WithSecure Elements

Administrator's Guide

目次

第 章
1

はじめに

トピック :

このガイドでは、WithSecure Elements (旧称F-Secure Protection Service for Business) の一般的な情報を説明します。

このガイドでは、最も一般的な導入方法について説明し、WithSecure Elementsポータルを使用してセキュリティ、ユーザーアカウント、サブスクリプションを管理する方法について説明しています。

1.1 免責事項

「F-Secure Business」は「WithSecure™」になり、 Elements Security Center and Businessのログインページに新しいロゴと名称が反映されています。

当社では製品のブランド変更を進めており、この期間中は、すべての変更が完了するまで、製品とポータルに F-Secure と WithSecure™ が混在する可能性があります。

1.2 WithSecure Elementsについて

WithSecure Elementsは集中管理システムを提供し、コンピュータとモバイル デバイスのセキュリティ管理を容易にします。

Endpoint Protectionソフトウェアを企業のデバイスにインストールすると、ポータルを使用してデバイスのセキュリティ監視・管理が可能になります。ソリューションプロバイダまたはサービスパートナーである場合、複数の会社に属するデバイスを簡単に管理することができます。

ポータルからカスタムのプロファイルを特定のデバイスに作成・適用し、企業のセキュリティ ポリシーに一致する共通の設定を実現できます。また、レポートや統計情報 (例: マルウェアや危険な Web サイトをしたブロック頻度) も確認できます。デバイスを最新の状態に保つためにポータルからソフトウェアのアップデートをダウンロード・配信できます。

Elements Endpoint Protectionを使用すると、次のことができます。

- コンピュータ (Windows、Mac)、サーバ (Windows、Linux、およびモバイル デバイス (Android) を保護する
- 保護しているデバイスのセキュリティ ステータスを1つの場所から監視
- 特定のデバイスに対してカスタム プロファイルを作成・適用して共通のセキュリティ設定を実現
- インストールしている製品に対するソフトウェア アップデートをダウンロード・配信
- 任意のデバイスにセキュリティの問題 (「重大」、「重要」、「情報」のカテゴリ) を通知
- 管理者アカウントとサブスクリプションを管理および表示する

1.3 製品と機能の概要

WithSecure Elementsは、コンピュータやモバイルのエンドポイントから、メールやサーバにもセキュリティを提供します。

WithSecure Elementsでは、Elements EPP、Elements Endpoint Detection and Response、Elements Vulnerabilityエージェントのインストールと管理を簡単に行うことができます。

Endpoint Protectionは以下の製品で構成されています。

- **WithSecure Elements EPP for Computers**ソフトウェアはすべてのwindowsとMacのデスクトップコンピュータに対してセキュリティ機能を提供します。
- **WithSecure Elements EPP for Servers**は、WindowsおよびLinux サーバを対象としたセキュリティ ソリューションです。新しいWithSecure Elements EPP for Serversは最新のツールを使用して、Windows サーバにの強力なセキュリティ機能を提供します。

  注: すべてのサーバ製品は、同じサブスクリプション キーで使用できます。この変更を反映するためにすべてのサーバ製品のサブスクリプション名がServer SecurityからWithSecure Elements EPP for Serversに変更されました。

  注: WithSecure Elements EPP for ComputersとWithSecure Elements EPP for Serversは同じインストーラを使用します。データガードによる追加のランサムウェア保護とアプリケーション制御によるアプリケーション固有の制限を搭載したPremium (プレミアム) バージョンが含まれています。

- **WithSecure Linux Security** は、Linux サーバを対象としたセキュリティ ソリューションです。
- **WithSecure Elements Vulnerability Management** - 脆弱性スキャンと管理のためのプラットフォームです。ネットワーク検出やポートスキャン、プラットフォームやサービスの脆弱性スキャン、Web アプリケーションスキャンなどを実行することができます。

- **WithSecure Elements Mobile Protection**は、AndroidおよびiOSデバイスを対象としたプロアクティブで包括的なセキュリティ機能を提供します。フィッシング対策、有害なWebサイトへのアクセス防止、マルウェアのブロック、潜在的な脆弱性の検出、公共のWi-Fiネットワークなどの安全でないネットワークに接続した際のネットワークトラフィックをプライベートに保ちます。

WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversには、次のような多くの高度な機能があります。

- ソフトウェアアップデーターは、オペレーティングシステムと他社製ソフトウェアを最新の状態に保ち、脅威を軽減するツールです。
- ディープガードは、高度なテクノロジを使用してヒューリスティック分析、動作、および評判分析に基づいた、極めて重要なセキュリティ層を提供します。
- デバイス制御 (WithSecure Elements EPP for Computersのみ) は、USB スティック、CD-ROM ドライブ、Web カメラなどのハードウェア デバイスを介して脅威がシステムにアクセスすることを防ぎます。また、読み取り専用アクセスなどを許可することで、データの漏洩を防ぎます。

WithSecure Elements Mobile Protectionは、ネットワークゲートウェイや有害コンテンツに対するセキュリティ保護などの高度な機能を多数提供します。「超軽量」技術を活用して、バッテリー消費とパフォーマンスへの影響を最小限に抑えます。VMware Workspace ONE、IBM Security MaaS360、Ivanti Endpoint ManagementおよびMicrosoft Intuneなどの外部MDMシステムと組み合わせて使用できます。

注： MDM の使用の詳細については、Elements Mobile Protectionを参照してください。

第 章
2

ポータルを使用する

トピック：

この章では、WithSecure Elementsポータルを日常的に利用する上で役立つ基本的な情報を提供します。

ここでは、次のタスクについて説明します。

- アクセス権の管理
- 新しい管理者アカウントを追加する
- 顧客企業を追加する
- *スコープセレクタ*を使用してポータルで表示される情報を設定する

WithSecure Elements製品を顧客企業のユーザに注文したり、企業のコンピュータやモバイルデバイスにインストールされているPSB製品のサブスクリプションを管理したりできます。

2.1 WithSecure Elements Endpoint Protectionを使い始める

WithSecure Elements Endpoint Protectionを使い始めることにおいて、一般的に5つのステップがあります。

1. WithSecureビジネスアカウントを作成します。
2. Elements Security Centerにログインします。
3. 組織にデバイスを追加します。
4. 組織内の他のユーザのために追加の管理者アカウントを作成します。
5. プロファイルの作成または複製、およびセキュリティ設定の編集。

2.2 ログイン

Elements Security Centerにログインする方法の説明。

WithSecure Elements Security Centerにアクセスするには、WithSecureビジネスアカウントが必要です。WithSecureパートナーから製品を購入すると、パートナーは通常、お客様の組織で最初の管理者用のビジネスアカウントを作成します。この場合、WithSecureからElements Security Centerにログインするための仮パスワードとリンクが記載されたメールが届いています。

アカウントがまだ作成されていないが、パートナーからサブスクリプションキーを受け取っている場合、サブスクリプションキーを使用して、組織内の最初の管理者のためにWithSecure Businessアカウントを作成することができます。これを行うには、特定の地域の企業自己登録リンクを使用します。

次のようにアカウントにログインします。

1. Webブラウザで次のリンクを開きます。https://elements.withsecure.com/
   [**ログイン**] ページが開きます。
2. ユーザ名を入力して [**ログイン**] を選択します。

   👉 **注：** ログイン情報をお持ちでない場合は、担当者にポータルサイトへのアクセス方法をお尋ねください。パスワードを忘れた場合は、[**パスワードを忘れた場合**] を選択すると、新しいパスワードを発行することができます。パスワードの再設定方法は、お客様のEメールアドレスに送信されます。

   ポータルが開きます。右上のナビゲーションメニューを使用してサービスを切り替えることができます。

2.2.1 多要素認証

多要素認証⊠MFA⊠は、二要素認証⊠2FA⊠とも呼ばれ、システムへのログインプロセスにおけるセキュリティを高める方法です。

MFAは、フィッシング攻撃やクレデンシャルスタッフィング攻撃などからユーザーと環境を保護します。

👉 **重要：** WithSecure Elementsポータルへのアクセスを安全に保つため、多要素認証⊠MFA⊠のご利用を強くお勧めします。ポータルを可能な限りスムーズにご利用いただくために、すぐにMFAをご利用いただくことをお勧めします。

👉 **重要:** バックアップとして、複数の多要素認証方法を使用することをお勧めします。唯一の多要素認証方法が失われた場合、アカウントを再作成する必要があります。

ユーザがユーザ名とパスワードを使ってシステムにログインするとき、ブラウザやパスワードマネージャの脆弱性などにより、その認証情報がすでに漏洩している可能性がある。これらの流出した認証情報は、攻撃者がシステムに侵入するために使用する、一般にアクセス可能なリストに載っている可能性がある。MFAが追加されると、ログイン時に追加のステップが必要になる。システム・アクセスは従来、ユーザー名とパスワードで保護されてきた。MFAは、あなたが持っているもの⊠セキュリティキーやデバイス⊠と、あなた自身であるもの⊠指紋や顔認証⊠という、追加の要素を導入します。

MFA方式

WithSecure Elementsアクセスを可能な限り安全に保つために、複数のMFA方式が用意されています。

方法には次のものがあります。

- **時間ベースのワンタイムパスワード（TOTP）**を使用した認証アプリケーション、例えばMicrosoft Authenticator、Google Authenticator、Auth0 Guardian、またはその他の認証アプリケーションが含まれます。認証アプリケーションには、6桁の認証コードが送信され、ログインダイアログに入力する必要があります。
- **Auth0 Guardian 認証アプリケーターによるプッシュ通知** - ボタンを1回クリックするだけで認証リクエストを承認できます。Auth0 Guardianマルチファクター認証アプリケーションはGoogle PlayとAppStoreで利用できます。
- **Short Message Service（SMS）メッセージによるワンタイムパスワード（OTP）のための電話番号** - 6桁の認証コードが、設定された携帯電話番号にSMSで送信されます。ログインダイアログにコードを入力して続行します。

  👉 **重要：** SMSメッセージはセキュリティの侵害や悪意のあるソフトウェアに対して脆弱であり、それらを受信することで追加料金が発生する場合もあります。そのため、安全な代替手段がない場合を除いて、SMSの使用を避けることをお勧めします。

- Yubico Yubikey、Google Titan、その他FIDO2標準（https://fidoalliance.org/fido2/）をサポートする**セキュアUSBキー**
- FIDO2標準（https://fidoalliance.org/fido2/）をサポートする**スマートフォンやその他のデバイス**
- デバイスの生体認証、指紋認証または顔認識、またはWebAuthn（https://www.w3.org/TR/webauthn/）を使用してデバイスからのWindows Hello。

  👉 **重要：** デバイスの生体認証は個々のデバイスに固有であり、**使用する唯一の認証方法であってはなりません**。使用するデバイスごとに、この認証方法を追加するよう求められます。

多要素認証の選択

1つ以上の多要素認証方法を選択する方法について説明します。

👉 **注：** 多要素認証方法を選択する前に

- モバイル デバイスにGoogle Authenticatorなどの認証アプリをインストールします。
- モバイル デバイスが QR コードを読み取れることを確認します。

最も安全な認証方法を選びましょう。FIDO2が最良の選択肢であり、認証アプリがそれに続く。SMSは最後の手段としてのみ使用してください。モバイルデバイスを紛失し、セキュリティキーや認証アプリをバックアップしていない場合、アカウンにアクセスできなくなりますのでご注意ください。

1つ以上の多要素認証方法を選択するには:

1. メールアドレスとパスワードでログインします。
2. 右上の を選択し、[**設定**] を選択します。

   👉 **注：** すでに1つ以上のMFAメソッドを構成している場合は、[**変更**] を選択します。

   [**多要素認証の設定**] ウィンドウが開きます。
3. [**追加**] を選択し、使用したい認証オプションを1つ以上選択します。
   [**本人確認**] 画面が開きます。
4. 画面の指示に従ってください。必要なアクションは、選択したMFA方法によって異なります。
   WithSecure Elementsのアカウントに多要素認証が設定されました。

   👉 **注：** バックアップとして複数の多要素認証方法を選択することをお勧めします。唯一の多要素認証方法が失われた場合、多要素認証をリセットする方法はありません。すべての多要素認証方法が失われた場合は、アカウントを再作成する必要があります。

MFAを使用すると、次回ログインするときに、システムはデバイスの生体認証を使用してログインプロセスを簡素化することを提案します。 特定のデバイスでそれらを使用するか、使用しないかを選択す

ることも、[後で通知する]オプションを選択してプロセスを延期することもできます。特定のデバイスで生体認証を使用してログインフローを簡素化することを選択した場合、ログインプロセス中に、指紋などを使用して2番目の要素の検証を実行できます。

多要素認証の削除

多要素認証⊠MFA⊠を削除する手順

多要素認証方法を削除するには:

1. メールアドレスとパスワードでログインします。
2. 多要素認証コードを入力して選択 [**続く**]。
3. 右上の を選択し、[**設定**] を選択します。
4. 選択する [**変化**]の隣に **多要素認証が有効**。
   の **本人確認**ウィンドウが開きます。
5. 画面上の指示に従います。
6. 選択する [**取り除く**]削除する多要素認証方法の横にある をクリックします。
7. メールアドレスとパスワードを入力してください。

2.3 ユーザ管理

アクセス権、顧客企業の追加と管理、および管理者アカウントの追加と管理について説明します。

2.3.1 アクセス権について

選択した種類の情報は表示できるが編集はできないように、アクセス権を制限することができます。

ユーザアカウントの作成時に、[**サーバは読み取り専用**] または [**コンピュータとモバイルは読み取り専用**] を選択することで可能です。

新しいアカウントを作成するとき、または既存のアカウントを編集するときに、アクセス権を設定することができます。アクセス権によって、セキュリティ設定⊠プロファイル⊠、デバイスの状態、ダッシュボード、セキュリティイベント、ソフトウェアアップデートなどのセキュリティ情報、セキュリティ操作⊠デバイスの削除、デバイスの隔離、プロファイルの更新など⊠、サブスクリプション、ユーザーアカウント、インストーラにアクセスすることができます。

読み取り専用の権利では、ユーザは操作を実行したり、他のユーザやプロファイルを管理したりすることができません。

注: サブスクリプションの管理はWithSecure Partnerポータルで行う必要があるため、特定のサブスクリプションの管理権限が削除されました。

2.3.2 管理対象企業間の移動

*スコープ セレクタ*を使用してWithSecure Elementsポータルで表示される情報を設定できます。

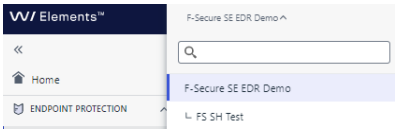
ポータルには、アクセス権を決定するさまざまなアカウント レベルがあります。

- ソリューションプロバイダー (SoP) は、サービス パートナーと企業グループを管理します。ポータルにアクセスして、直接管理されている会社、サービス パートナー、およびサービス パートナーの会社のセキュリティとサブスクリプションを管理できます。
- サービス パートナー (SeP) は企業のグループを管理します。ポータルにアクセスして、直接管理されている会社のセキュリティを管理できます。
- 各企業は単一の企業を管理します。SoP または SeP によって管理されている企業はプロバイダからのアクセスを要求できますが、独自のセキュリティを管理している企業はポータルへのフル アクセスを提供できます。SoP または SeP によって管理されている企業、あるいはWithSecure によって直接管理されている会社は、ポータルに対する読み取り専用の権利を取得します。

特定の会社にスコープ セレクタを重視するには

1. タイトルバーにある アイコンを選択します。

ドロップダウン メニューが表示され、アカウントに関連付けられている顧客企業を確認できます。



2. 検索フィールドで企業を選択するか、または企業名を直接入力し、**Enter** キーを選択します。
選択した企業の名前が青い背景色で表示され、選択した会社の関連情報を表示するためにページが更新されます。

2.3.3 新しい管理者を追加する

特定のユーザに*管理者*としての権限を与えることで、WithSecure Elementsポータルにおいて必要な権限を付与することができます。

管理者としての権限を付与することによって、社内の複数のデバイスや管理者自身の使用しているデバイスにおける、Endpoint Protectionソフトウェア/ライセンスの管理を行うことが可能になります。ソリューション プロバイダ、サービス パートナーあるいは会社アカウントの管理者を追加することも可能です。

企業アカウントを作成するには

1. [管理] で、 サイトバーの [**サブスクリプション**] を選択します。
[**組織の設定**] ページが開きます。
2. [**Endpoint Protectionのアカウント**] タブを選択します。
[**アカウント**] ビューが表示されます。
3. ポータル アカウントまたは特定の顧客企業の管理者アカウントを作成できます。
   - **ポータル アカウントの場合**、[*アカウント*] の横にある ••• アイコンを選択します。
   - **顧客企業の場合**、企業の名前の横にある ••• アイコンを選択します。
4. メニューから [**管理者を作成**] を選択します。
[**管理者の作成**] ページが開きます。
5. 次のようにユーザーの詳細を入力します。
   a) メール アドレスを入力します。

      注 : 常に固有のメール アドレスを使用することを推奨します。既存のアドレスを使用して、入力したメール アドレスがすでに使用されているというメッセージを受け取る必要がある場合、メールアドレスを一意にするために「+」と識別子をメールアドレス追加します (例: user.name+oldusername@company.com)。

   b) 新しい管理者のユーザ名を入力します。
   c) ユーザが使用する言語を選択します。
   d) 次の読み取り専用の権利を1つ選択します。
      - サーバ用に読み取り専用 - 通常の管理者がサーバを管理できないようにするには、このオプションを選択します。

        注 : 読み取り専用権限を持つ管理者は、サーバ権限を持つ管理者を追加できません。
      - コンピューターとモバイルデバイス用に読み取り専用-サーバ管理者がコンピュータとモバイルデバイスを管理できないようにするには、このオプションを選択します。

      注 : 別のWithSecure環境で作成されたアカウントにポータルへのアクセスを許可するには、同じメールアドレスを使用してPSBポータルにアカウントを作成する必要があります。メールアドレスを入力すると、システムは同じメールアドレスを持つアカウントが存在することを通知します。[**送信**] を選択すると、アカウントにWithSecure Elementsポータルへのアクセス権が付与されます。

6. [**送信**] を洗濯します。

新しい管理者アカウントが作成されます。

注： 新しいアカウントのパスワードの設定方法に関するメールがユーザに届きます。

2.3.4 新しいサービスパートナーを追加する

サービスパートナーアカウントを作成するには

1. [管理] で、 サイトバーの [サブスクリプション] を選択します。
   [組織の設定] ページが表示されます。
2. [Endpoint Protectionのアカウント] タブを選択します。
   [アカウント] ページが開きます。
3. [アカウント] の横にある ⋯ を選択し、次に [新しいサービス パートナー アカウントの作成] を選択します。
   「サービス パートナーの作成」ページを開きます。
4. 新しいサービス パートナー アカウントの名前を入力し、[作成] を選択します。
   サービス パートナー アカウントが作成されます。
5. [送信] を洗濯します。

新しいサービスパートナーの管理者アカウントが作成されます。

2.3.5 管理者を変更・削除する

管理者を変更・削除することができます。

1. [管理] で、 サイトバーの [サブスクリプション] を選択します。
   [組織の設定] ページが表示されます。
2. [Endpoint Protectionのアカウント] タブを選択します。
   [アカウント] ページが開きます。
3. 関連するアカウント名の横にある矢印をクリックします。
4. ログイン名の一覧で変更・削除する管理者アカウントの行にある ⋯ をクリックします。
   メニューが表示されます。
5. 管理者アカウントを変更するには
   a) [管理者の編集] を選択します。
   b) アカウント情報を編集して [保存] をクリックします。
   管理者アカウントの情報が更新されます。
6. 管理者アカウントを削除するには
   a) [管理者を削除する] を選択します。
   b) OK を選択すると、管理者が削除されます。
   管理者アカウントが削除されます。

2.3.6 パスワードを回復する

アカウントのパスワードを忘れた場合、[パスワードを忘れた場合]をクリックすることでパスワードを回復できます。

パスワードを回復するには

1. ログイン ページで [パスワードを忘れた場合] リンクをクリックします。
   [パスワードをリセットするメールが送信されました] ウィンドウが開きます。
2. ユーザ名またはメールアドレスを入力します。
3. [送信] を選択します。

パスワードの変更方法を記載したメールが届きます。

2.4 Elements製品を使用する

WithSecure Elements製品を使用するにはいくつかの手順が必要です。

1. 顧客企業を追加します⊠まだ追加されていない場合⊠。
2. サブスクリプションを取得しています。

   注： **管理** > **サブスクリプション**で、すべての製品、利用可能なサブスクリプションキー、およびそれらの有効期限を表示できます。
3. 顧客企業にサブスクリプションを追加します。
4. 製品を導入します。

   注： Elements製品を展開する手順については、一般的な展開方法を参照してください。

2.4.1 顧客企業を追加する

新しい「*顧客企業*」をWithSecure Elementsポータルのアカウントに追加するにはまず*規顧客*」を***WithSecure***パートナーポータルのアカウントに追加し、WithSecure Elementsを1つ以上購入する必要があります。

注: ソリューションプロバイダおよびサービスパートナーのみ企業アカウントを追加できます。

新しい顧客企業でライセンス・デバイスを管理する管理者アカウントが必要な場合、PSB ポータルを通じて管理者アカウント作成してください。

注： エフセキュア「パートナー ポータル」はWithSecure Elementsポータルと連携したオンライン サービスで、販売活動を支援するツール、資料、統合したオンライン注文システムおよびエフセキュア ソリューションのサポートを提供します。

パートナー ポータルのアカウントから新規顧客の発注書を追加したらWithSecure Elementsポータルのアカウントに新規顧客として自動的に追加されます。

以後、WithSecure Elements製品を顧客企業のユーザに提供できるようになり、購入した製品のライセンス管理も可能になります。

2.4.2 企業アカウントに新しいライセンス キーコードを追加する

企業アカウントに新しいライセンス キーコードを追加すると、WithSecure Elementsポータルにコンピュータを追加できます。

新しいライセンス キーコードを追加するには

注： ソリューション プロバイダおよびサービス パートナーのみ企業アカウントに新しいライセンス キーコードを追加できます。

1. [**管理**] で、 サイトバーの **サブスクリプション**] を選択します。
2. [**Endpoint Protectionのサブスクリプション**] タブを選択します。
3. 新しいライセンス キーコードの対象となる企業アカウントの名前の横で ⋯ を選択し、[**ライセンス キーコードを追加**] を選択します。
   「**ライセンス キーコードを追加する**」ページが開きます。
4. 企業アカウントの新しいライセンス キーコードを入力して [**追加**] を選択します。

新しいライセンス キーコードが企業アカウントに追加されます。

2.4.3 顧客企業に製品を注文する

顧客企業向けのWithSecure Elements製品は、WithSecureパートナーポータルから注文することができます。

注： ソリューション プロバイダおよびサービス パートナーのみが、顧客企業向けの製品を注文できます。

WithSecure Partner Portal経由でWithSecure Elements製品を注文するには

1. Webブラウザで次のリンクを開いて、ポータルにログインします。パートナーポータル

   注： WithSecure パートナー ポータルには、WithSecure Elementsポータルからの別のログイン資格情報が必要です。ログインの詳細がまだない場合は、ページ上の**認証情報のリクエスト**フォームに入力し、[**送信**] をクリックします。アクセス認証情報を受け取るまでに最大24時間かかります。

   「**オンライン注文**」ページが表示されます。
2. 既存の顧客企業に製品を注文するには
   a) メインページで [**顧客**] をクリックし、製品を注文する顧客企業名を選択します。
   b) 「[**注文**] 列で、[**新規SaaS注文**] または [**新規年間注文**] を選択します。
   [注文] ウィンドウが開きます。
   c) [**新規注文**] の下に、注文の参照番号を入力します。
   d) [**製品の注文**] で、[**製品を追加**] を選択します。
   e) 必要な製品を選択して注文の指示に従います。

   発注が完了すると、製品情報の変更は、WithSecureパートナーポータルおよびWithSecure Elementsポータル アカウントで更新されます。
3. 新規顧客企業に製品を注文するには
   a) メイン ページで、[**新規注文**] を選択します。
   b) 新規顧客企業の名前を入力し、[**新規追加**] 選択します。
   [**新規顧客**] ウィンドウが開きます。
   c) 顧客の詳細を入力し、[**保存**] を選択します。
   d) [**新規注文**] の下に、注文の参照番号を入力します。
   e) [**製品の注文**] で、[**製品を追加**] を選択します。
   f) 必要な製品を選択して注文の指示に従います。

   発注が完了すると、新規顧客企業が購入した製品と一緒にパートナーポータルアカウントにリストされます。

   注: 新規顧客企業がWithSecure Elementsポータルアカウントに表示されるまでに時間がかかる場合があります。

2.4.4 利用可能の製品ライセンスを表示する

利用可能の製品ライセンスを表示するには

1. [**管理**] で、 [**サブスクリプション**] を選択します。
   [サブスクリプション] ビューが開き、各製品のサブスクリプション、サブスクリプションキー、およびサブスクリプションが属する組織が表示されます。

   注： *スコープ セレクタが*すべての顧客企業を表示するように設定されている場合、デフォルトですべてのライセンスが表示されます。
2. フィルタリングを使用すると、次の情報を見つけることができます。
   - サブスクリプションキー - 関連するサブスクリプションキーを入力します
   - 製品 - 利用可能な製品のリストから選択します
   - 有効期限 - 有効なサブスクリプションを表示するには、[**有効**] を選択します。[**14日以内に期限切れ**] または [**60日以内に期限切れ**] と入力すると、まもなく期限切れになるサブスクリプションが表示されます。または、[**失効**] を選択すると、有効期限が切れたサブスクリプションのみが表示されます

- タイプ - 次のサブスクリプションタイプから選択できます⊠**商用用**、**評価用**、**政府用**、**教育用**、または**非再販用**。

特定の顧客企業が使用しているライセンスを確認するには*スコープ セレクタ*から対象の企業を選択します。

注： 特定の顧客企業を表示する場合、フィルタは適用されません。

2.4.5 サブスクリプション キーを変更する

WithSecure Elementsポータルからサブスクリプションキーを変更する方法を説明します。

サブスクリプション キーを変更するには

注: この機能は現在、パートナーアカウントおよび企業アカウントにおいて、次のソフトウェアの変更する場合に利用できます。WithSecure Elements EPP for Computers、WithSecure Elements EPP for Computers Premium、WithSecure Elements EPP for ServersまたはWithSecure Elements EPP for Servers PremiumからWithSecure Elements EDR and EPP for Computers、WithSecure Elements EDR and EPP for Computers PremiumまたはWithSecure Elements EDR and EPP for Servers Premiumへの変更。

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
「**デバイス**」ページが開きます。
2. サブスクリプションキーを変更するデバイスを選択します。
ページの下にメニューが表示されます。
3. [**サブスクリプションを変更**] を選択します。
4. 表示されるフィールドに新しいサブスクリプション キーを入力して、 [**ライセンスを変更する**] を選択します。

