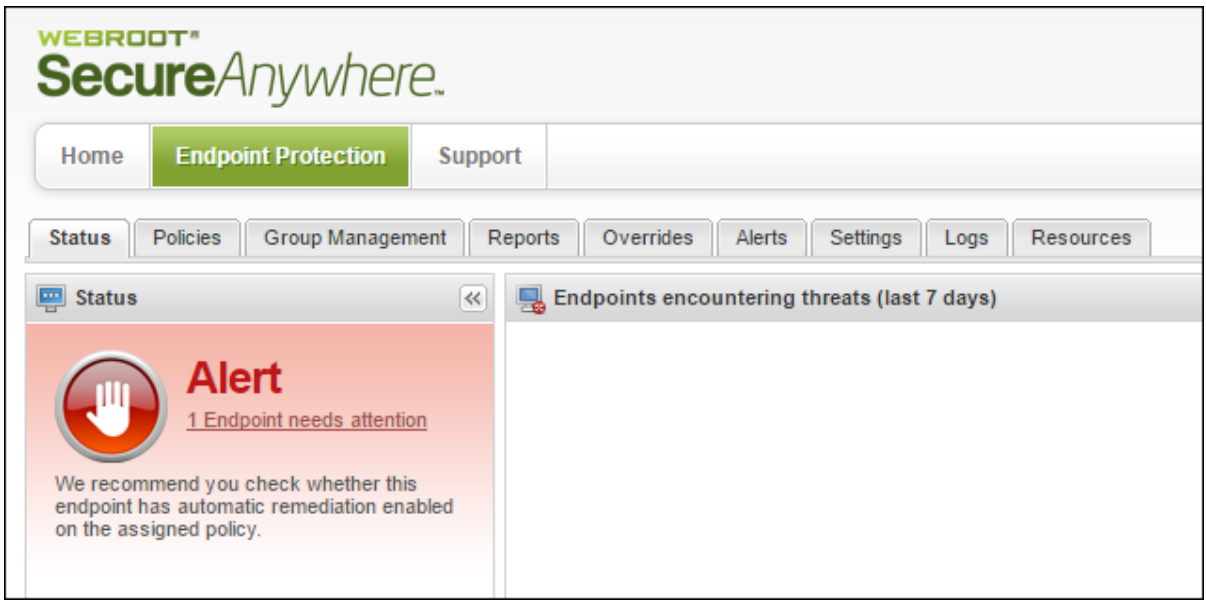
滞留時間のポップアップからのオーバーライドの適用

滞留時間のポップアップから、脅威として指定されたファイルにオーバーライドを適用することができます。これにより、今後そのファイルが再び検出および隔離されることはなくなります。

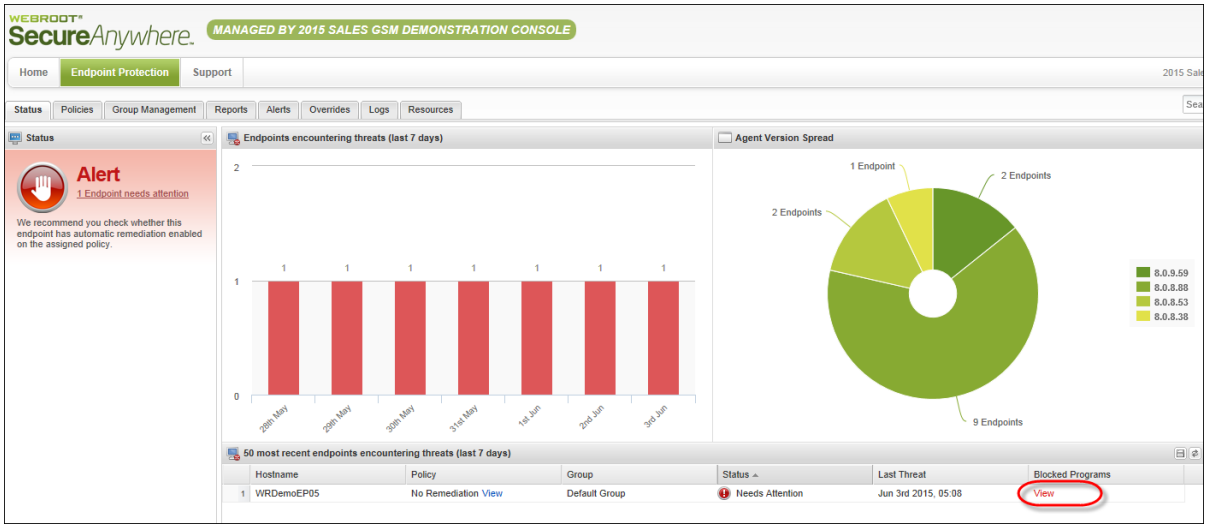
滞留時間のポップアップからオーバーライドを適用するには

1. エンドポイントプロテクションのコンソールにログインします。

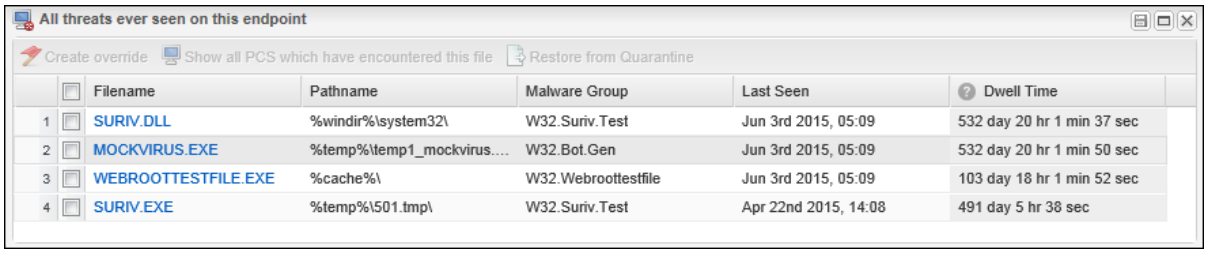
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



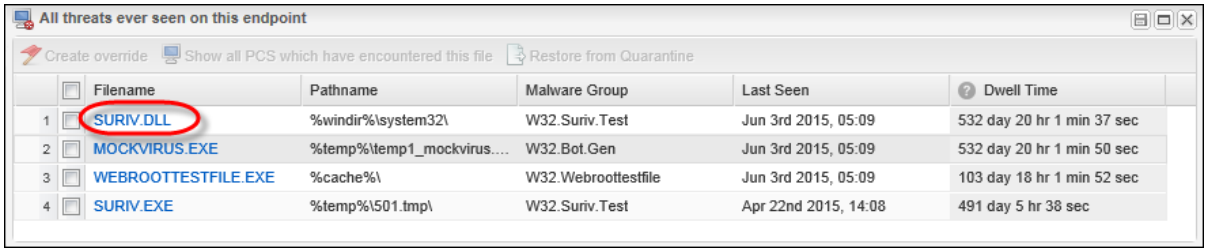
2. [脅威が存在した最近の 50 個のエンドポイント] エリアで、オーバーライドを作成するアイテムの [**表示**] リンクをクリックします。



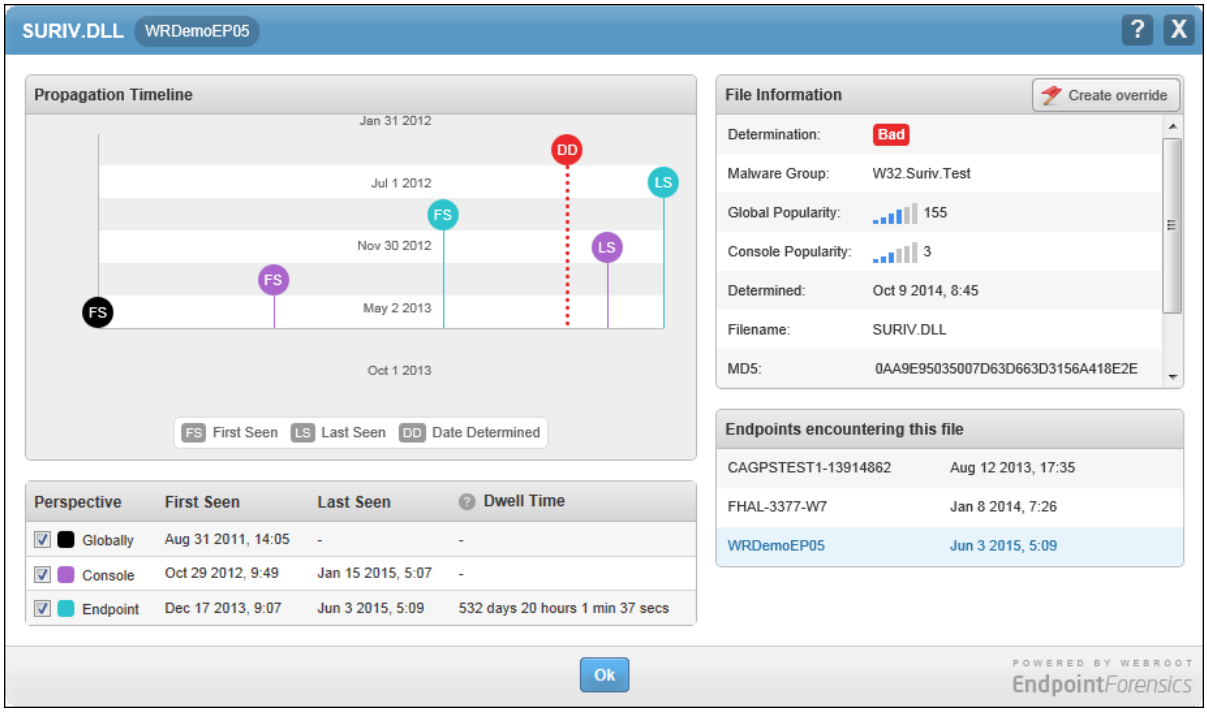
[このエンドポイントでこれまでに確認されたすべての脅威] ウィンドウが表示されます。



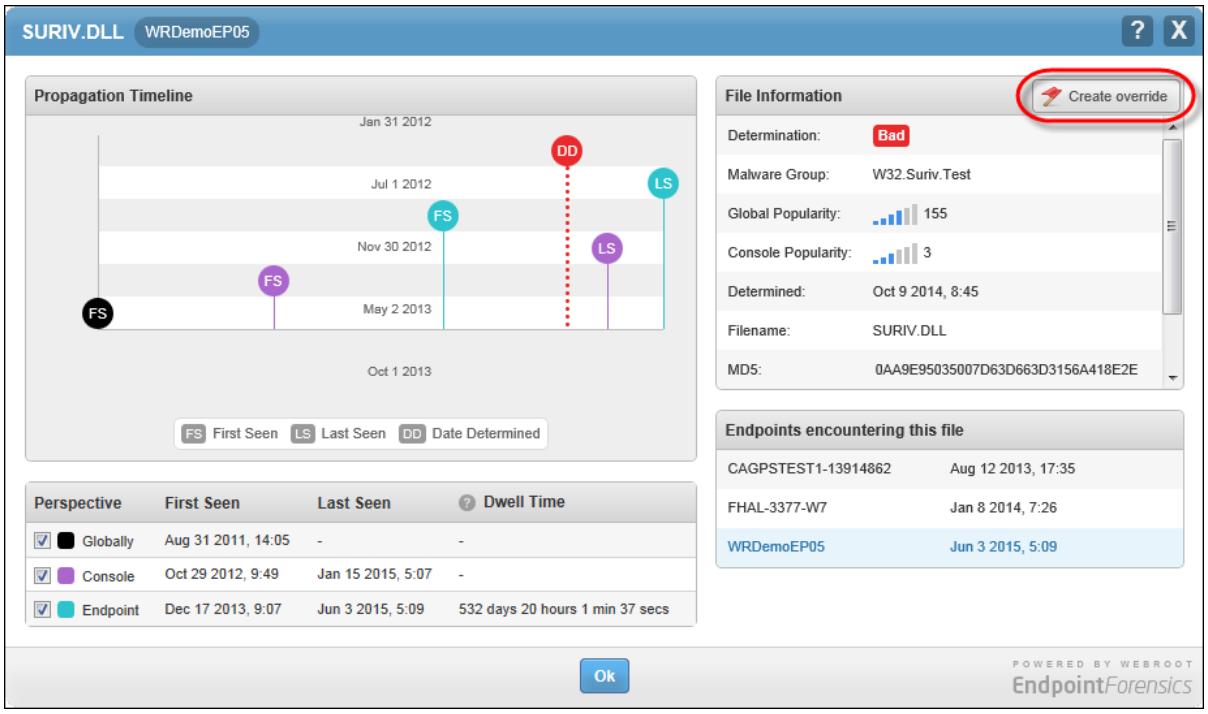
3. [ファイル名] カラムで、オーバーライドを作成するアイテムのリンクを選択します。



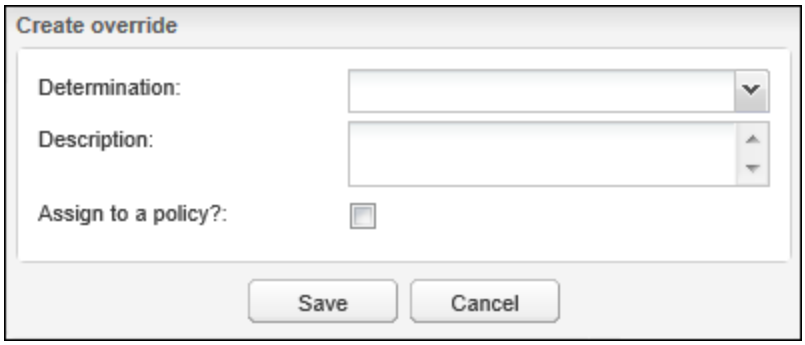
滞留時間のポップアップウィンドウが表示されます。


SURIV.DLL
WRDemoEP05
Propagation Timeline
Jan 31 2012
Jul 1 2012
Nov 30 2012
May 2 2013
Oct 1 2013
DD
LS
FS
LS
FS
FS
First Seen
LS
Last Seen
DD
Date Determined
File Information
Create override
Determination:
Bad
Malware Group:
W32.Suriv.Test
Global Popularity:
155
Console Popularity:
3
Determined:
Oct 9 2014, 8:45
Filename:
SURIV.DLL
MD5:
0AA9E95035007D63D663D3156A418E2E
Endpoints encountering this file
CAGPSTEST1-13914862
Aug 12 2013, 17:35
FHAL-3377-W7
Jan 8 2014, 7:26
WRDemoEP05
Jun 3 2015, 5:09
Perspective
First Seen
Last Seen
Dwell Time
Globally
Aug 31 2011, 14:05
-
-
Console
Oct 29 2012, 9:49
Jan 15 2015, 5:07
-
Endpoint
Dec 17 2013, 9:07
Jun 3 2015, 5:09
532 days 20 hours 1 min 37 secs
Ok
POWERED BY WEBROOT
EndpointForensics

4. [**オーバーライドの作成**] ボタンをクリックします。

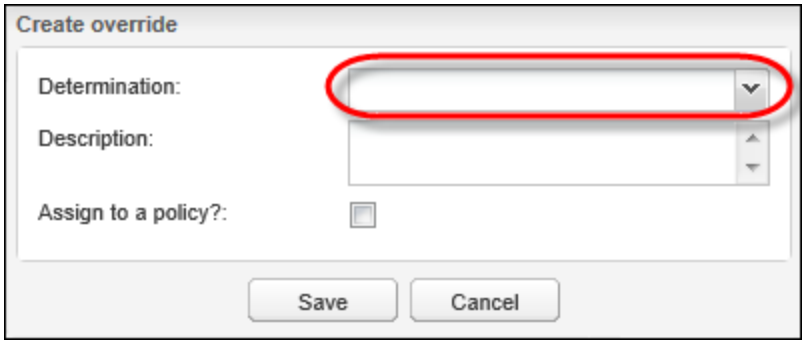


[オーバーライドの作成] ウィンドウが表示されます。



5. [判定] ドロップダウンメニューで、次のいずれかを選択します。

- **正当** - ファイルの実行を常に許可します。
- **不正** - 常にファイルを隔離します。

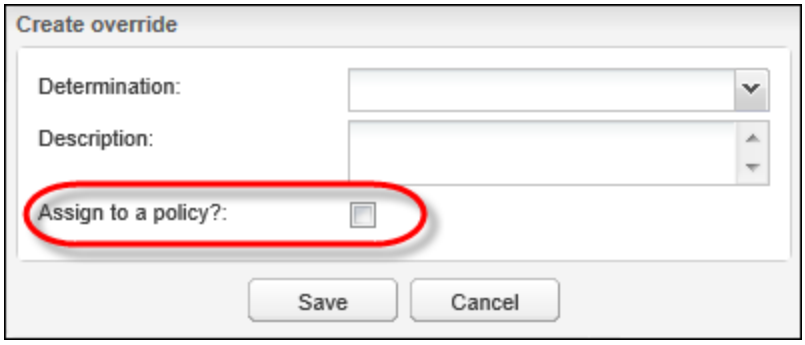


6. [説明] フィールドにオーバーライドの情報を入力します。

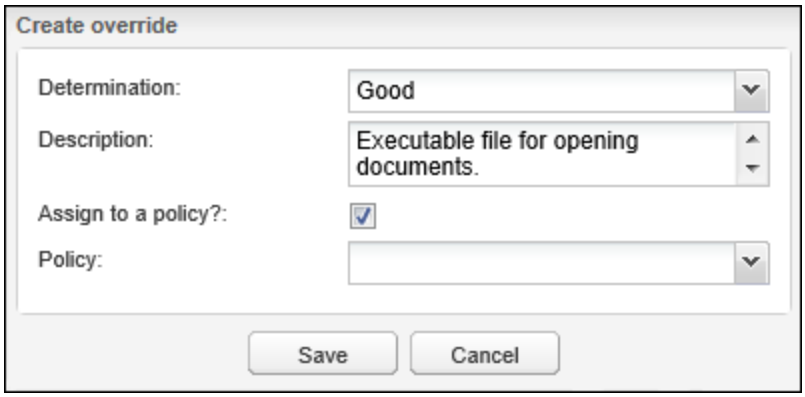
7. オーバーライドを適用するには、次のいずれかの操作を行います。

   - 特定のポリシーにオーバーライドを適用しない場合は、[**ポリシーに割り当てますか?**] チェックボックスを選択しません。

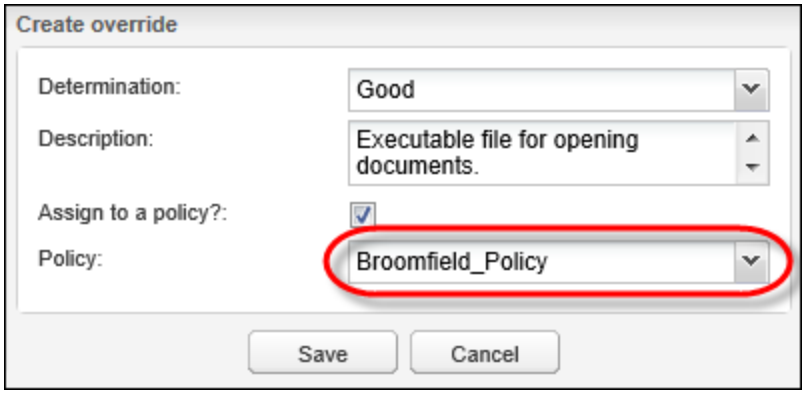
   - 特定のポリシーにオーバーライドを適用する場合は、[**ポリシーに割り当てますか?**] チェックボックスを選択します。



チェックボックスを選択した場合、[ポリシー] ドロップダウンメニューが表示されます。

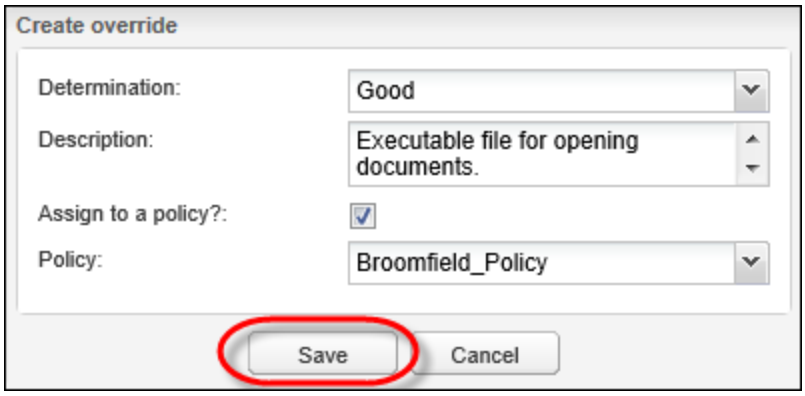


8. オーバーライドを適用するポリシーを選択します。



注意: グローバルにオーバーライドを適用することも、単一のポリシーに適用することもできます。ただし、両方を行うことはできません。

9. 設定が完了したら [**保存**] ボタンをクリックします。



10. SecureAnywhere がファイルを検出する方法をテストするには、[すべてのファイルとプロセスを再検証する] コマンドをそのエンドポイントに送信します。詳細については、「*エンドポイントへのコマンドの発行 ページ144*」を参照してください。

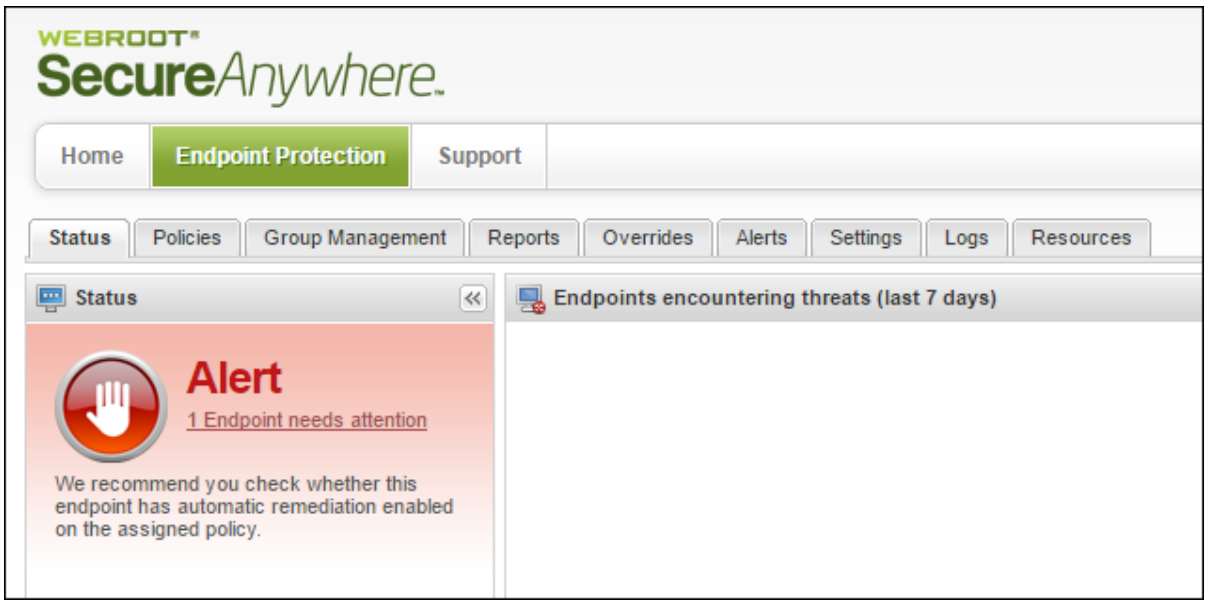
オーバーライドの表示

エンドポイントプロテクションに追加したオーバーライドは、[オーバーライド] タブ内に表示されます。

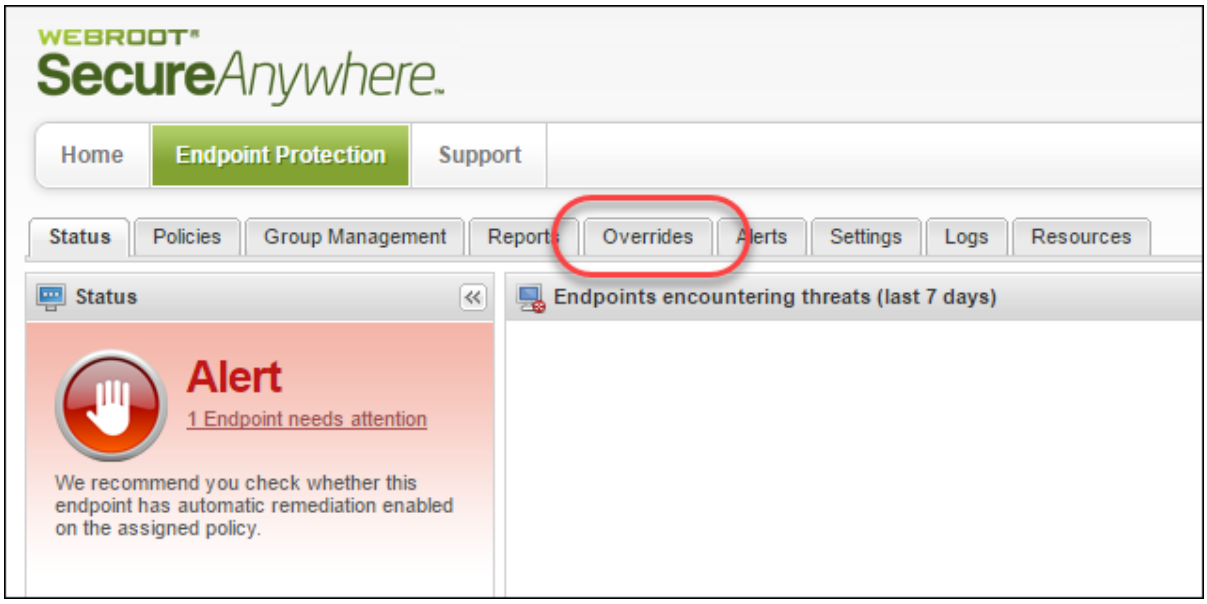
オーバーライドを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