注： **管理** > **サブスクリプション**の下に、選択した会社のデバイスに使用できるサブスクリプションキーがあります。

新しいサブスクリプション キーが選択したデバイスに適用されます。

2.4.6 サブスクリプションをアップグレードする

ここでは、サブスクリプションをアップグレードする方法とおよびアップグレードのオプションについて説明します。

サブスクリプションをアップグレードする

サブスクリプションをアップグレードするには2つの方法があります。

- サブスクリプション キーの種類を変更する (新しいサブスクリプションを注文する)
- デバイス上の別のサブスクリプション キーに変更する

サブスクリプションをアップグレードする際には、次のオプションがあります。

- WithSecure Elements EPP for Computers → WithSecure Elements EPP for Computers Premium
- WithSecure Elements EPP for Computers → WithSecure Elements EDR and EPP for Computers
- WithSecure Elements EPP for Computers → WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EPP for Computers Premium → WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EDR and EPP for Computers → WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EPP for Servers → WithSecure Elements EPP for Servers Premium
- WithSecure Elements EPP for Servers Premium → WithSecure Elements EDR and EPP for Servers Premium

注： WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversの Standard版とPremium版の両方、およびWithSecure Elements EDR and EPP for Computersまた

はWithSecure Elements EDR and EPP for Serversの任意の組み合わせに、同じインストーラファイルを使用できます。

WindowsコンピュータにWithSecure Elements EDRがインストールされている場合は、WithSecure Elements EDR for ComputersまたはWithSecure Elements EDR for Computers Premiumにアップグレードする前に、再インストールする必要があります。

2.5 管理対象のデバイスを追加する

WithSecure Elementsアカウントを使用してコンピュータまたはモバイルデバイスのセキュリティを監視および管理するには、まずコンピュータまたはモバイルデバイスにEndpoint Protectionソフトウェアをインストールする必要があります。

ソフトウェアがインストールされると、デバイスがポータルアカウントに追加されます。ポータルを通じて、セキュリティ製品のパフォーマンスを追跡したり、サブスクリプション、アップデート、およびその他の標準タスクを管理したりできます。

注: 新しいデバイスを追加すると、デフォルトのプロファイルが適用されます。

管理したいデバイスにEndpoint Protectionソフトウェアをインストールするには、いくつかの方法があります。

- デバイスのユーザへソフトウェア インストーラとインストールおよびアクティベーション方法を記載したメールを送ります。
- ポータルから直接ソフトウェアをダウンロードし、デバイスに転送します。

  注: これは、WithSecure Elements Mobile Protectionには適用されません。
- GPO、イメージ、またはRMMまたはMDMツールを使用してソフトウェアを展開します。

各デバイスの情報を含む CSV ファイルをインポートすることで一度に複数のモバイル デバイスを追加できます。

注: 新しいデバイスを追加する前に、Endpoint Protectionソフトウェアのサブスクリプションがあり、少なくとも1つの無料インストールが利用可能である必要があります。利用できる無料インストールの数によって、追加できるデバイスの数が決まります。

2.5.1 WithSecure ソフトウェアを導入する

ここでは、WithSecure Elements Endpoint Protectionの配布方法について説明します。

- 同じWithSecure Elements Agent for Computersインストールパッケージを使用して、以下のソフトウェアをインストールできます。どのソフトウェアをインストールするかは、サブスクリプションキーによって決まります。

  注: インストール手順については、「EXEファイルを使用して製品をインストールする」セクションを参照してください。

  - WithSecure Elements EPP for Computers
  - WithSecure ElementsEDRおよびEPPfor Computers
  - WithSecure Elements EDR for Computers

    注: スタンドアロンソフトウェアとしてインストールする場合、既存のエンドポイントソフトウェアの自動アンインストールをオフにするために、追加のコマンドラインパラメーター「`--skip-sidegrade`」を追加する必要があります。
  - WithSecure Elements EPP for Computers Premium (Windowsのみ)
  - WithSecure ElementsEDRおよびEPPfor Computers Premium (Windowsのみ)
  - WithSecure Elements Vulnerability Management (Windowsのみ)

- 同じWithSecure Elements Agent for Serversインストールパッケージを使用して、以下のソフトウェアをインストールできます。どのソフトウェアをインストールするかは、サブスクリプションキーによって決まります。
  - WithSecure Elements EPP for Servers
  - WithSecure Elements EDR for Servers (Windowsのみ)
  - WithSecure Elements EPP for Servers Premium (Windowsのみ)
  - WithSecure ElementsEDRおよびEPPfor Servers Premium (Windowsのみ)
  - WithSecure Elements Vulnerability Management (Windowsのみ)
- WithSecure Elements Mobile Protectionは、2つの方法でインストールすることができます。
  - WithSecure Elements EPPポータルから [**新しいデバイスを追加**] を使用してインストールメールを送信する。

    注: ElementsソフトウェアElements Connectorを除くでは、[**新しいデバイスを追加する**]を選択してデバイスを追加し、1つの招待状を送信するか、CSVファイルからデータをインポートして複数の招待状を送信するかを選択します。
  - サードパーティのMDMソフトウェアを介してインストールメールを送信する。
- WithSecure Elements Connectorのインストールについては、こちらの手順を参照してください。

メールでインストール リンクを送信する

WithSecure Elementsソフトウェアのインストールリンクを記載したメールを会社のユーザーに送信できます。

注: インストールリンクは30日間有効です。

このリンクを使用して、企業のユーザーは都合の良いときに、自分のデバイスに製品をインストールすることができます。インストールが完了すると、デバイスは次に表示されますWithSecure Elementsアカウント。

インストールするソフトウェアをユーザーに提供するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   [**デバイス**] の横の [**新しいデバイスの追加**] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。
   「**デバイス**」画面が表示されます。
2. [**デバイス**] の横の ••• を選択します。
   メニューが表示されます。
3. メニューから、[**新しいデバイスを追加する**] を選択します。
   [**新しいデバイスの追加**] ページが開きます。

   注: *スコープ セレクタ*が特定の企業を重視している場合、ホーム ページに [**新規デバイスを追加**]ボタンが表示され、「**新規デバイスを追加**」フォームをワンクリックで開けるようになります。
4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。
6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。
   複数の招待状を送る場合は、[**CSVファイルからインポート**] で [**ファイルを選択**] を選び、データをインポートするCSVファイルを選択します。複数のメールアドレスは、カンマで区切る必要があります。
7. [**送信**] を選択します。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

注： 保留中の招待を表示するには、まず [**デバイス**] の横にある ... を選択し、次に [**デバイスの招待の管理**] を選択します。

注： 対象のソフトウェアは [**新規デバイスを追加**] ページで選択したサブスクリプションキーを使用します。

デバイスに製品がインストールされ、アクティベートされると、[**デバイス**]ページに表示され、管理デバイスの招待のページから招待状が表示されなくなります。

ポータルからソフトウェアをダウンロードする

WithSecureソフトウェアのインストールパッケージはWithSecure Elementsポータルからダウンロードすることができます。

ソフトウェアをダウンロードするには

1. WithSecure Elementsにログインします。
2. サイドバーから [**ダウンロード**] をクリックします。
   「**ダウンロード**」ページが開きます。
3. 「**ソフトウェアをダウンロードする**」ページでダウンロードするソフトウェアを選択します。
   「インストーラのダウンロード」ページが開きます。
4. 次のことを実行します。
   a) ドロップダウン メニューから、インストーラをダウンロードする企業を選択します。
   b) 利用可能な製品とサブスクリプション キーを選択します。
5. [**ダウンロード**] を選択します。
   ソフトウェアがダウンロードされ、サブスクリプション キーがインストーラに埋め込まれます。

対象のソフトウェアをダウンロードした後、管理するコンピュータまたはモバイルデバイスにソフトウェアを転送・インストールできます。サブスクリプションキーは製品に埋め込まれます。

重要： WithSecure Elements EDR for Computersを持つデバイスに対して「WithSecure Elements EDRのみ」のサブスクリプション キーを使用しないでください。ソフトウェアが破損する可能性があり、その場合には手動で削除する必要があります。

ソフトウェアをダウンロードした後、ソフトウェアを導入する必要があります。

関連タスク

EXEファイルを使用して製品をインストールする

デバイスの自動削除を管理する

設定した日数が経過したオフラインのデバイスを自動的に削除するかどうかを選択できます。

注： この機能はモバイルデバイスには適用されません。

注： デバイスの自動削除は会社レベルでのみ設定できます。

デバイスが削除される前にオフラインにする必要がある期間を定義できます。削除されたデバイスがアクティブになると、サブスクリプションに空きシートがある場合、そのデバイスは管理ポータルに再度表示されます。サブスクリプションがいっぱいの場合、デバイスは管理ポータルに表示されず、保護されません。

デバイスの自動削除をオンにするには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   「**デバイス**」ページが開きます。
2. [**デバイス**] の横の ... を選択します。
   メニューが表示されます。
3. メニューから、[**自動削除を管理する**] を選択します。
   [**自動削除の管理**] ページが開きます。

4. [デバイスを自動的に削除します...] をオンにします。
5. ボックスに、デバイスが削除されるまでにオフラインになる日数を入力します。

   注 : 最小日数は7日です。

6. [保存] を選択します。

   重要 : 削除されたデバイスが削除後にアクティビティを再開した場合、サブスクリプションに空き容量がある場合、そのコンピュータは自動的にサブスクリプションに再度追加されます。ただし、サブスクリプションがいっぱいの場合、デバイスはサブスクリプションに戻されず、保護されないままになります。

2.5.2 招待の管理

受信者が1つのデバイスにアプリをインストールできるようにするインストールリンクを記載したメールを送信できます。

招待状を管理するには

1. [環境] のサイドバー から [デバイス] を選択します。

   [デバイス] の横の [新しいデバイスの追加] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。

   「デバイス」画面が表示されます。

2. 選択する [デバイスの招待を管理する]。
   の デバイスの招待を管理するページが開きます。

   の [保留中]タブには、まだ使用されていないインストールリンクを含む電子メールの招待状がリストされます。[期限切れ]タブには期限切れの電子メール招待状が一覧表示されます。

3. 保留中の招待については、[リマインダーを送信]インストール リンクが有効な限り (30 日間)。その後は、招待状は [期限切れ] タブに表示されます。
4. 期限切れの招待状については、次のオプションを選択して別の招待リンクを送信できます。[新しい招待状を送信]。

   注: ユーザーが退職したなど、不要になったデバイスがある場合は、期限切れの招待状をテーブルから削除できます。[削除保留中]。

2.6 ポータルでデバイスを管理する

選択したデバイスをポータルで管理する方法について説明します。

2.6.1 デバイスをリモートから管理する

選択したデバイスにコマンドを送信したり、WithSecure Elementsポータルを介してデバイスを管理したりすることができます。

デバイスをリモート管理するには

1. [環境] のサイドバー から [デバイス] を選択します。

   [デバイス] の横の [新しいデバイスの追加] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。

   「デバイス」画面が表示されます。
2. 次のいずれかのタブを選択します。
   - コンピュータ - WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversのデバイスを表示します
   - モバイルデバイス -WithSecure Elements Mobile Protectionを搭載したデバイスを表示します

- **コネクタ-** - WithSecure Elements Connectorを導入しているデバイスを表示します
- **保護されていないデバイス** - 顧客のActiveDirectoryにあるデバイス⊠EPP内にはない⊠を表示します

3. デバイスの名前の横にあるチェック ボックスを選択します。
ページの下にメニューが表示されます。
4. メニューから該当する操作を選択します。

注： 操作は**デバイスの詳細**ページでも確認できます。 一部の操作はここにのみ表示されます。

選択したデバイスが指示が送信されます。

関連概念
セキュリティを監視するページ122

2.6.2 デバイスを自動的に削除する

設定した日数にわたってオフラインになったデバイスを自動的に削除するようにポータルを設定できます。

注： この機能はモバイルデバイスには適用されません。

注： デバイスの自動削除は会社レベルでのみ設定できます。

自動削除を管理するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
「**デバイス**」ページが開きます。
2. [**デバイス**] の横の ··· を選択します。
メニューが表示されます。
3. [**自動削除を管理する**] を選択します。
[自動削除の管理] ページが開きます。
4. [**デバイスを自動的に削除する...**] オプションをオンにします。
5.
6. ボックスに、デバイスが削除されるまでにオフラインになる日数を入力します。

注： 最小日数は7日です。

7. [**保存**] を選択します。

重要： 削除されたデバイスが削除後にアクティビティを再開した場合、サブスクリプションに空き容量がある場合、そのコンピュータは自動的にサブスクリプションに再度追加されます。ただし、サブスクリプションがいっぱいの場合、デバイスはサブスクリプションに戻されず、保護されないままになります。

2.6.3 Active Directory の構成に基づいてデバイスを表示する

Active Directory の構成に基づいてデバイスを表示できます。

この機能を使用して、異なる Active Directory グループ内のデバイスに異なるプロファイルを割り当てることができます。

Active Directory の構成に基づいてデバイスを表示するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
「**デバイス**」画面が表示されます。
2. を選択 ﹀ 左上隅にあるアイコンをクリックします。
ドロップダウン メニューが表示され、アカウントに関連付けられているすべての顧客企業が一覧表示されます。

3. 対象となる企業を選択します。
4. [すべてのデバイス] の横にある ﹀ アイコンを選択します。

   注： ドロップダウン メニューは、企業に Active Directory グループに属するデバイスがある場合に表示されます。

   ドロップダウンメニューに、選択した企業の Active Directory 構成が表示されます。
5. 対象の Active Directory グループを選択すると、グループ内のすべてのデバイスが表示されます。

   注： Active Directoryの構造は、会社のコンピュータから報告されたデータに基づいて構築されるため、完全ではない可能性があります。新しいActive Directoryドメインは、次の操作を行うまでポータルに表示されません。WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversそのドメイン内のコンピューターでアクティブ化されます。

2.6.4 デバイスビューのカスタマイズ

フィルターを適用して、デバイス テーブルに表示する列を選択できます。

[デバイス] ビューをカスタマイズするには

1. [環境] のサイドバー から [デバイス] を選択します。
   「デバイス」画面が表示されます。
2. 表の上にあるドロップダウン メニューから、デバイスをフィルタリングするための列の名前と、選択した列の目的の値を選択します。

   注： 選択するとすべてのフィルターを削除できます [すべてのフィルターをクリア]。

   指定したフィルタの条件に一致するデバイスが一覧に表示されます。
3. テーブルの上の右隅で、|||を選択します。
   ドロップダウンメニューが開き、[表示されている列] リストが表示されます。
4. テーブルに表示させたい列を選択します。
   選択した列がテーブルに表示されます。
5. テーブルの列の順序を変更するには、次の手順を実行します。
   a) 移動する列の名前をポイントします。
   b) 列を表示する場所に応じて、リスト内で列を上下にドラッグします。
6. 1ページあたりの表に表示される行数を定義するには、次のようにします。
   a) テーブルの上の右隅で、⇆を選択します。
   b) ドロップダウンメニューから、必要な行数を選択します。
   行数は選択に応じて変わります。
7. 1ページの表に表示できるよりも多くのデバイスがある場合は、表の上にあるナビゲーション矢印 ⊠ ‹、 › ⊠を使用して、前または次のページに移動します。
8. 選択する [ビュー⊠] > [名前を付けて保存]右上隅にあるをクリックして、カスタマイズしたビューを保存します。

   注: カスタマイズしたビューを削除するには、まず以下を選択します。[ビューを削除する]を選択し、ビューの削除ウィンドウで削除したいビューを選択してから、[消去]。

2.6.5 診断ファイルを要求する

診断データを WithSecure のサポート チームにアップロードすることを許可するようにを顧客に要求できます。

管理対象アカウントのコンピュータに問題がある場合、WithSecure Elements Endpoint Protection管理者がコンピュータを選択して顧客に要求を出すことができます。顧客はFSDIAGファイル(診断データ)を収集してWithSecure Elementsポータルにアップロードできるようになります。診断ファイルは、問題と根本的な原因を詳しく調べるために不可欠です。

注： この機能は、Windows、サーバ (新しいWithSecure Elements EPP for Serversクライアントを含む)、およびコンピュータの両方でのみ使用できます。

診断ファイルを要求するには

1. 複数のアカウントを管理している場合、ポータルにログインして、関連する顧客アカウントを開きます。
2. 正しいアカウントを開いたら、[**環境**]で[**デバイス**]を選択し、関連するデバイス(問題があり、`fsdiag`ファイルが必要なデバイス) へのリンクを選択します。
   デバイスの詳細を含むページが開きます。
3. ページの下部にある**診断操作** > **診断ファイルのリクエスト**を選択します。
4. [**リクエスト**] を選択します。 プライバシー保護のため、エンド ユーザーに通知が表示されます。これはサーバー側では表示されません。

   注： 要求が顧客に送信されたことを確認するには、顧客アカウントで**サポート** > **fsdiag 操作を表示**を開きます。ここで、どのリクエストが行われ、有効期限を確認できます。

5. 顧客が FSDIAG ファイルの収集を許可していることを確認します。これを行うには、顧客のデバイスに通知が表示された際に [**許可**] を選択します。
6. 顧客がFSDIAG ファイルを許可した場合、**サポート** > **fsdiag 操作を表示** を開き、ファイルが現在システムにあることを確認します。
7. [**Fsdiag 操作**] ページで、作成されたFSDIAGファイルの参照番号を取得し、この番号と企業アカウント名、デバイス名をWithSecureサポートへのサポートチケットに記載します。サポート チケットで、WithSecureは参照番号を確認し、詳細な調査を行うためにファイルをダウンロードできます。

   注： FSDIAG ファイルは、WithSecure サポート、またはサポート目的でこの情報にアクセスする必要があるパートナーのみが閲覧できます。FSDIAGファイルは2週間過ぎた時点で自動的に削除されます。

第 章
3

一般的な展開方法

トピック：

ここでは、WithSecure Elementsソフトウェアを問題なく使用できるようにするための最も一般的な展開方法とツールについて説明します。

デバイスにソフトウェアをインストールするためのさまざまな方法とツールが増え続けています。エンドポイントデバイスを保護するには、通常、次のことが必要です。WithSecure Elements Agentがインストールされ、デバイスにアクティベートされます。

WithSecure Computer ProtectionとWithSecure Server Protectionに対応したWithSecure Elements Agentのインストーラは、WithSecure Elementsポータルの**管理**>**ダウンロード**からダウンロードできます。

注： WithSecure Elements Mobile Protectionは、App Store(iOS®やGoogle Play™Android™で入手されるため、ポータルからソフトウェアパッケージをダウンロードすることはできません。該当するWithSecure Elements Endpoint Protectionソフトウェアのインストーラをダウンロードして対象のデバイスに転送したらインストールを実行できます。

3.1 Windowsの展開方法

ここでは、Windowsデバイスの最も一般的な展開方法について説明します。

3.1.1 EXEファイルを使用した手動展開

このデプロイ方法は、ユーザーがサブスクリプションキーを見ることを許可されている小規模な環境に適しています。

注： ユーザーは、デバイスの管理者権限を持つ必要があります。

この展開方法を使用して、インストーラ ファイルをダウンロードし、製品をインストールしてから、サブスクリプション キーを手動で入力します。

注: インストールの特殊なケース、つまり、コマンドラインからインストーラーにパラメーターを渡す方法については、コマンドラインパラメータとMSIプロパティページ80 を参照してください。

製品をインストールするには

1. ポータルにログインします。

   注: または、ログインページで[**ダウンロード**]リンクを選択して、ログインせずにインストールファイルをダウンロードすることもできます。製品のサブスクリプションキーが必要になります。

2. [**管理**] で、サイトバーの [**ダウンロード**] を選択します。
   「**ダウンロード**」ページが開きます。
3. ダウンロードする製品の下で、[**EXE**] を選択します。

   注： EXEファイルにはサブスクリプションキーが含まれています。

   「**インストーラのダウンロード**」ページが開きます。
4. 最初に会社を選択し、次にサブスクリプションキーのある製品を選択して、[**ダウンロード**] を選択します。
   インストールファイルがダウンロードされます。
5. ダウンロードしたファイル`.exe`をダブルクリックしてインストールを開始させます。
   コマンドラインパラメータを使用するには、コマンドラインコマンドでインストールを開始します。

   ```
   installer_AB12-CD34-EF56-GH78_.exe
   ```

   ヒント： サイレントインストール`サイドグレードがないの場合`を実行する場合、インストーラファイル名に「`--silent`」を追加します (例: `installer_AB12-CD34-EF56-GH78_.exe --silent`)。インストーラのファイル名にライセンス キーコードを追加する必要があります。

6. 言語と再起動オプションを選択して [**次へ**] をクリックします。
7. 使用許諾契約を確認します。同意する場合、[**同意する**] を選択します。
8. 画面上の指示に従います。

3.1.2 MSIファイルを使用した手動展開

WithSecure Elements EPP for ComputersとWithSecure Elements EPP for Serversは、MSIファイルを使用してオフラインでインストールすることができます。

注： MSIファイルを他の展開オプションに使用することもできます。

注: インストールの特殊なケース、つまり、コマンドラインからインストーラーにパラメーターを渡す方法については、コマンドラインパラメータとMSIプロパティページ80 を参照してください。

製品をインストールするには

1. ポータルにログインします。

   注: または、ログインページで[**ダウンロード**]リンクを選択して、ログインせずにインストールファイルをダウンロードすることもできます。製品のサブスクリプションキーが必要になります。