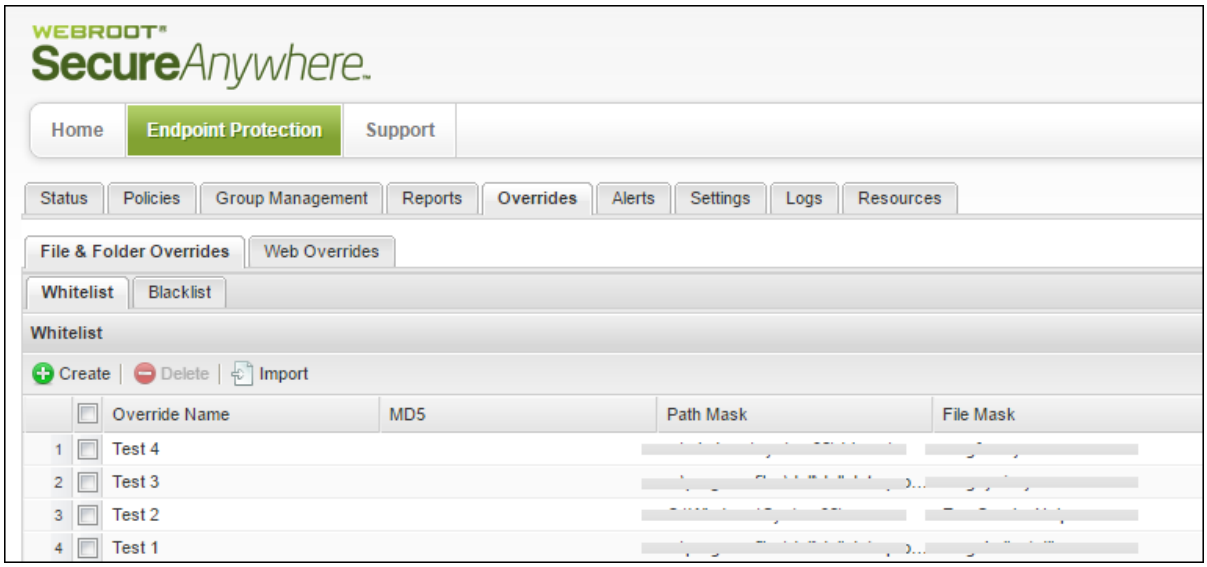
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



2. [**オーバーライド**] タブをクリックします。

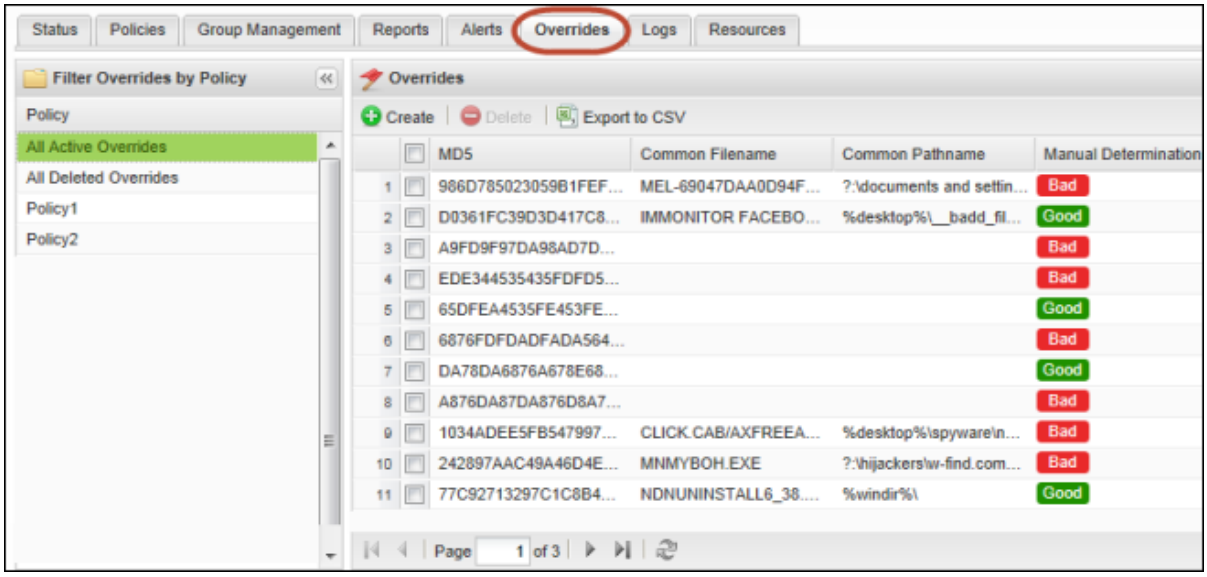


[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。

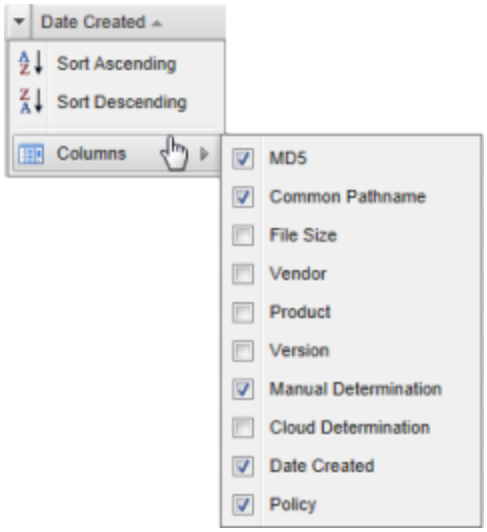


3. 左側のパネルでポリシーを選択すると、絞り込まれた結果が右側に表示されます。

   選択したオーバーライドは [手動判定] カラムに表示されます。



4. オーバーライドに関する追加のデータを表示または非表示にするには、まずカラム見出しをクリックしてドロップダウンメニューを表示します。カラムを追加する場合はチェックボックスを選択し、カラムを削除する場合はチェックボックスの選択を解除します。



カラムには次の情報が含まれています。

データ	説明
MD5	ファイルを固有に識別するための指紋のような働きをする、メッセージダイジェストアルゴリズム 5 の値。
コマンドファイル名	ファイルフォルダに表示される Windows ファイルの名前。これは静的なデータで、非表示にはできません。
共通のパス名	Windows フォルダ構造の名前。
ファイルサイズ	バイト単位でのファイルサイズ。
ベンダー	ファイルに関連するベンダーの名前。SecureAnywhere が情報を特定できる場合のみ。
製品	ファイルに関連する製品の名前。SecureAnywhere が情報を特定できる場合のみ。
バージョン	ファイルに関連する製品のバージョン。SecureAnywhere が情報を特定できる場合のみ。
手動判定	ユーザーによるファイルの [正当] または [不正] の指定。
クラウド判定	ウェブルートのファイル分類。[正当]、[不正]、[未判定] のいずれか。

データ	説明
作成されたデータ	このオーバーライドが定義された日付と時刻。
ポリシー	このオーバーライドが適用されたポリシー。

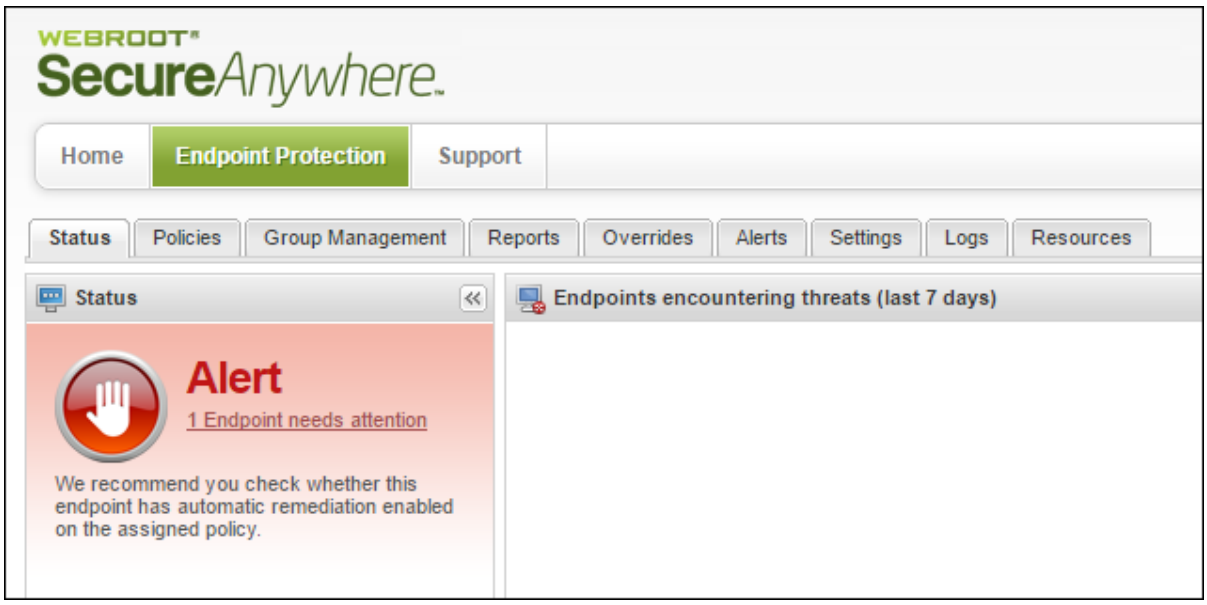
スプレッドシートへのオーバーライドのエクスポート

すべてのオーバーライド情報をスプレッドシートにエクスポートできます。他の管理者と共に設定の確認をする場合などに便利です。

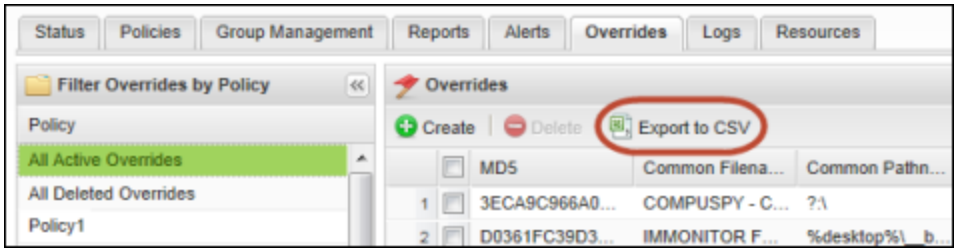
オーバーライドの設定をエクスポートするには

1. エンドポイントプロテクションのコンソールにログインします。

   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



2. サイトコンソールで [**オーバーライド**] タブをクリックします。
3. 右側のパネルで結果を絞り込むには、左側で目的のポリシーを選択します。
4. コマンドメニューバーの [**CSV にエクスポート**] アイコンをクリックします。



5. 表示されるプロンプトで、オーバーライドを CSV ファイルに保存します。

   エンドポイントプロテクションが "Overrides.csv" という名前のファイルにオーバーライドを保存します。さらにファイルを保存すると、*「verrides (2).csv」* のように、最初の名前に数字が追加されます。

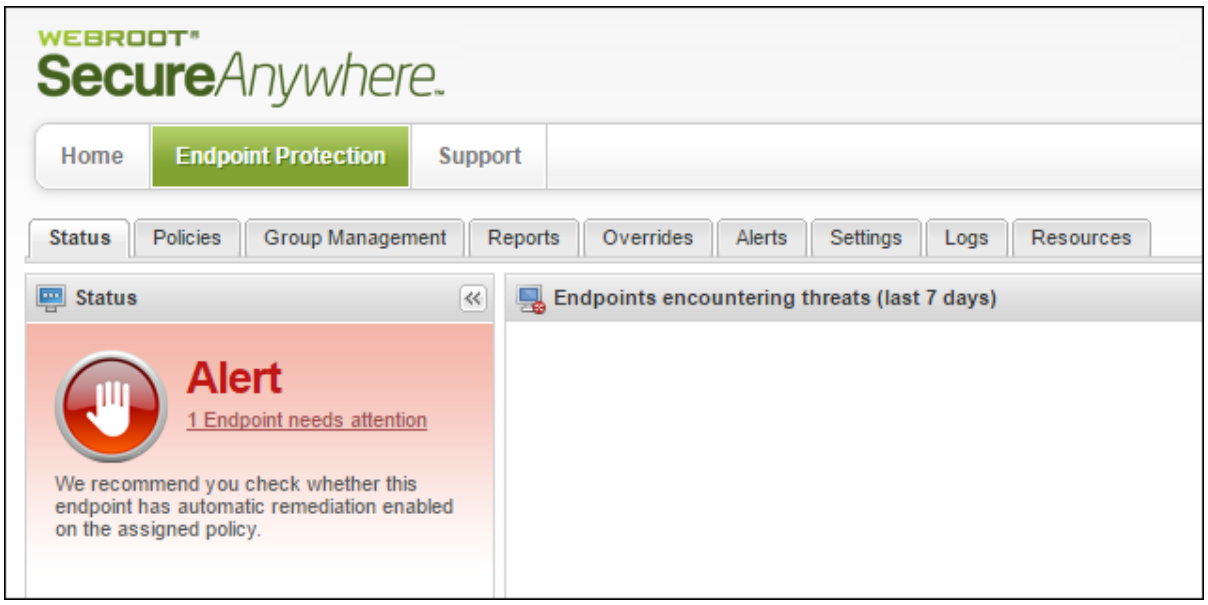
オーバーライドの削除

この手順に従うと、ホワイトリストまたはブラックリストのオーバーライドを削除できます。

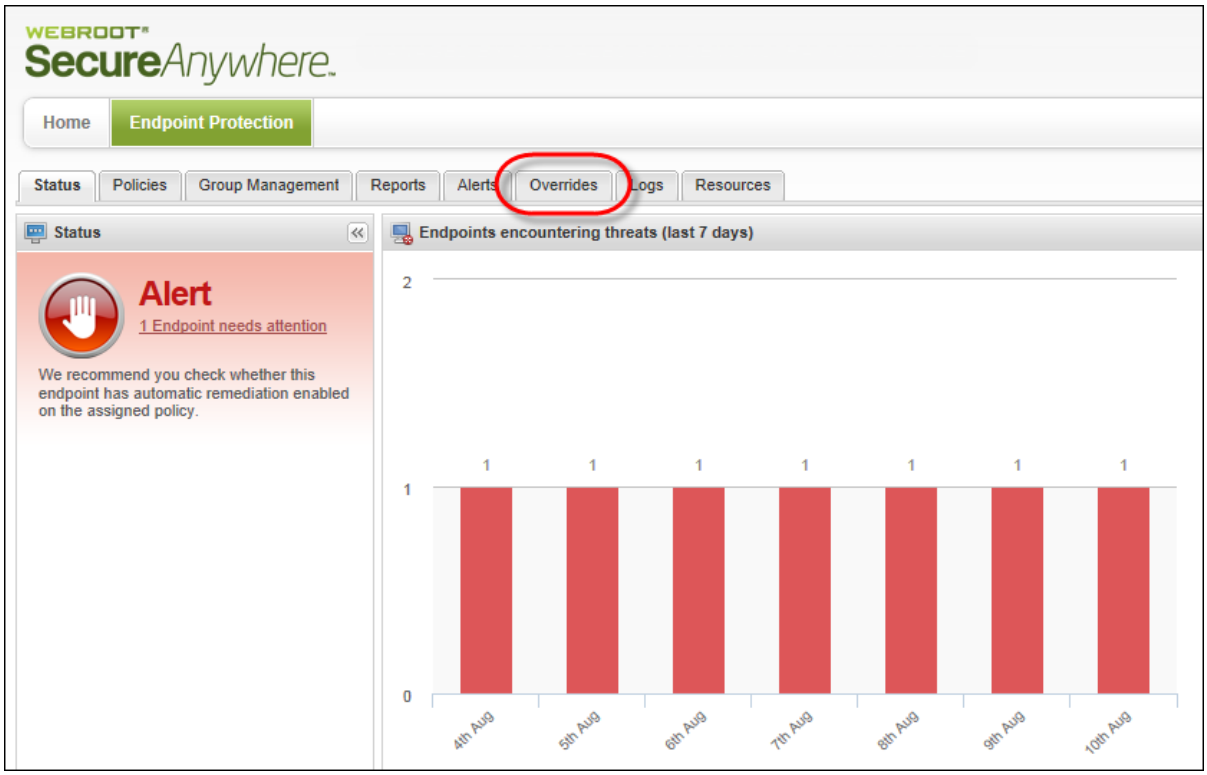
オーバーライドを削除するには

1. エンドポイントプロテクションのコンソールにログインします。

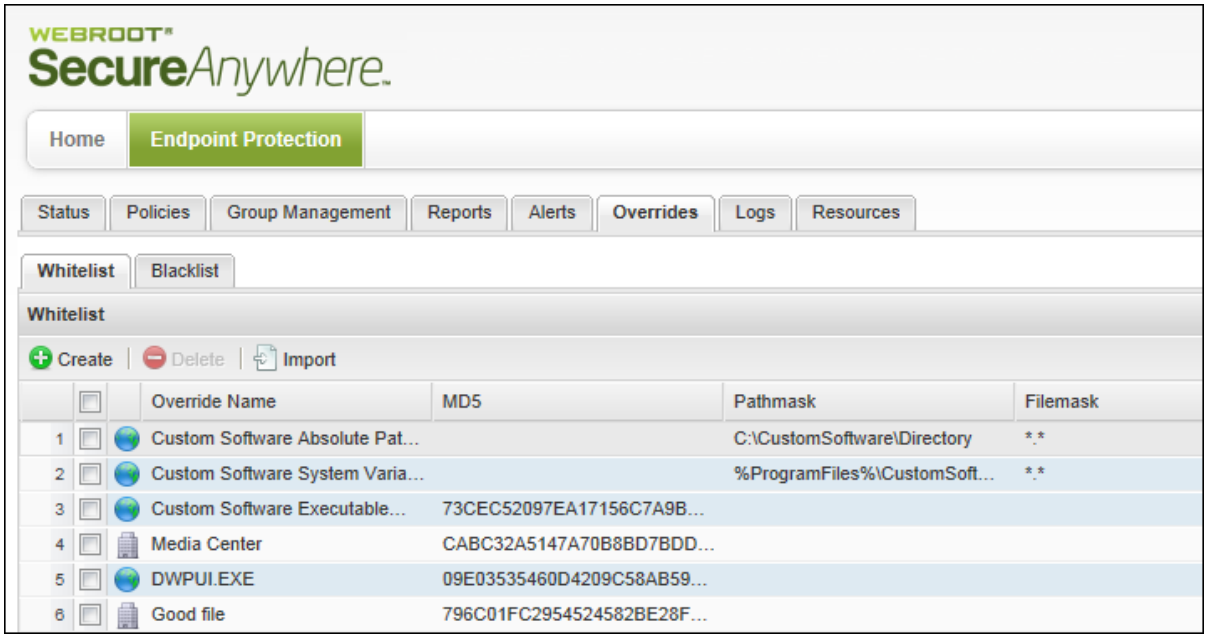
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



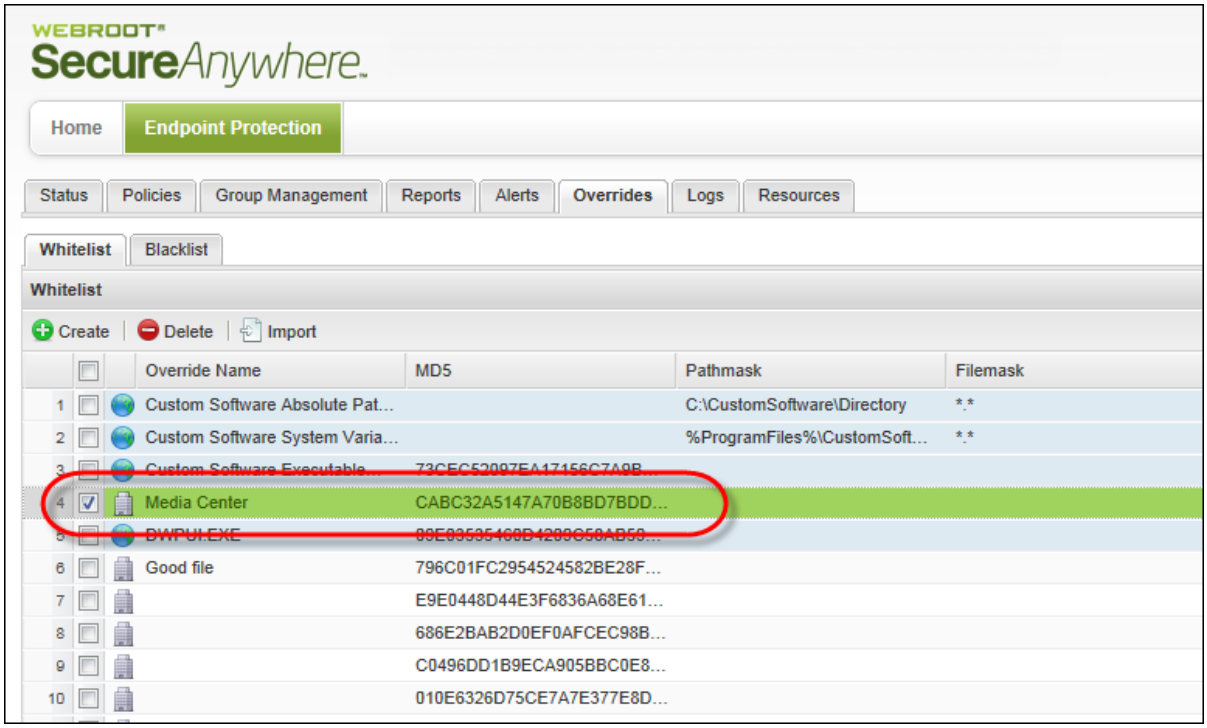
2. サイトコンソールで [**オーバーライド**] タブをクリックします。



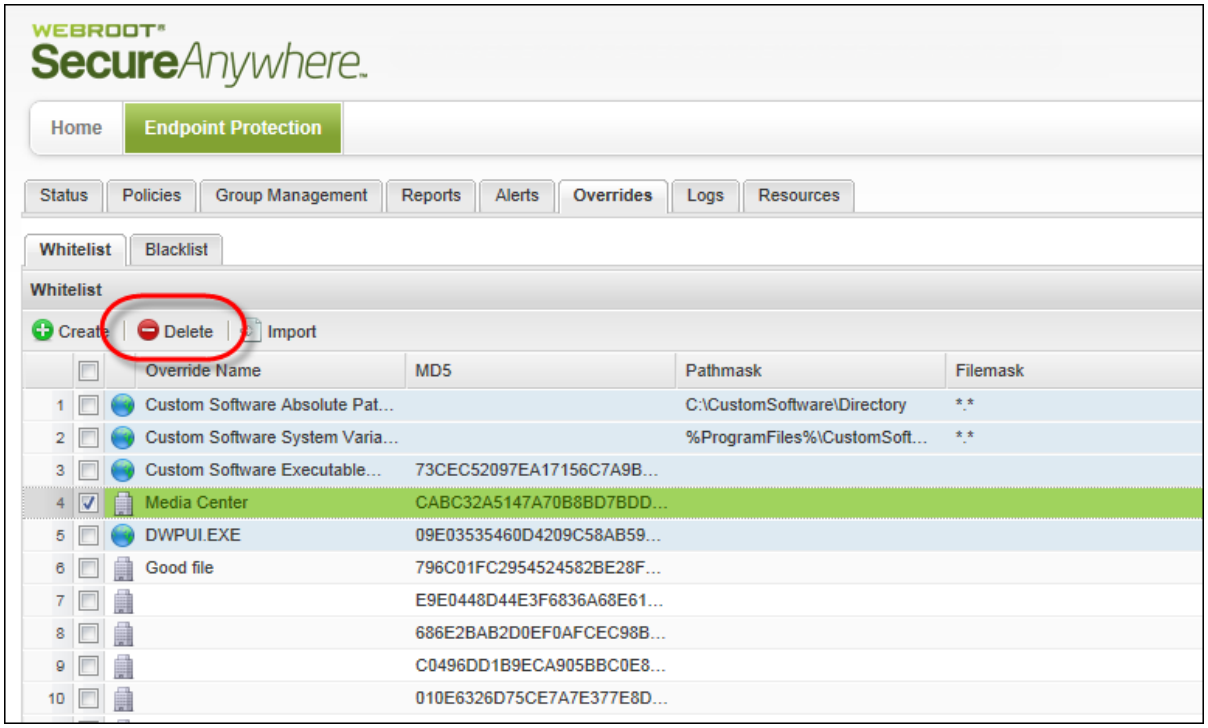
[ホワイトリスト] タブがアクティブになった状態で [オーバーライド] パネルが表示されます。



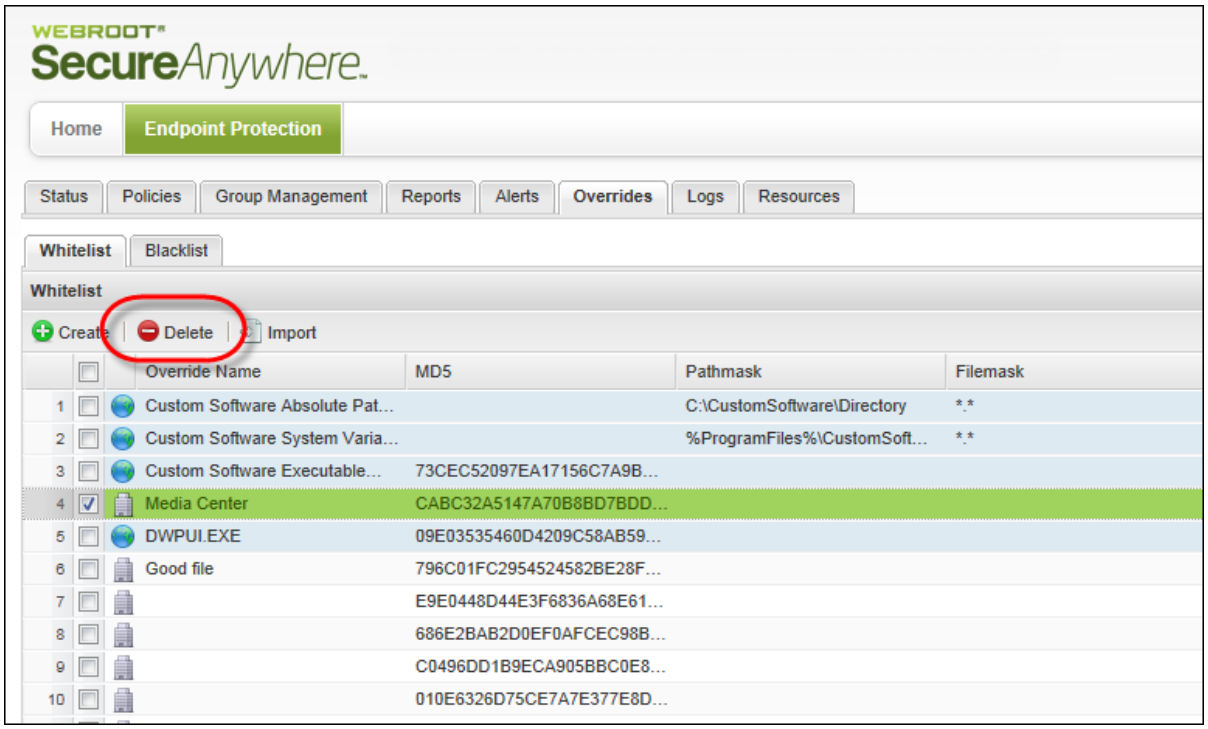
3. [ホワイトリスト] または [ブラックリスト] タブで、削除するオーバーライドを選択します。



[削除] ボタンが表示されます。



4. [**削除**] ボタンをクリックします。



ホワイトリスト / ブラックリストのエントリの削除を確認するウィンドウが表示されます。

5. [**はい**] ボタンをクリックします。

オーバーライドが削除されます。

第 11 章: ウェブのオーバーライドの使用

ウェブのオーバーライドの使用方法については、以下のトピックを参照してください。

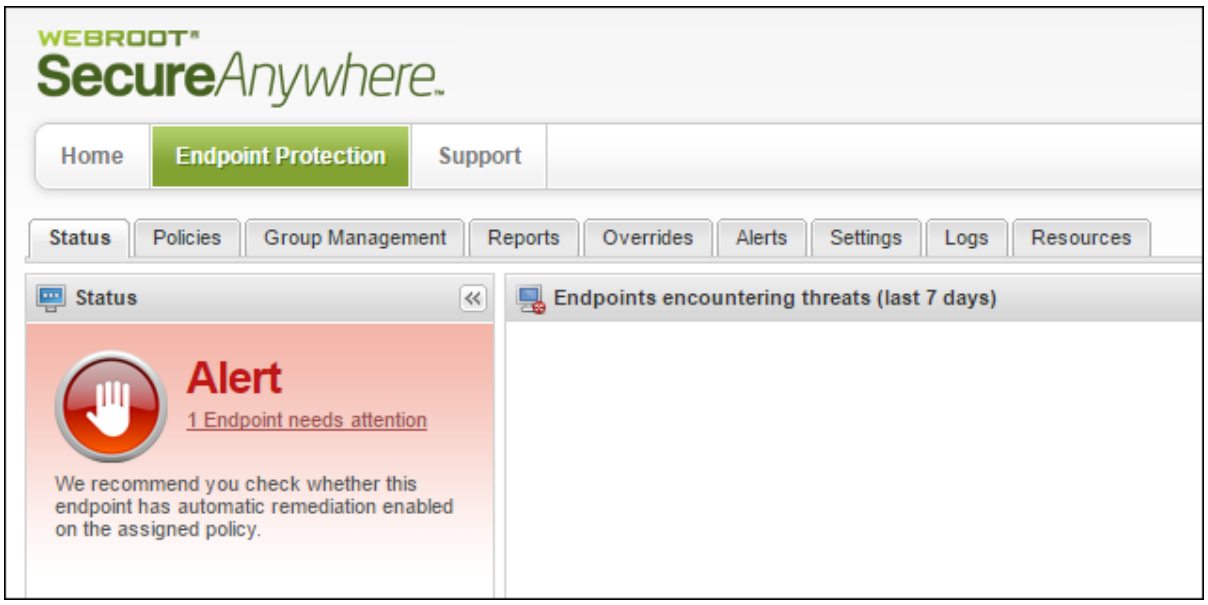
ウェブのオーバーライドの作成

[ウェブのオーバーライド] タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

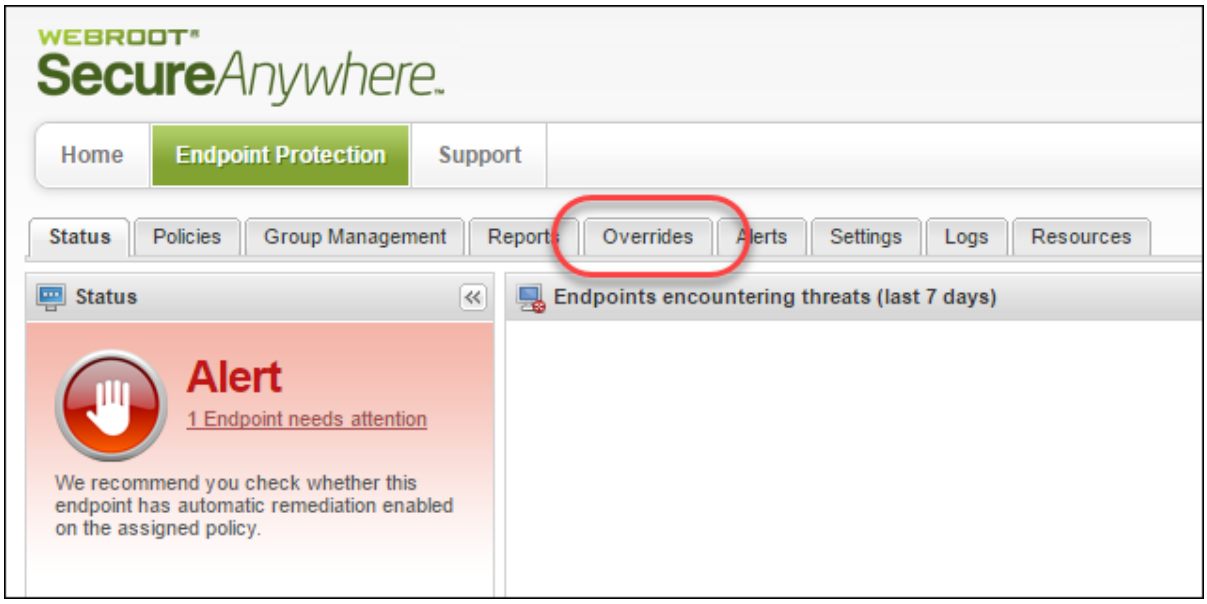
ウェブのオーバーライドを作成するには

1. エンドポイント プロテクションのコンソールにログインします。

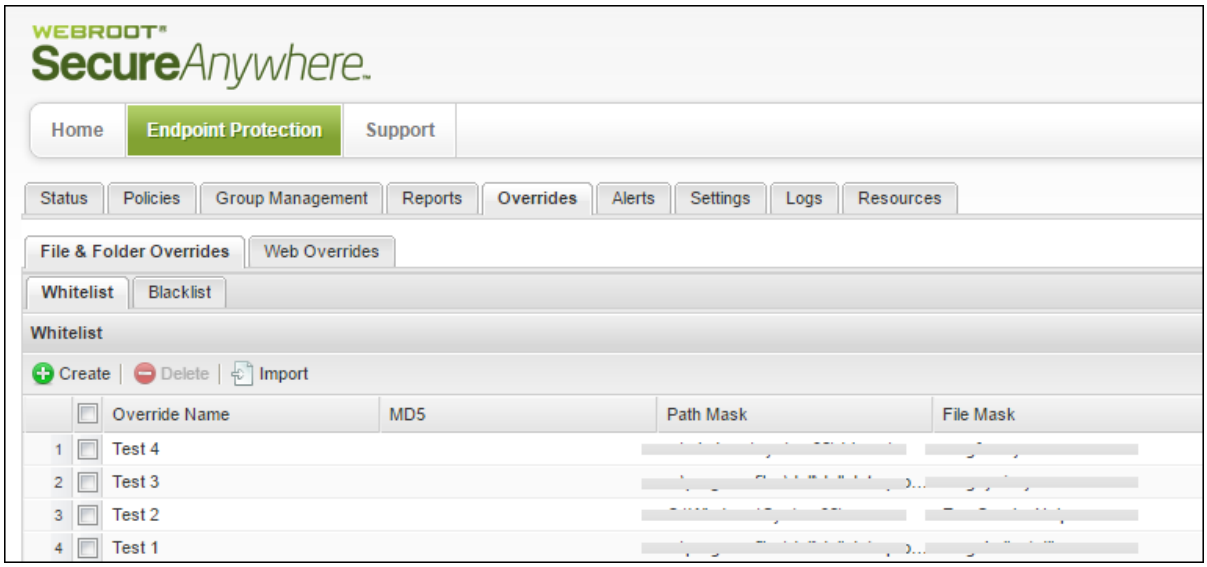
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



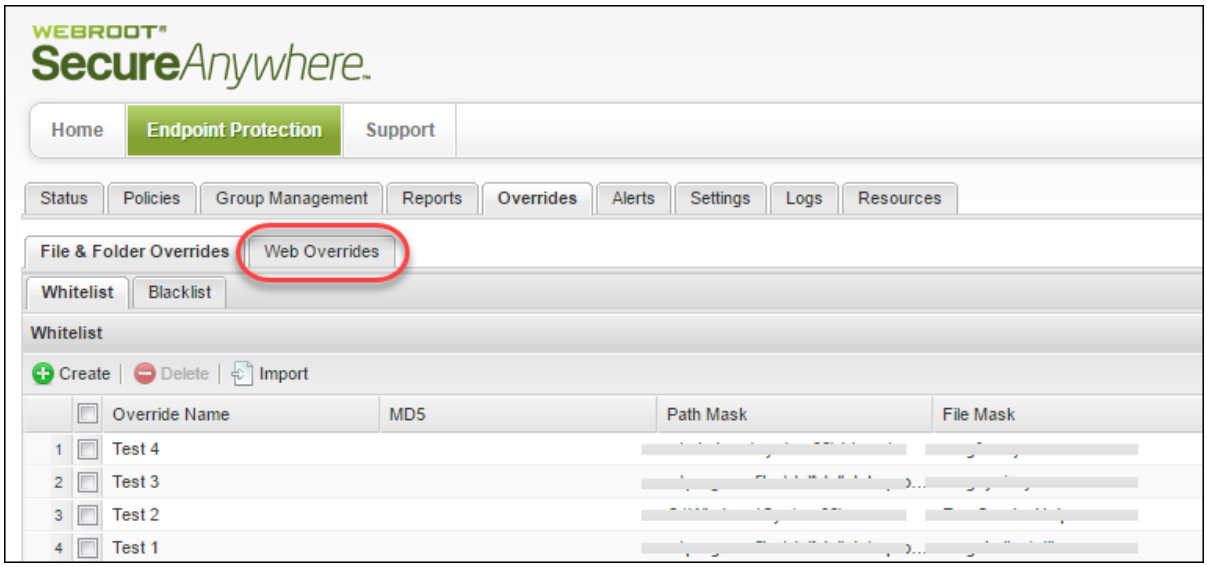
2. [**オーバーライド**] タブをクリックします。



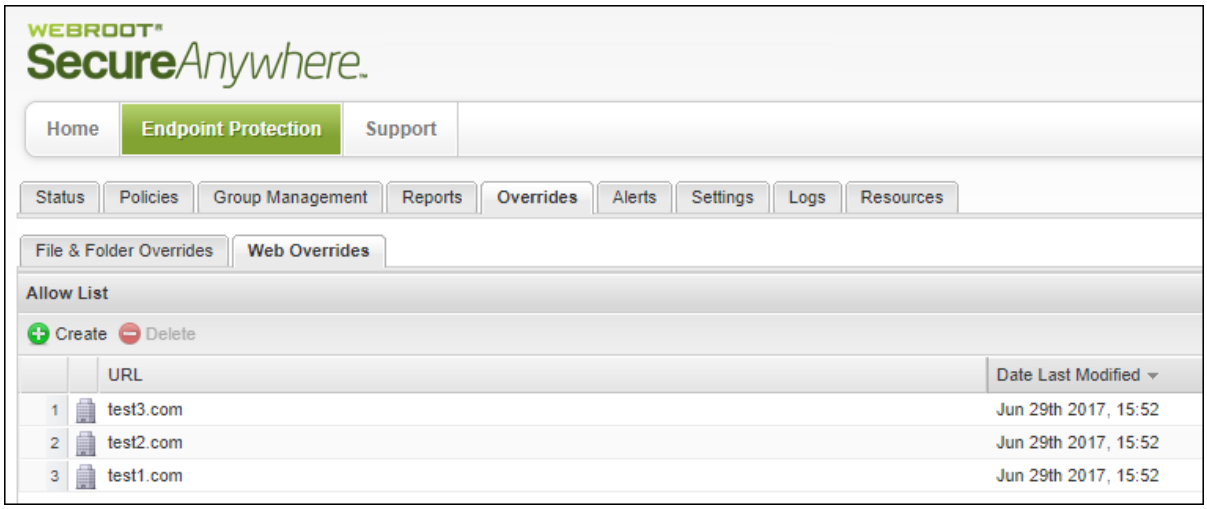
[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。



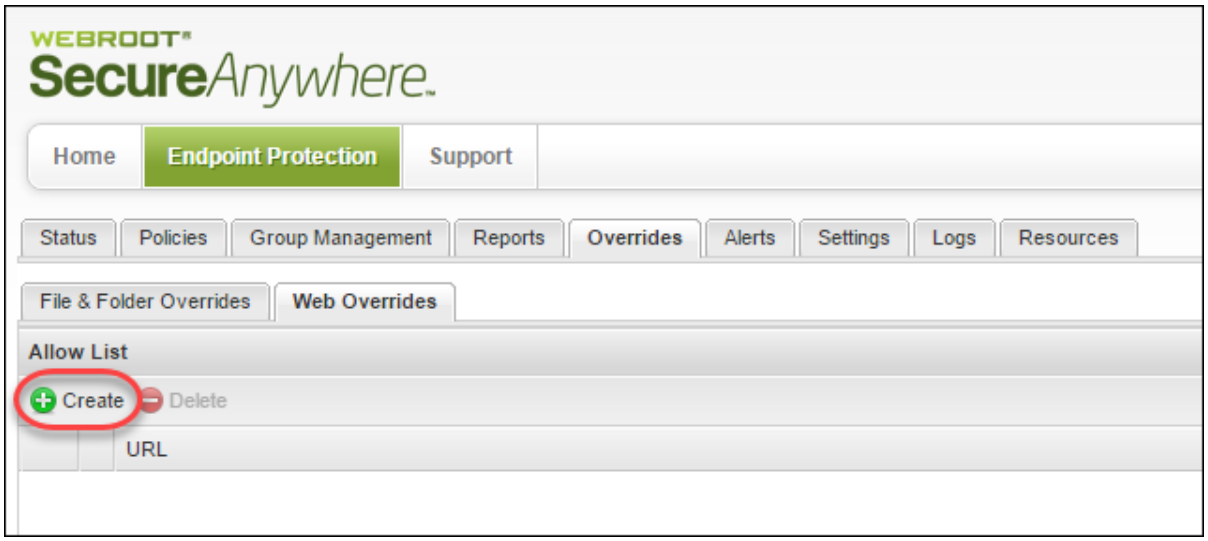
3. [**ウェブのオーバーライド**] タブをクリックします。



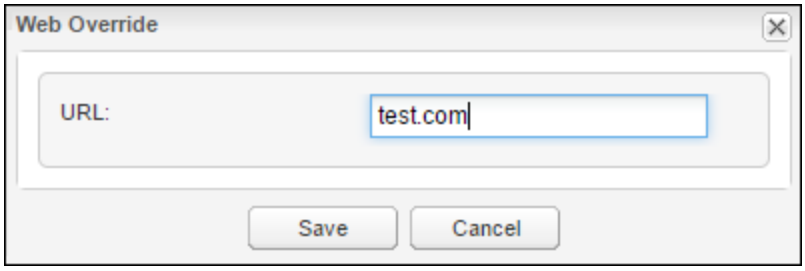
[ウェブのオーバーライド] タブが表示されます。



4. [**作成**] ボタンをクリックします。

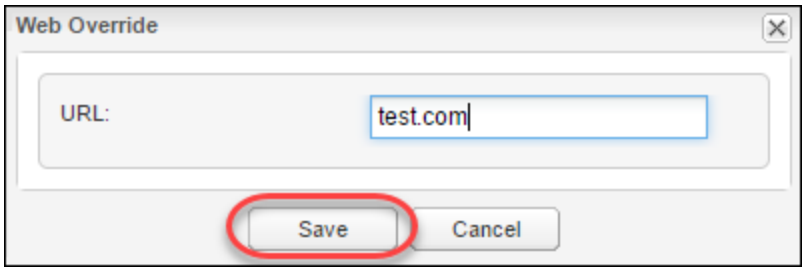


[ウェブのオーバーライド] ウィンドウが表示されます。

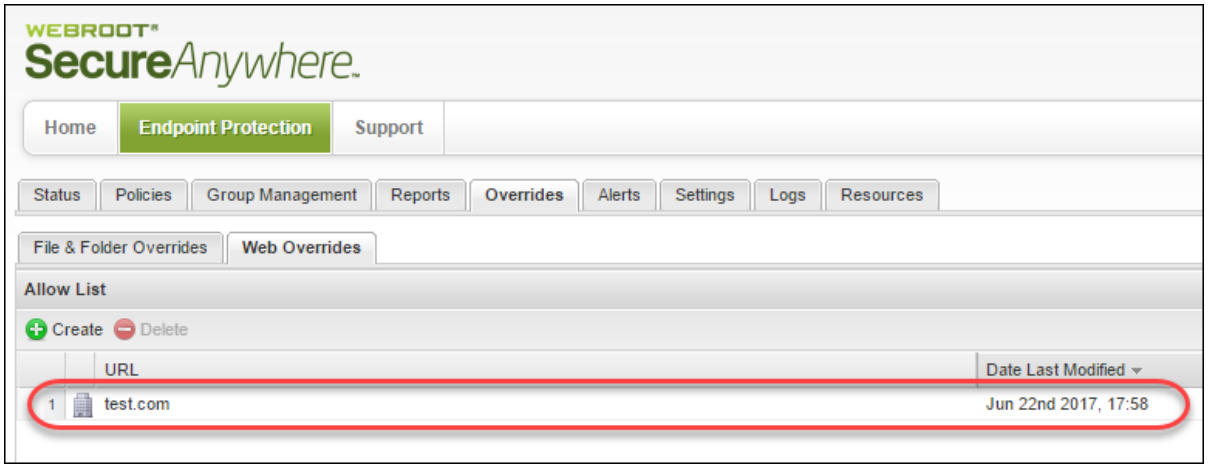


5. [URL] フィールドに、オーバーライドを作成する Web サイトの URL を入力します。

6. 設定が完了したら [**保存**] ボタンをクリックします。.