2. [**管理**] で、サイトバーの [**ダウンロード**] を選択します。
   「**ダウンロード**」ページが開きます。
3. ダウンロードする製品の下で、[**MSI**] を選択します。
   インストールファイルがダウンロードされます。
4. ダウンロードしたファイル⊠.msi⊠をダブルクリックしてインストールを開始させます。
   コマンドラインパラメータを使用するには、コマンドラインコマンドでインストールを開始します。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=AB12-CD34-EF56-GH78
LANGUAGE=en
```

   MSIファイルにプロパティを埋め込むか、コマンドラインで提供することによって、製品を設定することができます。MSIファイルにプロパティを埋め込む手順については、コマンドラインパラメータとMSIプロパティページ80 を参照してください。

   注: MSIファイルにプロパティを埋め込んでいる間に新しいMSIファイルを作成すると、電子署名が無効になります。

関連概念

コマンドラインパラメータとMSIプロパティページ80
.exeとMSIの両方のインストーラを構成して、あなたの環境の特別なニーズに適応させることが可能です。

関連タスク

Active Directory GPOで展開するページ29
この導入方法は、Active Directoryを使用し、グループポリシーでソフトウェアを豆腐したい企業に適しています。

3.1.3 メールでユーザーを招待する

この方法は、ユーザーがサブスクリプション キーを確認せずに単一のデバイスをインストールする場合に適しています。

ポータルからユーザーを招待するには、ダウンロードリンクを含む電子メールメッセージを送信します。WithSecure Elements Agent。

インストールするソフトウェアをユーザーに提供するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   [**デバイス**] の横の [**新しいデバイスの追加**] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。
   「**デバイス**」画面が表示されます。
2. デバイスの横にある ••• アイコンを選択します。
   メニューが表示されます。
3. メニューから、[**新しいデバイスを追加する**] を選択します。
   「**新規デバイスを追加**」フォームが表示されます。

注： *スコープ セレクタ*が特定の企業を重視している場合、ホーム ページに [**新規デバイスを追加**]ボタンが表示され、「**新規デバイスを追加**」フォームをワンクリックで開けるようになります。

4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。
6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。
   複数の招待状を送る場合は、[**CSVファイルからインポート**] で [**ファイルを選択**] を選び、データをインポートするCSVファイルを選択します。複数のメールアドレスは、カンマで区切る必要があります。
7. [**送信**] を選択します。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

   注： デバイスメニューの [**デバイス招待の管理**] を選択すると、保留中の招待を確認することができます。

   注： 対象のソフトウェアは [**新規デバイスを追加**] ダイアログで選択したサブスクリプションキーを使用します。

デバイスに製品がインストールされ、アクティベートされると、[**デバイス**]ページに表示され、管理デバイスの招待のページから招待状が表示されなくなります。

3.1.4 Active Directory GPOで展開する

この導入方法は、Active Directoryを使用し、グループポリシーでソフトウェアを豆腐したい企業に適しています。

インストールを行うには、次が必要となります。

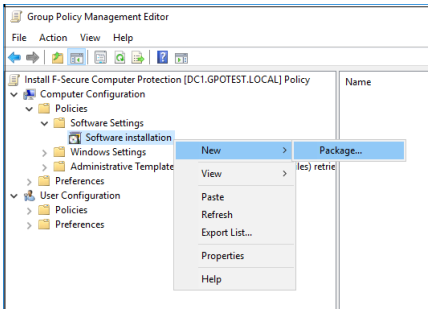
- Active Directory 環境
- 対象ドメインのすべてのメンバーにユニバーサルCRTがインストールされている必要があります。通常、これはWindowsのアップデートに付属しており、定期的にアップデートされるシステムに存在します。インストールで検出に失敗した場合、対応するエラー メッセージが対象システムの Windows イベントログに発行されます。手動でインストールまたは修復する必要がある場合、次のリンクをご覧ください。https://aka.ms/vs/16/release/vc_redist.x86.exe
- 対象ドメインのすべてのメンバーは、すべての UI 機能が正しく機能するために .NET Framework 4.7.2 をインストールしている必要があります。
- ここの手順に従って作成されたカスタマイズされたMSIまたはMSTファイル⊠推奨⊠。少なくとも、サブスクリプションキーを指定するためのVOUCHERのパラメータを追加していることを確認してください。
- インストールを行う前に競合製品を削除する必要がある場合の sidegrade .msi パッケージ: https://download.withsecure.com/PSB/latest/Sidegrade.msi。

WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversは、GPO および MSIパッケージを使用するその他の同様の展開方法を使用してリモートでインストールできます。この展開方法を使用するには、カスタムMSIパッケージ、サブスクリプションキーを含むMSTファイル、およびその他の環境設定を準備する必要があります。その後、パッケージでポリシーを定義し、デバイスに適用する必要があります。

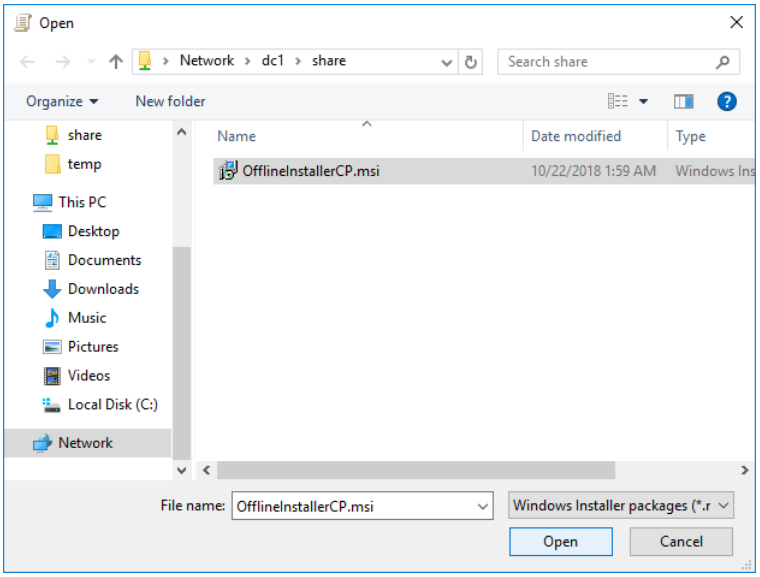
製品をインストールするには

1. MSIインストーラーとMSTファイル⊠使用している場合⊠をドメインコントローラーにコピーします。
2. グループ ポリシー 管理コンソールを開き、ドメインに関連付けする新しいグループ ポリシー オブジェクトを作成します。
3. **コンピュータ設定** > **ポリシー** > **ソフトウェア設定** > **ソフトウェア インストール**の順に開きます。

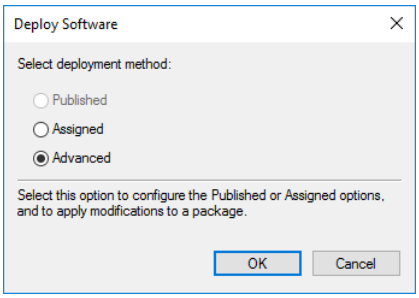
4. 右ペインを右クリックし、**新規** > **パッケージ**の順に選択します。



5. [ファイルを開く]ウィンドウで、`OfflineInstallerCP.msi`を選択してから[**開く**]を選択します。

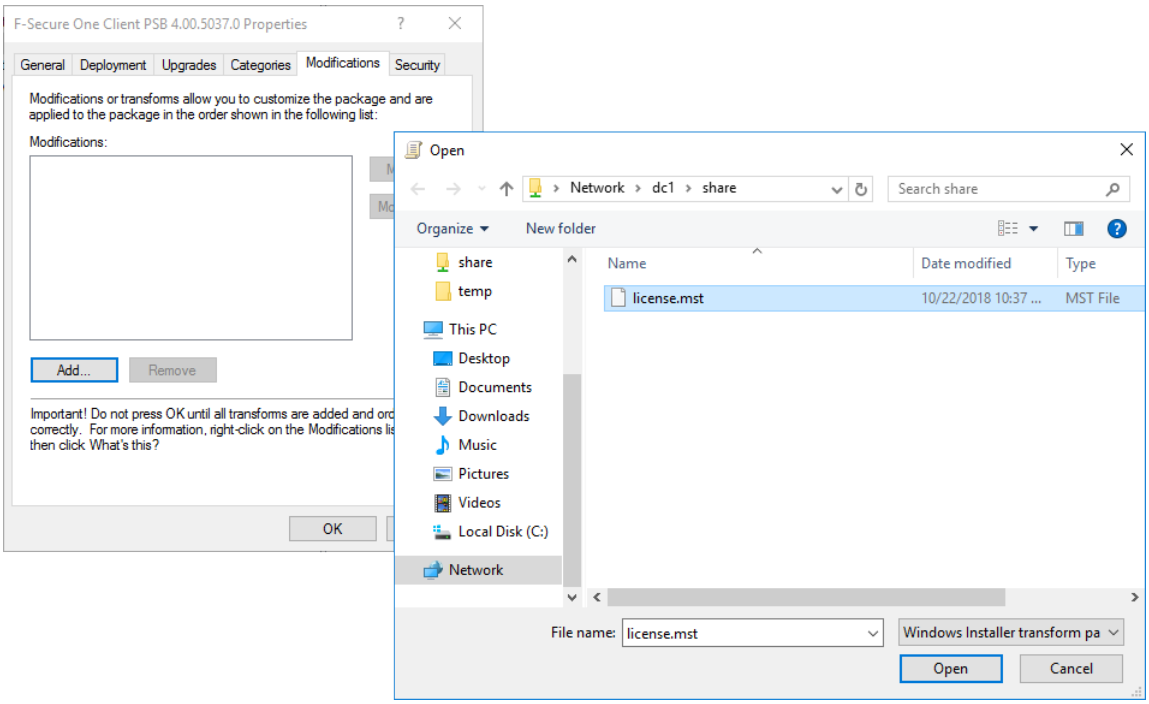


6. 「**ソフトウェアの展開**」ウィンドウで、[**詳細設定**]を選択してパッケージを構成し、[**OK**] を選択します。



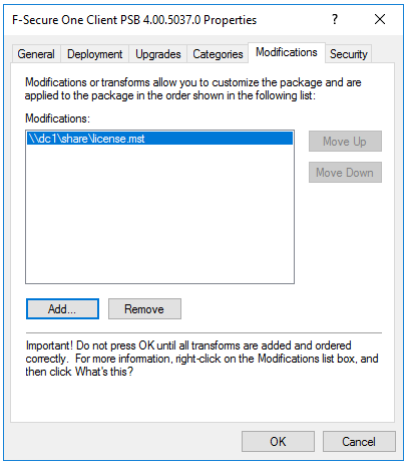
7. [**変更**] タブに移動し、[**追加**] を選択します。

8. [ファイルを開く]ウィンドウで、`license.mst`(前述の`FsMsiTool.exe`からの変換ファイル)を選択して、[開く]を選択します。これにより、変換ファイルのパスがGPO設定に追加されます。



手順3で製品の言語を指定するための `.mst` ファイルを用意した場合、`license.mst` ファイルを追加した同じ方法で、製品の言語コードを含むファイルを GPO 設定に追加します。

9. [OK] を選択して設定を保存します。



WithSecure Elements EPP for Computersは、GPO経由で展開できるようになりました。

ドメイン コンピュータで GPO 設定が更新され、コンピュータが再起動されると、パッケージが展開されます。

3.1.5 GPOを通じてブラウザ保護を設定する

WithSecureブラウザ保護の拡張機能をGoogle Chrome、Microsoft Edge、およびMozilla Firefoxに設定する方法を説明します。

注: この手順は、Elements Endpoint Protectionに特化したもので、管理者ユーザを対象としています。

WithSecureブラウザ保護は、インストールされているWithSecureセキュリティ製品にHTTPSプロトコルのサポートを提供するWebブラウザの拡張機能です。

注: この機能なしでも、非セキュアな接続⊠HTTP⊠のサポートが利用可能です。

この機能により、以下が許可されます。WithSecure不要なWebコンテンツをブロックし、評価アイコンを表示し、セキュアな接続が使用されている場合に検索エンジンのSafeSearchモードを有効にするための機能です。管理者として、これを有効にできます。WithSecureブラウザ保護を強化し、Windowsグループポリシーでその使用を強制します。

「WithSecure ブラウザ保護」拡張機能を Google Chrome にインストールする方法

この手順は、Elements Endpoint Protectionに特化したもので、管理者ユーザを対象としています。

ブラウザ保護拡張機能をインストールして有効にするには

1. 最新の Google Chrome グループ ポリシー テンプレート ADMX ファイルをダウンロードします。
2. 次のChrome管理用テンプレートファイルとシステムで使用している言語の言語フォルダを`C:\Windows\PolicyDefinitions`ディレクトリにコピーします

   `policy_templates/windows/admx/chrome.admx` および `google.admx`
3. これらのファイルと、システムで使用している言語の言語フォルダをSYSVOLフォルダ`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`にコピーします。

   例`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`

   > **注：**「PolicyDefinitions」フォルダがない場合、フォルダを作成する必要があります。
4. Windows グループ ポリシー管理コンソール`gpmc.msc`を開き、新しいグループ ポリシーを作成するか、既存のポリシーを編集します。

   > **注：** 詳細については、「Windows でグループ ポリシー管理用テンプレートのセントラル ストアを作成および管理する」を参照してください。
5. `Computer Configuration/Policies/Administrative Templates/Google/Google Chrome/Extensions/` に移動して、強制インストールされたアプリと拡張機能を設定し、以下のようにポリシーを編集します。
   a) ポリシーをオンにするには、[**有効**] を選択します。
   b) [オプション] で、[**表示...**] を選択し、次の値を入力します。

   ```
   imdndkajeppdomiimjkcbhkafeeooghd
   ```

   > **重要：** 2024年4月2日までは旧ID`jmjjnhpacphpjmnnlnccpfmhkcloaade`が使用されます。

   > **注：** 詳細については、Chromeブラウザポリシーを設定する方法 を参照してください。

グループポリシーを有効にすると、WithSecureブラウザ保護がオンになり、強制的にオンになります。

「WithSecureブラウザ保護」拡張機能を Microsoft Edge（Chromium）にインストールする方法

この手順は、Elements Endpoint Protectionに特化したもので、管理者ユーザを対象としています。

> **注：** WithSecureのブラウザ拡張機能は、Microsoft Group Policy Object（GPO）を介してGoogle Storeからインストールされます。デバイスがMicrosoft Active Directoryドメインのメンバーである必要があります。そうでない場合、このインストールを行うことはできません。

ブラウザ保護拡張機能をインストールするには

1. Microsoft Edgeポリシーファイルを使用して、次の操作を行います。
   a) 最新の Microsoft Edge（Chromium）グループ ポリシー テンプレート ADMX ファイルに移動します。

b) ブラウザのバージョンとビルド、お使いのOSの下にある [Windowsポリシーのダウンロード] を選択し、[同意してダウンロードする] を選択します。
c) ダウンロードしたcabファイルを解凍します。
d) 解凍したフォルダから、以下のファイルとフォルダーを`C:\Windows\PolicyDefinitions`フォルダとSYSVOLフォルダ`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`にコピーします。

- Microsoft Edge Chromium管理用テンプレート ファイル`msedge.admx`と`msedgeupdate.admx`
- システムで使用されている言語の言語フォルダ

注：「PolicyDefinitions」フォルダがない場合、フォルダを作成する必要があります。

2. Windows グループポリシー管理コンソール(gpmc.msc) を開き、次のいずれかを実行します。

注： 詳細については、「Windows で Microsoft Edge ポリシー設定を構成する」を参照してください。

- 新しいグループ ポリシーを作成する
- `Computer Configuration/Policies/Administrative Templates/Microsoft Edge/Extensions/Control`に移動して、次のようにポリシーを編集します。

a. ポリシーをオンにするには、[有効] を選択します。
b. [オプション] で、[表示...] を選択し、次の値を入力します。

```
aambijcigikmdoehgjhdepcpieghopdl
```

重要： 旧ID(cpikpibllpjmpnchjajlibnmmomnnhnm)は2024年4月2日まで使用されます。

グループポリシーを有効にすると、WithSecureブラウザ保護がオンになり、強制的にオンになります。

「WithSecure ブラウザ保護」拡張機能を Mozilla Firefox にインストールする方法

この手順は、Elements Endpoint Protectionに特化したもので、管理者ユーザを対象としています。

ブラウザ保護拡張機能をインストールするには

1. 最新の Mozilla Firefox グループ ポリシー テンプレート ADMX ファイルをダウンロードします。
2. cabファイルを解凍し、次のMozilla Firefoxの管理用テンプレートファイルとシステムで使用している言語の言語フォルダを`C:\Windows\PolicyDefinitions`ディレクトリにコピーします(`windows/mozilla.admx` および `firefox.admx`
3. ファイルと「en-US」フォルダを「SYSVOL」フォルダ`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`にコピーします。
   例`\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`

   注：「PolicyDefinitions」フォルダがない場合、フォルダを作成する必要があります。
4. Windows グループ ポリシー管理コンソール(`gpmc.msc`)を開き、新しいグループ ポリシーを作成するか、既存のポリシーを編集します。
5. `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions` に移動して、以下のようにポリシーを編集します。
   a) ポリシーをオンにするには、[有効] を選択します。

b) [オプション] で、[**表示...**] を選択し、次の値を入力します。

```
https://download.withsecure.com/online-safety/ws_firefox_https.xpi
```

6. `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions` に移動して、拡張機能の無効化と削除を防止し、以下のようにポリシーを編集します。
   a) ポリシーをオンにするには、[**有効**] を選択します。
   b) [オプション] で、[**表示...**] を選択し、次の値を入力します`ols_main@withsecure.com`

グループポリシーを有効にすると、WithSecureブラウザ保護がオンになり、強制的にオンになります。

3.1.6 Microsoft InTuneを使用したビジネスラインへの展開（Windows）

この導入方法は、Microsoft InTuneを使用し、デバイスへのインストールを自動化したい企業に適しています。

この展開方法を使用すると、WithSecure Elements Endpoint Protectionポータルまたはリンク（https://download.withsecure.com/PSB/latest/ElementsAgentOfflineInstaller.msi）からMSIインストーラーパッケージをダウンロードし、Microsoft Intuneで構成します。

> 👉 **注：** Microsoft Intune MDM を使用してAndroidおよびiOSアプリを展開する方法については、Elements Mobile ProtectionヘルプのMicrosoft Intune MDMを参照してください。

Microsoft Intune経由で製品をインストールするには

1. Microsoft Intuneポータルにログインします。
2. [**アプリ**] > [**すべてのアプリ**] > [**追加**]を選択します。
   [**アプリタイプの選択**] ペインが開きます。
3. [**その他の**] のアプリタイプで、**Line-of-business app（基幹業務アプリ）** > **選択**を選択します。
   ページが開き、[**アプリの追加**] の手順が表示されます。
4. [**アプリの追加**] ページで、[**アプリパッケージファイルを選択**] を選択します。
5. [**アプリパッケージファイル**] ペインで、[参照] アイコンを選択し、以前にダウンロードしたMSIインストーラパッケージを選択します。
6. アプリを追加するには、[**OK**] を選択します。
7. [**アプリケーション情報**] ページで、次の手順を実行します。
   a) [**アプリのバージョンを無視**] の横で、[**はい**] を選択して、Microsoft Intuneが自動アップグレードを正しく処理するようにします。
   b) Publisher（WithSecure）やアプリのコマンドライン引数などの詳細を入力します。たとえば、`VOUCHER=xxxx-xxxx-xxxx-xxxx`（サブスクリプションキーを挿入する）。

   > 👉 **注：** 一部の値は自動的に入力される場合があります。

   > 👉 **注：** サポートされているすべてのMSIプロパティはこちらで確認できます。

   > 👉 **注：** WithSecure Elements EPP Agentは、新しいバージョンが利用可能な場合、インストール直後に自動的にアップグレードされる場合があります。その場合、Microsoft IntuneまたはWindows Autopilotの展開プロセスに干渉する可能性があります。この問題を回避するために、UPGRADE_DELAY_MINUTESプロパティを指定することをお勧めします。

8. [**次へ**] を選択して、[**Assignments**] ページに移動します。
9. 優先グループ、ユーザ、またはデバイスを割り当て、[**次へ**] を選択します。
10. [**確認と作成**] ページで、アプリの値と設定が正しいことを確認します。
11. アプリをMicrosoft Intuneに追加するには、[**作成**] を選択します。

3.1.7 Microsoft IntuneをWindowsアプリ（Win32）として使用して展開する

この導入方法は、Microsoft InTuneを使用し、デバイスへのインストールを自動化したい企業に適しています。

この展開方法を使用すると、WithSecure Elements Endpoint Protectionポータルまたはリンク（https://download.withsecure.com/PSB/latest/ElementsAgentInstaller.exe）からEXEインストーラーをダウンロードし、Microsoft Intuneで構成します。

注： Microsoft Intune MDM を使用してAndroidおよびiOSアプリを展開する方法については、Elements Mobile ProtectionヘルプのMicrosoft Intune MDMを参照してください。

Microsoft Intune経由で製品をインストールするには

1. 次のコマンドを実行して、アップロードするインストーラ ファイルを準備します。

```
IntuneWinAppUtil.exe -c <setup_folder> -s ElementsAgentInstaller.exe -o
<output_folder>
```

`ElementsAgentInstaller.intunewin`というパッケージが作成されます。

注： これは、Windowsアプリ（Win32）としてアップロードされるあらゆるインストーラの標準的なステップです。IntuneWinAppUtilツールの詳細については、Microsoftのドキュメントを参照してください。

2. Microsoft Intuneポータルにログインします。
3. **[アプリ]** > **[すべてのアプリ]** > **[追加]**を選択します。
   [**アプリタイプの選択**] ペインが開きます。
4. [**その他の**] のアプリタイプで、**Windowsアプリ（Win32）アプリ** > **選択**を選択します。
   ページが開き、[**アプリの追加**] の手順が表示されます。
5. [**アプリパッケージファイル**] ペインで、[参照] アイコンを選択し、以前に作成したintunewinインストーラパッケージを選択します。
6. アプリを追加するには、[**OK**] を選択します。
7. [**アプリケーション情報**] ページで、次の情報を入力します。
   - 名前（WithSecure Elements Agent
   - 公開元（WithSecure
8. [**次へ**] を選択して、[**プログラム**] ページを開きます。
9. [プログラム] ページで、次の操作を行います。
   a) **install**コマンドを次のように入力します（

```
ElementsAgentInstaller.exe --silent --voucher <license-keycode>
```

   注： サポートされているすべてのコマンドラインオプションはここで確認できます。

   b) **uninstall**コマンドを次のように入力します（

```
powershell.exe -ExecutionPolicy Bypass $cmd =
[Microsoft.Win32.RegistryKey]::OpenBaseKey('LocalMachine',
'Registry32').OpenSubKey('SOFTWARE\F-
Secure\NS\default\OneClient').GetValue('UninstallCommand'); Start-Process
 -FilePath $cmd -ArgumentList '--silent' -Wait
```

10. [**次へ**] を選択して、[**Requirements**] ページに移動します。
11. [**要件**] ページで、WithSecure Elements Agentをインストールする前に、デバイスが満たす必要のある要件を入力します。

注： WithSecure Elements Agent のシステム要件はこちらで確認できます。

12. [次へ] を選択して、[検出ルール] ページを開きます。
13. [検出ルール] ページで、検出ルールのパラメーターを次のように設定します。
    - ルールの形式⊠検出ルールを手動で設定する
    - ルールの種類⊠レジストリ
    - キーパス⊠`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\Monitoring`
    - 値の名前⊠有効
    - 検出方法⊠値あり
    - 64ビットクライアントで32ビットアプリに関連付けられている⊠はい
14. [次へ] を3回選択して、[Assignments] ページに移動します。
15. 優先グループ、ユーザ、またはデバイスを割り当て、[次へ] を選択します。
16. [確認と作成] ページで、アプリの値と設定が正しいことを確認します。
17. アプリをMicrosoft Intuneに追加するには、[作成] を選択します。

3.1.8 仮想デスクトップインフラストラクチャ□VDI□システムの永続モードで展開する

ゴールデンイメージを使用して、CitrixやVMware Horizonサーバー、および他のVDI環境に製品をインストールする手順は次のとおりです。

注: ゴールデンイメージは、マスターイメージまたはクローンイメージと呼ばれることもあります。

インストールを行うには、次が必要となります。

- WithSecure Elements Endpoint Protectionポータルからダウンロードできるネットワークインストーラファイル。

  注: MSIオフラインインストーラを使用する場合は、UNIQUE_SIGNUP_ID=smbiosまたはUNIQUE_SIGNUP_ID=adguidパラメータを使用して使用できます。詳細については、コマンドラインパラメータとMSIプロパティページ80 を参照してください。

- イメージが使用される予定の対象会社のサブスクリプションキー。

コンピュータシステム管理BIOSグローバルユニーク識別子⊠SMBIOS GUID⊠は、デバイスが前回の製品インストールに使用された同じデバイスであるかどうかを検出します。世界中には、複数のコンピューターのSMBIOS GUIDが同じ場合が多いため、解決策は特別なフラグの後ろにあります。SMBIOS GUIDに頼ることができない環境で、デバイスがActive Directoryドメインに参加している場合、代わりにActive DirectoryコンピュータGUIDを使用できます。

ゴールデンイメージを準備する

ゴールデン イメージを準備する方法の説明。

ゴールデンイメージを準備するには

1. [管理] で、サイトバーの [ダウンロード] を選択します。
   「ダウンロード」ページが開きます。
2. WithSecure Elements Agent for ComputersまたはWithSecure Elements Agent for Serversで、[EXE]を選択して、実行中のゴールデンイメージテンプレートにネットワークインストーラファイルをダウンロードします。
3. 管理者権限でコマンド プロンプトを開きます。
4. コマンドプロンプトで次のコマンドを入力して、ツールを実行します。

```
<tool_folder>\installer.exe --use_smbios_guid
```

注: あるいは、`--usesmbiosguid`の代わりに`--useadguid`を使用して、デバイスをActive DirectoryコンピュータGUIDに関連付けることもできます。コマンドラインパラメータとMSIプロパティページ80 にある他のコマンドラインパラメータを使用することもできます。

5. まだ指定していない場合は、サブスクリプションキーを入力します。

6. ポータルでデバイスが正しく表示されていることを確認してください。

   注: このデバイスは、ゴールデンイメージの作成と更新にのみ使用されます。

7. 製品がすべての最新のコンポーネントとデータベースをダウンロードしてインストールするまで待ちます。
8. 次のコマンドを実行して、ポータルからログアウトします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe" --nokeycode
```

9. ゴールデンイメージテンプレートを作成します。

   重要: 次に、.NET Frameworkの説明に従って、ゴールデンイメージからサーバーを導入します。

ゴールデンイメージの更新

ゴールデン イメージを更新する方法の説明。

ゴールデン イメージを更新するには:

1. ゴールデン イメージを適切なサーバー インスタンスに復元します。
2. 次のコマンドを実行してポータルにログインします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe" --keycode
<subscription-key>
```

3. 右クリックしてWithSecure Elements Agentシステムトレイ領域のアイコンをクリックしてコンテキストメニューを開き、[**アップデートを確認**]。
4. すべての更新がインストールされるまでお待ちください。
5. 必要に応じて、Windows Update をインストールするなど、ゴールデン イメージにその他の変更を適用します。
6. 次のコマンドを実行して、ポータルからイメージをログアウトします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe" --nokeycode
```

7. 更新されたゴールデンイメージテンプレートを作成します。

ゴールデンイメージを使用してサーバーをデプロイする

Citrixのゴールデンイメージからサーバーを作成するテスト方法について説明します。

ゴールデンイメージを使用してサーバーをデプロイするには

1. イメージを新しいサーバーに復元します。
2. サーバが再起動し、ネットワークに接続できるようになったら、以下のインストール後のコマンドを実行して、ログアウトツールを実行することを確認してください。

```
"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe"
 --keycode <subscription-key>
```

   注: イメージの製品をインストールしたときに使用したものと同じサブスクリプションキーを使用する必要があります。セキュリティ上の理由から、このインストール方法でサブスクリプションを切り替えることはできません。

   新しいSMBIOS GUIDを使用する2番目のデバイス⊠サーバ⊠がWithSecure Elementsポータルに作成されます。

3. サーバが使用する通信IDを見つけるには、**設定** > **集中管理** > **一意のID**に移動します。IDはSMBIOS GUIDではありませんが、WithSecureが入力したIDであり、イメージを復元しても同じです。

   注: このMicrosoftの指示に従ってSMBIOS GUIを確認することもできます。

4. ゴールデンイメージが更新され、それをサーバに再展開する場合は、上記の手順1⊠3を繰り返します。
   サーバは、ポータルのデバイス情報とプロファイル情報を使用して、同じSMBIOS GUIDでシステムに再登録されます。

復元または新規導入したデバイスのプロファイルを設定する

ゴールデンイメージに設定されたプロファイルは、イメージを復元するときに使用されることはありません。

新しいデバイスのイメージを初めて復元すると、ポータルのプロファイル セクションで定義されたプロファイル割り当てルールに基づいて、デバイスは会社のデフォルト プロファイルを自動的に取得します。プロファイルのプロファイル ID 値をコピーして、次のいずれかを実行することで、設定を上書きし、手動でプロファイルを指定できます。

- コマンドラインに次のコマンドを入力します。

```
"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe" --profile-id
<profile-id>
```

  注: このパラメータは、他のデフォルトのプロファイル割り当てをオーバーライドします。

- `fs_oneclient_logout.exe`ツールを実行する前に、Active Directoryグループにデバイスを登録します。これにより、システムに登録する際に、デバイスはActive Directoryグループに割り当てられたデフォルトのプロファイルを使用します。
- 新しいデバイスを追加した後、ポータルで手動でプロファイルを設定します。

注: 同じSMBIOS GUIDの同じデバイスを再度リストアすると、そのデバイスに最後に定義されたプロフ ァイルが自動的に使用されます。デバイスの追加時にプロファイルを手動で設定した場合、デバイスを復元するときには、そのデバイスに設定したプロファイルが使用されます。

3.2 Macデバイスの展開方法

ここでは、Macデバイスの最も一般的な展開方法について説明します。

3.2.1 製品の自動インストール、アクティベーション、構成

WithSecure Computer Protection for Macを自動的にインストールして構成し、サブスクリプションを有効にする方法について説明します。

製品を自動的にインストールする

サイレントインストールを実行する方法について説明します。

macOSは、ユーザの操作を必要としない製品パッケージのサイレントインストールをサポートしています。`Terminal`または`ssh`を使用して製品をインストールできます。

サイレントインストールを実行するには

次のコマンドを実行します。

```
sudo installer -pkg /path/to/pkg -target /
```

注: 詳細とオプションについては、manインストーラを参照してください。

注: 使用している配布ツールが`.pkg`インストーラを必要とする場合、`.mpkg`インストーラを`.pkg`に変更することができます。

サブスクリプションをアクティベートするには

製品のサブスクリプションをアクティベートする方法の説明。

製品をインストールしたら、アクティベートする必要があります。

注: サブスクリプションを更新する場合、アクティベーションを行う必要はありません。

ユーザーの操作なしで自動的にアクティブ化する方法は2つあります。

- 製品パッケージ名にサブスクリプションキーを埋め込むことができます。製品はインストールのプロセス中にアクティベートされます。
- WithSecure Elements EPP for Computers (Mac)バージョン17.8.32555以降で配布される`activator`ツールを使用して製品をアクティベートできます。

サブスクリプションをアクティベートするには

注: サブスクリプションをアクティブにするには、インターネットのアクセスが必要です。

1. サブスクリプションキーを製品パッケージ名に埋め込んで製品をアクティベートするには、次のいずれかを実行します。
   - WithSecure Elementsポータルから製品インストールパッケージをダウンロードするときにサブスクリプションキーを選択します
   - 製品パッケージを以下の形式になるように手動で変更します `F-Secure_PSB_Mac_Installer[XXXX-XXXX-XXXX-XXXX-XXXX].pkg`

     注: ソフトウェア管理ツールが角括弧を受け入れない場合は、代わりに二重下線を使用できます `F-SecurePSBMacInstallerXXXX-XXXX-XXXX-XXXX-XXXX.pkg`

   製品はインストールのプロセス中にアクティベートされます。
2. `activator`ツールを使用して製品をアクティベートするには、次のコマンドを入力します。

```
/Library/F-Secure/bin/activator --subscription-key "<subscription key>"
```

注: `activator`ツールは、WithSecure Elements EPP for Computers (Mac)バージョン17.8.32555以降で配布されます。

デフォルトのプロファイルとインストールタグを割り当てる

製品をインストールした後、サブスクリプションをアクティベートする前に、デバイスにデフォルトのプロファイルとインストールタグを割り当てることができます。

デフォルトのプロファイルとインストールタグを割り当てるには

1. 製品をインストールした後、次のコマンドを入力してデフォルトのプロファイルをカスタマイズできます。

```
/Library/F-Secure/bin/activator --profile-id <your profile id>
```