ウェブのオーバーライドが作成されます。



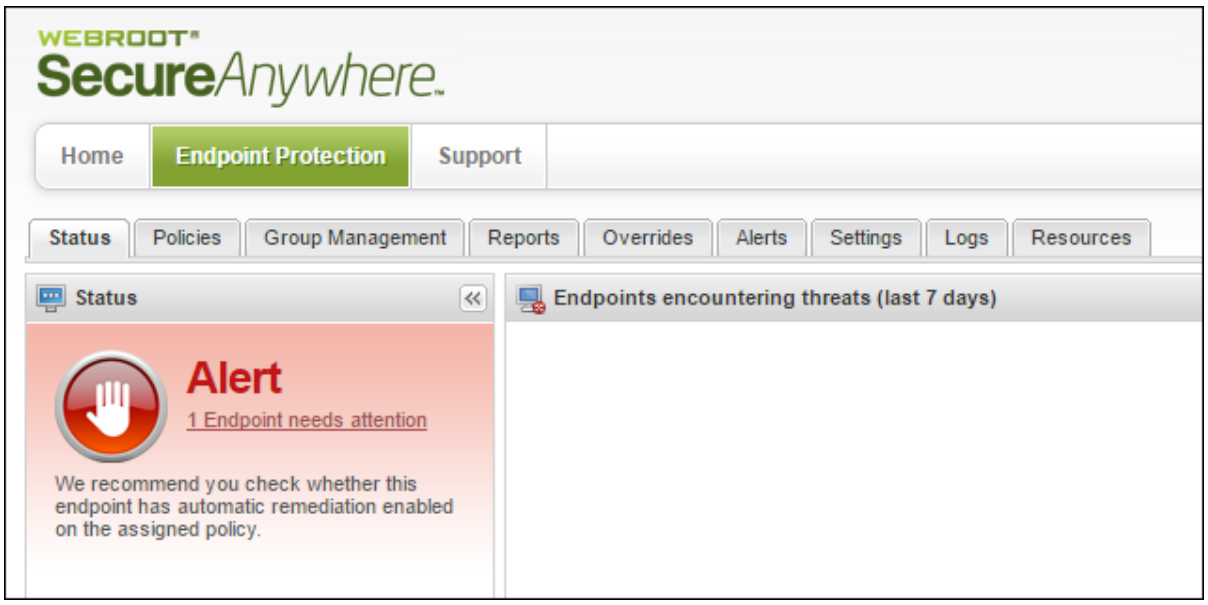
[グループの管理] でのウェブのオーバライドの作成

[グループの管理] タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

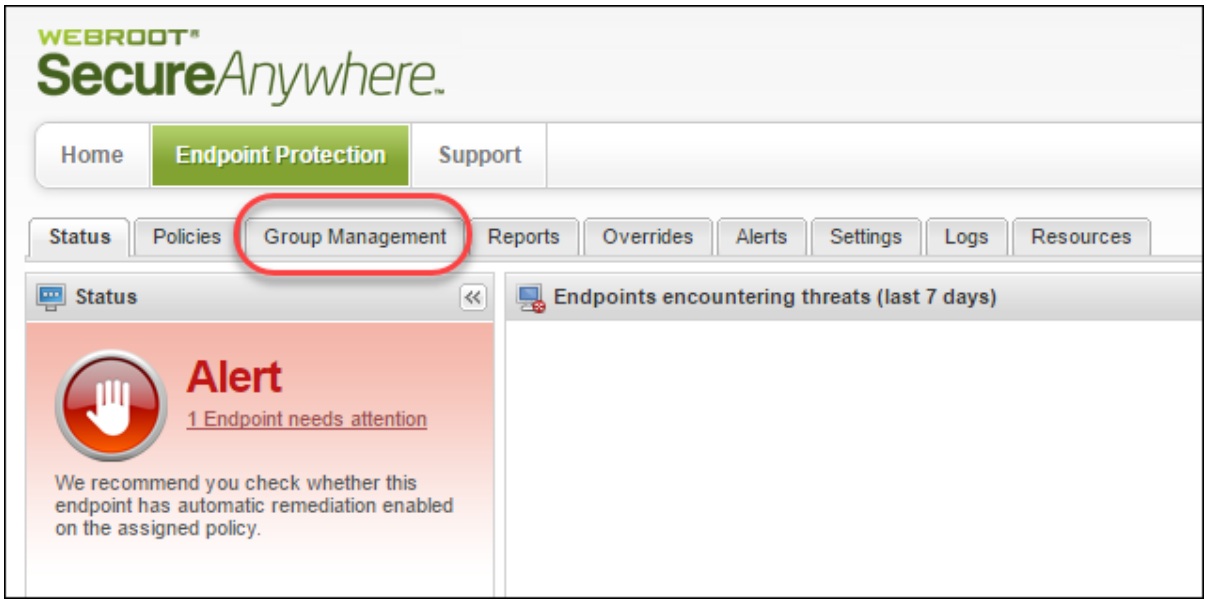
[グループの管理] タブでウェブのオーバーライドを作成するには

1. エンドポイントプロテクションのコンソールにログインします。

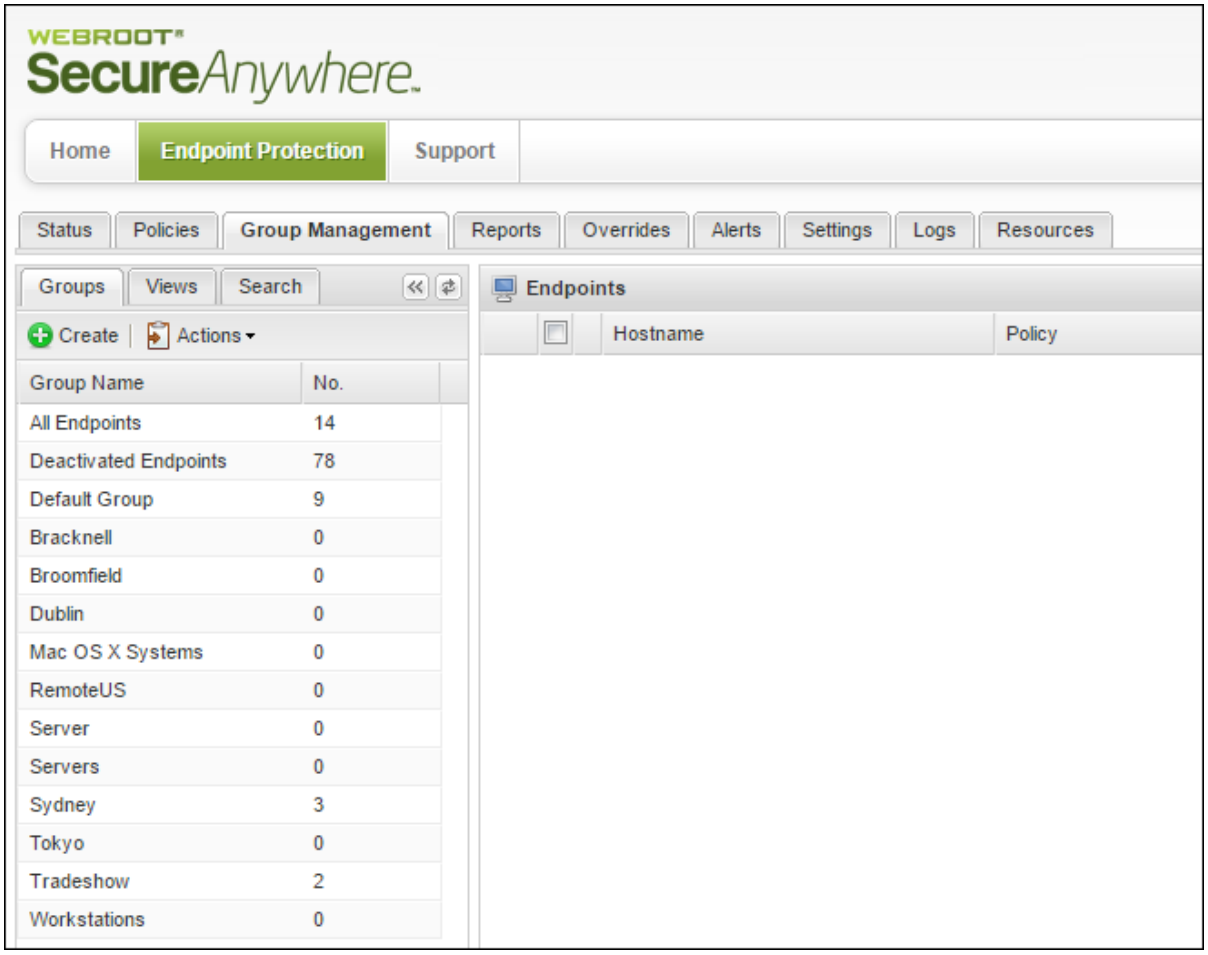
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



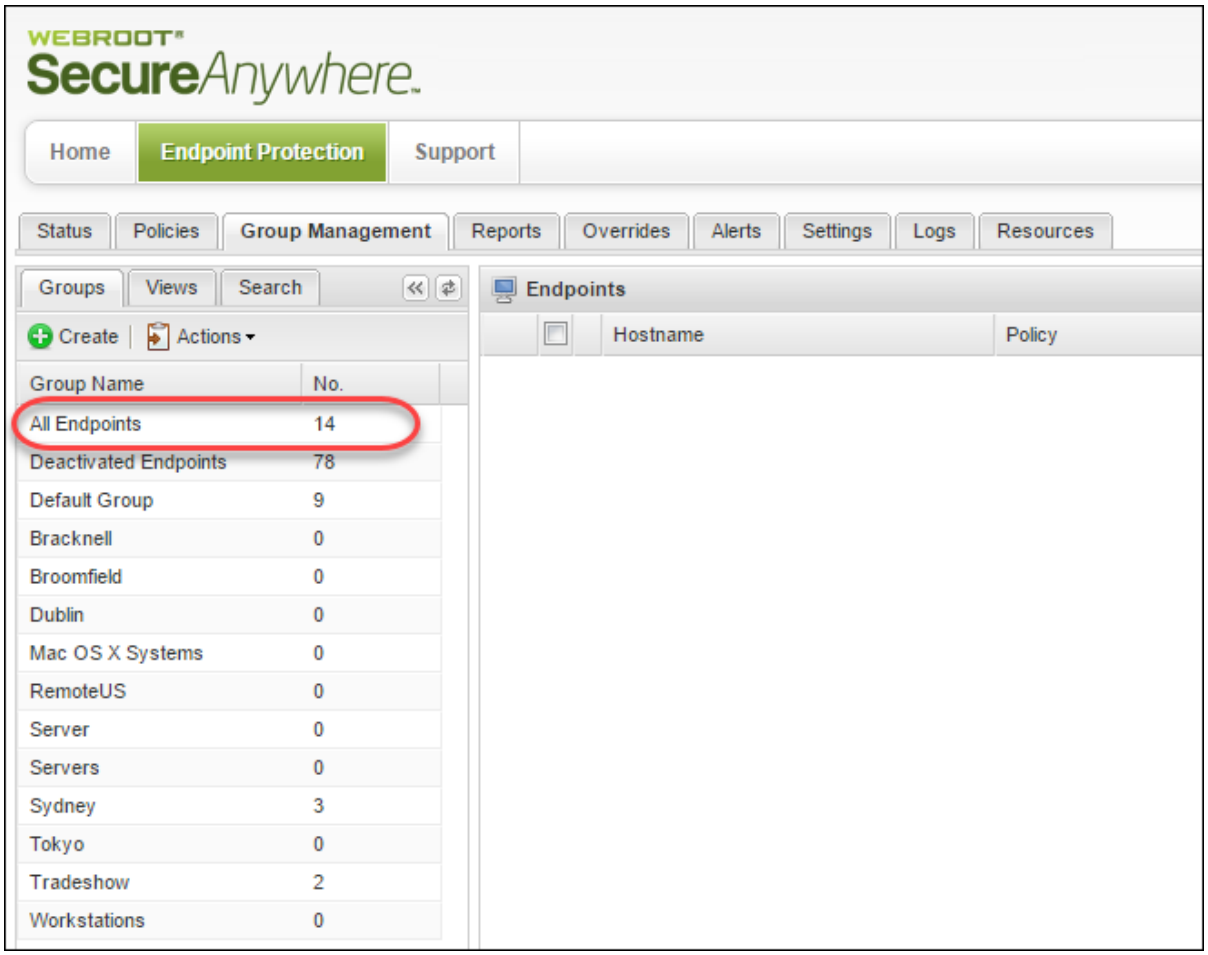
2. [**グループの管理**] タブをクリックします。



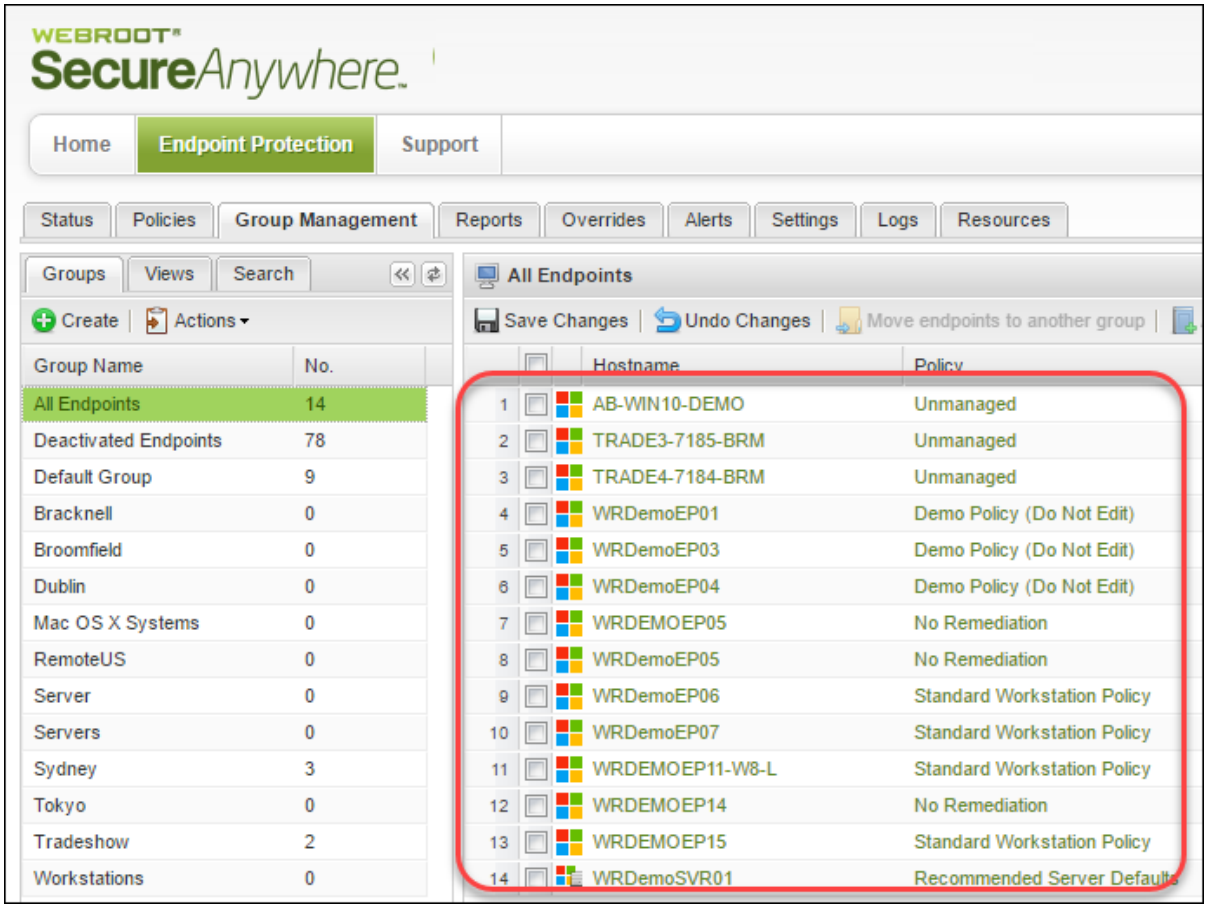
[グループの管理] タブが表示されます。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Support
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Groups
Views
Search
Create
Actions
Group Name
No.
All Endpoints 14
Deactivated Endpoints 78
Default Group 9
Bracknell 0
Broomfield 0
Dublin 0
Mac OS X Systems 0
RemoteUS 0
Server 0
Servers 0
Sydney 3
Tokyo 0
Tradeshow 2
Workstations 0
Endpoints
Hostname
Policy

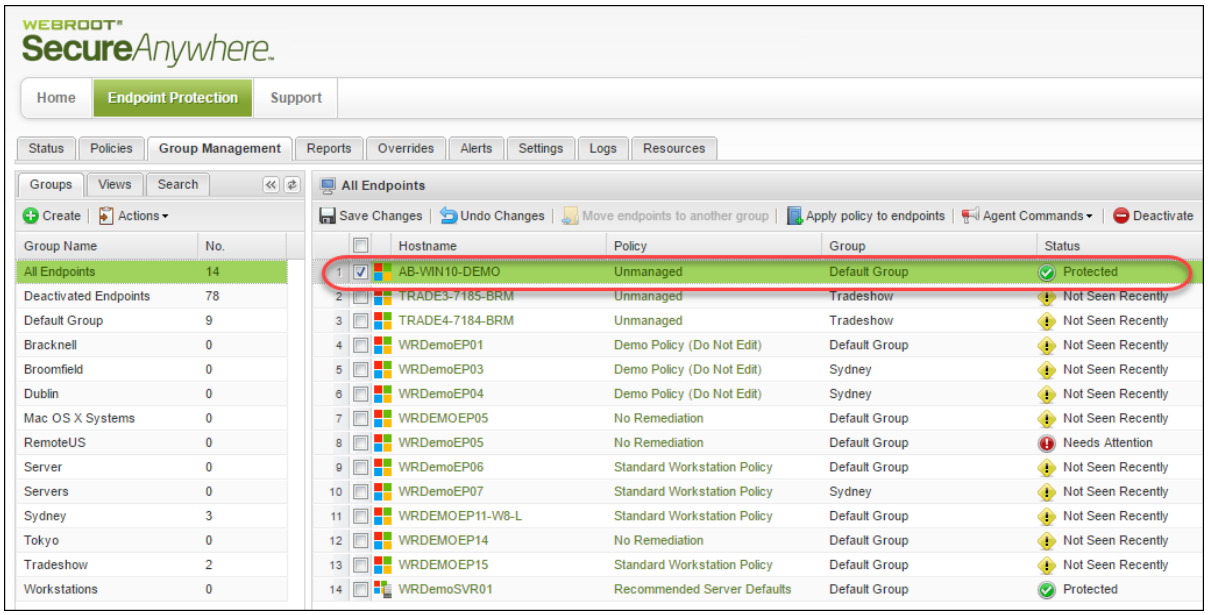
3. [グループ名] カラムで [**すべてのエンドポイント**] を選択します。



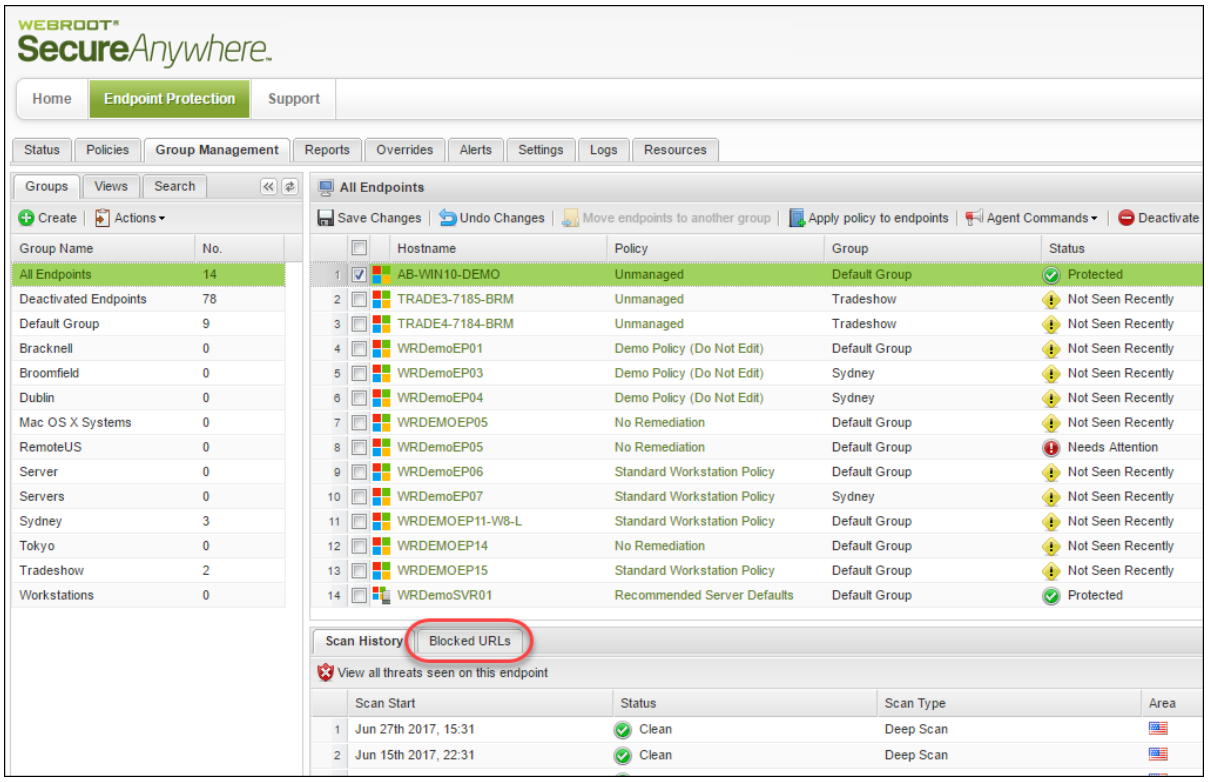
[すべてのエンドポイント] エリアにすべてのエンドポイントが表示されます。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Support
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Groups
Views
Search
Create
Actions
Group Name
No.
All Endpoints 14
Deactivated Endpoints 78
Default Group 9
Bracknell 0
Broomfield 0
Dublin 0
Mac OS X Systems 0
RemoteUS 0
Server 0
Servers 0
Sydney 3
Tokyo 0
Tradeshow 2
Workstations 0
All Endpoints
Save Changes
Undo Changes
Move endpoints to another group
Hostname
Policy
1 AB-WIN10-DEMO Unmanaged
2 TRADE3-7185-BRM Unmanaged
3 TRADE4-7184-BRM Unmanaged
4 WRDemoEP01 Demo Policy (Do Not Edit)
5 WRDemoEP03 Demo Policy (Do Not Edit)
6 WRDemoEP04 Demo Policy (Do Not Edit)
7 WRDEMOEP05 No Remediation
8 WRDemoEP05 No Remediation
9 WRDemoEP06 Standard Workstation Policy
10 WRDemoEP07 Standard Workstation Policy
11 WRDEMOEP11-W8-L Standard Workstation Policy
12 WRDEMOEP14 No Remediation
13 WRDEMOEP15 Standard Workstation Policy
14 WRDemoSVR01 Recommended Server Defaults