   サブスクリプションをアクティブ化した後、COSMOS設定のプロファイルID値をデバイスに設定します。例 `--profile-id 18062053`

   注: プロファイルIDを見つけるには、プロファイルエディタでプロファイルを開きます。 プロファイルIDは、次のURLにあります `https://emea.psb.f-secure.com/#/c1234567/profiles/computer-protection/edit/1112223/generalSettings`。この例では、最初の値`c1234567`は会社のプロファイルIDであり、2番目の値`1112223`はプロファイルIDです。
2. 次のコマンドを入力して、カスタマイズされたインストールタグを割り当てることができます。

```
/Library/F-Secure/bin/activator --tags "<tags>"
```

サブスクリプションをアクティベートすると、カスタマイズされたタグがデバイスに割り当てられます。

3. 製品をアクティベートする前に、デフォルトのプロファイルとインストールタグにパラメータを追加できます。activatorツールと使用可能なオプションの使用方法の詳細については、次のコマンドを入力してヘルプを参照してください。

```
/Library/F-Secure/bin/activator --help
```

次の出力が表示されます。

```
USAGE: activator [--profile-id <profile-id>] [--tags "<tags>"] ^
[--subscription-key "<subscription-key>" ^

OPTIONS:^
-p, --profile-id <profile-id> ^
 ID of the desired PSB profile. Example: 123456.
-t, --tags <tags> Installation tags values. Example: "PSB=tag1:tag2:tag3,^

 department=R&D,role=engineer". ^
-s, --subscription-key <subscription-key> ^
 Subscription key to activate. ^
-h, --help Show help information.
```

一般的な配布シナリオ

以下に、配布の一般的なシナリオを示します。Elements Endpoint Protectionソフトウェア。

以下の方法で製品を配布できます。

- ssh
- MDMまたは別のソフトウェア配布ソリューション⊠Munkiなど⊠による製品の手動アクティベーションと構成
- MDM または他のソフトウェア配布ソリューションを使用して、カスタム パッケージを使用して製品をアクティブ化し、構成します。
- MDM または他のソフトウェア配布ソリューション。1 つのパッケージを使用して製品のインストールとアクティベーションの両方を実行します。

注: MDMとは別に、別のソフトウェア配布ソリューションを使用することもできます。パッケージのインポート手順については、サードパーティソリューションのドキュメントを参照してください。

ソフトウェアを配布する

WithSecure Elements EPP for Computers (Mac)の配布方法について説明します。

1. 次の方法で、ssh経由でソフトウェアを配布できます。
   a) scpまたは別の方法を使用して、インストールパッケージを対象のマシンにコピーします。
   b) sshを使用して、対象のマシンでインストーラを実行します。

注: サイレントインストールの詳細については、「製品の自動インストール」を参照してください。

   c) sshを使用して、対象のマシンで必要な構成パラメータを指定してactivatorを実行します。
2. MDMや他のソフトウェア配布ソリューション⊠Munkiなど⊠を使用してソフトウェアを配布するには、以下のように製品を手動でアクティベートおよび構成します。
   a) インストールパッケージをMDMにインポートして、組織内のMacコンピューターにソフトウェアをインストールできるようにします。
   b) sshを使用して、対象のコンピュータ上で必要な構成パラメータを指定してactivatorを実行します。
   c) コンピュータをアクティベートし、WithSecure Elementsポータルに接続します。

3. アクティベーションと構成にカスタムパッケージを使用してMDMで製品を配布するには、次の手順を実行します。
   a) インストールパッケージをMDMにインポートして、組織内のMacコンピュータに製品をインストールできるようにします。
   b) 次のようにactivatorの呼び出しを使用して、カスタムmacOSソフトウェアパッケージを作成し、配布ソフトウェアにインポートします。

      注: macOSで提供されるpkgbuildユーティリティを使用してパッケージを作成します。

```
PROFILE_ID=<desired profile id>
TAGS=<desired installation tags>
ACTIVATION_KEY=<subscription key>

ACTIVATION_PACKAGE_SCRIPTS=./scripts
echo """#!/bin/zsh
/Library/F-Secure/activator \\
 --profile-id $PROFILE_ID \\
 --tags \"$TAGS\" \\
 --subscription-key \"$ACTIVATION_KEY\"
""" > ./$ACTIVATION_PACKAGE_SCRIPTS/postinstall
chmod +x ./$ACTIVATION_PACKAGE_SCRIPTS/postinstall
ACTIVATION_PACKAGE_IDENTIFIER=com.your-company.f-secure.macprotection.activation
pkgbuild \
 --nopayload \
 --scripts $ACTIVATION_PACKAGE_SCRIPTS \
 --identifier $ACTIVATION_PACKAGE_IDENTIFIER \
 "${ACTIVATION_PACKAGE_IDENTIFIER}.pkg"
```

      注: --nopayloadフラグは、パッケージがmacOSにインストールされているパッケージにリストされていないことを意味します⊠システムにファイルをインストールしない⊠。

   c) 必要な数だけアクティベーションパッケージを作成し、特定のデバイスまたはデバイスグループに割り当てます。

      注: 元のパッケージはそのままの状態で、指定された署名を保持します。macOSがカスタムパッケージを検証するには、署名と公証が必要です。

4. 製品のインストールとアクティベーションを1つのパッケージでMDMで配布する場合は、次の手順を実行します。
   a) 次のprepare-installer.shスクリプトを使用して、インストールパッケージに基づく特別な製品パッケージを作成します。

```
prepare-installer.sh \
 /path/to/com.f-secure.macprotection.mpkg \
 /path/to/install-and-activate.pkg \
 "<Signing identity>" \
 "<profile id>" \
 "<installation tags>" \
 "<subscription key>"
```

      注: スクリプトをそのまま、またはインスピレーションとして使用して、ニーズにより適した独自のスクリプトを作成できます。

関連概念

macOSでのソフトウェアの署名と公証ページ48

カスタム製品パッケージを検証し、macOSへのインストールを許可するには、パッケージに署名と公証が必要です。

MDMプロファイルを使用して製品を設定する

MDMプロファイルは、組織内の多数のデバイスに製品をセットアップするのに役立ちます。

> 👉 **注：** これらの説明は、製品バージョン 23.2 以降に適用されます。製品バージョン24.1以降の手順については、プレアナウンスメントをご参照ください。新しいWithSecureクライアント。macOS版。

製品構成をデバイスに展開するためのMDMプロファイルを作成するには、次の手順に従います。

1. システム環境設定のMDMプロファイルを生成します。
   次のテンプレートを使用して、独自のMDMプロファイルを作成または拡張します。

   > 👉 **注：** テンプレート内のすべての`PayloadUUID`および`PayloadIdentifier`値を独自の値に置き換えます。たとえば、`uuidgen`コマンドラインツールを使用してUUIDを生成できます。

   すべてのWithSecureカーネル拡張を許可する

   > 👉 **注：** macOS 10.15.5以前で必要です。詳細については、Apple Developerのドキュメントを参照してください。。
   > https://developer.apple.com/documentation/devicemanagement/systemextensions

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
 <dict>
 <key>AllowUserOverrides</key>
 <true/>
 <key>AllowedTeamIdentifiers</key>
 <array>
 <string>6KALSAFZJC</string>
 </array>
 <key>PayloadDescription</key>
 <string>Allows F-Secure Kernel Extensions</string>
 <key>PayloadDisplayName</key>
 <string>F-Secure Kernel Extensions</string>
 <key>PayloadIdentifier</key>

<string>com.apple.syspolicy.kernel-extension-policy.88C7AA59-0157-4267-B00B-E908A7D50123</string>

 <key>PayloadType</key>
 <string>com.apple.syspolicy.kernel-extension-policy</string>
 <key>PayloadUUID</key>
 <string>88C7AA59-0157-4267-B00B-E908A7D50123</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
 <key>PayloadOrganization</key>
 <string>F-Secure Corporation</string>
 </dict>
 </array>
 <key>PayloadDisplayName</key>
 <string>F-Secure CP and RDR Profile</string>
 <key>PayloadIdentifier</key>
 <string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
 <key>PayloadRemovalDisallowed</key>
 <false/>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
```

```
 <string>00000000-0000-0000-0000-000000000001</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

すべてのWithSecureシステム拡張を許可する

注： macOS 10.15.5以降で必要です。詳細については、Apple Developerのドキュメントを参照してください。
https://developer.apple.com/documentation/devicemanagement/systempolicykernelextensions

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
 <dict>
 <key>AllowUserOverrides</key>
 <true/>
 <key>AllowedTeamIdentifiers</key>
 <array>
 <string>6KALSAFZJC</string>
 </array>
 <key>PayloadDescription</key>
 <string>Allows F-Secure System Extension</string>
 <key>PayloadDisplayName</key>
 <string>F-Secure System Extension</string>
 <key>PayloadIdentifier</key>

<string>com.apple.system-extension-policy.B1E740C4-052A-4B64-AB54-2962327B6512</string>

 <key>PayloadType</key>
 <string>com.apple.system-extension-policy</string>
 <key>PayloadUUID</key>
 <string>B1E740C4-052A-4B64-AB54-2962327B6512</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
 <key>PayloadOrganization</key>
 <string>F-Secure Corporation</string>
 </dict>
 </array>
 <key>PayloadDisplayName</key>
 <string>F-Secure CP and RDR Profile</string>
 <key>PayloadIdentifier</key>
 <string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
 <key>PayloadRemovalDisallowed</key>
 <false/>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>00000000-0000-0000-0000-000000000001</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

WithSecureシステム拡張のコンテンツフィルタリングを許可する

注： macOS 10.15.5以降で必要です。詳細については、Apple Developerのドキュメントを参照してください。
https://developer.apple.com/documentation/devicemanagement/webcontentfilter

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
 <dict>
 <key>UserDefinedName</key>
 <string>F-Secure Firewall</string>
 <key>PluginBundleID</key>
 <string>com.f-secure.fsmac.gui</string>
 <key>FilterDataProviderBundleIdentifier</key>
 <string>com.f-secure.fsmac.gui.FSCSystemExtension</string>
 <key>FilterDataProviderDesignatedRequirement</key>
 <string>identifier "com.f-secure.fsmac.gui.FSCSystemExtension" and anchor
 apple generic and certificate leaf[subject.OU] = "6KALSAFZJC"</string>
 <key>FilterSockets</key>
 <true/>
 <key>FilterPackets</key>
 <false/>
 <key>FilterBrowsers</key>
 <false/>
 <key>FilterType</key>
 <string>Plugin</string>
 <key>PayloadDescription</key>
 <string>Allow F-Secure Firewall to filter network traffic</string>
 <key>PayloadDisplayName</key>
 <string>F-Secure Firewall</string>
 <key>PayloadIdentifier</key>

<string>com.apple.webcontent-filter.9FF6DE99-59E2-47A1-8918-CE259D92E785</string>

 <key>PayloadType</key>
 <string>com.apple.webcontent-filter</string>
 <key>PayloadUUID</key>
 <string>9FF6DE99-59E2-47A1-8918-CE259D92E785</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
 <key>PayloadOrganization</key>
 <string>F-Secure Corporation</string>
 </dict>
 </array>
 <key>PayloadDisplayName</key>
 <string>F-Secure CP and RDR Profile</string>
 <key>PayloadIdentifier</key>
 <string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
 <key>PayloadRemovalDisallowed</key>
 <false/>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>00000000-0000-0000-0000-000000000001</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

WithSecureプロセスにフルディスクアクセスを許可する

注： 必須。詳細については、Apple Developerのドキュメントを参照してください
https://developer.apple.com/documentation/devicemanagement/privacypreferencespolicycontrol/services

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
 <dict>
 <key>PayloadDescription</key>
 <string>Grant Full Disk Access to F-Secure processes</string>
 <key>PayloadDisplayName</key>
 <string>Grant Full Disk Access to F-Secure processes</string>
 <key>PayloadIdentifier</key>

<string>com.apple.TCC.configuration-profile-policy.F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>

 <key>PayloadUUID</key>
 <string>F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
 <key>PayloadType</key>
 <string>com.apple.TCC.configuration-profile-policy</string>
 <key>PayloadOrganization</key>
 <string>F-Secure Corporation</string>
 <key>Services</key>
 <dict>
 <key>SystemPolicyAllFiles</key>
 <array>
 <dict>
 <key>Identifier</key>
 <string>com.f-secure.fsmac.gui</string>
 <key>IdentifierType</key>
 <string>bundleID</string>
 <key>CodeRequirement</key>
 <string>identifier "com.f-secure.fsmac.gui" and anchor apple generic and
certificate leaf[subject.OU] = "6KALSAFZJC"</string>
 <key>Allowed</key>
 <true/>
 <key>Comment</key>
 <string>Grant Full Disk Access to F-Secure processes</string>
 </dict>
 <dict>
 <key>Identifier</key>
 <string>com.f-secure.fsmac.gui.FSCSystemExtension</string>
 <key>IdentifierType</key>
 <string>bundleID</string>
 <key>CodeRequirement</key>
 <string>identifier "com.f-secure.fsmac.gui.FSCSystemExtension" and anchor
 apple generic and certificate leaf[subject.OU] = "6KALSAFZJC"</string>
 <key>Allowed</key>
 <true/>
 <key>Comment</key>
 <string>Grant Full Disk Access to F-Secure System Extenison'</string>
 </dict>
 </array>
 </dict>
 </dict>
 </array>
 <key>PayloadDisplayName</key>
 <string>F-Secure CP and RDR Profile</string>
 <key>PayloadIdentifier</key>
 <string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
 <key>PayloadRemovalDisallowed</key>
 <false/>
 <key>PayloadType</key>
 <string>Configuration</string>
```

```
 <key>PayloadUUID</key>
 <string>00000000-0000-0000-0000-000000000001</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

WithSecureプロセスのユーザ通知を許可する

注： 必須。詳細については、Apple Developerのドキュメントを参照してください。
https://developer.apple.com/documentation/devicemanagement/notifications/notificationsettingsitem

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
 <key>PayloadContent</key>
 <array>
 <dict>
 <key>NotificationSettings</key>
 <array>
 <dict>
 <key>AlertType</key>
 <integer>2</integer>
 <key>BadgesEnabled</key>
 <true/>
 <key>BundleIdentifier</key>
 <string>com.f-secure.fsmac.gui</string>
 <key>CriticalAlertEnabled</key>
 <false/>
 <key>NotificationsEnabled</key>
 <true/>
 <key>ShowInLockScreen</key>
 <true/>
 <key>ShowInNotificationCenter</key>
 <true/>
 <key>SoundsEnabled</key>
 <true/>
 </dict>
 </array>
 <key>PayloadEnabled</key>
 <true/>
 <key>PayloadDescription</key>
 <string>Allow notifications for F-Secure products</string>
 <key>PayloadDisplayName</key>
 <string>Allow notifications for F-Secure products</string>
 <key>PayloadIdentifier</key>

<string>com.apple.notificationsettings.A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>

 <key>PayloadType</key>
 <string>com.apple.notificationsettings</string>
 <key>PayloadUUID</key>
 <string>A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
 <key>PayloadOrganization</key>
 <string>F-Secure Corporation</string>
 </dict>
 </array>
 <key>PayloadDisplayName</key>
 <string>F-Secure CP and RDR Profile</string>
 <key>PayloadIdentifier</key>
 <string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
 <key>PayloadRemovalDisallowed</key>
```

```
 <false/>
 <key>PayloadType</key>
 <string>Configuration</string>
 <key>PayloadUUID</key>
 <string>00000000-0000-0000-0000-000000000001</string>
 <key>PayloadVersion</key>
 <integer>1</integer>
</dict>
</plist>
```

2. 作成したMDMプロファイルをMDMサービスにインポートし、それを使用して組織内のデバイスに構成を展開します。

   注： 詳細については、MDMサービスのドキュメントを参照してください。

sysext 設定を含む MDM プロファイルを jamf にインポートする

sysext設定を含むMDMプロファイルをインポートする方法の説明 jamfポータル。

注： これらの手順は、製品バージョン 23.2 以前に適用されます。

MDM プロファイルをインポートするには:

1. jamfポータルにログインします。
2. 選択する [コンピューター] > [構成プロファイル]。
   の 構成プロファイルページが開きます。
3. 新しいプロフィールを作成するには、まず [新しい]。
4. 上の 新しいmacOS構成プロファイルページ、選択 [オプション] > [一般的な]。
5. 次のことを実行します。
   a) 新しいプロファイルの名前を入力します。
   b) レベルのドロップダウンメニューから、[コンピュータレベル]。
   c) 配布方法のドロップダウンメニューから、[自動的にインストール]。
6. システム拡張機能を構成するには、次の手順を実行します。
   a) 下 [オプション]、 選択する [システム拡張]。
   b) の中に 表示名ボックスに入力 エフセキュア。

      注： バージョン24.1以降の場合は、セキュア。

   c) システム拡張タイプのドロップダウンメニューから、[許可されたシステム拡張機能]。
   d) チーム識別子ボックスに入力します 6KALSAFZJC。

      注： バージョン24.1以降の場合は、V928P8X763。

   e) 許可されたシステム拡張機能の下に入力 `com.f-secure.fsmac.gui.FSC`システム拡張機能。

      注： バージョン24.1以降の場合は、`com.withsecure.wsagent.wssystemextension`

   f) 下 [取り外し可能なシステム拡張機能]、 選択する [追加]次のように入力します。

```
com.f-secure.fsmac.gui.FSCSystemExtension
```

7. [保存] を選択します。

macOSでのソフトウェアの署名と公証

カスタム製品パッケージを検証し、macOSへのインストールを許可するには、パッケージに署名と公証が必要です。

パッケージに署名して公証する最も簡単な方法は、Appleから配布署名証明書を取得することです。詳細については、Apple のドキュメントを参照してください。

`pkgbuild`、`productbuild`または`productsign`ユーティリティを使って配布証明書を指定することができます。カスタム製品パッケージに正常に署名したら、公証する必要があります。詳細については、「配布前のmacOSソフトウェアの公証」を参照してください。

👉 **注：** インストーラの`-allowUntrusted`フラグを使用すると、パッケージのインストール中にmacOSでの証明書の検証をバイパスできます。一部のMDMソリューションは、署名されていないパッケージのインストールをサポートしていますが、推奨されるソリューションではありません。

3.2.2 メールでユーザーを招待する

この方法は、ユーザーがサブスクリプション キーを確認せずに単一のデバイスをインストールする場合に適しています。

ポータルからユーザーを招待するには、ダウンロードリンクを含む電子メールメッセージを送信します。WithSecure Elements Agent。

インストールするソフトウェアをユーザーに提供するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   [**デバイス**] の横の [**新しいデバイスの追加**] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。
   「**デバイス**」画面が表示されます。
2. デバイスの横にある ••• アイコンを選択します。
   メニューが表示されます。
3. メニューから、[**新しいデバイスを追加する**] を選択します。
   「**新規デバイスを追加**」フォームが表示されます。

   👉 **注：** *スコープ セレクタ*が特定の企業を重視している場合、ホーム ページに [**新規デバイスを追加**]ボタンが表示され、「**新規デバイスを追加**」フォームをワンクリックで開けるようになります。
4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。
6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。
   複数の招待状を送る場合は、[**CSVファイルからインポート**] で [**ファイルを選択**] を選び、データをインポートするCSVファイルを選択します。複数のメールアドレスは、カンマで区切る必要があります。
7. [**送信**] を選択します。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

   👉 **注：** デバイスメニューの [**デバイス招待の管理**] を選択すると、保留中の招待を確認することができます。

   👉 **注：** 対象のソフトウェアは [**新規デバイスを追加**] ダイアログで選択したサブスクリプション キーを使用します。

デバイスに製品がインストールされ、アクティベートされると、[**デバイス**]ページに表示され、管理デバイスの招待のページから招待状が表示されなくなります。

3.3 Linuxデバイスの展開方法

ここでは、Linuxデバイスの最も一般的な展開方法について説明します。

3.3.1 WithSecure Elementsと使用するために製品をインストールする

これらの導入方法は、Linuxデバイスを使用しており、導入したい企業に適しています。WithSecure Elements Agent。

WithSecure Elements AgentLinuxでは、管理対象エンドポイント デバイスにエージェントをインストールするための 2 つの代替方法が提供されています。

- DEB または RPM パッケージ
- 汎用インストーラーパッケージ

Linux ディストリビューションに基づいて適切なパッケージ形式を選択します。

- DEBパッケージは、DebianおよびUbuntuシステムと互換性があります。
- RPM パッケージは、AlmaLinux、Amazon Linux、Rocky Linux、CentOS、Oracle Linux、Red Hat Enterprise Linux、および SUSE Linux Enterprise Server システムと互換性があります。
- サポートされているすべてのシステムで汎用インストーラー パッケージを使用できます。

いずれかのインストーラーを使用する場合は、インストーラーをダウンロードし、依存関係がインストールされていることを確認します。次に、コマンドを実行して製品をアクティブ化します。

製品をWithSecure Elementsの管理モードでインストールすると、WithSecure Elementsポータルを使用して製品のインストールを一元的に管理できます。

インストール プロセスは、製品のインストールとアクティベーションの 2 つのステップで構成されます。製品では、データベースの更新とサブスクリプションの検証のためにクラウド サービスへの接続が必要です。サブスクリプションが 2 週間検証されない場合、製品は動作を停止します。

DEB または RPM パッケージを使用して製品をインストールする

DEB または RPM パッケージを使用して製品をインストールするための手順。

1. 製品をインストールするには、次の手順を実行します。
   a) ログイン WithSecure Elements Security Center。
   b) 選択する **[エンドポイント保護]** > **[ダウンロード]**。
   c) 下 [**サーバー向けセキュアエレメントエージェント**]DEB または RPM インストーラー パッケージをダウンロードします。
   d) rootとしてLinuxホストにログインします。
   e) 必要な依存関係がインストールされているかどうかを確認するには、Linux 保護システム要件。
   f) システム パッケージ マネージャーを使用して、エンドポイント デバイスにインストーラー パッケージを展開します。
      - DEB ベースのディストリビューションでは、次のコマンドを実行します。

        ```
        dpkg -i f-secure-linuxsecurity.deb
        ```

      - RPM ベースのディストリビューションでは、次のコマンドを実行します。

        ```
        rpm -Uvh f-secure-linuxsecurity.rpm
        ```

2. 製品をアクティブ化するには、次のコマンドを実行します。

   ```
   /opt/f-secure/linuxsecurity/bin/activate --psb --subscription-key
   SUBSCRIPTION-KEY --profile-id PROFILE-ID
   ```

   注： SUBSCRIPTION-KEY を製品のサブスクリプション キーに置き換えます。--profile-id パラメータはオプションですが、これを追加すると、エージェントのインストールをポータル

のプロファイル エディタ ビューで使用可能なプロファイルの1つに関連付けることができます。PROFILE-ID をプロファイルの数値識別子に置き換えます。

注: あなたは `--オーバーライドディストリビューション`公式にサポートされていないディストリビューションに製品をインストールするオプション。たとえば、`--override-distro rhel:8.6`。WithSecureサポートされていないディストリビューションに関する問題についてはサポートを提供できません。

注: アクティベーション プロセス中に HTTP プロキシを使用するには、--http-proxy コマンドライン オプションを追加します。このオプションは、次の形式で使用できます。

- `--http-proxy=ホスト:ポート:` これにより、指定された ホストそして ポート認証を必要とせずにネットワーク プロキシとして使用されます。ポート番号が指定されていない場合は、デフォルトのポート番号 3128 が使用されます。
  例:`--http-proxy=proxy.example.com:8080`。
- `--http-proxy=ユーザー名:パスワード@ホスト:ポート:`これにより、指定されたホストとポートがネットワーク プロキシとして使用され、指定されたユーザー名とパスワードが認証資格情報として使用されるよう製品が構成されます。ユーザー名またはパスワード内の特殊文字には URL エンコードを使用します。たとえば、パスワードに「@」文字が含まれている場合は、%40 として入力します。
  例:`--http-proxy=abc:x%40y%40z@proxy.example.com:8080`。

汎用インストーラー パッケージを使用して製品をインストールする

汎用パッケージを使用して製品をインストールするための手順。

1. 製品をインストールするには、次の手順を実行します。
   a) ログイン WithSecure Elements Security Center。
   b) 選択する **[エンドポイント保護]** > **[ダウンロード]**。
   c) 下[**サーバー向けセキュアエレメントエージェント**]汎用インストーラーパッケージをダウンロードします。
   d) rootとしてLinuxホストにログインします。
   e) 必要な依存関係がインストールされているかどうかを確認するには、Linux 保護システム要件。
   f) ダウンロードした汎用インストーラー ファイルで次のコマンドを実行します。

```
tar -xf f-secure-linuxsecurity-installer.tar
```

2. 製品をアクティブ化するには、次のコマンドを実行します。

```
./f-secure-linuxsecurity-installer --subscription-key SUBSCRIPTION-KEY
--profile-id PROFILE-ID
```

注: SUBSCRIPTION-KEY を製品のサブスクリプション キーに置き換えます。PROFILE-ID パラメータはオプションですが、これを追加すると、エージェントのインストールをポータルのプロファイル エディタ ビューで使用可能なプロファイルの1つに関連付けることができます。PROFILE-ID をプロファイルの数値識別子に置き換えます。

注: インストールのサブスクリプションキーとプロファイルIDを指定するには、`f-secure-linuxsecurity-installer`プログラムを実行する前に、プログラムが次のいずれかのパターンに一致することを確認します。
`f-secure-linuxsecurity-installer-[サブスクリプションキー]`または
`f-secure-linuxsecurity-installer-[サブスクリプションキー]-[profile=プロファイルID]`サブスクリプション キーと profile=PROFILE-ID を [] 括弧で囲むことが重要です。名前を変更したインストーラ プログラムは、コマンド ライン引数なしで実行できます。

注: あなたは `--オーバーライドディストリビューション`公式にサポートされていないディストリビューションに製品をインストールするオプション。例:`--override-distro`

`rhel:8.6`。WithSecureサポートされていないディストリビューションに関する問題についてはサポートを提供できません。

注: あなたは `--`オーバーライドディストリビューション公式にサポートされていないディストリビューションに製品をインストールするオプション。たとえば、`--override-distro rhel:8.6`。WithSecureサポートされていないディストリビューションに関する問題についてはサポートを提供できません。

注: アクティベーション プロセス中に HTTP プロキシを使用するには、--http-proxy コマンドライン オプションを追加します。このオプションは、次の形式で使用できます。

- `--http-proxy=`ホスト`:`ポート: これにより、指定された ホストそして ポート認証を必要とせずにネットワーク プロキシとして使用されます。ポート番号が指定されていない場合は、デフォルトのポート番号 3128 が使用されます。
  例:`--http-proxy=proxy.example.com:8080`。
- `--http-proxy=`ユーザー名`:`パスワード`@`ホスト`:`ポート:これにより、指定されたホストとポートがネットワーク プロキシとして使用され、指定されたユーザー名とパスワードが認証資格情報として使用されるよう製品が構成されます。ユーザー名またはパスワード内の特殊文字には URL エンコードを使用します。たとえば、パスワードに「@」文字が含まれている場合は、%40 として入力します。
  例:`--http-proxy=abc:x%40y%40z@proxy.example.com:8080`。

3.4 モバイルデバイスの展開方法

ここでは、モバイルデバイスの最も一般的な展開方法について説明します。

WithSecure Elements Mobile Protection次の方法でモバイル デバイスに展開できます。

- インストールメールを送信してユーザーを招待する WithSecure Elementsポータル
- MDMの使用

ユーザーを招待して展開

この方法は、小規模な環境、教育機関、BYOD (Bring your own device) 環境に適しています。

注: ユーザーは、デバイスの管理者権限を持つ必要があります。

リモートにいる、サブスクリプションキーを知らない、デバイスの管理者権限を持つユーザーにアプリを展開する必要がある場合は、このインストール方法を使用すると便利です。リンクを使用すると、会社のユーザーは自分の都合の良いときに自分のデバイスの1つに製品をインストールできます。製品がインストールされると、デバイスが Elements Endpoint Protectionアカウント。

この展開方法を使用すると、ダウンロードリンクを含む電子メールメッセージを送信してユーザーを招待します。WithSecure Elements Mobile Protection。

注: インストールリンクは30日間有効です。

インストーラーファイルには、1回限りのインストールトークンが埋め込まれており、サブスクリプションキーは非表示のままです。これにより、ユーザーは1つのデバイスにソフトウェアをインストールし、その後、 WithSecure Elements ポータル。

インストールするには WithSecure Elements Mobile Protectionエンドポイントデバイスでは、新しいデバイスを Elementsポータルにアクセスし、電子メール アドレスや名、姓などのユーザー情報を入力します。

注: ポータルには、追加されている場合は姓と名が表示されます。追加されていない場合は、システムは電子メール アドレスとエイリアスをチェックします。いずれの情報も利用できない場合は、UUID が表示されます。

MDM を使用した展開

展開中 WithSecure Elements Mobile ProtectionMDM の使用は、既存の MDM ソリューションが既に提供している基本的なセキュリティ機能に加えて、モバイル デバイスに追加のセキュリティを提供したい組織に最適です。このソリューションは、マルウェア、フィッシング、データ盗難などに対するセキュリティを大幅に強化します。

WithSecure Elements Mobile Protection次の MDM と統合できます。

- Google Workspace Endpoint Management（Android端末のみ）
- VMware Workspace ONE（旧称 Airwatch）
- Microsoft Intune
- IBM Security MaaS360
- Ivanti Endpoint Management（旧称 MobileIron Cloud）
- Miradore
- Samsung Knox（Android端末のみ）

WithSecure Elements Mobile Protectionはプロファイル登録ごとに展開できます。つまり、エンド デバイスに個人用と仕事用の両方のプロファイルがある場合、両方のプロファイルにアプリをインストールする必要があります。

ヒント： 最初に1つのデバイスで登録をテストすることを強くお勧めします。

注： 変数は通常、MDMプラットフォームでWithSecure Elements Mobile Protectionが構成されている場合に定義されます。変数は、アプリがメールアドレス、ユーザー名、またはUUIDで登録されているかどうかを定義します。例：

- アプリを設定しない場合は、デバイス名の下に表示されるUUIDが使用されます。WithSecure Elementsポータル。
- メールアドレスを設定した場合、ポータルのデバイス名の下に表示されます。

MDMプラットフォームでアプリを設定したら、変更しないでください。変更する場合は、まずデバイスをMDMプラットフォームから削除する必要があります。<keywd id="keyword_0AF5161AC5B74A51BADEA11BAD93BB8C">WithSecure Elements</keywd>ポータルからアプリを削除し、重複が作成されるため、MDM エージェントからもアプリを削除してください。

3.4.1 メールでユーザーを招待する

この方法は、ユーザーがサブスクリプション キーを確認せずに単一のデバイスをインストールする場合に適しています。

ポータルからユーザーを招待するには、ダウンロードリンクを含む電子メールメッセージを送信します。WithSecure Elements Agent。

インストールするソフトウェアをユーザーに提供するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   [**デバイス**] の横の [**新しいデバイスの追加**] オプションは、会社レベルでのみ表示されます。管理対象企業間の移動ページ13 すべての顧客企業を表示するように設定されている場合は、管理する企業を選択します。
   「**デバイス**」画面が表示されます。
2. デバイスの横にある アイコンを選択します。
   メニューが表示されます。
3. メニューから、[**新しいデバイスを追加する**] を選択します。
   「**新規デバイスを追加**」フォームが表示されます。

   注： *スコープ セレクタ*が特定の企業を重視している場合、ホーム ページに [**新規デバイスを追加**]ボタンが表示され、「**新規デバイスを追加**」フォームをワンクリックで開けるようになります。
4. 製品を選択します。
5. ドロップダウンメニューから、招待状を送信する言語を選択します。

6. 招待状を送りたい相手のメールアドレスや、その他の任意事項を入力します。
   複数の招待状を送る場合は、[CSVファイルからインポート] で [ファイルを選択] を選び、データをインポートするCSVファイルを選択します。複数のメールアドレスは、カンマで区切る必要があります。
7. [送信] を選択します。
   リストアップされた受信者には、ダウンロードサイトへのリンクと、選択した製品のダウンロードとインストールの手順が記載されたメールが送信されます。

   注： デバイスメニューの [デバイス招待の管理] を選択すると、保留中の招待を確認することができます。

   注： 対象のソフトウェアは [新規デバイスを追加] ダイアログで選択したサブスクリプションキーを使用します。

デバイスに製品がインストールされ、アクティベートされると、[デバイス] ページに表示され、管理デバイスの招待のページから招待状が表示されなくなります。

Androidデバイスへのアプリのインストールとアクティベーション

次の手順に従って、アプリをAndroidデバイスにインストールするようにユーザーに指示します。

注： 次の手順は、エンドユーザを対象にしています。

管理者からアプリのインストールを指示するメールが届きます。メールには、1台のデバイスにアプリをインストールするためのリンクと、ライセンスをアクティブ化するためのリンクが含まれています。

アプリをインストールするには

1. 招待メールを開きます。
2. Androidの横にあるリンクを選択します。
   Google Play Storeに移動し、WithSecure Mobile Protectionアプリをダウンロードしてインストールすることができます。
3. デバイスにアプリをインストールした後、インストールメールに戻り、[Android用にアクティベート] を選択して、サブスクリプションをアクティベートします。

   注： アクティベーションリンクは29日間有効ですが、一度しか使用できません。メールに記載されているユーザー名とパスワードを使用してアプリにログインしても、ライセンスを有効にできない場合は、アクティベーションリンクを使用してみてください。最初にアクティベーションリンクを選択し、何らかの理由でそれがうまくいかない場合、認証情報を手動で入力することはできません。

   WithSecure Mobile Protectionアプリが開きます。
4. 確認されたら、[許可] を選択して、アプリに必要な権限を付与します。

   注： アプリが有害なアイテムをスキャンできるようにするには、写真、メディア、ファイルへのアクセス許可が必要です。

iOSデバイスへのアプリのインストールとアクティベーション

インストールするには、以下の手順に従うようユーザーに指示します。WithSecure Elements Mobile ProtectioniOS デバイス上で。

注： 次の手順は、エンドユーザを対象にしています。

管理者からアプリのインストールを指示するメールが届きます。メールには、1台のデバイスにアプリをインストールするためのリンクと、ライセンスをアクティブ化するためのリンクが含まれています。

アプリをインストールするには

1. 招待メールを開きます。
2. iOSの横にあるリンクを選択します。

AppStoreに移動し、WithSecure Mobile Protectionアプリをダウンロードしてインストールすることができます。

3. デバイスにアプリをインストールした後、インストールメールに戻り、[**iOS用にアクティベート**]を選択して、サブスクリプションをアクティベートします。

   注： アクティベーションリンクは29日間有効ですが、一度しか使用できません。メールに記載されているユーザー名とパスワードを使用してアプリにログインしても、ライセンスを有効にできない場合は、アクティベーションリンクを使用してみてください。最初にアクティベーションリンクを選択し、何らかの理由でそれがうまくいかない場合、認証情報を手動で入力することはできません。

   WithSecure Elements Mobile Protectionアプリが開きます。

4. 確認されたら、[**許可**] を選択して、アプリに必要な権限を付与します。

   注： 重要なイベントについて通知するには、アプリに許可が必要です。

3.4.2 Google Workspace MDM を使用した導入

Google Workspace MDMを使用してWithSecure Elements Mobile ProtectionアプリをAndroidデバイスに展開する方法について説明します。

AndroidアプリをGoogle Workspace Endpoint Managementに追加する

AndroidデバイスでGoogle Workspace MDMに許可されたアプリとしてWithSecure Elements Mobile Protectionを追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

  注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

製品をGoogle Workspace MDMに追加するには

1. Google Workspace管理コンソールにログインします。
2. ダッシュボードで、**[アプリ]** > **[ウェブとモバイルアプリ]** を選択します。
3. **[Webおよびモバイルアプリ]** ページで、**[アプリの追加]** > **[プライベートAndroidアプリの追加]** を選択します。
4. **[Managed Androidアプリ]** ページで、**[Playストアの検索]** を選択し、検索ボックスに「`mobile protection elements`」を入力します。
5. アプリを選択してから、**[承認]** > **[選択]** を選択します。
6. **[ユーザーアクセス]** で、希望のオプションを選択し、**[次へ]** を選択します。

7. [アクセス方法]で、希望のオプションを選択し、[完了] を選択します。

AndroidアプリがGoogle Workspace MDMに追加されます。

Androidアプリの構成

Androidアプリを構成する方法を説明します。

注: Google Workspaceは変数をサポートしていません。ただし、登録キー フィールドでは、サブスクリプション キーを標準形式の変数として受け入れます。したがって、サブスクリプション キーはそのまま入力し、メール アドレスは入力しないでください。入力すると、すべてのデバイスが同じメールアドレスで表示されます。WithSecure Elements Endpoint Protectionポータル。メールアドレスを空白のままにしておくと、WithSecure Elements Mobile Protectionインストールされているデバイスはデバイス UUID とともに表示されます。

1. [管理コンソール] ページの [管理対象構成] で、[管理対象構成の追加] を選択します。
2. [管理された構成] ページで、構成の名前を入力し、次の手順を実行します。
   a) [登録キー] フィールドに、製品のサブスクリプションキーを入力します。
      サブスクリプションキーは、WithSecure Elements Security Centerの Endpoint Protectionのサブスクリプション で確認できます。
   b) それぞれのフィールドに名と姓を入力します⊠オプション⊠。
   c) [エイリアス] フィールド⊠オプション⊠に、別名を入力します。
   d) [メールアドレス] フィールド⊠オプション⊠に、メールアドレスを入力します。
   e) [環境] フィールド⊠オプション⊠に、「2」と入力します。
3. [保存] を選択します。

3.4.3 VMware Workspace ONE MDM を使用した展開

展開方法の説明 WithSecure Elements Mobile Protectionアプリ付き VMware Workspace ONE(旧称 Airwatch) Android および iOS デバイスへの MDM。

注: これらの手順には、ユーザーとデバイスを作成および構成する方法に関する情報は含まれていません。

iOSアプリをVMware Workspace ONE MDMに追加する

追加方法の説明 WithSecure Elements Mobile ProtectioniOSアプリから VMware Workspace ONE⊠⊠⊠。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注: WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。
- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Apple StoreからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、管理 > サブスクリプション から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[MDMサーバ構成] を選択すると、証明書をダウンロードすることができます。

注: 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. 上の VMware Workspace ONE管理ポータルにアクセスするには、[リソース] > [アプリ]。
2. [パブリック] タブを選択します。
3. 選択する [アプリケーションを追加]。
4. [アプリケーションの追加] ビューで、次の手順を実行します。
   a) 「管理者」フィールドに組織を追加します。
   b) [プラットフォーム] ドロップダウンメニューから、[AppleiOS] を選択します。
   c) 名前フィールドにアプリケーション名を入力します。例[セキュアモバイル保護]。
   d) [次へ] を選択します。
   [検索] ページが開きます。
   e) 国ドロップダウンメニューから国を選択し、[選択する]。
   「アプリケーションの追加 - WithSecure Mobile Protection」ビューが開きます。
   f) 開いたビューの下にある [名前]、 入力 WithSecure Mobile Protectionデフォルトで検出されない場合は、[保存して割り当てる]。

次に、iOSアプリを構成する必要があります。

iOSアプリの構成

設定方法の説明 WithSecure Elements Mobile ProtectioniOSアプリで VMware Workspace ONE。

1. 下 [割り当て] > [分布]、 次のように入力します
   - 名前 - アプリの名前 (WithSecure Mobile Protection)
   - 説明 - 課題の説明オプション
   - 割り当てグループ - アプリを割り当てるグループを選択します。例:[すべてのデバイス]。
   - アプリの配信方法 - アプリの配信方法を選択します。[オート]または [オンデマンド]。
2. を選択 [制限]タブをクリックし、必要なオプションをオンにします。
3. 次に、[トンネルとその他の属性]タブをクリックしてオプションを確認します。
4. [アプリケーション構成の送信] タブを選択します。
5. オンにします [構成を送信]オプションを選択し、次の操作を実行します。
   a) 次に、[追加]アプリを自動的にアクティブ化できるように、構成キーとデバイス識別の詳細を追加します。
   b) [構成キー] で、次の構成エントリの値を入力します。
      - *運命登録キー*- サブスクリプションキー
      - *ファーストネーム*オプション - デバイスを識別しやすくするための名前WithSecure Elementsポータル
      - *苗字*オプション - デバイスを識別しやすくするための名前 WithSecure Elementsポータル
      - ***E**メール*- ユーザーのメールアドレス
      - *エイリアス*(オプション) - ユーザーの別名
   c) オプションキーの入力については、[ルックアップ値の挿入] を選択し、それぞれの変数を選択します。アプリケーションがユーザーデバイスにデプロイされると、フィールドは自動的に入力されます。
6. [新規作成] を選択します。
7. 開いたビューで、[保存]。
8. 割り当てられたデバイスのプレビューページで、追加したデバイスが表示されたら、[公開]。
9. メインビューで、[デバイス][リストビュー]。
   あなたのデバイスがリストに表示されます。

AndroidアプリをVMware Workspace ONE MDMに追加する

WithSecure Elements Mobile Protection Android アプリをVMware Workspace ONE MDM に追加する方法について説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました

- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. VMware Workspace ONE管理ポータルで、**[アプリとブック]** に移動し、**[ネイティブ]** を選択します。
2. 次に、「パブリック」タブで、[**アプリケーションを追加**]。
3. [アプリケーションの追加] ページで、次の手順を実行します。
   a) **[プラットフォーム]** ドロップダウンメニューから、**[Android]** を選択します。
   b) **[ソース]** フィールドで、**[アプリストアの検索]** を選択します。
   c) [**名前**] フィールドに「`WithSecure Elements Mobile Protection`」と入力します。
   d) [**次へ**] を選択します。
4. [アプリ] ビューで、[**WithSecure Elements Mobile Protection**] を選択します。
5. の中に [**セキュアエレメントモバイル保護**]表示、選択 **[承認する]** > **[選択する]**。
6. [アプリケーションの編集] ビューで、**[利用規約]** タブを選択します。
7. から [**開発キット**]ドロップダウンメニューで選択 [**MP 文字列@ WithSecure**]。
8. **[保存して割り当てる]** を選択します。

管理対象アプリケーションの表示

VMware Workspace ONE MDMで管理対象アプリケーションを表示する方法を説明します。

1. の中に VMware Workspace ONEコンソールウィンドウで選択 [**アプリと書籍**]そしてその下 [**アプリケーション**]、 選択する [**リストビュー**]。
   [リストビュー] ページが開きます
2. **[パブリック]** タブを選択します。

   の WithSecure Elements Mobile Protectionアプリは、VMware Workspace ONE管理ポータル。

VMware WorkspaceONEを使用したAndroid Enterpriseの導入

この章では、VMware Workspace ONEを使用してAndroid EnterpriseコンテキストでWithSecure Elements Mobile Protectionアプリを展開する方法について説明します。

VMware Workspace ONE MDMでのAndroidEnterpriseのセットアップ

Android EnterpriseコンテキストでWithSecure Elements Mobile ProtectionのAndroidアプリをセットアップする方法について説明します。

Android Enterpriseコンテキストでアプリを導入するには、会社にGoogle管理者アカウントが必要です。すべてのユーザーは、事前定義されているか、登録時に生成されたアカウントを持っている必要があります。

ドメイン管理者は、EMMトークンと証明書を生成し、VMware Workspace ONEをEMMプロバイダーとしてバインドする必要があります。

Android Enterpriseをセットアップするには

1. VMware Workspace ONE管理ポータルにログインします。
2. [グループと設定] に移動し、[すべての設定] を選択します。
3. [設定] ビューで [デバイスとユーザー] > [アンドロイド] を選択します。
4. [Android]で、[Android EMM登録] を選択します。
5. 右上隅にあるアカウントアイコンを選択し、[Googleアカウントの管理] を選択します。
6. メールアドレスとパスワードでログインします。
7. [Bring Android to Work] ページで、[開始] を選択します。
   [Android EMM登録] ページが開きます。
8. サービス アカウントが設定されたら、[登録設定] タブと [登録制限] タブの設定を受け入れ、[保存] を選択します。
   設定が保存されます。

VMware Workspace ONEにプロファイルを追加する

プロファイルを追加する方法の説明。

1. VMware Workspace ONE管理ポータルで、]アプリとブック] > [すべてのアプリとブック設定] に移動します。
   [設定] ページが開きます。
2. ナビゲーションペインで、[設定とポリシー] > [プロファイル] を選択します。
   [プロファイル] ビューが開きます。
3. [プロファイルの追加] > [SDKプロファイル] > [Android] を選択します
   [新しいAndroidプロファイルの追加] ページが開きます。
4. [全般] を選択し、新しいプロファイルの名前と説明を入力して、[保存] を選択します。

Androidアプリを追加する

Android Enterprise コンテキストで WWithSecure Elements Mobile Protection AndroidアプリをVMware Workspace ONE MDMに追加する方法について説明します。

1. VMware Workspace ONE管理ポータルで、[アプリとブック] > [アプリケーション] > [ネイティブ].を選択します。
   [リストビュー] が開きます
2. [パブリック] タブを選択し、[アプリケーションの追加] を選択します。
3. [アプリケーションの追加] ビューで、次の手順を実行します。
   a) [プラットフォーム] ドロップダウンメニューから、[Android] を選択します。
   b) アプリケーション名を入力します`mobile protection elements`
   c) [次へ] を選択します。
      [アプリ] ページが開きます。
4. [`WithSecure Elements Mobile Protection`]を選択します。
5. の中に WithSecure Elements Mobile Protection表示、選択 [承認する] > [選択する]。
   [アプリケーションの編集] ビューが開きます。
6. を選択[開発キット]タブから、[アプリケーションプロファイル]ドロップダウンメニューで選択[MP文字列 @ WithSecure]。
7. [保存して割り当てる] を選択します。
   [WithSecure Elements Mobile Protection - 割り当て] ページが開きます。
8. [配布] を選択して、次の手順を実行します。
   a) [名前] フィールドに、ディストリビューションの名前`alldevices`など]を入力します。
   b) [割り当て] グループで、希望するデバイス配布グループを選択します。
9. 次に、[アプリケーションの構成] を選択し、次の手順を実行します。
   a) [登録キー] フィールドに、製品サブスクリプションキーを入力します。

      注： WithSecure Elements Mobile Protectionのサブスクリプションキーは、WithSecure Elements Security Centerの [Endpoint Protection] > [サブスクリプション] で確認できます。

   b) [名]オプション] フィールドに、{FirstName} と入力します

c) [名前⊠オプション⊠] フィールドに、**{LastName}** と入力します
d) [エイリアス⊠オプション⊠] フィールドに、**{EnrollmentUser}** と入力します
e) [電子メール⊠オプション⊠] フィールドに、**{EmailAddress}** と入力します
f) [**新規作成**] を選択します。
[割り当て] タブが開きます。

10. [**保存**] を選択します。
[割り当てられたデバイスのプレビュー] ページが開きます。
11. [**公開**] を選択します。

Androidアプリの構成

Android EnterpriseコンテキストでVMware Workspace ONE MDM のWithSecure Elements Mobile Protection Android アプリを構成する方法について説明します。

Androidアプリを構成するには

1. VMware Workspace ONE管理ポータルで、[**アプリケーションの編集**] ページを選択します。
2. [**割り当て**] タブを選択し、割り当てグループを定義します。
3. [**アプリケーション構成の送信**] を選択します。
4. [**構成キー**] で、次の構成エントリに値を追加します。

注： リセラーは値を提供します。

- fate_registration_key - ライセンスキー
- first_name (オプション) - ユーザーを識別しやすくする名前 WithSecure Elements Endpoint Protectionポータル
- last_name (オプション) - ユーザーを識別しやすくする名前 WithSecure Elements Endpoint Protectionポータル

オプションのキーについては、[**ルックアップ値の挿入**] を選択し、それぞれの変数を選択します。アプリケーションがユーザーデバイスにデプロイされると、フィールドは自動的に入力されます。

5. [**詳細と割り当て**] の下にある残りのアプリ設定を入力し、[**保存して公開**] を選択して、アプリを [**リストビュー**] に追加します。

証明書を使用してデバイスを登録する

証明書を使用してデバイスを登録する方法について説明します。

注： サブスクリプションが必要です WithSecure Elements Mobile Protection with External MDM これをする。

証明書を使用してデバイスを登録するには

1. ログイン WithSecure Elements Endpoint Protection会社の管理者アカウントでポータルにアクセスします。
2. 下 [**サブスクリプション**]、 選択する
そして選択 [**外部MDMサーバーの構成**]
3. 証明書ファイルをダウンロードして保存します。
4. 上の VMware Workspace ONE管理ポータルにアクセスするには、[**リソース プロファイルとベースライン**] > [**新しいプロフィールを追加**]。

注： 既存のプロファイルを使用して証明書を事前構成することもできます。

5. 下 [**資格**]、 選択する [**追加**]ダウンロードした証明書をアップロードするには WithSecure Elements Endpoint Protectionポータル。
6. [**保存して発行**] を選択します。
7. プロファイルをデバイスに割り当てます。

3.4.4 Microsoft Intune MDM を使用した展開

Microsoft Intune MDM を使用してWithSecure Elements Mobile Protectionアプリを Android および iOS デバイスに展開する方法について説明します。

Microsoft Intune MDMを使用したiOSアプリの導入

WithSecure Elements Mobile Protection iOSアプリをMicrosoft Intune MDMに導入する方法を説明します。

iOSアプリをMicrosoft Intune MDMに追加する

WithSecure Elements Mobile Protection iOSアプリをMicrosoft Intune MDMに追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Apple StoreからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. Microsoft Intuneポータルにログインします。
2. **[アプリ]** > **[iOS/iPadOS]** > **[追加]** を選択します。
   [**アプリタイプの選択**] ペインが開きます。
3. **「アプリケーションの種類]** ドロップダウンメニューから、**[iOSのストアアプリ]** を選択し、**[選択]** を選択します。
4. **[アプリの追加]** ビューで、**[アプリストアの検索]** を選択します。
   [AppStoreの検索] ペインが開きます。
5. [検索] フィールドに「`WithSecure Mobile Protection`」と入力します。
6. **WithSecure Elements Mobile Protection** > **選択**を選択します。
   [アプリの追加] ビューが開きます。
7. **[アプリ情報]** タブで、**[はい]** を選択して、WithSecure Mobile Protectionを機能アプリとしてポータルサイトに表示し、**[次へ]** を選択します。
8. [割り当て] タブの **[必須]** で、**[すべてのユーザーを追加]** を選択し、**[次へ]** を選択します。
9. **[レビュー+作成]** タブで、**[作成]** を選択します。
10. 完了したら、**[アプリの追加]** ブレードで **[OK]** を選択します。

WithSecure Elements Mobile ProtectionアプリがMicrosoft Intune MDMに追加されます。

次に、アプリ構成ポリシーを追加します。

iOSアプリ構成ポリシーに追加する

管理対象のiOSデバイスにWithSecure Elements Mobile Protectionアプリの構成ポリシーを追加する方法について説明します。

アプリ構成ポリシーを作成するには

1. **[アプリ]** を選択します。
   [アプリの概要] ペインが開きます。
2. **[ポリシー]**で、**[アプリ構成ポリシー]** を選択します。
3. **[追加]** > **[管理対象デバイス]** を選択します
   [アプリ構成ポリシーの作成] ペインが開きます。
4. **[基本]** タブで、次の手順を実行します。
   a) [**名前**] フィールドに「WithSecure Mobile Protection」と入力します。
   b) **[プラットフォーム]** ドロップダウンメニューから、**[iOS/iPadOS]** を選択します。
   c) **[ターゲットアプリ]** の横にある**[アプリの選択]** を選択します。
   [関連付けられたアプリ] ペインが開きます。
   d) **WithSecure Elements Mobile Protection** を選択し、**OK** > **次へ**を選択します。
   [設定] タブが開きます。
5. 次のことを実行します。
   a) **[構成設定の形式]** ドロップダウンメニューから、**[構成デザイナーを使用する]** を選択します。
   b) 値の型については、 次参照してください。構成デザイナーを使用するページ61
   c) [**次へ**] を選択します。
   [割り当て] タブが開きます。
   d) **[含まれるグループ]**で、**[すべてのユーザーを追加]** を選択し、**[次へ]** を選択します。
   [レビュー+作成] タブが開きます。
   e) [**新規作成**] を選択します。

アプリ構成ポリシーが作成され、割り当てられました。

iOSデバイスにアプリをインストールする必要があります。

構成デザイナーを使用する

Intuneに登録されているかどうかに関係なく、デバイス上のアプリに対して構成デザイナーを使用できます。

デザイナーを使用すると、特定の構成キーと値を構成できます。また、各値のデータ型を指定する必要があります。構成内のキーと値ごとに、以下を設定します。

- 構成キー - 特定の設定構成を一意に識別するキー。
- 値のタイプ-構成値のデータ型。タイプには、整数、実数、文字列、またはブール値が含まれます。
- 構成値 - 構成の値。

以下のキーと値は必須です WithSecure Elements Mobile Protectionライセンスのアクティベーション。

キー	種類	値	参考
fate_registration_key	文字列	ABCD-EFGH-IJKL-MNOP	例⊠実際の値は再販業者から提供されます。

エンドユーザーはVPNをオフにすることができません WithSecure Elements Mobile Protectionアプリ自体を無効にしたり、個々の保護機能を無効にすることはできません。この機能の詳細と制限については、「VPN を自動的にオンにしておく」をご覧ください。

以下のオプションキーは、WithSecure Elements Endpoint Protectionポータル。使用 Microsoft Intune適切な値を取得するための動的変数。Intune で機能する次のキーと値が見つかりました。

キー	種類	値	参考
Eメール	文字列	{{郵便}}	

キー	種類	値	参考
環境	整数	2	
エイリアス	文字列	{{ユーザー名}}	

Microsoft Intune MDMを使用したAndroidアプリの展開

WithSecure Elements Mobile ProtectionアプリをMicrosoft Intune MDMに導入する方法を説明します。

AndroidアプリをMicrosoft Intune MDMに追加する

WithSecure Elements Mobile ProtectionアプリをMicrosoft Intune MDMに追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. Microsoft Intuneポータルにログインします。
2. **[アプリ]** > **Android** > **[追加]** を選択します。
   [**アプリタイプの選択**] ペインが開きます。
3. **[アプリケーションの種類]** ドロップダウンメニューから、**[Managed Google Playでアプリ]** を選択し、**[選択]** を選択します。
4. **[Managed GooglePlay]** ビューの [検索] フィールドに、「`WithSecure Elements`」と入力します。
   [アプリ] ビューが開きます。
5. [**WithSecure Elements Mobile Protection**]を選択します。
6. 開いたビューで、**[承認]** > **[承認]** を選択します。
7. **[承認設定]** タブで、**[アプリが新しい権限をリクエストしたときに承認を維持する]** を選択し、**[完了]** を選択します。
   [Managed GooglePlay] ビューが開きます。
8. 左上隅にある **[同期]** を選択します。
   [Androidアプリ] ビューが開きます。
9. [**更新**]を選択し、[**WithSecure Elements Mobile Protection**]を選択します。
   [**WithSecure Elements Mobile Protection**] ビューが開きます。
10. **[管理]で**、**[プロパティ]** を選択します。
    [**WithSecure Elements Mobile Protectionのプロパティ**] ビューが開きます。
11. **[割り当て]** の横にある**[編集]** を選択します。
    [アプリケーションの編集] ビューが開きます。

12. [割り当て] タブで、次の手順を実行します。
    a) [必須] で、[すべてのユーザーを追加] を選択します。
    b) [確認+保存] を選択します。
    c) [レビュー+保存] タブで [保存] を選択します。

WithSecure Elements Mobile ProtectionアプリがMicrosoft Intune MDMに追加されます。

次に、アプリ構成ポリシーを追加します。

Androidアプリ構成ポリシーの追加

管理対象のAndroidデバイスにWithSecure Elements Mobile Protectionの構成ポリシーを追加する方法について説明します。

1. [アプリ] を選択します。
   [アプリの概要] ペインが開きます。
2. [ポリシー]で、[アプリ構成ポリシー] を選択します。
3. [追加] > [管理対象デバイス] を選択します
   [アプリ構成ポリシーの作成] ペインが開きます。
4. [基本] タブで、次の手順を実行します。
   a) [名前] フィールドに「WithSecure Mobile Protection」と入力します。
   b) [プラットフォーム] ドロップダウンメニューから、[Android Enterprise] を選択します。