4. ウェブのオーバーライドを作成するエンドポイントを選択します。



5. [**ブロックされた URL**] タブをクリックします。



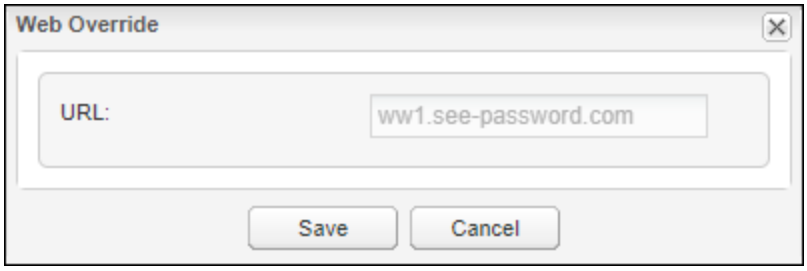
[ブロックされた URL] タブが表示されます。

6. ウェブのオーバーライドを作成する URL を選択します。

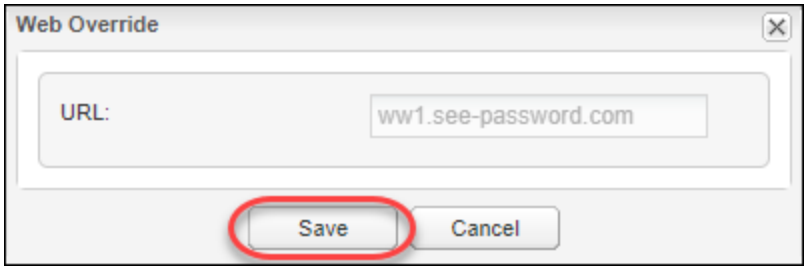
[オーバーライドの作成] アイコンがアクティブになります。

7. [**オーバーライドの作成**] アイコンをクリックします。

[ウェブのオーバーライド] ウィンドウが表示されます。[URL] フィールドには選択した URL が表示されています。



8. [**保存**] ボタンをクリックします。



URL が許可リストに追加されます。

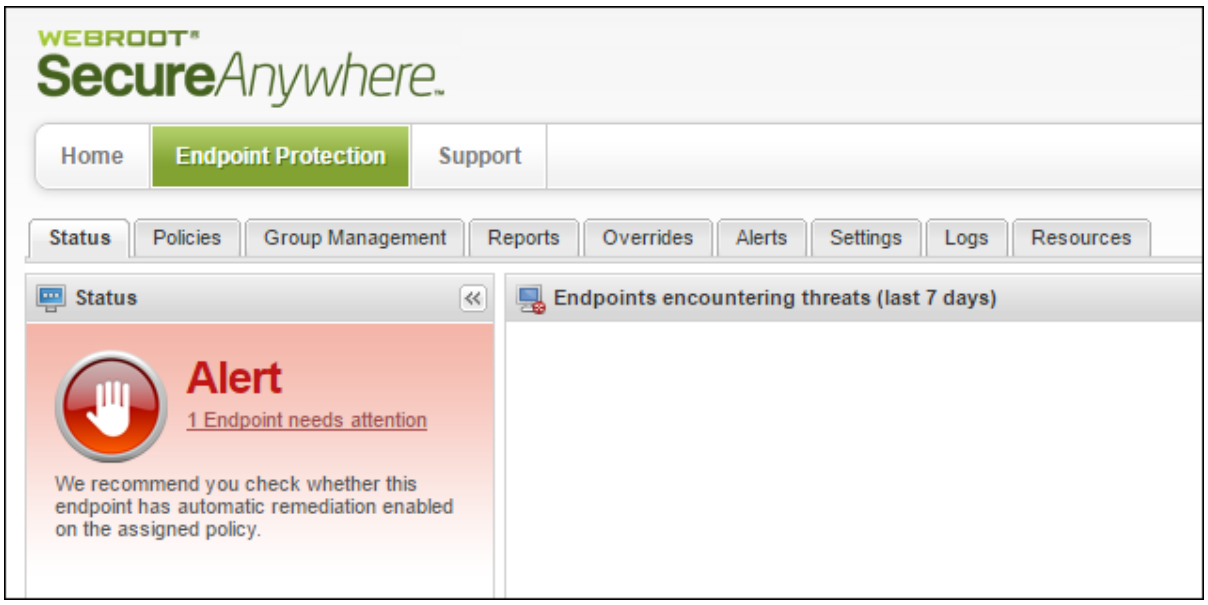
[レポート] でのウェブのオーバライドの作成

[レポート] タブでウェブのオーバーライドを作成するには、次の手順に従ってください。

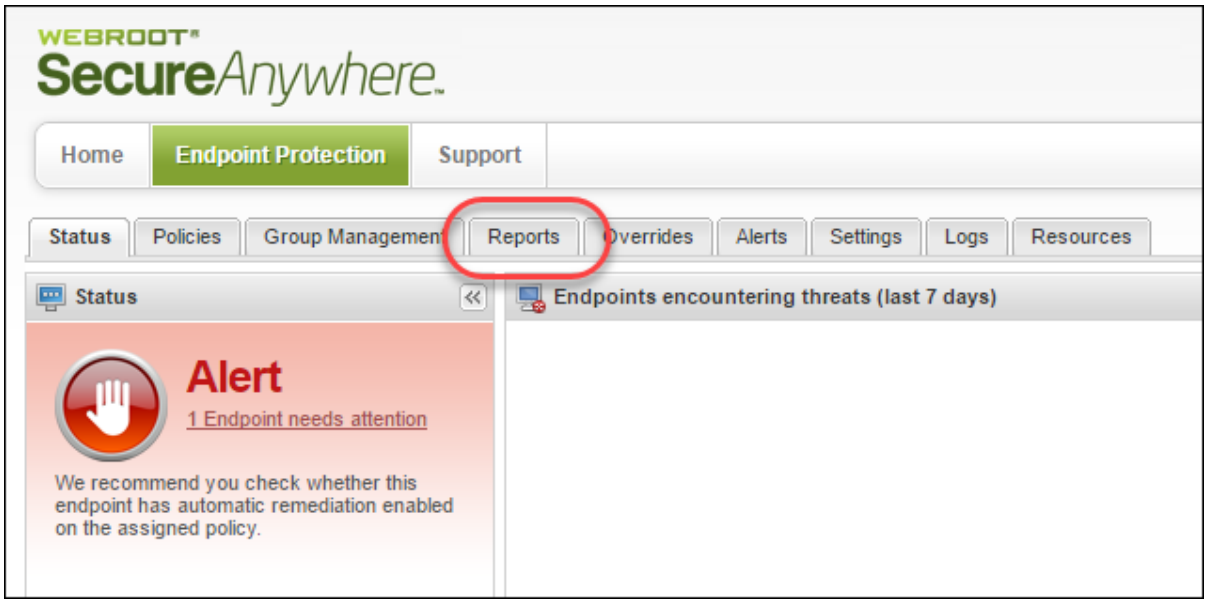
[レポート] タブでウェブのオーバーライドを作成するには

1. エンドポイント プロテクションのコンソールにログインします。

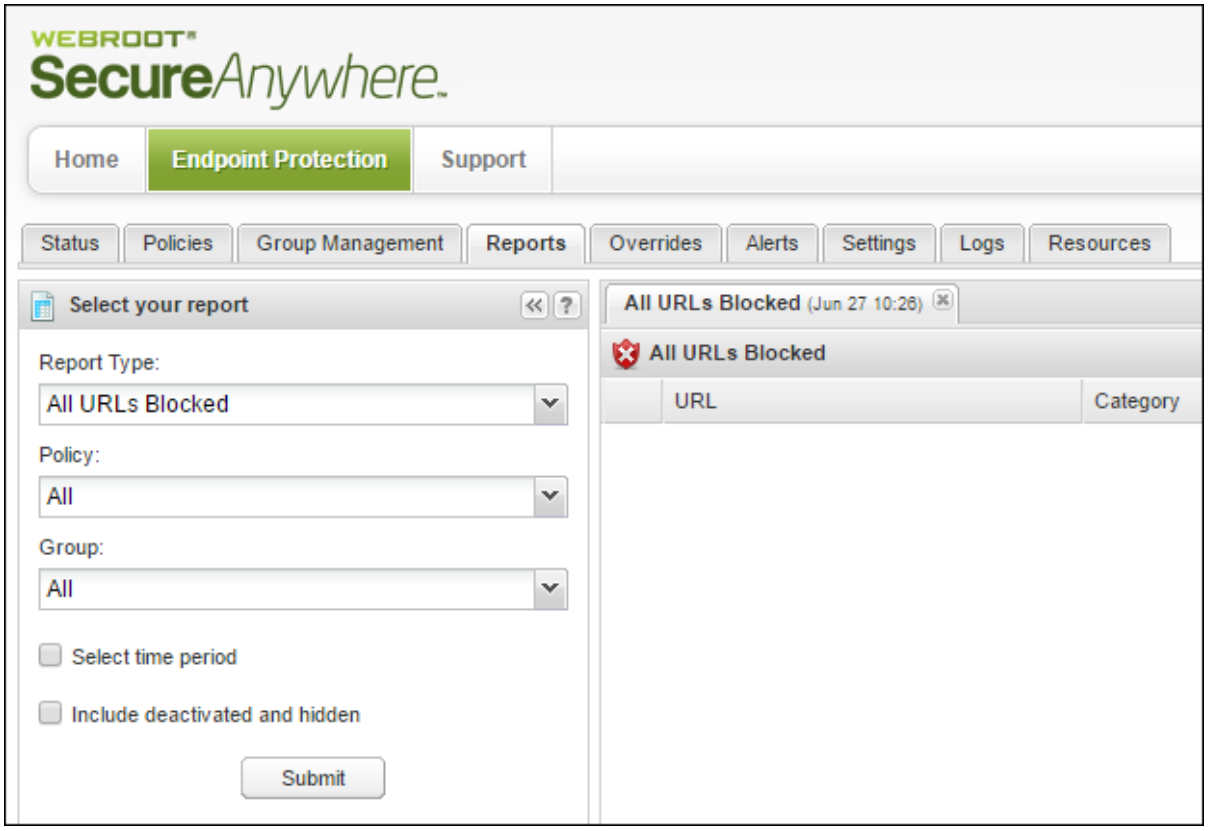
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



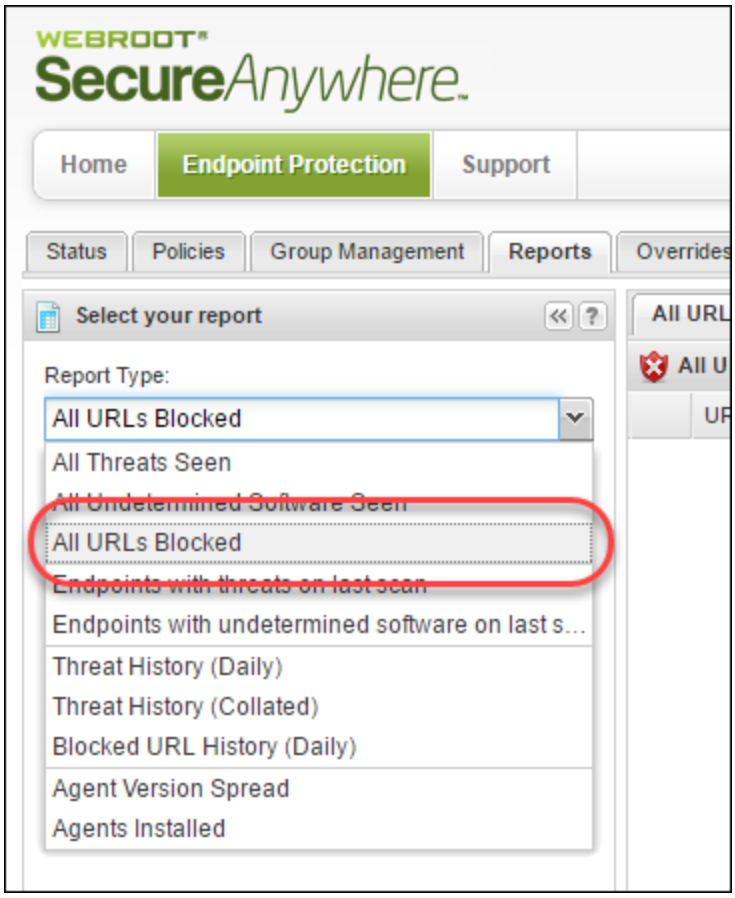
2. [**レポート**] タブをクリックします。



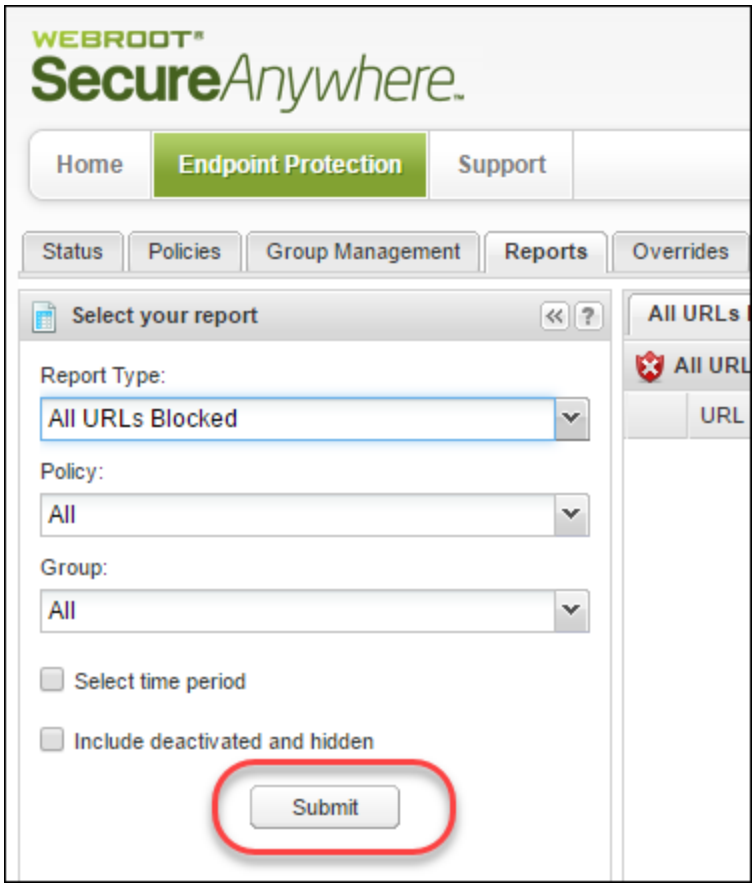
[レポート] タブが表示されます。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Support
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Select your report
Report Type:
All URLs Blocked
Policy:
All
Group:
All
Select time period
Include deactivated and hidden
Submit
All URLs Blocked (Jun 27 10:26)
All URLs Blocked
URL
Category

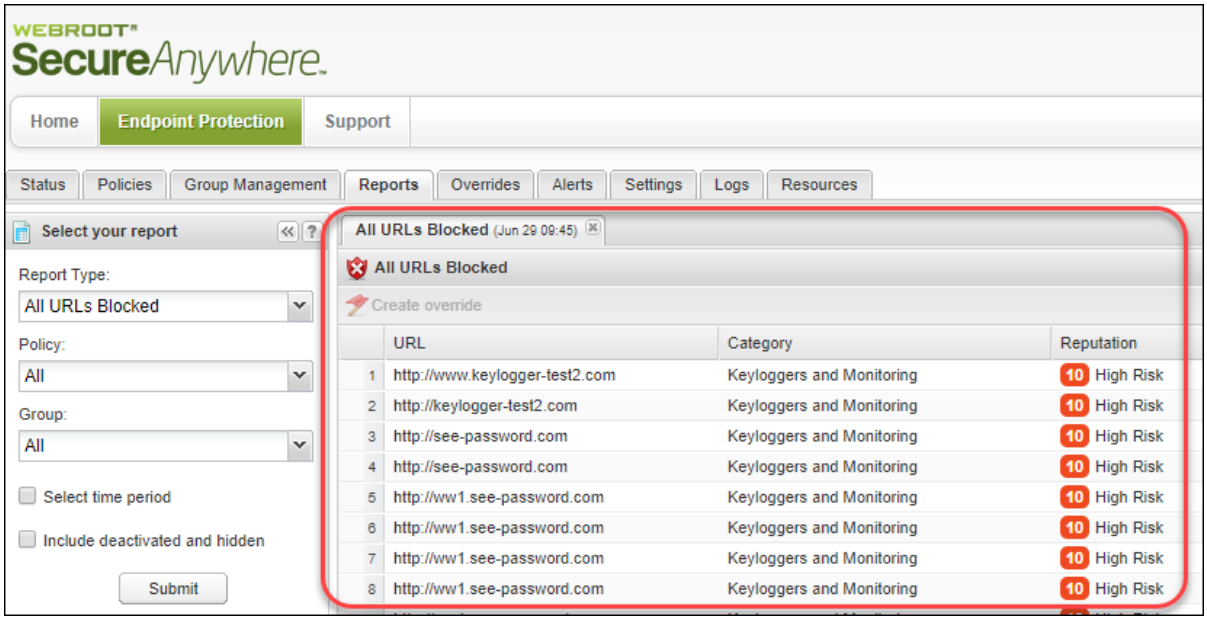
3. [レポートの種類] ドロップダウンメニューで [**ブロックされたすべての URL**] を選択します。



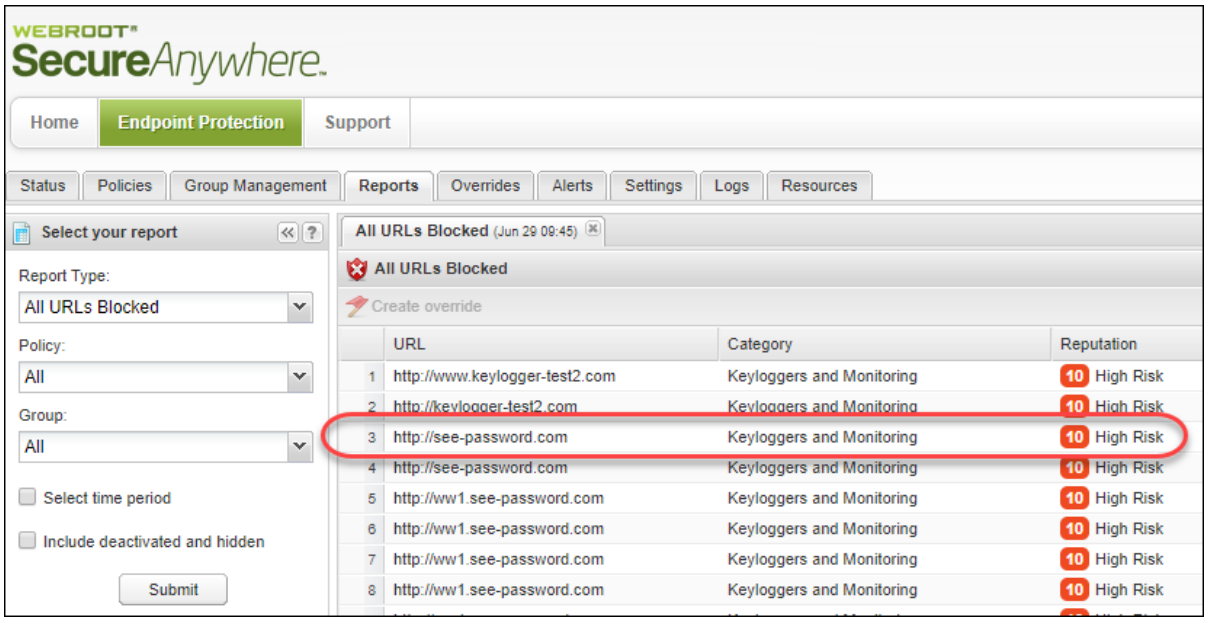
4. [**送信**] ボタンをクリックします。



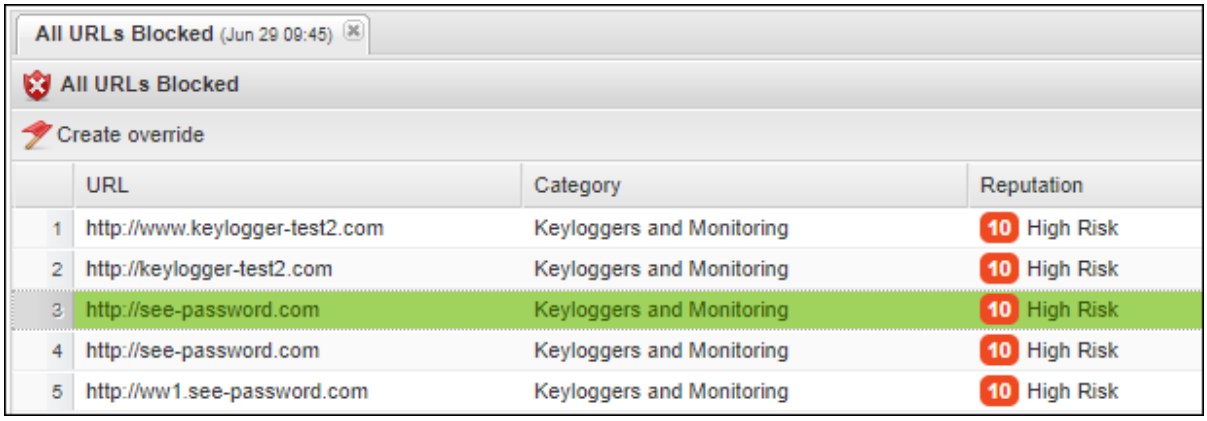
[ブロックされたすべての URL] エリアに、ブロックされた URL のリストが表示されます。



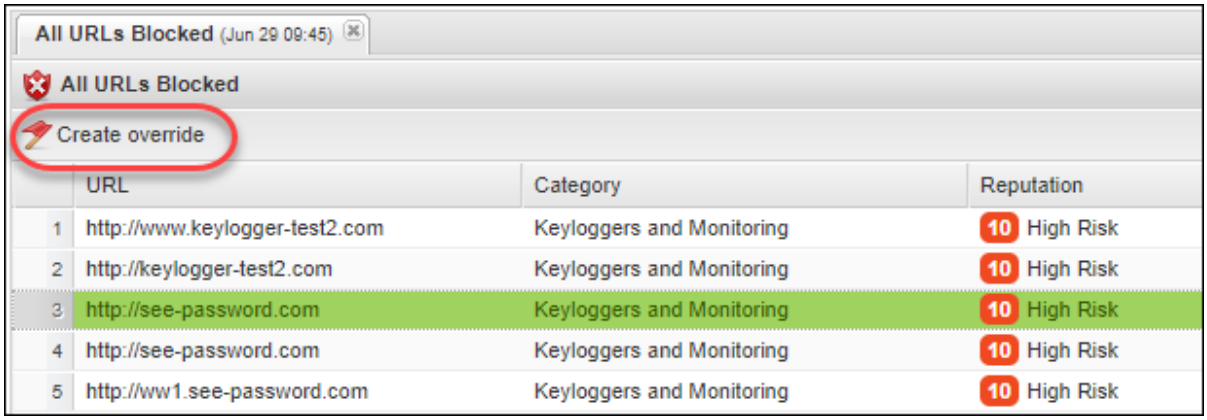
5. [ブロックされたすべての URL] エリアで、許可する URL を選択します。



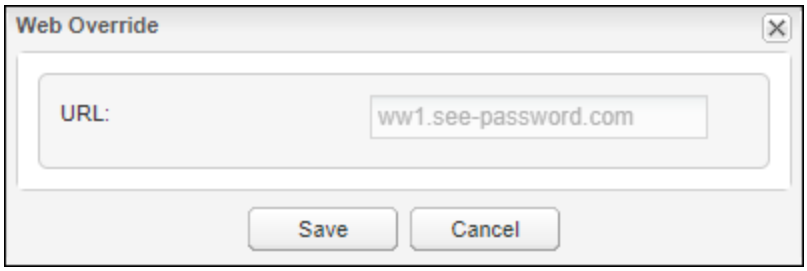
[オーバーライドの作成] アイコンがアクティブになります。



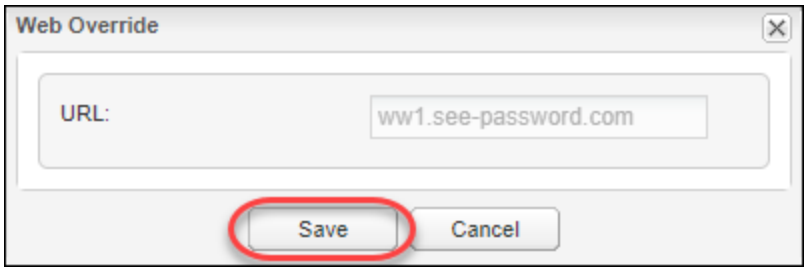
6. [**オーバーライドの作成**] アイコンをクリックします。



選択した URL が表示された状態の [オーバーライドの作成] ウィンドウが表示されます。



7. **保存**] ボタンをクリックします。



URL が許可リストに追加されます。

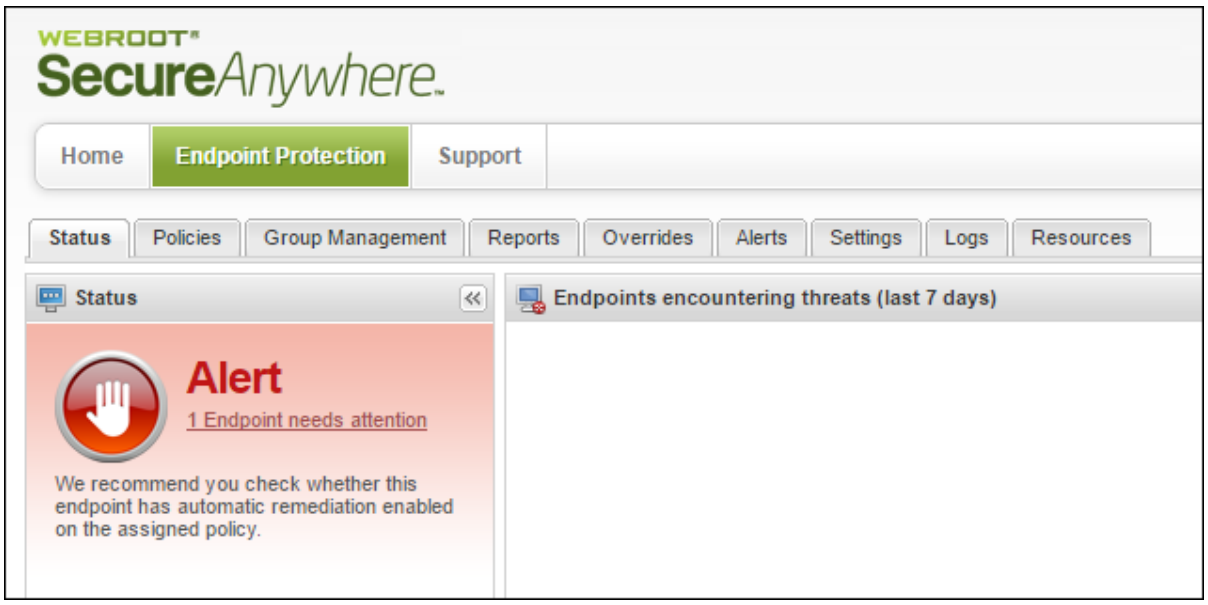
ウェブのオーバーライドの編集

ウェブのオーバーライドを編集するには、次の手順に従ってください。

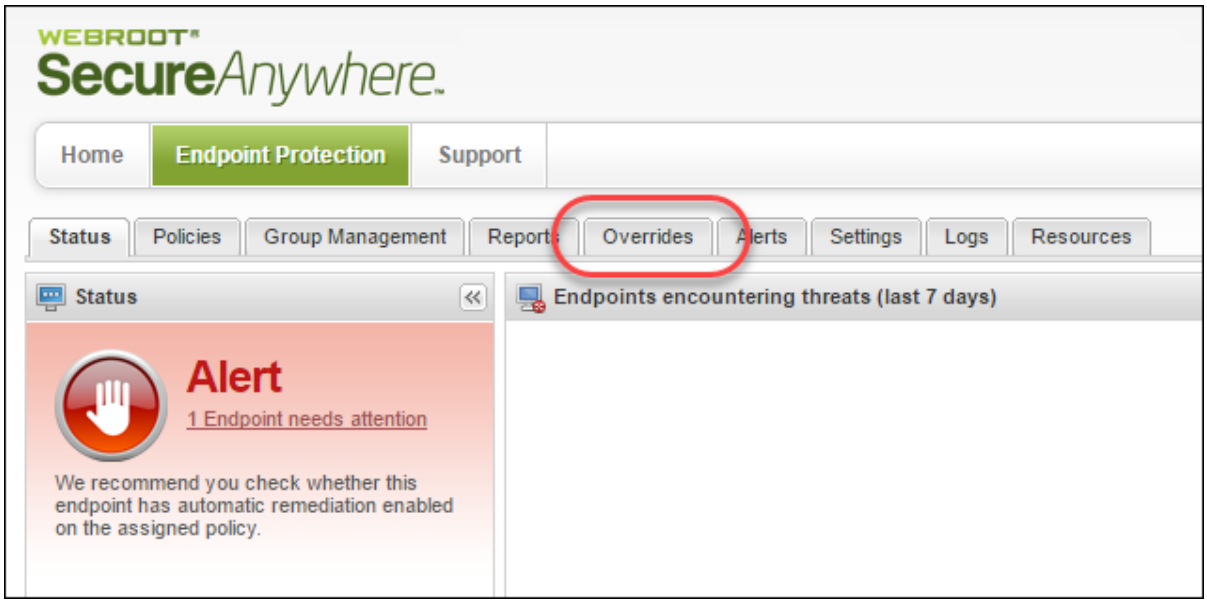
ウェブのオーバーライドを編集するには

1. エンドポイント プロテクションのコンソールにログインします。

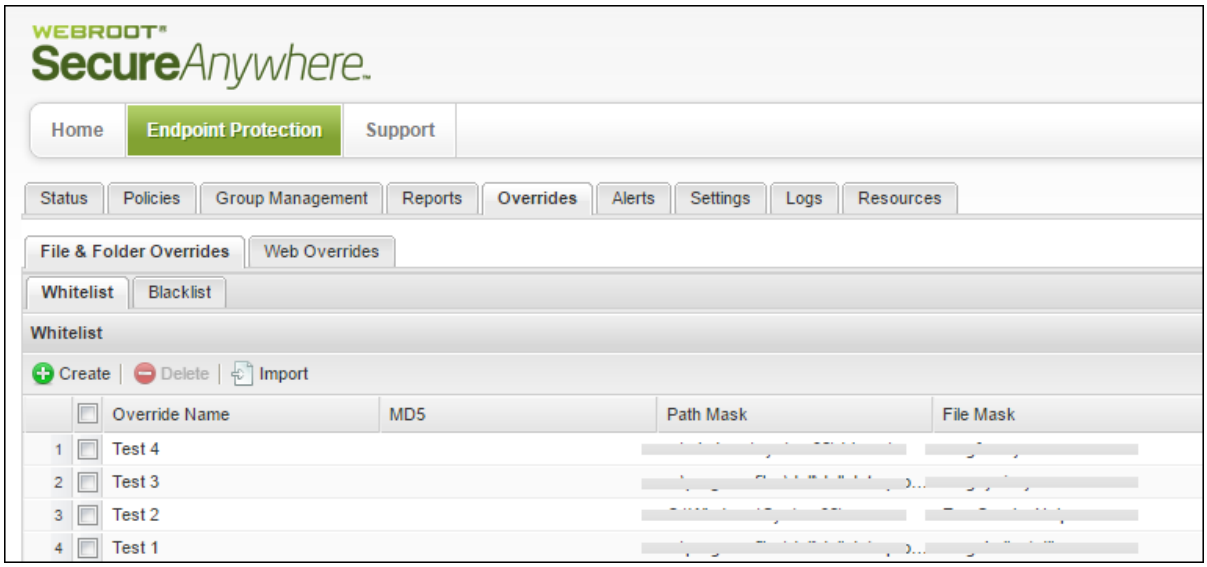
   [状態] タブがアクティブになった状態でエンドポイント プロテクションのコンソールが表示されます。