   c) [プロファイルタイプ] ドロップダウンメニューから、[個人所有の仕事用プロファイルのみ] を選択します。
   d) [ターゲットアプリ] の横にある[アプリの選択] を選択します。
      [関連付けられたアプリ] ペインが開きます。
   e) WithSecure Elements Mobile Protection を選択し、OK > 次へを選択します。
   [設定] タブが開きます。
5. 次のことを実行します。
   a) 構成設定 で [構成設定の形式] ドロップダウンメニューから、[構成デザイナーを使用する] を選択します。
   b) [+追加] を選択します。
   c) 右側に開くペインで、次を選択します。
      - 登録キー
      - エイリアス▯オプション▯
      - メールアドレス▯オプション▯
      - 環境▯オプション▯
   d) [OK] を選択します。
   e) 値タイプを選択し、以下の設定キーの設定値を入力します。
      - fate_registration_key: 値のタイプ▯[文字列]、構成値▯ [`WithSecure Elements Mobile Protection`サブスクリプション キー]。

        注: WithSecure Elements Mobile Protectionのサブスクリプションキーは、WithSecure Elements Security Centerの 管理 > サブスクリプション で確認できます。
      - エイリアス▯値タイプ▯文字列、構成値▯`{{username}}`
      - メールアドレス▯値の種類▯文字列、構成値▯`{{mail}}`
      - env▯値タイプ▯整数、構成値▯2

        注: env構成キーとその値は、VPNエンドポイントの接続先を定義します。
   f) [次へ] を選択します。
      [割り当て] タブが開きます。
   g) [含まれるグループ]で、[すべてのユーザーを追加] を選択し、[次へ] を選択します。
      [レビュー+作成] タブが開きます。
   h) [新規作成] を選択します。

アプリ構成ポリシーが作成され、割り当てられました。

Androidデバイスにアプリをインストールする必要があります。

アプリへの権限の付与

サイレントアクティベーションのためにアプリに許可を与える方法を説明します。

1. ログイン Microsoft Endpoint Manager管理者センター。
2. 選択する **[アプリ]** > **[アプリ構成ポリシー]** > **[追加]** > **[管理対象デバイス]**。

   注： 管理対象デバイスまたは管理対象アプリのいずれかを追加できます。詳細については、アプリ構成をサポートするアプリ。

3. **[基本]**ページで、次の詳細を入力します。
   - 名前 - ポータルに表示されるプロフィールの名前
   - 説明 - ポータルに表示されるプロフィールの説明
   - デバイス登録タイプ - デフォルトのオプションは [**管理対象デバイス**]
4. 下 [**プラットフォーム**]、 選択する [**Androidエンタープライズ**]。
5. **[ターゲットアプリ]** の横にある **[アプリの選択]** を選択します。
   [**関連付けられたアプリ**] ペインが開きます。
6. 上の[**関連アプリ**]ペインで、構成ポリシーに関連付ける管理対象アプリを選択し、[**わかりました**]。
7. **[次へ]** > **[追加]** を選択します。
   の **権限を追加する**ペインが開きます。
8. 上書きする権限を選択します。

   注: 付与された権限は、選択したアプリのデフォルトのアプリ権限ポリシーを上書きします。

9. 各権限の権限状態を設定します。次のオプションから選択できます。
   - プロンプト - ユーザーに承諾または拒否するように促します
   - 自動付与 - ユーザーに通知せずに自動的に承認します
   - 自動拒否 - ユーザーに通知せずに自動的に拒否します。
10. **[確認+保存]** を選択します。
    設定が保存されます。

3.4.5 IBM MaaS360 MDMを使用した展開

展開方法の説明 WithSecure Elements Mobile Protectionアプリ付き IBM MaaS360 Android および iOS デバイスへの MDM。

IBM MaaS360 MDMを使用したiOSアプリの導入

このセクションでは、WithSecure Elements Mobile ProtectioniOSアプリから IBM MaaS360 MDM とその展開方法。

iOSアプリをIBM MaaS360 MDMに追加する

WithSecure Elements Mobile Protection iOSアプリをIBM MaaS360 MDMに追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Apple StoreからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

> **注：** 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. 管理者としてIBM MaaS360管理者ポータルにログインします。
2. **[アプリ」]** ビューを開きます。
3. ドロップダウンリストから**[追加]、[iTunes AppStoreアプリ]** の順に選択します。
4. の中に **アプリの詳細** タブで検索して選択 [**セキュアモバイル保護**]アプリ。
   必要に応じてアプリのカテゴリを調整します。
5. **[ポリシーと配布]** タブを開き、使用する配布方法とグループを選択します。
6. **[構成]** タブを開きます。
   構成には、次の必須属性が含まれています。
   - ***fate_registration_key*** - ライセンスキー

   firstName、lastName、email、およびaliasキーを使用して、ポリシー構成にユーザーデータを追加できます。
7. [**追加**] を選択します。

の WithSecure Elements Mobile Protectionアプリは **アプリ** リスト。

iOSアプリの配布

の WithSecure Elements Mobile ProtectioniOS アプリは、定義された配布グループ内のユーザーに配信されます。

IBM MaaS360 MDMを使用したAndroid Enterpriseの導入

この章では、IBM MaaS360 MDMを使用してAndroid EnterpriseコンテキストでWithSecure Elements Mobile Protectionアプリを展開する方法について説明します。

Android Enterpriseの構成

Android Enterprise を設定する方法を説明します。

> **注：** デバイスを登録する前に、Android Enterpriseを設定する必要があります。

1. IBM MaaS360管理ポータルで、**[セットアップ]** > **[サービス]** を選択します。
2. **[モバイルデバイス管理]**で、**[Android Enterprise Solutionを有効にする][管理されたGoogle Playアカウントを介して有効にする⊠ビジネス向けのGスイートなし⊠]** で**[ここ]** を選択します。
   [Android Managed GooglePlayアカウントの有効化の確認] ウィンドウ。
3. **[有効]** を選択します。
4. **[セキュリティチェック]** ウィンドウで、パスワードを入力し、**[確認]** を選択します。
   GooglePlayが開きます。
5. **[Bring Android to work]** ページで、**[開始]** を選択し、次の手順を実行します。
   a) ビジネスの名前を入力し、**[次へ]** を選択します。
   b) [連絡先の詳細] ページで、名前、メールアドレス、電話番号⊠オプション⊠を入力し、**[Managed Google Play 契約]を読んで同意します]** オプションを選択し、**[確認]** を選択します。
6. **[登録完了]** を選択します。
   セットアップが完了しました。

次に、WithSecure Elements Mobile Protectionアプリ。

WithSecure Elements Mobile Protectionアプリを追加する

追加方法の説明 WithSecure Elements Mobile Protectionアプリに IBM MaaS360 ⊠⊠⊠。

1. IBM MaaS360管理ポータルで、**[アプリ]** > **[カタログ]** を選択します。
2. [アプリカタログ] ページで、**[追加]** > **[Android]** > **[Google Playアプリ]** を選択します。
3. [検索] ボックスに「`WithSecure Elements Mobile Protection`」と入力します。
4. **WithSecure Elements Mobile Protection** を選択し、[**選択**]を選択します。
5. 権限の承認ウィンドウで、[**承認する**]アプリを追加します。

次に、アプリを構成する必要があります。

アプリの構成

WithSecure Elements Mobile Protectionアプリの設定方法について説明します。

1. Google Playアプリの追加ウィンドウで、**構成**タブ、選択 [**アプリ設定を構成する**]そして次の操作を行います。
   a) [登録] フィールドに、製品のサブスクリプションキーを入力します。

   > **注：** WithSecure Elements Mobile Protectionのサブスクリプションキーは、WithSecure Elements Security Centerの **[Endpoint Protection]** > **[サブスクリプション]** で確認できます。

   b) それぞれのフィールドに名と姓を入力します⊠オプション⊠。
   c) [エイリアス] フィールド⊠オプション⊠に、別名を入力します。
   d) [メールアドレス] フィールド⊠オプション⊠に、メールアドレスを入力します
   e) [環境] フィールド⊠オプション⊠に、「2」と入力します。
2. [**追加**] を選択します。
   [セキュリティチェック] ウィンドウが開きます。
3. パスワードを入力し、**[確認]** を選択します。
   アプリが追加されます。

アプリの配布

選択したターゲットにアプリを配布する方法を説明します。

1. アプリカタログページの [**セキュアエレメントモバイル保護**]、 選択する [**ビュー**]。
2. 開いたページの右上隅にある **[配布]** を選択します。
   [アプリの配布] ウィンドウが開きます。
3. [ターゲット] ドロップダウンメニューから次のいずれかのオプションを選択します。
   - 特定のデバイス
   - グループ
   - すべてのデバイス
4. **[配布]** を選択します。

3.4.6 Ivanti Endpoint Managementを使用した展開

展開方法の説明 WithSecure Elements Mobile Protectionアプリ付き Ivanti Endpoint Management⊠旧称 MobileIron CloudMDM など、Android および iOS デバイスへのソフトウェア デプロイをサポートします。

Ivanti Endpoint Managementを使用したiOSアプリの導入

iOSアプリを展開する方法の説明 Ivanti Endpoint Management。

WithSecure Elements Mobile Protection iOS アプリを Ivanti Endpoint Management に追加する

追加方法の説明 WithSecure Elements Mobile ProtectioniOSアプリから Ivanti Endpoint Management。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Apple StoreからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

iOSアプリを追加するには Ivanti Endpoint Management:

1. 上の Ivanti Endpoint Management管理ポータルにアクセスするには、**アプリ**ページを選択して [**追加**]。
2. **[App Store]** を選択します。
3. 「`WithSecure Elements Mobile Protection`」を検索します。
4. アプリを選択してから、**[次へ]** を選択します。
5. アプリの説明が正しいことを確認し、**[次へ]** を選択します。
6. アプリの配布を設定し、**[次へ]** を選択します。

iOSアプリ管理の構成

iOSアプリ管理を構成する手順を説明します。

1. **[構成]** ページで、**[iOS Managedアプリの構成]** を選択してから、**[+]** を選択します。
2. iOS 7以降の管理対象アプリの設定で、次の手順を実行します。
   a) この設定の名前を入力します。例:`Secure Elements Mobile Protection`ライセンス構成。
   b) の中に [**運命登録キー**]フィールドに入力してください WithSecure Elements Endpoint Protection ライセンスキー。
3. この構成のディストリビューションをセットアップします。
4. その他の必要な構成をセットアップし、**[完了]** を選択します。

追加の構成キー

次の Ivanti Endpoint Management変数は、ネットワーク上のデバイスを識別するために使用できます。WithSecure Elementsポータル。

注： キー名の大文字と小文字は区別されます。

キー	値
fate_registration_key	`ABCD-EFGH-IJKL-MNOP`
***E**メール*	`$ userEmailAddress`
ファーストネーム	`$ userFirstName`
last_name	`$ userLastName`
エイリアス	`$ userDisplayName`

Ivanti Endpoint Management を使用した Android アプリの導入

Androidアプリを展開する方法の説明 Ivanti Endpoint Management。

設定できます WithSecure Elements Mobile Protection次のいずれかの方法で:

- サブスクリプションキーとその他の変数を追加してアプリを手動で設定します。Ivanti Endpoint Management下 [**アプリの構成**][**Android 向けの管理構成**]。
- MDMサーバー構成証明書を使用してアプリを構成します。この証明書は、WithSecure Elementsポータル。証明書は次の場所で見つかります。[**サブスクリプション**]選択して ••• 最後に WithSecure Elements Mobile Protection行。

WithSecure Elements Mobile Protection Android アプリを Ivanti Endpoint Management に追加する

追加方法の説明 WithSecure Elements Mobile ProtectionAndroidアプリに Ivanti Endpoint Management。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。
- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

Androidアプリを追加するには Ivanti Endpoint Management:

1. の中に Ivanti Endpoint ManagementMDM管理ポータルにアクセスするには、[**アプリ**]選択して [**追加**]。
2. メニューから選択 [**グーグルプレイ**]。
3. 「`WithSecure Elements Mobile Protection`」を検索します。
4. アプリを選択し、クリックします [**選択する**]。

5. アプリのカテゴリが正しいことを確認します。オプションで、[説明] ボックスにアプリ情報を追加できます。
6. [次へ] を選択します。
7. アプリをすべてのスペースに委任するかどうかを選択し、[次]。
8. 優先配布グループを選択し、[次]。

次に、アプリを構成する必要があります。

Androidアプリ管理を手動で構成する

Android アプリ管理を手動で構成する方法について説明します。

1. 下 [アプリの構成] > [Android 向けの管理構成]プラスアイコンを選択します。
   [構成設定] ビューが開きます。
2. 次のことを実行します。
   a) 構成の名前を入力します。
   b) 下 [管理された構成]、 選択する [インストール時に自動起動]。
   c) 必ず [値が定義された設定のみをプッシュする]が選択されます。
   d) の隣に [登録キー]サブスクリプションキーを入力します。

      注 : サブスクリプションキーは、WithSecure Elementsポータル。

   e) メールアドレス欄に ${ユーザーメールアドレス}値として。
   f) 選択する [権限の管理]。
      の 権限を選択ウィンドウが開きます。
   g) すべてのオプションを選択し、クリックします [選択する]。
   h) 下 [ランタイム権限]ドロップダウンメニューをすべて確認し、[自動付与]を選択し、[次]。
      の [アプリの構成]ページが開きます
3. の隣に [デバイスにインストール]プラスアイコンを選択し、次の操作を行います。
   a) 構成設定の名前を入力します。
   b) オンにする [デバイスのインストール構成]。
   c) を選択 [アプリ更新モード]オプションを選択し、ドロップダウンメニューから [優先度が高い]。
   d) [次へ] を選択します。
      [構成設定] ページが開きます。
4. の隣に [プロモーション]プラスアイコンを選択し、次の操作を行います。
   a) 構成設定の名前を入力します。
   b) 選択する [注目リスト]。
   c) [次へ] を選択します。
5. の隣に [委任されたデバイス権限]プラスアイコンを選択し、次の操作を行います。
   a) 構成設定の名前を入力します。
   b) 選択する [アプリ構成の管理]。
   c) [次へ] を選択します
6. [完了] を選択します。
   の WithSecure Elements Mobile Protectionアプリカタログに追加されます。

証明書を使用して Android アプリを構成する

証明書を使用してAndroidアプリを構成する方法について説明します。

1. 上の [Ivanti エンドポイント管理]管理ポータルにアクセスするには、構成ページを選択して [追加]。
2. [証明書] を選択します。
3. 証明書の名前を入力します。
4. アップロード WithSecure Elements証明書 WithSecure Elements Mobile Protection。

   注 : 証明書は以下からご覧いただけます。WithSecure Elementsポータル。

5. [次へ] を選択します。
6. 次のページで、証明書を展開するための優先オプションを選択し、[完了] を選択します。

注： 証明書をデバイスに展開して有効化するには、手動または自動で証明書を展開する必要があります。WithSecure Elements Mobile Protection。

Ivanti Endpoint Management を使用した Android Enterprise の導入

この章では、WithSecure Elements Mobile Protectionアプリの Android Enterprise文脈 Ivanti Endpoint Management。

WithSecure Elements Mobile Protectionアプリを追加する

追加方法の説明 WithSecure Elements Mobile Protectionアプリに Ivanti Endpoint Management。

1. の中に Ivanti Endpoint Management管理ポータルで選択 [管理者] > [グーグル] > [Androidエンタープライズ]。
   [AndroidEnterprise] ページが開きます。
2. [推奨設定の開始] で、[Googleを承認] を選択します。
3. [登録完了] を選択します。
4. [アプリ] > [アプリカタログ] を選択し、[+追加] を選択します。
   [アプリの追加] ウィザードが開きます。
5. 「ビューを選択」のドロップダウンメニューから、[グーグルプレイ]。
6. 「Google Playストアを検索...」ボックスに、セキュアエレメントモバイル保護。
7. アプリを選択してから、[承認] > [承認] を選択します。
8. [完了] > [選択] > [次へ] を選択します。
9. 「説明」ビューで、[次]。
10. 代理人ビューで、[次]。
11. 配布ビューで、希望するオプションを選択し、[次]
12. 設定ビューの横にある [Android 向けの管理構成]プラスアイコンを選択します。
    [構成設定] ページが開きます。
13. 名前欄に名前を入力し、[管理された構成]、 以下をせよ
    a) [登録キー] フィールドに、製品のサブスクリプションキーを入力します。

注： WithSecure Elements Mobile Protectionのサブスクリプションキーは、WithSecure Elements Security Centerの 管理 > サブスクリプション で確認できます。

    b) それぞれのフィールドに名と姓を入力しますオプション。
    c) [エイリアス] フィールドオプションに、別名を入力します。
    d) [メールアドレス] フィールドオプションに、メールアドレスを入力します。
    e) [環境] フィールドオプションに、「2」と入力します。
14. [このアプリ構成の配布] で、[アプリを使用しているすべてのユーザー] を選択し、[次へ] を選択します。
15. [アプリの構成] ページで、[完了] を選択します。
    WithSecure Elements Mobile Protectionに表示されます アプリカタログページ。

3.4.7 Miradore MDMを使用した展開

展開方法の説明 WithSecure Elements Mobile Protectionアプリ付き Miradore MDM Android および iOS デバイスに。

注: これらの手順には、ユーザーとデバイスを作成および構成する方法に関する情報は含まれていません。

iOSアプリをMiradore MDMに追加する

WithSecure Elements Mobile Protection iOSアプリをMiradore MDMに追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

> **注：** WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Apple StoreからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

> **注：** 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. Miradore管理ポータルで、左側のペインメニューから**[管理]** > **[アプリケーション]** を選択します。
2. [アクション] メニューで、**[追加]** > **[iOSアプリケーション]** を選択します。
   [アプリケーションの追加] ウィザードが開きます。
3. [アプリケーションの追加] ウィザードで、次の手順を実行します。
   a) 手順1で、**[App Store]** > **[次へ]** の順に選択します。
   b) 手順2で、次の詳細を入力します。
      - 名前⊠`WithSecure Elements Mobile Protection`
      - App Store ID⊠`1549210826`
      - App Storeの国⊠使用する国を選択してください
      - パッケージ名⊠`com.f-secure.mobileprotection`
      - 説明⊠使用する説明を入力します。
      - デバイスが登録解除されたら、**[アプリケーションの削除]** を選択します。

   c) [**新規作成**] を選択します。
   d) 手順3で、情報が正しいことを確認し、**[閉じる]** を選択します。

iOSアプリの構成

設定方法の説明 WithSecure Elements Mobile ProtectioniOSアプリで Miradore⊠⊠⊠。

1. の中に Miradore管理ポータルで、セキュアエレメントモバイル保護アプリケーション リストのエントリ。
2. **[構成]** タブに移動し、**[新規追加]** を選択します。
   [構成設定の作成] ビューが開きます。
3. 最初の設定に次の値を追加します。
   - 設定⊠`fate_registration_key`
   - データタイプ⊠文字列
   - 値⊠サブスクリプションキーを入力します
4. **[追加]** を選択して、新しい設定を構成に追加します。
5. **[追加]** を選択して、新しい設定を構成に追加します。
   これらの2つの必須設定を構成した後、オプション設定を追加できます。

6. ユーザーの詳細を追加するには、[新規追加] を選択し、次の値を使用します。

   ヒント： ユーザーの詳細は、デバイスを識別するのに役立ちます。

設定	データタイプ	ユーザー変数
ファーストネーム	文字列	[ユーザー] > [名] を選択します
last_name	文字列	[ユーザー] > [姓] を選択します
***E**メール*	文字列	[ユーザー] > [メールアドレス] を選択します
エイリアス	文字列	[メールアドレス] > [ユーザーの表示名] を選択します

Miradore MDMへのAndroidアプリの追加

WithSecure Elements Mobile Protection AndroidアプリをMiradore MDMに追加する方法を説明します。

Miradore MDMは、XMLファイルまたはGooglePlayストアのInstallReferrerサービスを使用して、アプリにライセンス情報を提供できます。MDMへのアプリの追加を開始する前に、使用する方法を選択してください。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注： WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、**管理** > **サブスクリプション** から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[**MDMサーバ構成**] を選択すると、証明書をダウンロードすることができます。

注： 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

1. Miradore管理ポータルで、左側のペインメニューから[管理] > [アプリケーション] を選択します。
2. 右側の[アクション] メニューで、**追加** > **Androidアプリケーション** を選択します。
   [アプリケーションの追加] ウィザードが開きます。
3. [アプリケーションの追加] ウィザードで、次の手順を実行します。
   a) 手順1で、[GooglePlayストア] を 選択してから [次へ] を選択します。
   b) 手順2で、次の詳細を入力します。
      - 名前⊠`WithSecure Elements Mobile Protection for Android`
      - パッケージ名⊠`com.fsecure.mp.ucf`
      - 説明⊠使用する説明を入力します。
      - ユーザーへの通知⊠ユーザーに表示する情報を入力します。
      - ホーム画面へのショートカットの追加⊠アプリへのショートカットを作成する場合に選択します。

c) [リファラーのインストール] フィールドに次の情報を追加します。

- インストールリファラーサービスを使用してライセンス情報を配信する場合は、次の場所にあるインストールリファラー文字列を使用します。WithSecure Elementsサービス。[Google PlayダウンロードURL]とともに WithSecure Elements Mobile Protectionアクティベーション文字列。utm-mediumから始まる文字列の後半部分をコピーします。アプリに追加情報を送信する場合は、アクティベーション文字列に追加の要素を追加できます。

4. [新規作成] を選択します。
5. 手順4で、情報が正しいことを確認し、[閉じる] を選択します。

3.4.8 Samsung Knoxを使用した展開

Samsung Knox を使用した WithSecure Elements Mobile Protection アプリを Android デバイスに展開する方法について説明します。

注: この手順には、ユーザーとデバイスを作成および構成する方法に関する情報は含まれていません。

Samsung Knox を使用した Android アプリの展開

Samsung Knox を使用して Android アプリを展開する方法を説明します。

Android アプリを Samsung Knox に追加する

WithSecure Elements Mobile Protection Androidアプリを Samsung Knoxに追加する方法を説明します。

WithSecure Elements Mobile ProtectionをMDMと統合する前に、次の前提条件が満たされていることを確認してください。

- エンドデバイスを登録しました
- ポリシー制限のあるプロファイルを設定しました

  注 : WithSecureは、特に言及されていない限り、プロファイルやポリシーに関するサポートや説明を提供しません。
- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効なWithSecure Elements Mobile Protectionのサブスクリプション

統合は、次のもので構成されます。

- Google PlayストアからMDMにアプリを追加する
- アプリを割り当て、WithSecureが提供するサブスクリプション キを使用して構成する、または
- MDMサーバ構成証明書をWithSecure Elementsポータルからダウンロードします。ポータルにログインし、管理 > サブスクリプション から最初に関連する会社を選択し、[WithSecure Elements EPP for Mobiles] の横にある3つの点を選択し、[MDMサーバ構成] を選択すると、証明書をダウンロードすることができます。

注 : 一部のMDMでは、証明書を使用しないとアプリを連携できない場合があります。一部のMDMでは、証明書を使用しないとアプリを統合できない場合があります。詳細は、関連するMDMの説明書を参照してください。

Android アプリを Samsung Knox に追加するには:

1. ログイン Samsung Knoxコンソール。
2. 選択する [応用]。
   [アプリケーション] ページが開きます。
3. [追加] を選択します。
4. アプリケーションタイプの選択画面で、[Androidプラットフォーム] > [パブリックマネージドGoogle Play]を選択し、[わかりました]。
5. アプリケーションの追加ページで、セキュアエレメントモバイル保護アプリケーションを検索します。

注: 選択したプラットフォームの国を変更するには、[国を設定]次に国を選択します。

6. 検索結果で、まず追加したいアプリケーションを選択し、次に [選択する]。
7. 必要に応じて、次のインポートされた情報を編集します。
   - 名前 - アプリケーションの名前を入力します
   - カテゴリ-アプリケーションのカテゴリを選択します。[カテゴリを管理する]、アプリケーションカテゴリを追加または編集できます。
   - 説明 - アプリケーションの説明を入力します
8. 続行するには、次のいずれかのオプションを選択してください。
   - 選択する [保存して割り当て]情報を保存し、アプリケーションの割り当てに進むには、[続く]。
   - 選択する [保存]情報を保存してアプリケーションリストに戻ります。このアプリケーションは後で割り当てることができます。

Androidアプリの割り当てと構成

Androidアプリの割り当てと設定方法について説明します。

重要: 親組織にプロファイルを割り当てると、そのサブ組織はそのプロファイルを継承します。ただし、サブ組織はアプリケーションとコンテンツを継承しません。

Samsung Knox で Android アプリを割り当てて構成するには:

1. 選択する [応用]。
   [アプリケーション] ページが開きます。
2. [割当]を選択し、[WithSecure Elements Mobile Protection]を選択します。
   「アプリケーションの割り当て」ページが開きます。
3. 次の割り当て設定を構成します。
   - ターゲットデバイス-次のいずれかのオプションを選択できます。[Androidエンタープライズ]、[Android レガシー]、 または [Android エンタープライズ + レガシー]。
   - 設置エリア - 指定された設置エリアを表示します
   - インストール タイプ - 利用可能なオプションのいずれかを選択します。
     - [マニュアル]- デバイスユーザーがアプリケーションを手動でインストールできるようにする
     - [自動取り外し可能]-アプリケーションが自動的にインストールされるように設定します。デバイス ユーザーは、アプリケーションを手動で削除することもできます。
     - [自動取り外し不可、Android Management API のみ]
   - インストール後に自動実行 (非 Android 管理 API) - インストール後すぐにアプリケーションを起動するように設定できます。
   - 自動更新モデル-利用可能なオプションは次のとおりです[デフォルトの更新]、[優先度が高い]、そして [延期90日]。
4. 管理対象構成の横にある [設定を設定する]そして次の操作を行います。
   - 管理対象構成フィールドに、わかりやすい名前を入力します。例:仕事。
   - 登録キーフィールドに、WithSecure Elements Mobile Protectionサブスクリプションキー。
   - エイリアスフィールドに以下を入力します。$ユーザー名$。
   - メールアドレス欄に $メールアドレス$。
   - [環境] フィールドに、「2」と入力します。

     注: WithSecure Elementsに登録されたデバイスは、値を設定するとメールアドレスとともに表示されます。$ メールアドレス$。
5. 変更を保存するために [保存] を選択します。
6. [ターゲット] で、アプリケーションを割り当てるグループを選択します。

3.5 一般的なユースケースの処理

一般的なユースケースを処理する方法に関する手順。

3.5.1 WithSecure MSI変換ツールを使用する

WithSecure変換ツールを使用して、カスタマイズされたクライアントアプリケーションを作成する方法を説明します。

このツールを使用すると、カスタムパラメータ、たとえばサブスクリプションキーをインストーラに埋め込むことができるため、インストール中に指定する必要がなくなります。MSIファイルは、Elements Agentをインストールするためにカスタマイズされたクライアントアプリケーションを作成する便利な方法です。Active Directoryグループポリシー経由でインストールする場合など、MSIファイルが必要な場合があります。ただし、好みに応じて使用できる他の方法もあります。

WithSecure MSI変換ツールでは、カスタマイズされたMSIファイルまたは設定のみを含むMSTファイルを作成することができます。どちらかを選択する場合は、以下を考慮してください。

- カスタマイズされたMSIインストーラを作成する
  - インストーラーにすべての設定が含まれているため、便利な方法です
  - オリジナルのMSIファイルを変更すると、パッケージの署名が無効になります。つまり、独自の証明書で再度署名するか、署名されていないソフトウェアのインストールを許可する必要があります。
- 別のMSTファイルを作成する
  - この方法では、構成用に別のファイルが作成されます。
  - インストーラーの署名を変更しないため、便利な方法です

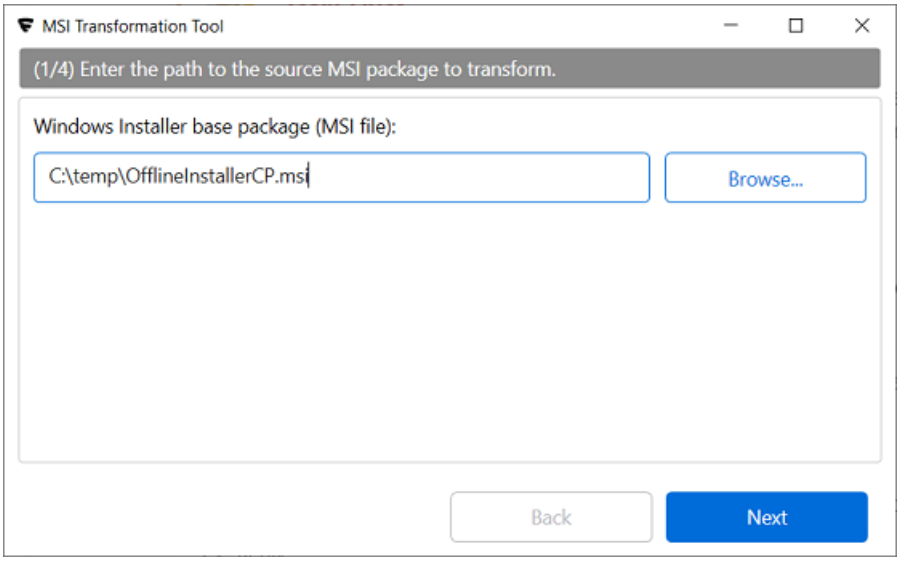
MSI変換ツールを使用するには、次のようにする必要があります。

- WithSecure Elementsポータルのダウンロードセクションから MSI形式のWithSecure Elements Agentの最新バージョンをダウンロードします。

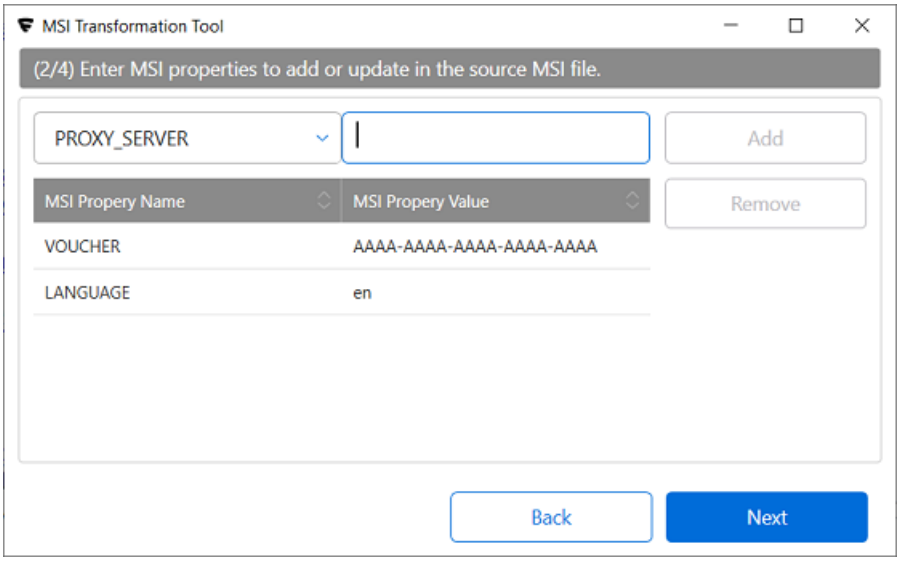
  👉 **重要：** MSIファイルの有効期限は8ヶ月です。8ヶ月以上前にMSIファイルをダウンロードした場合は、新しいMSIファイルをダウンロードする必要があります。
- ここからWithSecure MSI変換ツール（FsMsiTool_ui.exe）をダウンロードしてください。
- コマンドラインパラメータとMSIプロパティページ80 で利用可能なオプションをよく理解してください。

MSI変換ツールを使用するには

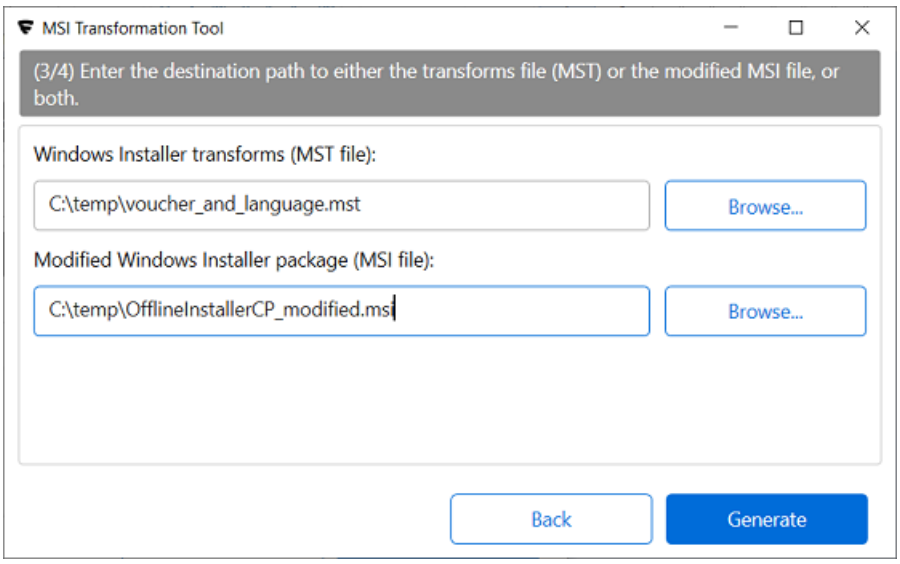
1. MSI 変換ツールを起動します。
2. 開いたページで、Elements Agent の MSIインストーラーへのパスを指定し、[次へ] を選択します。



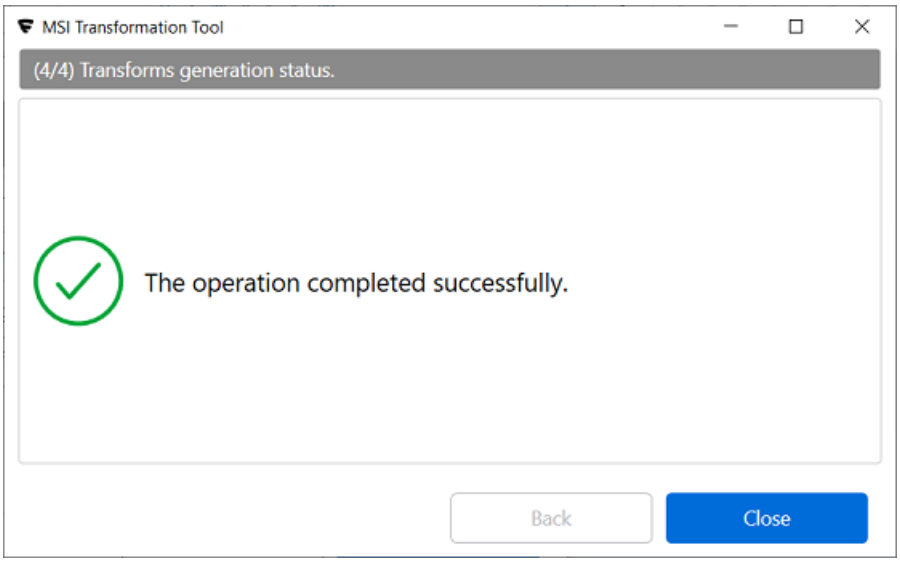
3. 追加する1つ以上のMSIプロパティを指定し、[次へ] を選択します。



4. 出力MSIファイルまたはMSTファイル、あるいはその両方を指定します。



5. [生成] を選択してファイルを作成します。



関連概念

コマンドラインパラメータとMSIプロパティページ80

.exeとMSIの両方のインストーラを構成して、あなたの環境の特別なニーズに適応させることが可能です。

3.5.2 クライアントに設定を割り当てる

すべてのクライアント設定は、製品固有の設定のバンドルであるプロファイルを使用して管理されます。

プロファイル割り当てルールを追加する

プロファイルの割当ルールを追加する方法の説明。

プロファイルを割り当てる推奨方法は、ポータルでプロファイル割り当てルールを使用することです。プロファイル割り当てルールは、デフォルトプロファイルを置き換えます。これらは、システムに追加された新しいデバイスに自動的に適用され、表中の上から下への順番で実行されます。最初に一致したルールが新しいデバイスに適用されます。一致するルールがない場合は、デフォルトのルールが適用されます。

注： デバイスがADグループやIP、DNS、ホストアドレスを変更したときに、ルールに基づいてプロファイルとラベルをデバイスに自動的に割り当てる設定をオンにするかどうかを選択できます。

注: デフォルトのプロファイルでは、ウイルス対策機能のオフやアンインストールが可能で、ほとんどの機能を制御できるため、より厳格な独自のプロファイルを作成することをお勧めします。

プロファイル割り当てルールを追加するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. [**プロファイル割り当てルール**] タブを選択します。
   ビューが開き、各デバイスタイプのデフォルトのアウトブレイクルールとプロファイル割り当てルールが表示されます。
3. [**ルールを追加**] を選択します。
   [ルールの追加] ウィンドウが開きます。
4. 次の情報を入力します。
   - 条件を選択します。
   - 選択した条件に基づいて、値を選択または入力します。
   - クライアントの種類を選択します（Windowsワークステーション、Windowsサーバー。Linux、Macコンピュータ。
   - 割り当てるプロファイルを選択します。
   - ルールにラベルを追加します（オプション）。
   - ルールの説明を追加します。
5. [**ルールを追加**] を選択します
   新しいルールがテーブルの一番上に追加されます。
6. 次のいずれかの方法で、作成したルールの順序を変更できます。
   - ルールを目的の位置にドラッグ＆ドロップします。
   - 移動するルールの行で、[アクション] 列から [**トップに移動**]また [**一番下に移動**] を選択します。

     注： 既存のデフォルト ルールは、常にルールの一番下にあります。作成したルールをデフォルトルールより下に移動することはできません。
7. ページ下部の [**ルールが変更されました**] バナーで、[**変更内容を保存**] を選択します。

   注： 変更を保存した後、システムがすべてのデバイスのルールを評価するように選択できます。

新しいルールがテーブルに追加されました。

クライアントのインストール時にプロファイルIDを指定する

ユースケースに一致するルールを作成できない場合は、クライアントのインストール中にプロファイルを指定することで、割り当てられるプロファイルを制御できます。

プロファイル ID を指定するには:

1. 次のようにして、プロファイル設定からプロファイル ID をコピーします。
   a) 下 [**セキュリティ構成**]、 選択する [**プロフィール**]をクリックし、プロファイルを選択します。
   b) 割り当てるプロファイルを編集します。
   c) プロフィール設定の上部に表示されるプロフィール ID をコピーします。
2. コマンドラインまたはスクリプトからクライアントをインストールする場合は、例の番号を自分のプロファイルに表示される番号に置き換えることで、コマンドにパラメータを追加できます。