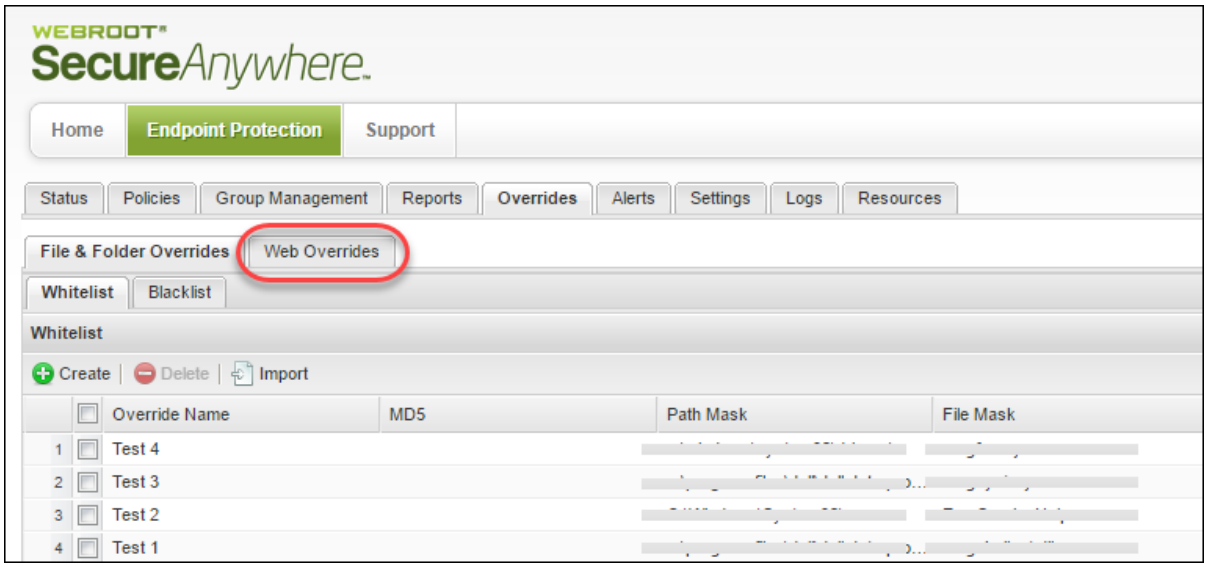
2. [**オーバーライド**] タブをクリックします。



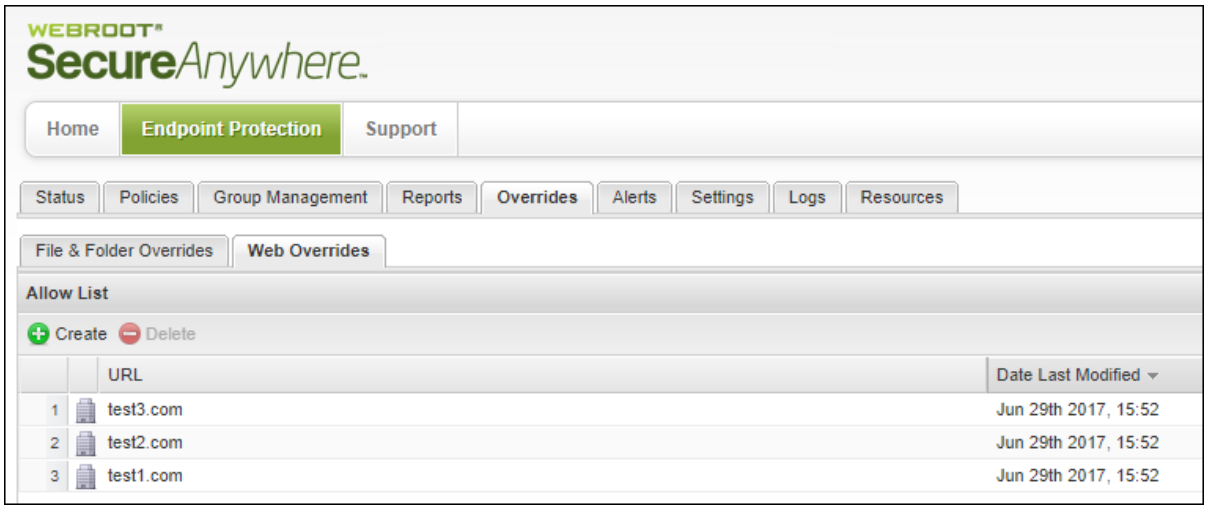
[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。



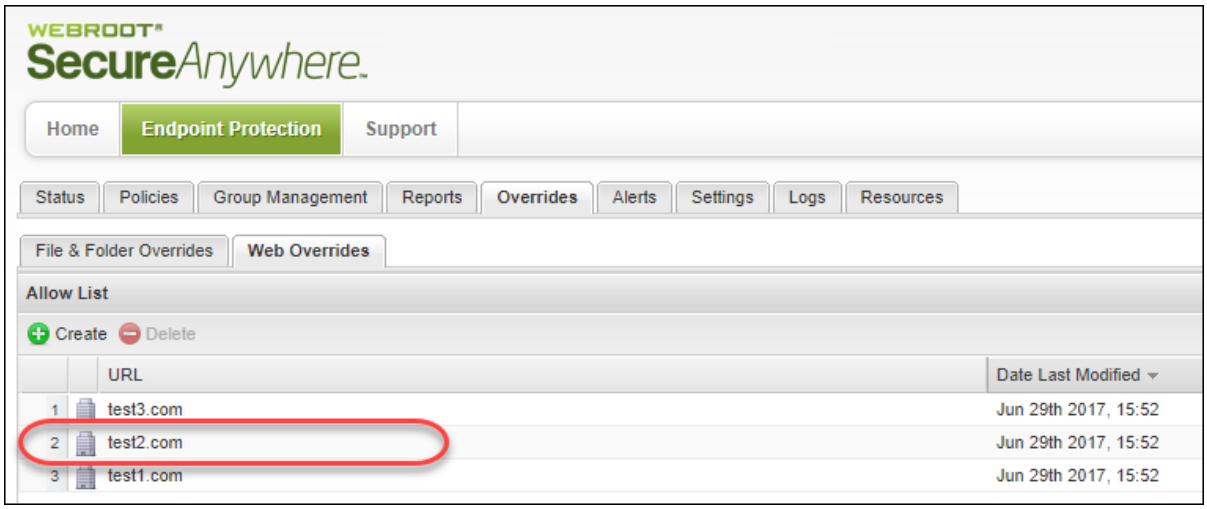
3. [**ウェブのオーバーライド**] タブをクリックします。



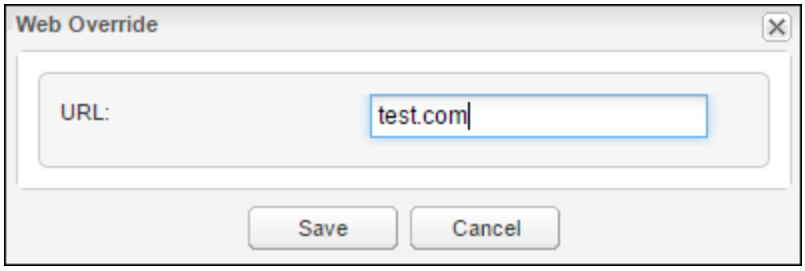
[ウェブのオーバーライド] タブが表示されます。



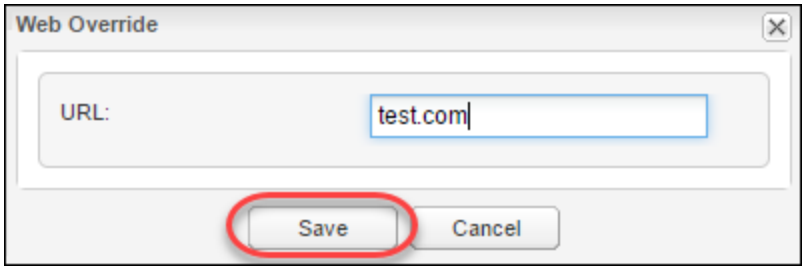
4. [許可リスト] で、編集するウェブのオーバーライドを選択し、ダブルクリックします。



[ウェブのオーバーライド] ウィンドウが表示されます。



5. 必要に応じて、ウェブのオーバーライドを編集します。
6. 設定が完了したら [**保存**] ボタンをクリックします。



編集内容が保存されます。

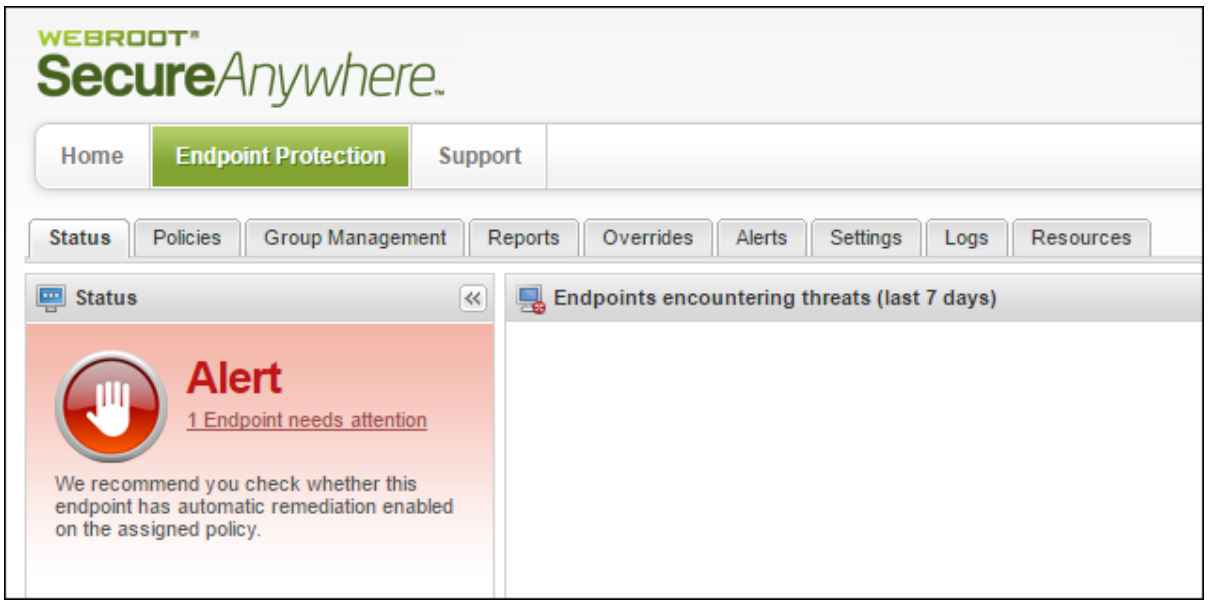
ウェブのオーバーライドの削除

ウェブのオーバーライドを削除するには、次の手順に従ってください。

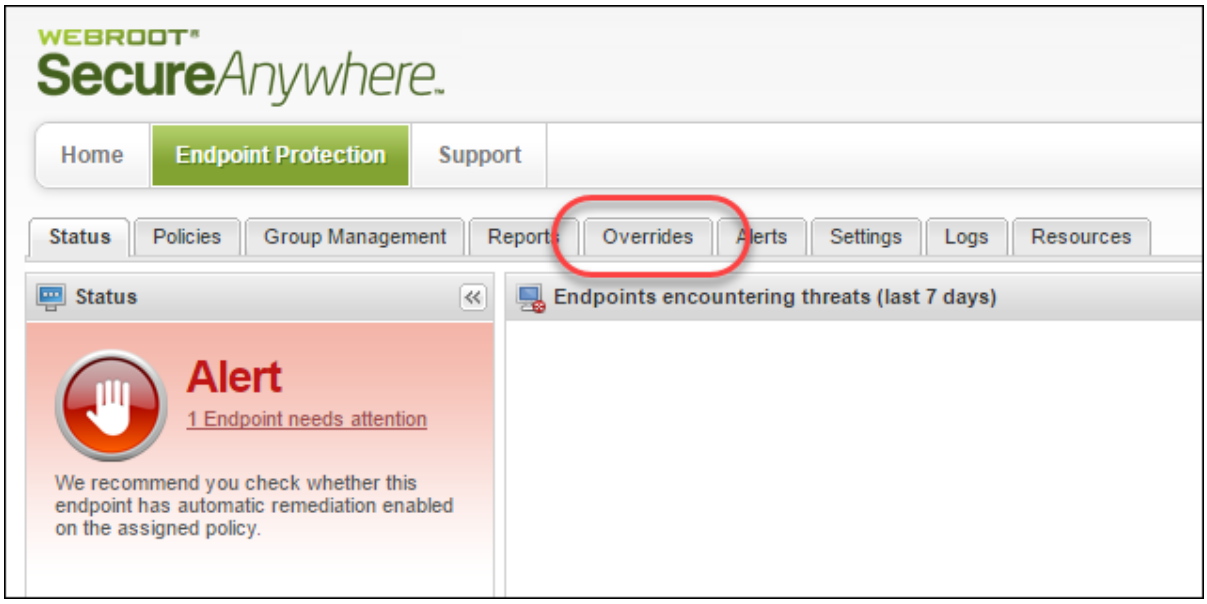
ウェブのオーバーライドを削除するには

1. エンドポイントプロテクションのコンソールにログインします。

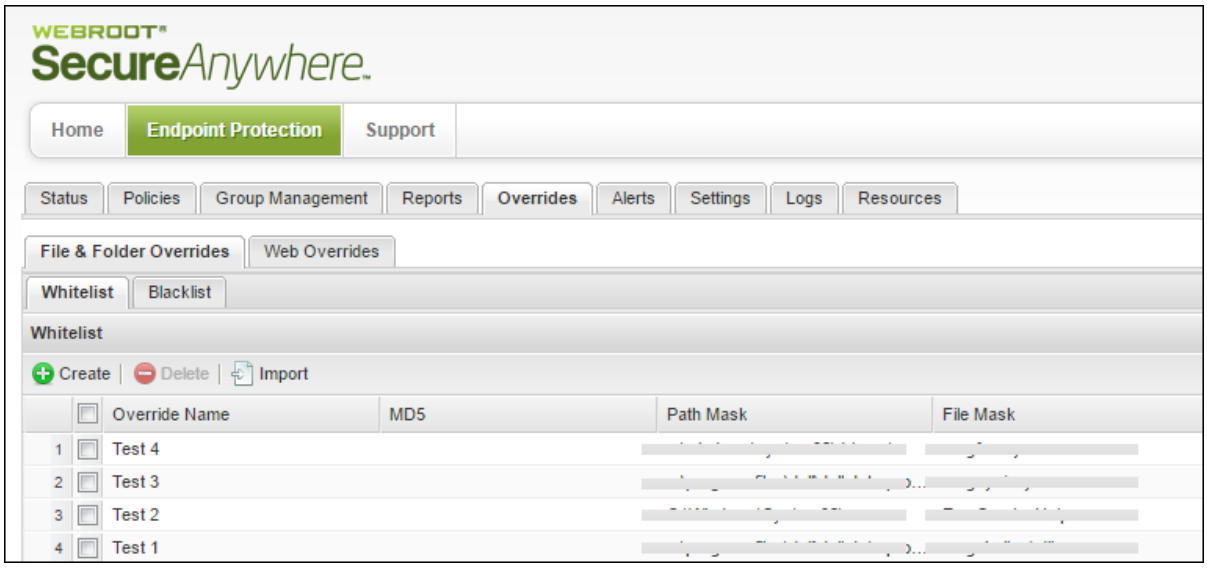
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのコンソールが表示されます。



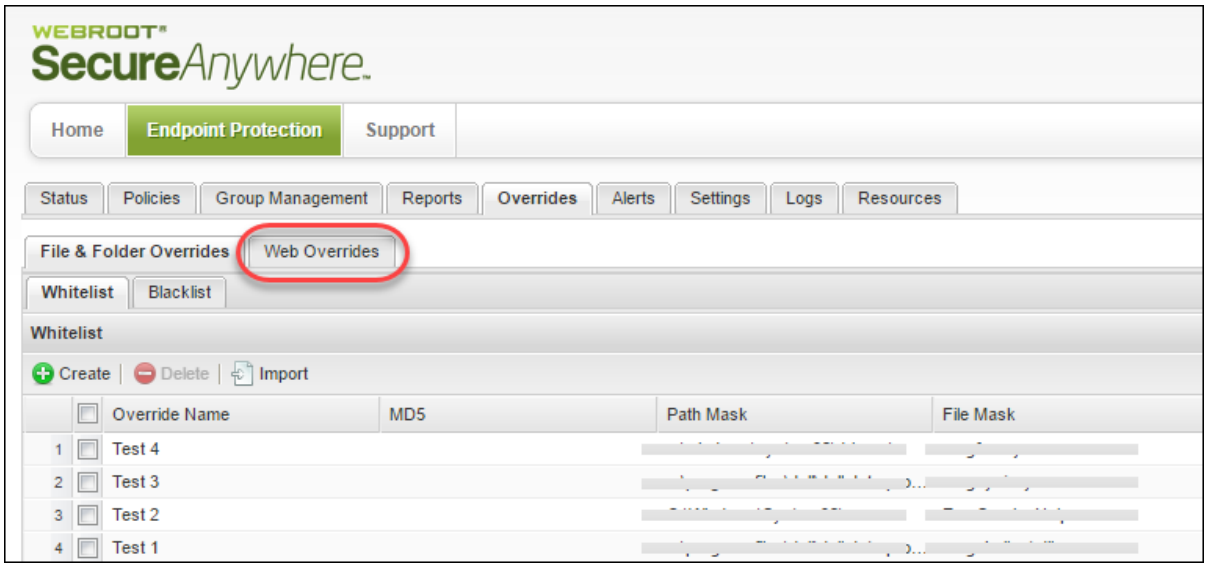
2. [**オーバーライド**] タブをクリックします。.



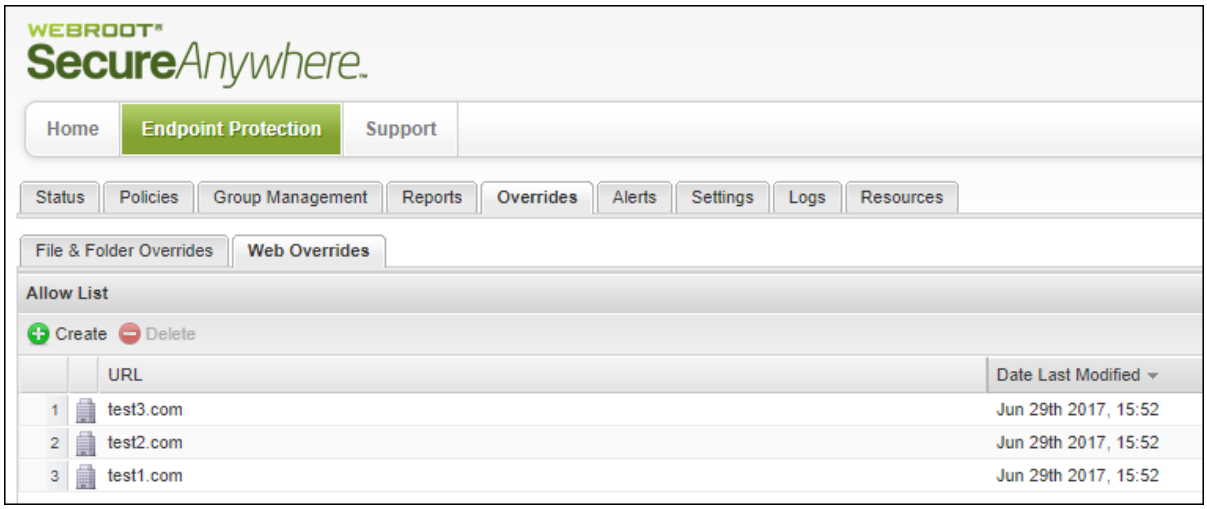
[ファイル / フォルダのオーバーライド] タブがアクティブになった [オーバーライド] タブが表示されます。