```
ElementsAgentInstaller.exe --profile-id=117525
```

3. カスタム MSI インストーラーを作成する場合は、例の番号を自分のプロファイルに表示される番号に置き換えて、次のパラメーターを追加します。

```
PROFILE_ID=117525
```

> **注:** プロファイル ID をインストール パラメータとして渡すと、上記で説明したプロファイル割り当てルールは評価されません。

プロファイルを手動で割り当てる

プロファイルを手動で割り当てる方法の説明。

設定を手動で割り当てるには:

1. クライアントをインストールしたら、WithSecure Elementsポータル。
2. 下 [**環境**]、 選択する [**デバイス**]次に、1 つまたは複数のデバイスを選択します。
   ページの下にメニューが表示されます。
3. [**プロファイルを指定する**] を選択します。
4. ドロップダウン メニューから、選択したデバイスに割り当てるプロファイルを選択します。
5. [**プロファイルを指定する**] を選択します。
   プロファイルは選択したデバイスに割り当てられます。

3.5.3 ポータル内のデバイスを複製せずに Elements Agent を再インストールする

エージェント インストールのライフサイクルについて説明します。これにより、エージェント インストール中に発生する可能性のある最も一般的な落とし穴を回避できます。

ポータルでは、デバイスはデバイス名を主な識別子としてリストされます。実際には、クラウドサービスでは、何百万ものデバイスの一意性を識別するために、より細かい方法が必要です。このため、インストール中に一意のUUIDが生成されます。デフォルトでは、WithSecure Elements使用している管理ソフトウェアをアンインストールする WithSecure Elements Agent再インストールすると、新しい UUID が生成され、同じ名前の2番目のデバイスがポータルに表示されます。これがまれなケースであれば問題にはなりませんが、場合によっては、Intune などの管理ソフトウェアによって、オペレーティング システムのアップグレードの一環としてすべてのソフトウェアが再インストールされる可能性があり、その場合は準備しておくことをお勧めします。

Elements Agent を再インストールする際の問題を回避する

Elements Agentの再インストール中に潜在的な問題を回避するには、生成されたUUIDとともにデバイス固有の識別子をバックエンドに送信する必要があります。現在、次の2つのオプションがサポートされています。

- コンピューター SMBIOS GUID(マザーボード上の一意の識別子)
- AD GUID(Active Directory からのデバイスの一意の識別子)

識別子	説明	既知の問題点
SMBIOS GUID	デバイスのシステム管理BIOS識別子は、製造元が設定した一意の識別子を使用して各コンピューターのマザーボードを定義するDMTF 標準です。 この識別子を使用することをお勧めします。	まれに、メーカーが標準に従わず、すべてのデバイスに同じ値を割り当てたり、このフィールドをサポート連絡先情報などの別の目的に使用したりすることがあります。潜在的な問題を軽減するために、すべてのデバイスがバックエンドで共通の識別子を共有するケースを防ぐために、既知の問題のある値に対してこのパラメータの使用を制限しています。これらの問題は非常にまれであり、ビジネス用に販売されているラップトップで発生する可能性は低いことに注意してください。
AD GUID	デバイスが会社のActive Directoryに登録されるときに生成される一意の識別子 **注：** これは、イメージが起動されるたびにSMBIOS が変更される非永続的な VDI 展開など、SMBIOS GUID が機能しない場合に推奨されます。	この識別子は、Elements Agentがインストールされる前にActive Directory に登録されているコンピューターに対してのみ機能します。 デバイスが削除され、その後Active Directory に再度追加された場合、Elements Agent を再インストールすると、ポータルでデバイスが複製される可能性があります。

インストール中にこれらのパラメータを使用すると、次のことが起こります。

- 初回インストール
  - Elements Agentインストールの一環として一意のUUIDを生成します
  - 登録中、Elements Agentサブスクリプションキー、生成されたUUID、およびSMBIOS GUIDまたはAD GUIDを、両方が保存されているバックエンドに送信します。
  - 新しいデバイスが Elementsポータル
- 次のインストール:
  - Elements Agentインストールの一環として一意のUUIDを生成します
  - 登録中、Elements Agentサブスクリプションキー、生成されたUUID、およびSMBIOS GUIDまたはAD GUIDをバックエンドに送信します。
  - バックエンドは、同じサブスクリプション キーを持ち、同じ SMBIOS GUID または AD GUID を使用するデバイスを識別し、それらを既存のデバイスに接続します。
  - 新しいデバイスは追加されません Elementsポータルですが、既存のものが更新されています。

注： すべてのインストールで同じサブスクリプション キーを使用する必要があります。

.exe ファイルを使用して Elements Agent をインストールする場合は、次のパラメータを使用します。

- 識別子としての SMBIOS GUID:

```
c:\path\to\installer.exe --use_smbios_guid
```

- 識別子としての AD GUID:

```
c:\path\to\installer.exe --use_ad_guid
```

.msi ファイルを使用して Elements Agent をインストールする場合は、次のパラメータを使用します。

- 識別子としての SMBIOS GUID:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=smbios
```

- 識別子としての AD GUID:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=adguid
```

注：

インストール時に使用できるパラメータの完全なリストは以下にあります。コマンドラインパラメータとMSIプロパティページ80。

3.6 特殊なケースの取り扱い

特殊なケースのためにインストーラーに渡すことができるパラメーターがいくつかあります。

ユーザーにサブスクリプション キーの入力を求めないインストーラーを作成するには、ファイル名にキーを追加します。

```
installer.exe   installer_xxxx-xxxx-xxxx-xxxx-xxxx.exe
```

インストール時に特殊なケース、つまりコマンドラインからインストーラーにパラメータを渡す方法を処理する場合は、以下のオプションの完全なリストを参照してください。

3.6.1 コマンドラインパラメータとMSIプロパティ

.exeとMSIの両方のインストーラを構成して、あなたの環境の特別なニーズに適応させることが可能です。

利用可能なパラメータは多数あり、それぞれに特定の目的があります。インストレーションガイドには通常、特定のフローに必要なパラメータが記載されていますが、その場合でも、必要に応じてパラメータを追加するオプションがあります。

.exeファイルでパラメータを使用する

.exeファイルでは、コマンドライン引数としてパラメータを追加することを意味します。例えば、インストーラの引数としてサブスクリプションキーを渡すことで、以下のようにインストール中にユーザーが入力する手間を省くことができます。

```
installer.exe --voucher aaaa-bbbb-cccc-dddd-eeee --language en
```

一部のexeパラメータでは、長いオプション‘-language’と短いオプション‘-l’の両方が利用できます。

.MSIファイルでパラメータを使用する

MSIファイルはカスタマイズされたインストーラパッケージで、パッケージング中に設定を埋め込むことができます。これらのパッケージをカスタマイズするための特別なツールがありますが、他のソリューションも利用可能です。

MSIファイルに引数を渡す方法は3つあります。

- カスタマイズしたMSIファイルに引数を埋め込む
- MSIファイルが参照する.MST‘MSI変換’ファイルを作成する

- コマンドラインからMSIファイルを実行し、例えば以下のように引数を渡します。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=aaaa-bbbb-cccc-dddd-eeee
LANGUAGE=en
```

WithSecure MSI変換ツールの使用方法については、WithSecure MSI変換ツールを使用するページ75 を参照してください。

EXEファイルまたはMSIパッケージを使用して製品をインストールする場合、次のコマンドラインパラメータとプロパティを使用できます。

EXEパラメータ	MSIプロパティ	説明
--profile-id<ID>	***PROFILE_ID***	目的のプロファイルID値を設定します。例 `--profile-id 18062053`。プロファイルIDを見つけるには、プロファイルエディタでプロファイルを開きます。ページの上部 割り当てられたコンピュータの数と最後に編集された日付の下 にプロファイルIDが表示されます。 EXEパラメータの例 `--profile-id 180238` MSIプロパティの例 `PROFILE_ID=180238`

--language <id>
-l <id>
	言語	インストールで使用する言語を選択します。パラメータ「id」は、IETF形式の有効な言語識別子である必要があります。
		ID値には次のいずれかを指定できます en、cs、da、de、el、en、es-MX、es、et、fi、fr-CA、fr、hu、it、ja、ko、nl、no、pl、pt-BR、pt、ro、ru、sl、sv、tr、zh-HK、zh-TW、zh。
		例:
		`C:\Users\<username>\Downloads>installer.exe --languge en`または
		`C:\Users\<username>\Downloads>msiexec /i installer.msi LANGUAGE=en`
		たとえば、「-language <id>」パラメータを指定せずに、または「LANGUAGE = <id>」MSIプロパティを指定せずにinstallerコマンドを使用すると、製品はシステム設定に基づいて言語を自動的に検出します。
		例:
		`C:\Users\<username>\Downloads>installer.exe`
		また
		`C:\Users\<username>\Downloads>msiexec /i installer.msi`

EXEパラメータ	MSIプロパティ	説明
--silent -s		サイレント インストールの順序を設定します。ユーザに対してダイアログは表示されません。EULT(使用許諾書)は同意されると想定されます。キーコードが埋め込まれている(設定されている)場合、インストール時にソフトウェアがキーコードを自動的に適用します。それ以外の場合、ソフトウェアはキーコードがない状態 (失効した初期状態) になります。インストールがコンピュータの再起動を必要とする場合、ダイアログは表示されませんが、実行可能リターンコードは99で、再起動後も自動的に続行されます。
--voucher <subscription key>	***VOUCHER***	サブスクリプションキーを設定します。サブスクリプションキーは、インストーラファイル名に埋め込まれているかのように処理されます。サブスクリプションキーがファイル名に存在し、コマンドラインにも追加されている場合、コマンドラインはファイル名サブスクリプションキーを上書きします。 EXEインストーラとは異なり、MSIパッケージのファイル名にサブスクリプションキーを埋め込むことはできません。
--proxy <url>	***PROXY_SERVER***	製品のインストール時に、すべてのリクエストがこのプロキシを介して送信されます。例--proxy http://proxy.gtn:3128
--skip-sidegrade <省略するオプション>	***SIDEGRADE_SKIPLIST***	EXEパラメータインストール中にサイドグレードから除外する競合他社の製品のリストを指定できます。「*」を指定すると、すべてのサイドグレードを省略します。 競合する名前の前に [skip-reboot] を追加すると、サイドレードが再起動を必要しないことを示すことができます(サイドグレードは実行されます)。 • --skip-sidegrade "Sophos Cloud Endpoint|HitmanPro.Alert" • --skip-sidegrade "HitmanPro.Alert|SG16|SG1" • --skip-sidegrade "*" - サイドグレードしない (WithSecure製品を含む) • --skip-sidegrade "[skip-reboot]*" - すべての問題/競合が削除され、再起動は必要ありません • --skip-sidegrade "[skip-reboot]Sophos Cloud Endpoint|SG1" - Sophos Cloud Endpoint が再起動せずにアンインストールされ、SG1 は競合として検出されない MSIプロパティインストール中に競合する製品の削除をスキップするには、このプロパティに値「*」を指定します。

EXEパラメータ	MSIプロパティ	説明
--installation-tags <tags>	***INSTALLATION_TAGS***	バックエンドポータル (WithSecure Elements Endpoint Protection、WithSecure Elements Endpoint Detection and Response、WithSecure Elements Vulnerability Management) に報告されるインストール タグ。例。 `--installation-tags "PSB=psb-tag1:psb-tag2:psb-tag3, RADAR=radar-tag1:radar-tag2:radar-tag3,department=accounting,role=secretary"`。 現在、WithSecure Elements Endpoint Protection ポータルはこれらのタグを PSB=psb-tag1:psb-tag2:psb-tag3から「label」フィールドにコンマ区切り値として格納します。文字列の最大長は255文字です。タグにコンマやコロンを含めることはできません。
--use_smbios_guid	***UNIQUE_SIGNUP_ID=smbios***	このデバイスの一意な識別子としてSMBIOSGUIDを使用します。デフォルトでは、管理ポータルから削除されていないデバイスに本製品を再インストールすると、新しい識別子が生成されます。その結果、重複したデバイスが作成されます。このコマンドラインパラメータを使用すると、再インストールされた製品を既存のデバイスにリンクし、新しいエントリーが作成されるのを防ぐことができます。 👉 **注：** 製品を再インストールするときに新しいサブスクリプションキーを使用すると、ポータルに新しいデバイスが作成されます。 👉 **注：** 製品を通常どおりアンインストールすると、ポータルから自動的に削除されます。 このコマンドラインパラメータを使用することで、デバイスが自動的に削除されるのを防ぐことができます。

EXEパラメータ	MSIプロパティ	説明
--use_ad_guid	***UNIQUE_SIGNUP_ID=adguid***	このデバイスの一意な識別子として、Active Directoryコンピュータオブジェクト GUIDを使用します。デフォルトでは、管理ポータルから削除されていないデバイスに本製品を再インストールすると、新しい識別子が生成されます。その結果、重複したデバイスが作成されます。このコマンドラインパラメータを使用すると、再インストールされた製品を既存のデバイスにリンクし、新しいエントリーが作成されるのを防ぐことができます。 👉 **注：** 製品を再インストールするときに新しいサブスクリプションキーを使用すると、ポータルに新しいデバイスが作成されます。 👉 **注：** 製品を通常どおりアンインストールすると、ポータルから自動的に削除されます。 このコマンドラインパラメータを使用することで、デバイスが自動的に削除されるのを防ぐことができます。
--disable_defender	***DISABLE_DEFENDER***	`--disable_defender`コマンドラインまたは`DISABLE_DEFENDER=1` msiプロパティを使用して、サーバ上のWindows Defenderをオフにしてアンインストールします。バージョン2016以降のWindows ServerにはWindows Defenderがありますが、セキュリティセンターはありません。そのため、別のセキュリティソフトウェアがインストールされても、Windows Defenderは自動的にオフになりません。通常、GPOまたは別の標準的な方法を使用してDefenderをオフにすることができます。それができない場合は、代わりにこれらのインストールオプションを使用することができます。
--skip-dotnet		インストール中に.Netをインストールすることは避けてください。.Netを自分で処理するには、[プロファイル] > [一般設定] > [自動更新] で製品の更新時に [**クライアントに.Netの管理を許可する**] をオフにします。
--connector-proxy <url>	***CONNECTOR_PROXY***	製品のインストール時に、すべての要求が最終プロキシとしてコネクタを介して送信されます。 例：`--connector-proxy http://proxy.gtn:3128`
--upgrade-delay <minutes>	***UPGRADE_DELAY_MINUTES***	最新バージョンへのセルフアップグレードが許可されるまでの分数を指定します。このオプションは、即時のセルフアップグレードが好ましくない展開シナリオに役立ちます。既知のシナリオの1つは、Microsoft Intuneを使用した展開です。