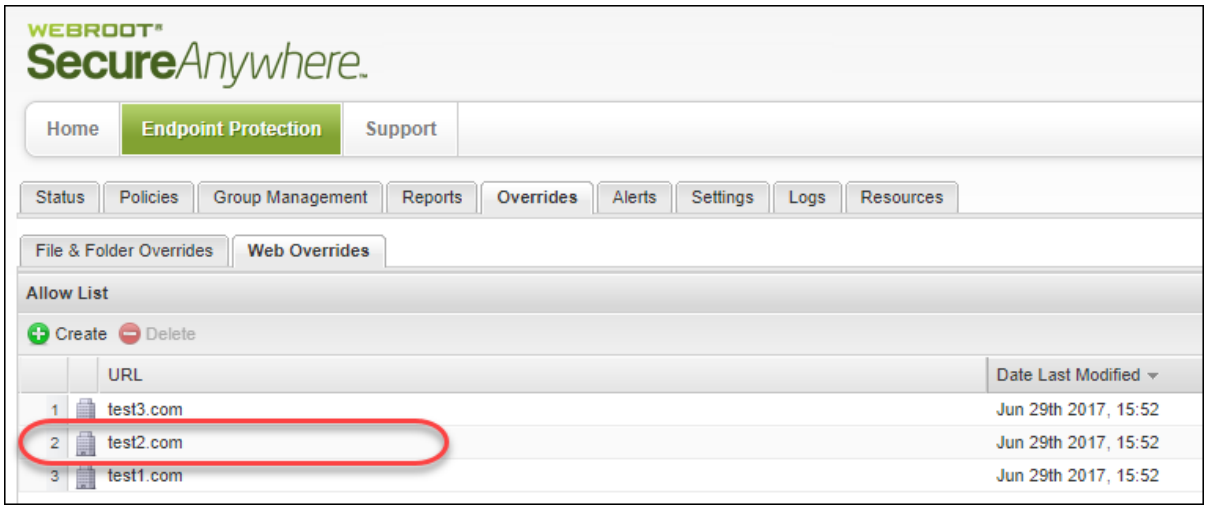
3. [**ウェブのオーバーライド**] タブをクリックします。



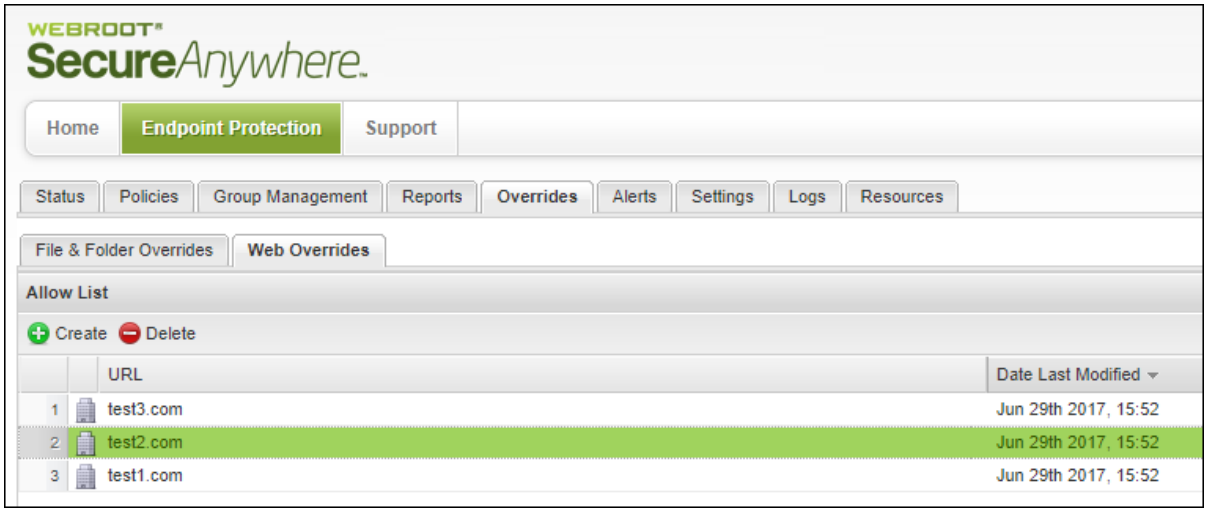
[ウェブのオーバーライド] タブが表示されます。



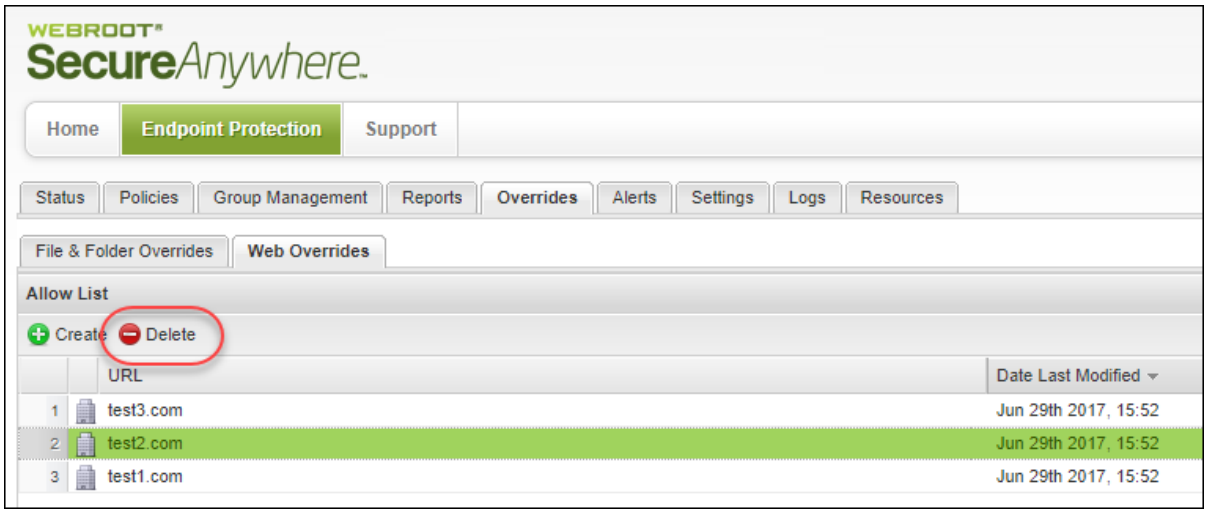
4. [許可リスト] エリアで、削除するウェブのオーバーライドを選択します。



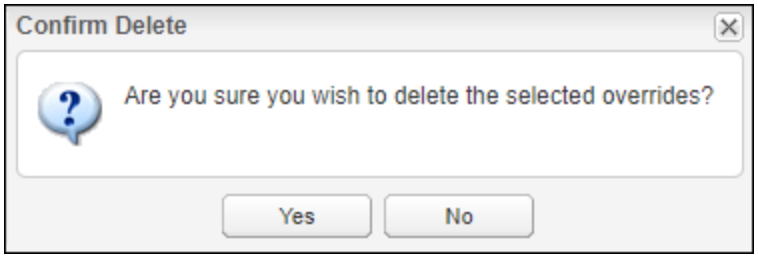
[削除] アイコンがアクティブになります。



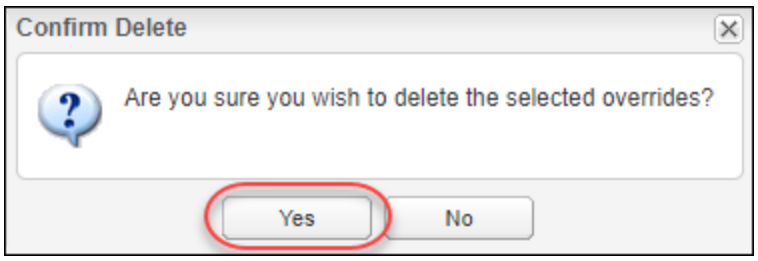
5. [**削除**] アイコンをクリックします。



確認メッセージが表示されます。



6. [**はい**] ボタンをクリックします。



ウェブのオーバーライドがシステムから削除されます。

第 12 章: 設定の管理

設定の管理方法については、以下のトピックを参照してください。

データフィルタの設定

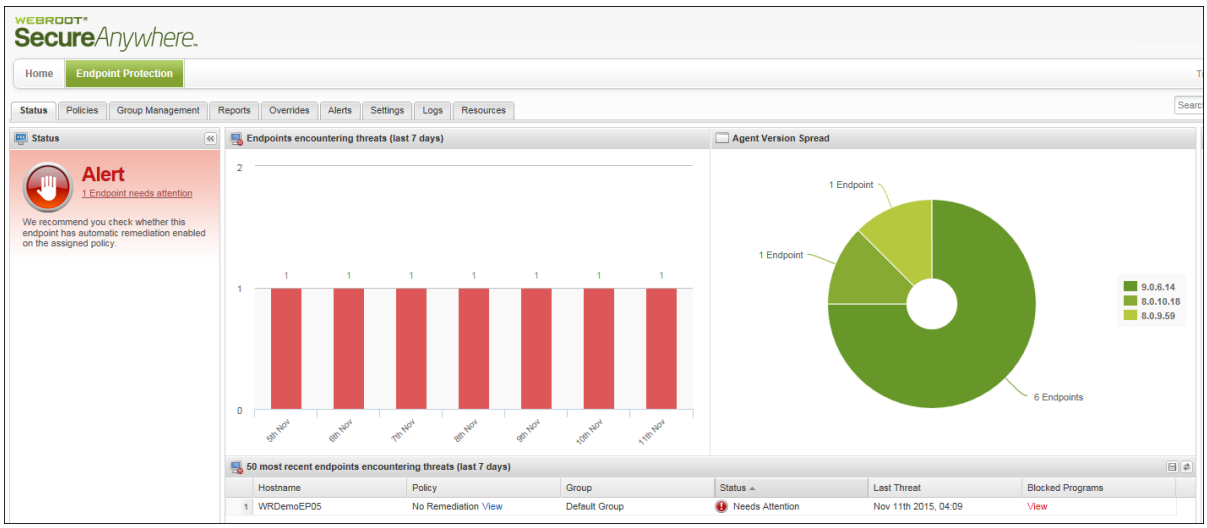
エンドポイントプロテクションの管理コンソールでは、一定の期間中に確認されていないエンドポイントをデータから削除して、サイトの現状について最も正確なデータを表示することができます。

1カ月、2カ月、3カ月、6カ月、または12カ月確認されていないすべてのエンドポイントをデータセットで非表示にするか、EPコンソールがGSMで管理されている場合はGSMデータフィルタ設定を継承できます。すべてのデータを表示するよう選択することもできます。

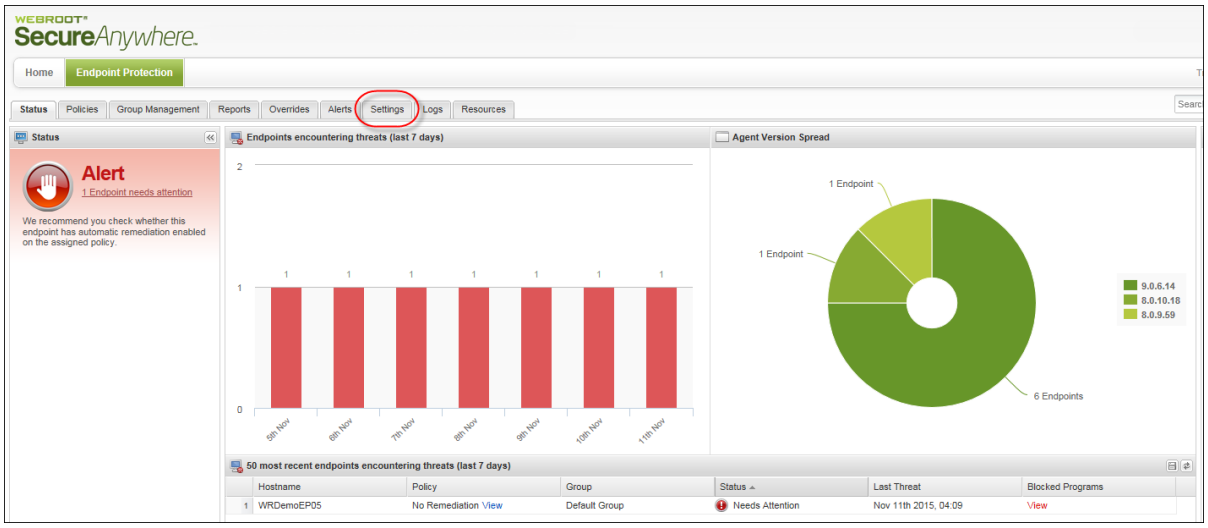
データフィルタを設定するには

1. エンドポイントプロテクションのコンソールにログインします。

   [状態]タブがアクティブになった状態でエンドポイントプロテクションのパネルが表示されます。



2. [**設定**] タブをクリックします。

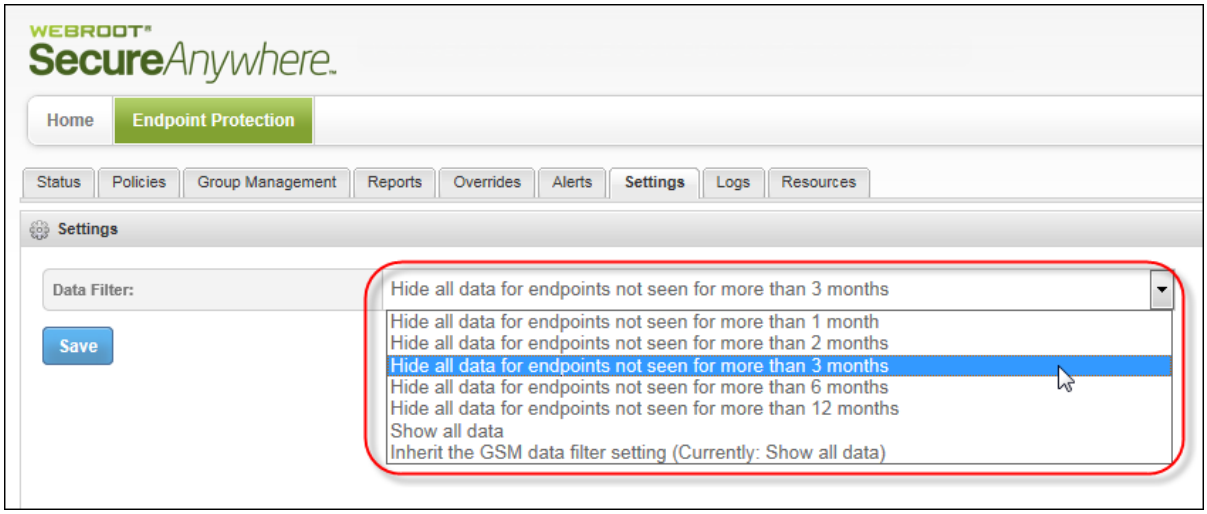


[設定] パネルが表示されます。

3. [データフィルタ] ドロップダウンメニューで、次のいずれかを選択します。

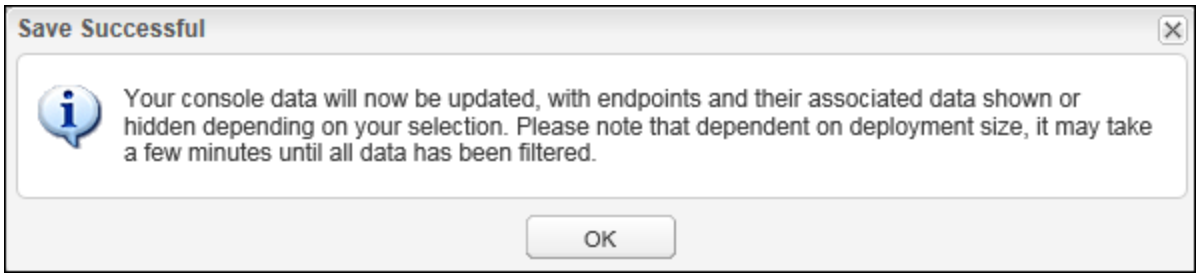
- **1 カ月間確認されていないエンドポイントのデータをすべて非表示にする**
- **2 カ月間確認されていないエンドポイントのデータをすべて非表示にする**
- **3 カ月間確認されていないエンドポイントのデータをすべて非表示にする 6 カ月間確認されていないエンドポイントのデータをすべて非表示にする**
- **12 カ月間確認されていないエンドポイントのデータをすべて非表示にする**
- **すべてのデータを表示 (デフォルト設定)**

- **GSM データフィルタ設定を継承**

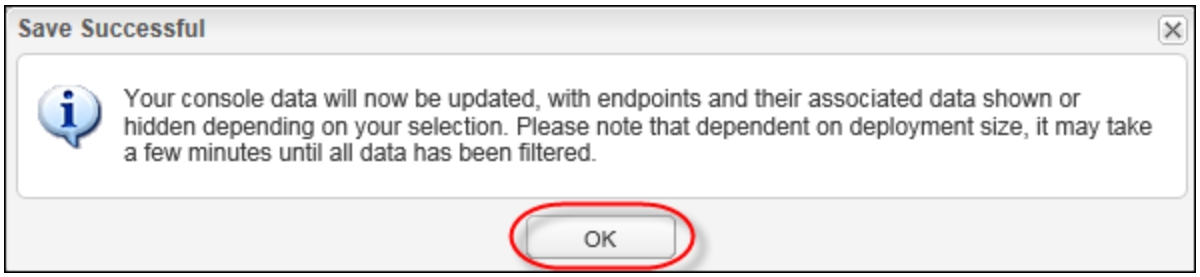


4. **保存**] ボタンをクリックします。

保存が完了したことを示すメッセージが表示されます。



5. [**OK**] ボタンをクリックします。



設定が更新され、ログエントリが作成されます。詳細については、「*データフィルタログの表示 ページ 524*」を参照してください。

第 13 章: ログの表示

ログの表示方法については、以下のトピックを参照してください。

変更ログの表示

変更ログでは、次の各タイプのイベントがいつ発生したのかを確認することができます。

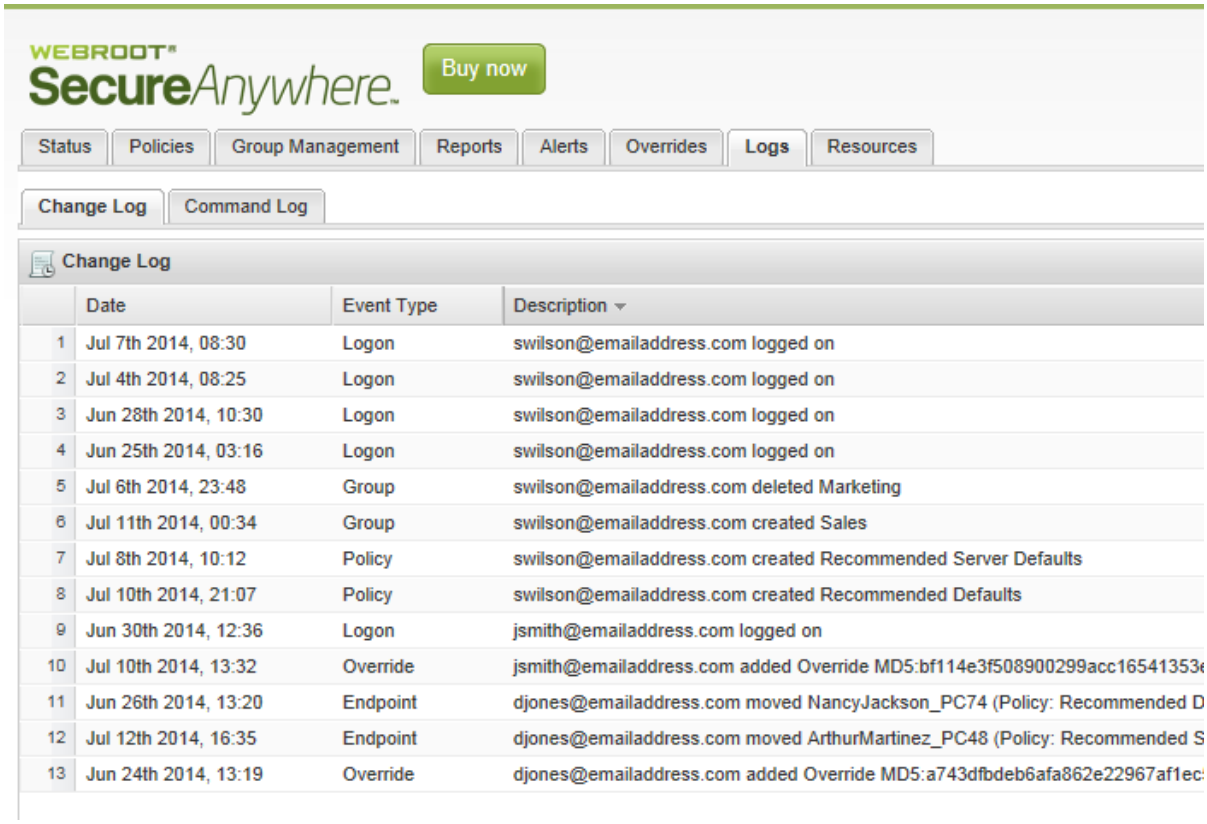
- **ログオン** - 管理者の管理ポータルへのログイン。
- **ポリシー** - ポリシーの作成、変更、削除。
- **エージェントコマンド** - コマンドの開始。
- **オーバーライド** - オーバーライドの作成、変更、削除。
- **グループ** - グループの作成、変更、削除。
- **エンドポイント** - エンドポイントの名前の変更、または別のグループへの移動。
- **レポート** - レポートの生成。

変更ログは、日付範囲、イベントのタイプ、ユーザー、グループ、ポリシー別にフィルタリングできます。

変更ログを表示するには

1. エンドポイントのポータルで [**ログ**] タブをクリックします。

   デフォルトで [変更ログ] が表示されます。このログには変更イベントが一覧表示され、リストを絞り込むためのフィルタが用意されています。



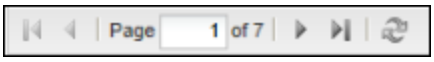
2. 左側のペインの [変更ログをフィルタリング] のオプションを使用して、データを絞り込みます。データのフィルタリングの条件は次のとおりです。

   - **[開始日] および [終了日]** - これら 2 つのフィールドに *mm/dd/yyyy* 形式で日付を入力するか、カレンダーのアイコンをクリックして日付を指定します。
   - **イベントの種類** - ドロップダウンリストでイベントを選択します。イベントには、グループ、エンドポイント、ポリシーの変更や、オーバーライド、ユーザーのログオンなどがあります。
   - **ユーザーの選択** - ドロップダウンリストからユーザーを選択します。
   - **グループの選択** - ドロップダウンリストからグループを選択します。
   - **ポリシーの選択** - ドロップダウンリストからポリシーを選択します。

3. フィルタリング条件を選択したら、[**送信**] をクリックします。

4. 次のいずれか、または両方の操作を行います。

   - データが 50 アイテムを超える場合は、下の**左向き**矢印と**右向き**矢印をクリックしてページ間を移動します。

   - データをアップデートするには、[**更新**] アイコンをクリックします。

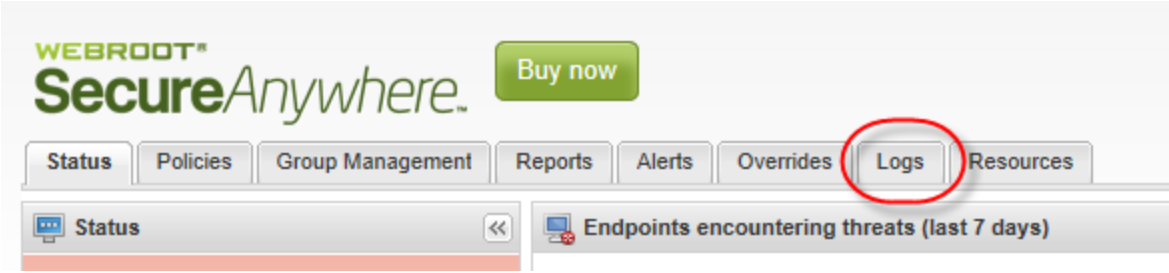
コマンドログの表示

コマンドログでは、最近処理したコマンドと未処理のコマンドに関する情報を確認できます。ログには次のデータが含まれています。

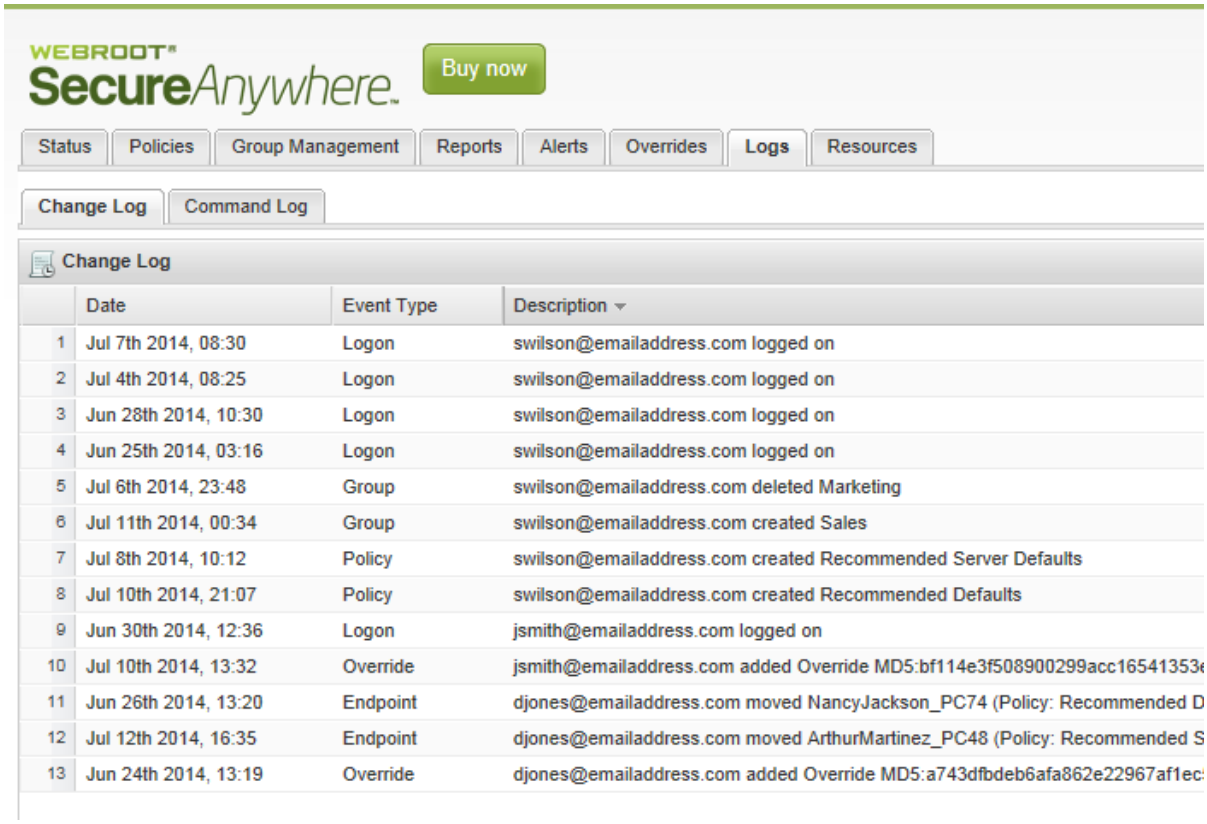
- **ホスト名** -コマンドを受信したエンドポイントの名前。
- **コマンド** - エンドポイントに対して発行されたコマンド。
- **パラメータ** - ファイルの完全なパス名など、コマンドの実行に使用された追加のパラメータ。
- **リクエストされた日** - 管理ポータルからコマンドが送信された日付。
- **ステータス** - [時間切れ] または [実行済み]。24 時間で時間切れとなります。

コマンドログを表示するには

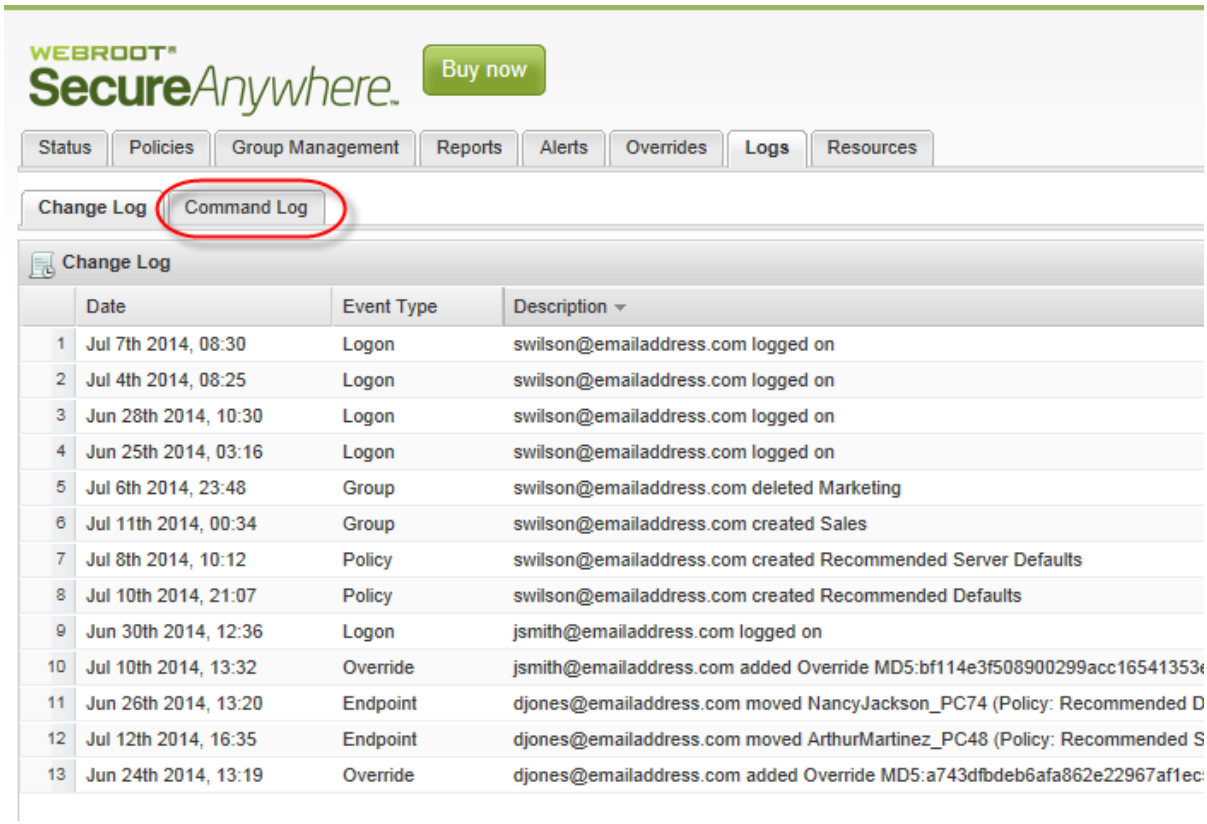
1. エンドポイントのポータルで [**ログ**] タブをクリックします。



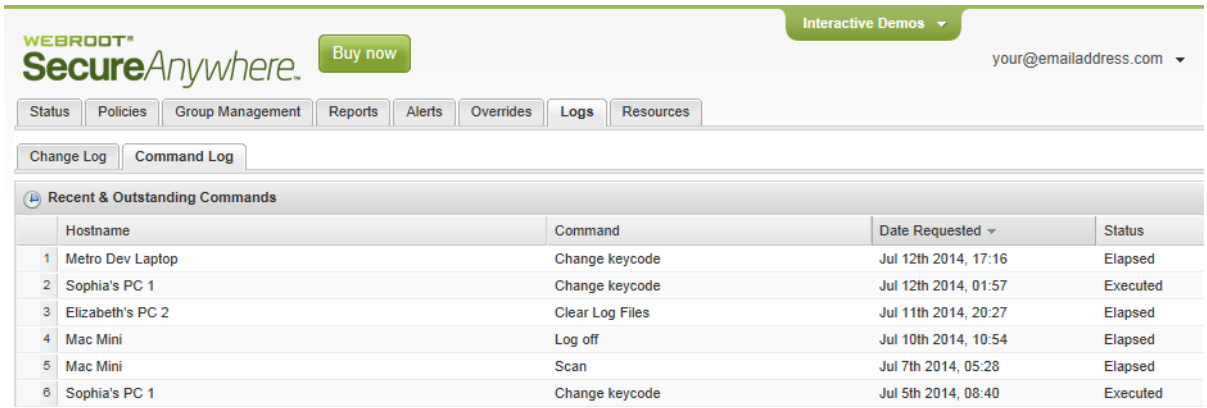
T[変更ログ] タブがアクティブになった状態で [ログ] パネルが表示されます。


WEBROOT
SecureAnywhere
Buy now
Status
Policies
Group Management
Reports
Alerts
Overrides
Logs
Resources
Change Log
Command Log
Change Log
Date
Event Type
Description
1 Jul 7th 2014, 08:30 Logon swilson@emailaddress.com logged on
2 Jul 4th 2014, 08:25 Logon swilson@emailaddress.com logged on
3 Jun 28th 2014, 10:30 Logon swilson@emailaddress.com logged on
4 Jun 25th 2014, 03:16 Logon swilson@emailaddress.com logged on
5 Jul 6th 2014, 23:48 Group swilson@emailaddress.com deleted Marketing
6 Jul 11th 2014, 00:34 Group swilson@emailaddress.com created Sales
7 Jul 8th 2014, 10:12 Policy swilson@emailaddress.com created Recommended Server Defaults
8 Jul 10th 2014, 21:07 Policy swilson@emailaddress.com created Recommended Defaults
9 Jun 30th 2014, 12:36 Logon jsmith@emailaddress.com logged on
10 Jul 10th 2014, 13:32 Override jsmith@emailaddress.com added Override MD5:bf114e3f508900299acc16541353e
11 Jun 26th 2014, 13:20 Endpoint djones@emailaddress.com moved NancyJackson_PC74 (Policy: Recommended D
12 Jul 12th 2014, 16:35 Endpoint djones@emailaddress.com moved ArthurMartinez_PC48 (Policy: Recommended S
13 Jun 24th 2014, 13:19 Override djones@emailaddress.com added Override MD5:a743dfbdeb6afa862e22967af1ec

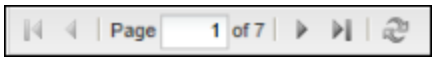
2. [**コマンド ログ**] タブをクリックします。



[コマンド ログ] パネルが表示されます。



3. データが 50 アイテムを超える場合は、下のナビゲーションボタンを使用してページ間を移動します。



4. データをアップデートするには、[**更新**] アイコンをクリックします。

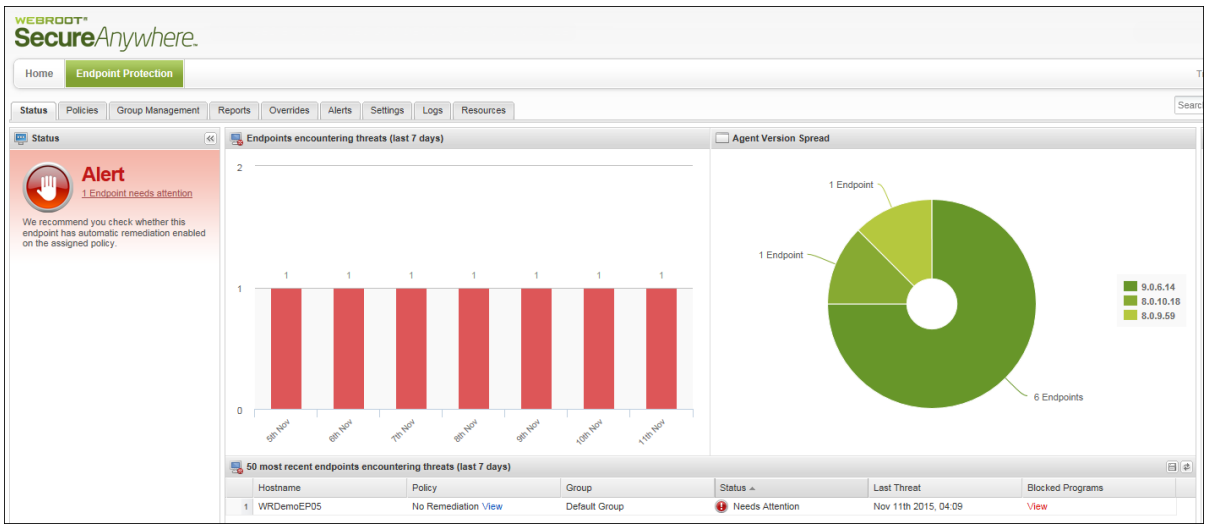
データフィルタログの表示

データフィルタの設定に加えられたすべての変更は、データフィルタログに記録されます。

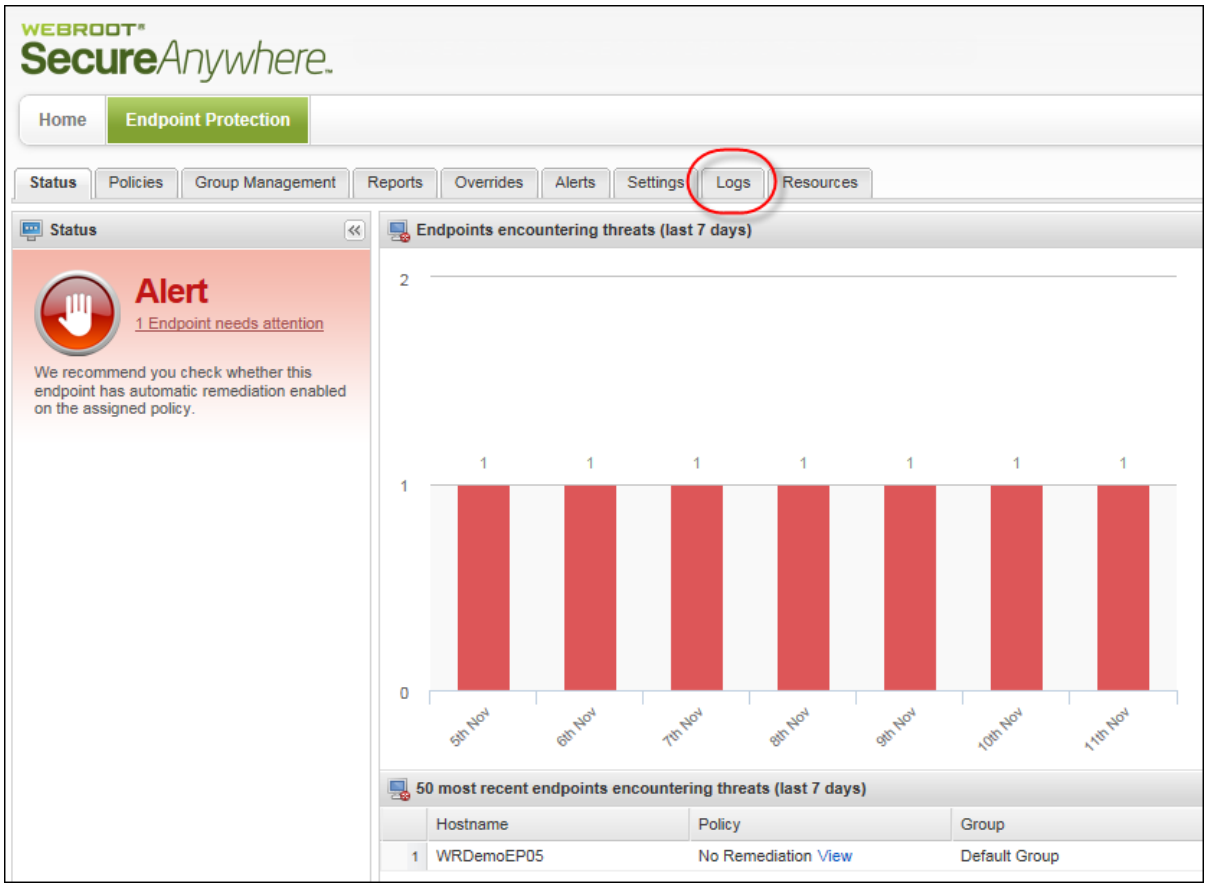
データフィルタログを表示するには

1. エンドポイントプロテクションのコンソールにログインします。

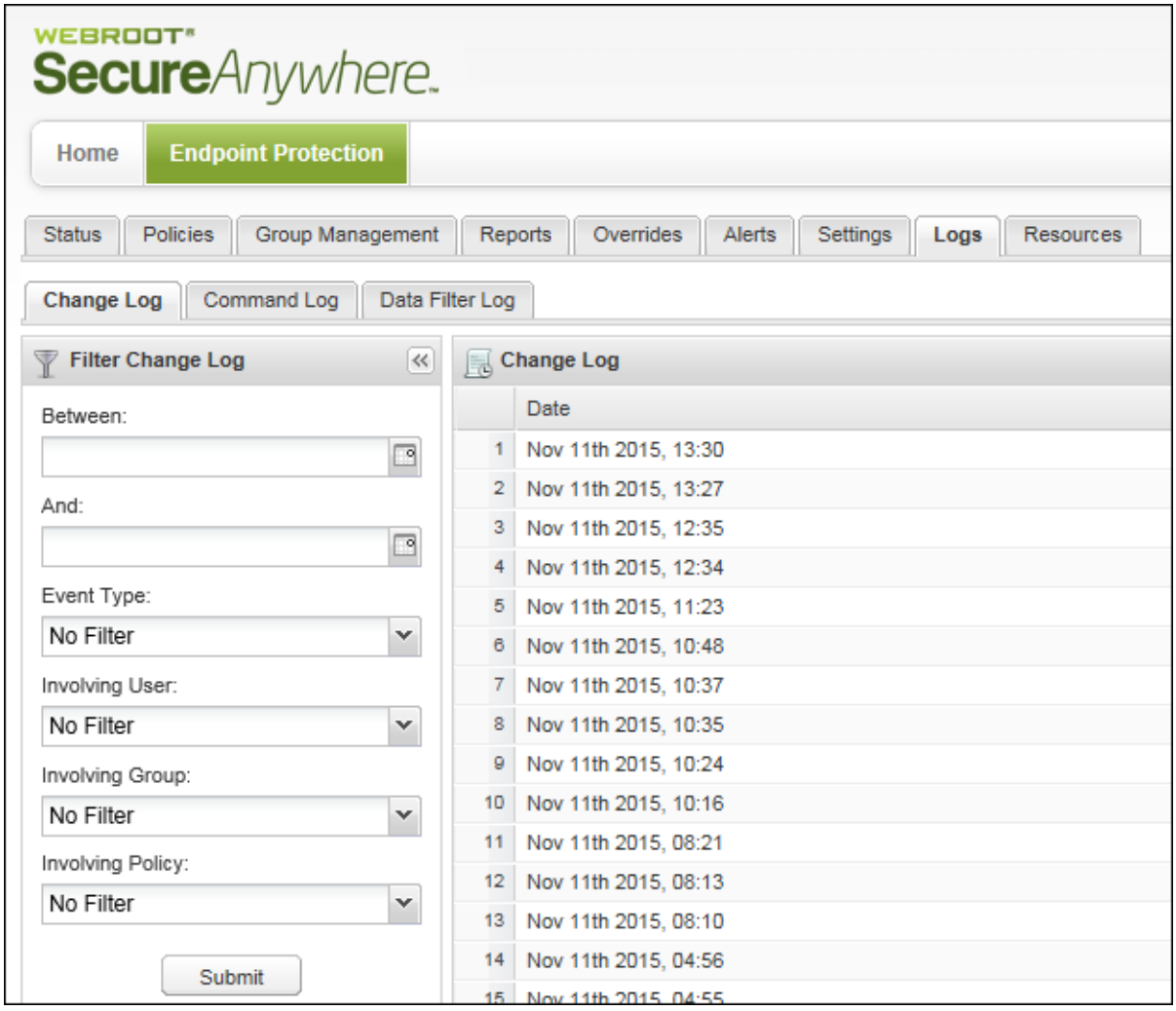
   [状態] タブがアクティブになった状態でエンドポイントプロテクションのパネルが表示されます。



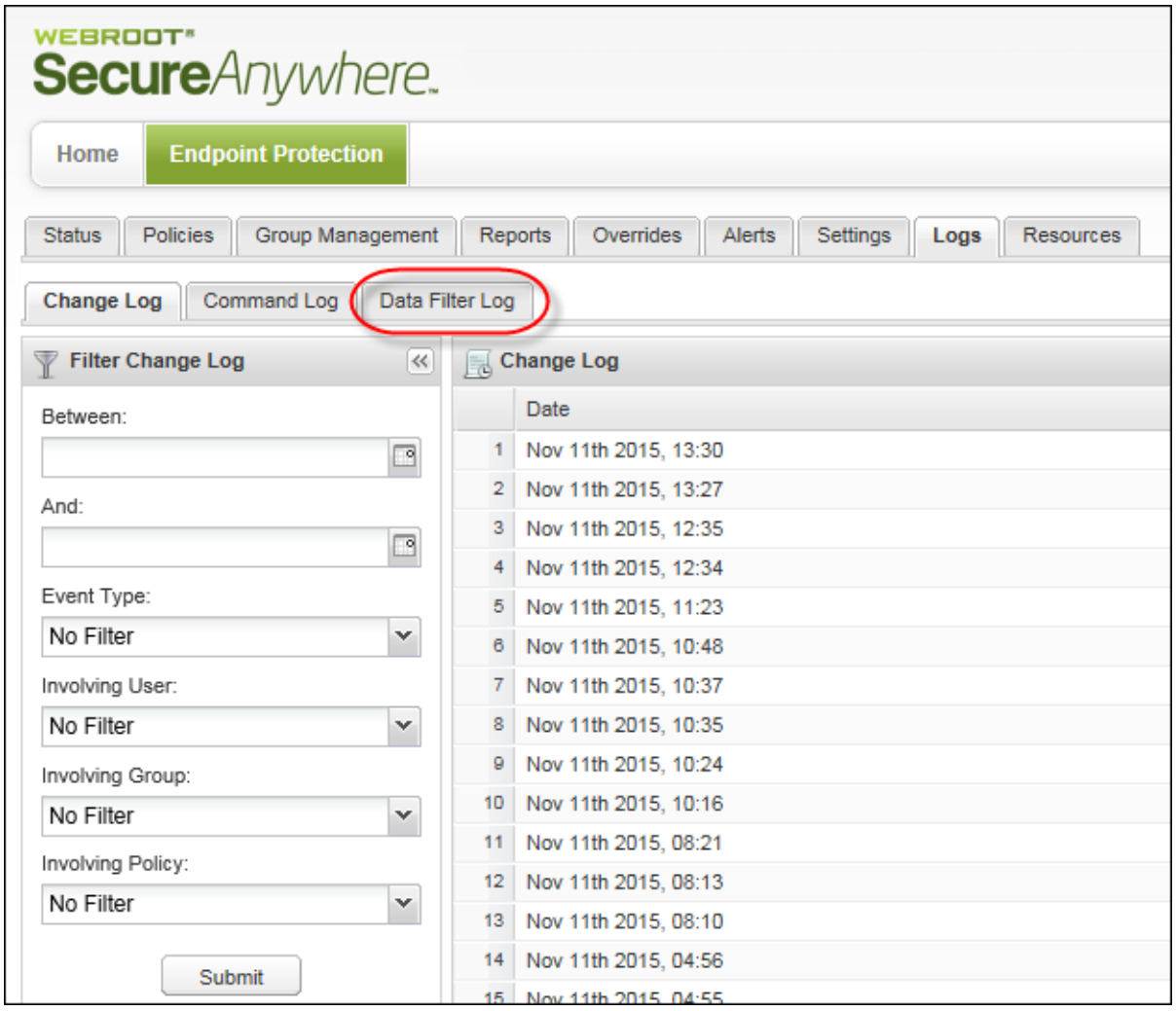
2. [**ログ**] タブをクリックします。



T[変更ログ] タブがアクティブになった状態で [ログ] パネルが表示されます。

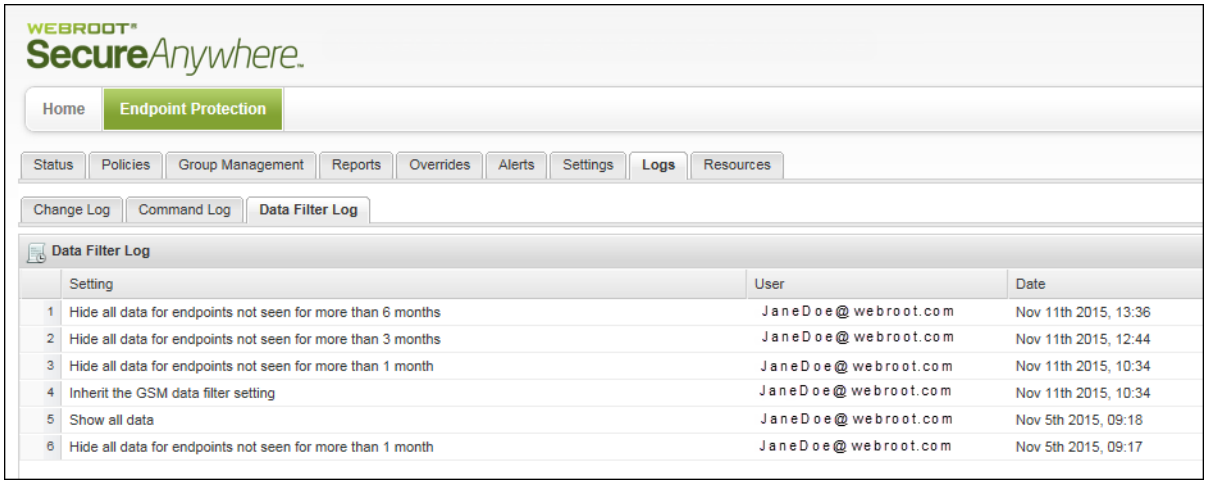

WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Change Log
Command Log
Data Filter Log
Filter Change Log
Between:
And:
Event Type:
No Filter
Involving User:
No Filter
Involving Group:
No Filter
Involving Policy:
No Filter
Submit
Change Log
Date
1 Nov 11th 2015, 13:30
2 Nov 11th 2015, 13:27
3 Nov 11th 2015, 12:35
4 Nov 11th 2015, 12:34
5 Nov 11th 2015, 11:23
6 Nov 11th 2015, 10:48
7 Nov 11th 2015, 10:37
8 Nov 11th 2015, 10:35
9 Nov 11th 2015, 10:24
10 Nov 11th 2015, 10:16
11 Nov 11th 2015, 08:21
12 Nov 11th 2015, 08:13
13 Nov 11th 2015, 08:10
14 Nov 11th 2015, 04:56

3. [**データフィルタログ**] タブをクリックします。



[データフィルタログ] パネルが表示され、追加した変更ごとに以下の情報を提示します。

- **設定** - 選択されたフィルタのオプション。
- **ユーザー** - 変更を行ったユーザーの名前。
- **日付** - 変更が加えられた日付。


WEBROOT
SecureAnywhere
Home
Endpoint Protection
Status
Policies
Group Management
Reports
Overrides
Alerts
Settings
Logs
Resources
Change Log
Command Log
Data Filter Log
Data Filter Log
Setting
User
Date
1 Hide all data for endpoints not seen for more than 6 months JaneDoe@webroot.com Nov 11th 2015, 13:36
2 Hide all data for endpoints not seen for more than 3 months JaneDoe@webroot.com Nov 11th 2015, 12:44
3 Hide all data for endpoints not seen for more than 1 month JaneDoe@webroot.com Nov 11th 2015, 10:34
4 Inherit the GSM data filter setting JaneDoe@webroot.com Nov 11th 2015, 10:34
5 Show all data JaneDoe@webroot.com Nov 5th 2015, 09:18
6 Hide all data for endpoints not seen for more than 1 month JaneDoe@webroot.com Nov 5th 2015, 09:17

第 14 章: 使用状況データへのアクセス

使用状況データへのアクセスの詳細については、以下のトピックを参照してください。

使用状況データへのアクセスについて

使用状況コンソールには、ウェブルートの製品とサービスに関する詳細な情報が表示されます。このコンソールで、セキュリティ意識向上のためのトレーニングの使用状況データにアクセスできるようになりました。

詳細については、GSM 管理者ガイドの「設定の操作」セクションのトピック「使用状況データへのアクセス」を参照してください。

第 15 章: WSA Business エンドポイントプロテクションのサポート

ウェブルートのサポートオプションおよびその他のリソースの詳細については、以下のトピックを参照してください。

テクニカル サポートを受けるには

ウェブルートではさまざまなサポートオプションを提供しています。次のいずれかの方法をご利用ください。

- ナレッジベースで回答を探す。
- オンライン文書で回答を探す。
- ヘルプチケットを送信する。
- ウェブルートのオンライン ビジネス フォーラムを利用する。

索引

S

V

W

あ

い

う

え

さ

し

す

せ

へ

ほ

ま

め

ゆ

り

れ

ろ

漢字