ローカルMSIインストールの場合、必要なプロパティをコマンドラインに直接渡すことができます。

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=XXXX-XXXX-XXXX-XXXX-XXXX
LANGUAGE=en
```

この構文は、一部のリモート監視および管理⊠RMM⊠ソフトウェアでもサポートされています。 Active Directoryグループポリシーを介してリモートでインストールする場合は、プロパティをMSI変換ファイル⊠.mst⊠に渡すか、MSIパッケージに直接埋め込むことができます。

関連概念

仮想デスクトップインフラストラクチャ⊠VDI⊠システムの永続モードで展開するページ36
ゴールデンイメージを使用して、CitrixやVMware Horizonサーバー、および他のVDI環境に製品をインストールする手順は次のとおりです。

関連タスク

Active Directory GPOで展開するページ29
この導入方法は、Active Directoryを使用し、グループポリシーでソフトウェアを豆腐したい企業に適しています。

3.6.2 製品をアンインストールするためのコマンド

コマンドプロンプトから製品をアンインストールする場合、次のコマンドラインコマンドを使用できます。

実行ファイル	実行パラメータ	説明
fs_uninstall_32.exe	***[--silent]***	`fs_uninstall_32.exe`の場合、`C:\Program Files\F-Secure\PSB` directoryまたは`C:\Program Files (x86)\F-Secure\PSB`に移動します。 サイレント モードでは、`--silent`パラメータを使用できます。
msiexec	***/x {PRODUCT_CODE} [/qn]***	製品コードを見つけるには、PowerShellコマンドラインで次のコマンドを入力します。 `get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name`。 サイレント モードでは、`/qn` パラメータを使用できます。

注： オプションのパラメーターは [角括弧] 内にあります。

第 章
4

プロファイルを管理する

トピック :

ここでは、アカウント内のワークステーション、サーバー、およびモバイルデバイスのセキュリティソフトウェア設定を管理する手順を説明します。

コンピュータ、またはWithSecure Elements Mobile Protectionがインストールされているモバイルデバイスのセキュリティ設定に対して、ユーザーができることを制御できます。プロファイルは、デバイスに適用可能な設定の集合体です。特定のグループのユーザまたはデバイスに使用できます。

- 初心者ユーザ。初心者用のプロファイルを指定した場合、ユーザによるセキュリティ設定の変更を制限することができます。
- コンピュータのタイプ、「ノート」または「デスクトップ」。ノート用のプロファイルは外出先などセキュリティに問題がある場所でインターネットを利用するときに適切です。デスクトップ用のプロファイルは固定した場所での利用に適切です。

注 : プロファイルが指定されていない場合、プリセットのデフォルトプロファイルが自動的に指定されます。プリセットのプロファイルは、ユーザの迷惑にならないように設計されています。

プリセットの設定よりも厳密な設定で独自のプロファイルを作成することをお勧めします。既存のプロファイルを新しいプロファイルのベースとして使用できます。

より安全なプロファイル設定では、たとえば、設定がロックされ、改ざん防止がオンになり、外部USBストレージからファイルを実行できず、ユーザは製品をアンインストールできません。

4.1 Elements EPP for ComputersとElements EPP for Serversでプロファイルを管理する

ここではWithSecure Elements EPP for ComputersとWithSecure Elements EPP for Serversでプロファイルを管理する方法を説明します。

4.1.1 新しいコンピュータ プロファイルを作成する

特定のコンピュータに指定できるプロファイルを作成することができます。

新しいプロファイルを作成するには

1. WithSecure Elementsにログインします。
2. [セキュリティ構成] で、[プロファイル] を選択します。
   「プロファイル」ページが開きます。
3. [Windowsコンピュータ用] または [Windowsサーバ用] タブを選択し、[プロファイルを作成] を選択します。
   [Windowsコンピュータ用プロファイル] または [Windowsサーバ用プロファイル] を選択します。
4. 新しいプロファイルの名前と説明を入力してください。新しいプロファイルのラベルを選択することもできます。
5. 設定を変更して、[保存して発行] を選択します。
   新しいプロファイルが作成されます。

4.1.2 プロファイル割り当てルールを追加する

プロファイルの割当ルールを追加する方法の説明。

プロファイルを割り当てる推奨方法は、ポータルでプロファイル割り当てルールを使用することです。プロファイル割り当てルールは、デフォルトプロファイルを置き換えます。これらは、システムに追加された新しいデバイスに自動的に適用され、表中の上から下への順番で実行されます。最初に一致したルールが新しいデバイスに適用されます。一致するルールがない場合は、デフォルトのルールが適用されます。

注： デバイスがADグループやIP、DNS、ホストアドレスを変更したときに、ルールに基づいてプロファイルとラベルをデバイスに自動的に割り当てる設定をオンにするかどうかを選択できます。

注: デフォルトのプロファイルでは、ウイルス対策機能のオフやアンインストールが可能で、ほとんどの機能を制御できるため、より厳格な独自のプロファイルを作成することをお勧めします。

プロファイル割り当てルールを追加するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [プロファイル割り当てルール] タブを選択します。
   ビューが開き、各デバイスタイプのデフォルトのアウトブレイクルールとプロファイル割り当てルールが表示されます。
3. [ルールを追加] を選択します。
   [ルールの追加] ウィンドウが開きます。
4. 次の情報を入力します。
   - 条件を選択します。
   - 選択した条件に基づいて、値を選択または入力します。
   - クライアントの種類を選択します（Windowsワークステーション、Windowsサーバー。Linux、Macコンピュータ。
   - 割り当てるプロファイルを選択します。
   - ルールにラベルを追加します（オプション）。
   - ルールの説明を追加します。

5. [ルールを追加] を選択します
   新しいルールがテーブルの一番上に追加されます。
6. 次のいずれかの方法で、作成したルールの順序を変更できます。
   - ルールを目的の位置にドラッグ⊠ドロップします。
   - 移動するルールの行で、[アクション] 列から [トップに移動]また [一番下に移動] を選択します。

   注: 既存のデフォルト ルールは、常にルールの一番下にあります。作成したルールをデフォルトルールより下に移動することはできません。
7. ページ下部の [ルールが変更されました] バナーで、[変更内容を保存] を選択します。

   注: 変更を保存した後、システムがすべてのデバイスのルールを評価するように選択できます。

新しいルールがテーブルに追加されました。

4.1.3 Active Directory でグループのデフォルト プロファイルを設定する

Active Directory 階層内の場所に基づいて、グルーっプのデフォルト プロファイルを設定できます。

Active Directory 階層内の任意のグループにデフォルト プロファイルを設定できます。デフォルト プロファイルを設定しない場合、追加するデバイスは親グループからデフォルト プロファイルを継承します。

新しいデバイスをWithSecure Elements EPPに追加すると、システムは新しいデバイスから Active Directory 構造に関する情報を自動的に受信します。

注: デフォルトのActiveDirectoryプロファイルは、ポータルに追加された新しいデバイスにのみ割り当てられます。[デバイスがADグループを変更するとき]をオフにすると、そのADグループのプロファイルがそのデバイス設定に自動的に割り当てられ、AD階層内のデバイスの場所が変更されても、デバイスプロファイルは変更されません。設定をオンにしてデバイスの場所を変更すると、デバイスプロファイルが10分以内に新しいADデフォルトプロファイルで更新されます。設定がオフで、プロファイルを手動で適用した場合、AD階層内のデバイスの場所が変更されても、デバイスプロファイルはそのままです。

Active Directory でデバイスのデフォルト プロファイルを設定するには

1. [プロファイル] を開き、[デフォルトのプロファイル] を選択します。
2. [Active Directory] で、デフォルト プロファイルを変更する Active Directory グループに移動します。
3. [メニュー] の列で、[変更] を選択します。
   [デフォルト プロファイルの変更] ウィンドウが開きます。
4. ドロップダウン メニューから、デフォルトのプロファイルを選択し、[変更] を選択します。

   注: WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversのプロファイルを個別に選択できます。

4.1.4 プロファイルを編集する

既存のプロファイルを変更した場合、プロファイルが指定されているコンピュータに変更が反映されます。

プロファイルを編集するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. いずれかのタブを選択し、編集するプロファイルを選択します。
3. 現在のプロファイルの保存を変更するために [保存して発行] を選択します。

   注: 編集した設定を複数のプロファイルに適用する場合、[保存して複数のプロファイルに公開]を選択します。ただし、変更を複数のプロファイルに公開すると、切り替え可能(オン/オフ) の設定のみ保存されることに注意してください。

プロファイル設定に加えた変更は、選択したプロファイルを持つすべてのデバイスに適用されます。

4.1.5 スキャン除外の設定

ファイルまたはフォルダをスキャンから除外するように製品を設定します。

注： これは EDR センサー スキャンには適用されません。

スキャンの除外を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. 選択する [Windows コンピューターの場合]をクリックし、プロファイルを選択します。
の Windows コンピュータのプロファイル開きます。
3. [一般設定] を選択します。
4. [すべてのセキュリティスキャンからフォルダやファイルを除外する] で、[除外を追加する] リンクを選択します。
5. の中に パス列に、除外するファイルまたはフォルダーへのパスを追加します。
指定されたパスにあるフォルダとファイルは、すべてのセキュリティスキャンと対策から除外され、WithSecureによって保護されません。これは、指定されたフォルダ内のサブフォルダにも適用されます。たとえば、`/Users/*/folder-to-exclude/*`すべてのユーザーの「除外フォルダ」にあるすべてのものを除外します。

   重要： これは、スキャンから絶対に除外する必要があるファイルまたはフォルダにのみ使用してください。たとえば、スキャンから「/*」を除外すると、システムボリューム全体と、その中のすべてのフォルダ、サブフォルダ、およびファイルがすべてのセキュリティ対策から除外されます。

4.1.6 アーカイブファイルのスキャン

圧縮されたアーカイブ ファイルをチェックするために手動スキャンを設定できます。

アーカイブスキャンは圧縮されたファイル内のファイルをスキャンできます`ZIP`、`7Z`、`JARARJ`、`LZH`、`TAR`、`TGZ`、`GZ`、`CAB`、`RAR`、`BZ2`、`R??`、 そして `0??`アーカイブ。

注: これはデフォルトのリストであり、将来変更される可能性があります。管理者は、Elements Endpoint Protection ポータルでリストを変更できます。

注: アーカイブスキャンでは、ファイルの内容を一時的にディスクに解凍する必要がある場合があります。一時ファイルに必要なスペースは、アーカイブ内のコンテンツによって異なります。[プロフィール]巨大なアーカイブをスキャンするときにディスク使用量を制限するために、一時ファイルの最大サイズを設定できます。

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. [Windowsコンピュータ用] または [Windowsサーバー用] タブを選択します。
3. 編集するプロファイルの名前を選択します。
4. 下[手動スキャン]、必ず[圧縮ファイル□ZIP、RARなど□内をスキャンします]オンになっています。
5. アーカイブのスキャン設定は、「含まれる拡張機能」の下にリストされます。設定を変更するには、次の手順を実行します。
   a) 下 [スキャンするファイル] ドロップダウンメニューから、[次の拡張子を持つファイル]。
   b) 下 [含まれる拡張機能]拡張機能リストを編集します。
   c) [保存して発行] を選択します。

4.1.7 プロファイルをエクスポートする

WithSecure Elementsポータルでは、プロファイルをJSONファイルとしてエクスポートすることができます。

プロファイルをエクスポートするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. エクスポートするプロファイルを開きます。
3. 右上隅で、 を選択してから、[ファイルをエクスポート] を選択します。
   エクスポートしたプロファイルを保存したり、JSON編集ツールで編集したりできます。

4.1.8 プロファイルをエクスポートする

WithSecure Elementsポータルでは、プロファイルを別のプロファイルにインポートすることができます。

注： 以前にエクスポートされたElements Endpoint Protectionプロファイルだけでなく、他のエクスポートされたファイルもインポートできます。たとえば、WithSecureポリシーマネージャからエクスポートされたプロファイルをインポートできます。

プロファイルをインポートするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. 以前にエクスポートしたプロファイルをインポートするプロファイルを開きます。
3. を選択してから [プロファイルをインポート] を選択します。
   プロファイルは、JSONファイルで選択したプロファイルにインポートされます。変更されたすべての設定が強調表示されます。
4. 変更点を見直して、次のいずれかを行います。
   - 変更を保存するために [保存して発行] を選択します。
   - 変更を拒否するには、[キャンセル] を選択します。

4.1.9 プロファイルを削除する

プロフィールを削除すると、WithSecure Elementsポータル。

削除したプロファイルは対象のデバイスからは削除されません。

プロファイルを削除するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. 選択する 削除するプロファイルの横にある をクリックします。
3. [プロファイルを削除] を選択し、[OK] を選択します。
   プロファイルがポータルから削除されます。

4.1.10 プロファイルを指定する

プロファイルを指定するには

1. [環境] のサイドバー から [デバイス] を選択します。
   「デバイス」画面が表示されます。
2. プロファイルを割り当てるデバイスを選択します。
3. ページの下で [プロファイルを指定する] を選択します。
4. ドロップダウン メニューで、使用するプロファイルを選択します。
5. [指定する] を選択します。

選択したプロファイルがデバイスに指定されます。

4.1.11 プロファイルの比較

プロファイルを選択して、あるプロファイルから別のプロファイルに値を比較したりコピーしたりできます。

プロファイルを比較するには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. [Windowsコンピュータ用] または [Windowsサーバー用] タブを選択します。
3. 選択する ••• 比較したいプロフィールの横にある [プロフィールを比較して編集する]。
4. 上の 比較するプロフィールを選択ページで比較するプロファイルを1つ以上選択し、[次]。
選択したプロファイルで異なる設定を示す表を含むページが開きます。違いは太字で表示されます。

   注: 一度に表示されるプロファイルは 2 つだけです。 複数のプロファイルを選択した場合は、ページ上部のドロップダウン メニューから、比較するプロファイルを選択できます。
5. あるプロファイルから別のプロファイルに値をコピーするには、右矢印と左矢印を使用します。

4.1.12 エンドユーザによるコンピュータプロファイル設定の変更をブロックする

ユーザーが変更できないように、各設定を個別にロックまたはロック解除するか、すべての設定を同時にロックまたはロック解除するかを選択できます。

注: プロファイルの横に黒い鍵がある場合、プロファイルは「読み取り専用」です。つまり、エンドユーザが変更する設定を変更することはできません。

プロファイルの設定をロックするには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. ロックまたはロック解除するカスタムプロファイルを選択します。
[プロファイル] ページが開きます。
3. 右上隅の ••• を選択してから、次のいずれかのオプションを選択します。

[すべての設定をロックする]	鍵のアイコンがある設定をすべてロックします。この操作により、ユーザはこれらの設定を変更できなくなります。
[すべての設定のロックを解除する]	鍵のアイコンがある設定のロックをすべて解除します。この操作により、ユーザは該当する設定を変更できるようになります。

4.1.13 データのエクスポート、インポート、および置換

選択したプロファイルのテーブルからデータをエクスポートし、同じテーブルまたは別のプロファイルの同様のテーブルに置き換えたりインポートしたりすることができます。WithSecure Elements EPP ポータル。

これらのオプションを使用すると、テーブルをカスタマイズし、データをエクスポートし、エクスポートしたファイルのデータをテキストエディタで編集して、同じプロファイルまたは別のプロファイルにアップロードできます。

注: エクスポートしたデータを同様のテーブルにのみインポートすることができます。特定のプロファイルのアプリケーション制御の除外ルールテーブルからデータをエクスポートした場合、

別のアプリケーション制御の除外規則テーブル同じプロファイルまたは別のプロファイルにあるもの にのみデータをインポートできます。たとえば、ディープガード保護のルールテーブルにはインポートできません。

テーブルからのデータをエクスポートする

テーブルからJSONファイルにデータをエクスポートする方法を説明します。

テーブルからデータをエクスポートするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. 目的のプロファイルを選択します。
3. 上の プロフィールページで、関連する設定を選択し、設定がオンになっていることを確認します。
たとえば、除外ルールテーブルからデータをエクスポートするには、[アプリケーション制御] > [除外事項]。除外ルールテーブルが開きます。
4. テーブルの右上隅で、 ••• を選択してから、[ファイルをエクスポート JSON)] を選択します。

   注: •••アイコンが表示されない場合は、関連する設定がオンになっていることを確認してください。
5. エクスポートしたJSONファイルを保存します。

   注: エクスポートしたファイルをテキストエディタで編集してから、同じプロファイルまたは別のプロファイルにインポートすることができます。
6. [完了] を選択します。

データをインポートする

選択したプロファイルのテーブルにデータをインポートする方法を説明します。

使用すると [ファイルからインポート (JSON)]オプションを選択すると、テーブル内の既存のエントリは更新または削除されず、新しいエントリのみが追加されます。

注: エクスポートしたデータを同様のテーブルにのみインポートすることができます。たとえば、選択したプロファイルのアプリケーション制御の除外ルールテーブルからデータをエクスポートした場合、別のアプリケーション制御の除外規則テーブル同じプロファイルまたは別のプロファイルにあるもの にのみデータをインポートできます。たとえば、ディープガード保護のルールテーブルにはインポートできません。

データをインポートするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. 目的のプロファイルを選択します。
3. 上の プロフィールページで、関連する設定を選択し、設定がオンになっていることを確認します。
たとえば、除外ルールテーブルにデータをインポートするには、[アプリケーション制御] > [除外事項]。除外ルールテーブルが開きます。
4. テーブルの右上隅で、 ••• を選択してから、[ファイルからインポート JSON)] を選択します。

   注: •••アイコンが表示されない場合は、関連する設定がオンになっていることを確認してください。
5. エクスポートされたJSONファイルに移動してインポートします。

   注: JSONファイルからデータをインポートすると、一意でない値がインポートされなかったり、部分的にしかインポートされないことがあります。後者の場合、アプリケーションは、

インポートされなかった値を補完する必要があります。このような場合は、**ファイルから置換JSON**オプションを使用することを推奨します。

6. [**保存して発行**] を選択します。
   変更が保存され、現在のプロファイルに公開されます。

テーブルのデータを置き換える

テーブル内のデータを置き換える方法について説明します。

[**ファイルから置換JSON**] 選択すると、テーブル内の既存の値がすべて削除され、JSONファイル内の値に置き換えられます。

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. 目的のプロファイルを選択します。
3. 上の **プロフィール**ページで、関連する設定を選択し、設定がオンになっていることを確認します。
   たとえば、除外ルールテーブルのデータを置き換えるには、**[アプリケーション制御]** > **[除外事項]**。**除外ルール**テーブルが開きます。
4. テーブルの右上隅で、 ••• を選択してから、[**ファイルから置換JSON)**] を選択します。

   注: •••アイコンが表示されない場合は、関連する設定がオンになっていることを確認してください。

5. エクスポートされたJSONファイルに移動し、テーブルのデータを置き換えます。
   テーブルのすべての値が削除され、インポートされたJSONファイルのデータに置き換えられます。
6. [**保存して発行**] を選択します。
   変更が保存され、現在のプロファイルに公開されます。

4.1.14 WindowsコンピュータプロファイルでWithSecure Elements Connectorを使用する

WithSecure Elements Connectorは、WithSecure Elements EPP for Computersクライアントにアップデートをダウンロードする際に帯域幅の使用を最小限に抑えます。

このプロキシは、GUTS2アップデート (マルウェア署名データベース) をキャッシュします。Elements Connectorが利用できない場合、WithSecure Elements EPP for Computersクライアントは自動的にGUTS2 に直接アクセスするようにフォールバックします。

WithSecure Elements Connectorを構成し、WithSecure Elements EPP for Computersプロファイルで使用するには

1. WithSecure Elements Connectorの最新版をダウンロードおよびインストールします。
   - Windowsの場合は、 ここのの指示に従ってください。
   - Linux:
     a. こちらのの指示に従ってください。

        注: WithSecure Elements Connectorをインストールする前に次のコマンドでlibstdc++パッケージをインストールします。

        - `yum install libstdc++.i686`
        - `yum install libstdc++.x86_64`

     b. プロキシを設定します。
        1. 次のコマンドを使用します: `/opt/f-secure/fspms/bin/fspms-config`
        2. 確認されたら、サーバのアドレスに 0.0.0.0 を指定します
        3. WithSecure Elements Connectorを手動で管理するには `/etc/init.d/fspms {start|stop|restart|status}` を入力します。

c. WithSecure Elements Connectorログでクライアントのアップデートを確認します。`/var/opt/f-secure/fspms/logs`

ログの解説

ログ	説明
`request.log`	クライアントから受信した要求を応答ステータスとともに一覧表示します。たとえば、503ステータスは、アップデートがGUTS2からまだダウンロードされていなく、後でもう一度やり直すこと促していることを意味しています。
`fspms-serve-updates.log`	このログには、クライアントからの質問がリストされます。一部のアップデートが適用されてなく、クライアント側から 503 ステータスで要求が受信された場合、その理由がこのログに書き込まれます。
`fspms-download-updates.log`	GUTS2 からのダウンロードを一覧表示します。

2. WithSecure Elements Connectorを使用するために、Windowsコンピュータのプロファイルを設定します。
   a) [**セキュリティ構成**] で、**プロファイル** > **Windows用**を選択します。
   b) 編集するプロファイルを選択します。
   c) [**一般設定**] でプロキシ設定を見つけます。

      この設定は、手順1で設定したローカル サーバアドレスを表します。このプロファイルがコンピュータに割り当てられると、クライアントでも確認できるようになります。

   d) クライアントを開き、**ツール** > **アップデートを確認** > **詳細を表示**の順に選択します。
   e) [**更新を確認する**] ウィンドウが開いたら、[**詳細を表示**] リンクをクリックします。
   f) **共通の設定** > **アップデート**を開き、[アップデート サーバ] フィールド (WithSecure Elements Connectorの⊠アドレス値) でアドレスを確認して、[**今すぐ更新**] をクリックします。

   エラーなしでチェックが実行されます。

   注： WithSecure Elements Connectorは、デフォルトでポート80を使用します。ポートがWindows ファイアウォールによってブロックされていないことを確認してください。

4.1.15 ディープガードを設定する

ディープガードは、動作ベースの保護とアクセス制御保護の両方を備えた追加のセキュリティ層を提供します。

異常な動作や危険性のあるシステム変更を検出するために実行中のアプリケーションを監視します。

注: ディープガードは、たとえば、ランサムウェアに対する重大な保護を提供するため、有効にしておくことを強く推奨します。

ディープガードが有効になっていると、以下のセキュリティ機能が有効になります。

- エクスプロイト保護
- ランサムウェア保護
- ヒューリスティック分析
- 動作監視

ディープガードを設定するには

1. ディープガードを有効にするには

a) [セキュリティ構成] で、[プロファイル] を選択します。
「プロファイル」ページが開きます。
b) 使用するプロファイルを選択します。
c) [リアルタイム スキャン] を開きます。

注： リアルタイム スキャンが有効であることを確認します。

d) [ディープガード] を有効にします。

2. ディープガード スキャンからアプリケーションを除外するルールを追加できます。

注: ディープガードはランサムウェアなどに対する重大なセキュリティ保護を提供するため、絶対に必要な場合にのみアプリケーションを除外することを推奨します。

注： アプリケーションを除外すると、そのアプリケーションがアクセスするファイルも無視されます。

a) [ディープガード保護ルール] の [有効] 列で、ルールをオンにします。
b) [アプリケーション SHA-1] 列で、SHA-1 ハッシュを使用してアプリケーションを識別します。SHA-1 計算機を使用して40文字の SHA-1 ハッシュを生成できます。
コマンドプロンプトで次のコマンドを入力して、SHA-1ハッシュも生成できます。

```
certutil -hashfile "filename.exe" SHA1
```

注: アプリケーションをアップグレードすると、新しいハッシュを計算する必要があります。

c) [備考] 列でアプリケーションの名前やその他の識別情報を保存できます。このフィールドはエンドユーザに表示されません。
d) [信頼] 列で、ディープガードによるアプリケーションの処理方法を選択します。有効にすると、ディープガードはアプリケーションに対するすべての操作を許可します。無効にすると、ディープガードは常にアプリケーションの実行を阻止します。

3. [完了] を選択します。

4.1.16 デバイス制御を使用する

デバイス制御は、セキュリティ保護のために特定のハードウェア デバイスをブロックします。

デバイス制御は、USBストレージ、DVD/CD-ROM ドライブなど、外部ネットワークからマルウェアがネットワークに広がることを阻止します。ブロックされているデバイスがクライアントコンピュータに接続すると、デバイス制御はデバイスへのアクセスを防ぐためにデバイスをオフにすることができます。

デバイス制御の設定

ユーザが USB デバイス (Web カメラやハードディスクなど) にアクセスする方法や、取り外し可能な大容量記憶装置にインストーラを実行できるかの制限を設定できます。

デバイス制御を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. プロファイルを選択します。
3. 左のメニューから [デバイス制御] を選択します。
4. [デバイス制御] を有効にします。

注： デバイス制御が有効の場合、コンピューターに接続されているすべてのデバイスが、デバイスページの [Connected devices] に表示されます。

5. 「リムーバブル大容量記憶装置」では、次のいずれかのオプションを有効にできます。

- 書き込みアクセスを許可する - このオプションがオフの場合、ユーザはファイルをリムーバブル大容量記憶装置にコピーできません。リムーバブルマスストレージデバイスは、データの読み取りのみが可能です。
- 実行可能ファイルの実行を許可する - このオプションがオフの場合、リムーバブルマスストレージデバイスからのファイルの実行は禁止されます。

マスクを使用してデバイスを除外する

デバイスアクセスルールを適用したくないデバイスを除外することができます。

たとえば、すべてのUSBデバイスを除外したい場合は、デバイスIDをすべて入力するのではなく、"USB*"というマスクを使用してデバイスを絞り込むことができます。

マスクを使用してデバイスを除外するには

1. デバイスIDを検索するには、[**環境**] で、[**デバイス**] を選択します。
「**デバイス**」ページが開きます。
2. 目的のデバイスを選択します。
デバイスの詳細ページが開きます。
3. [**接続されたデバイスデバイス**] タブを選択します。
4. [**デバイスIDでフィルタリングする**] フィールドに、「USB*」などのマスクを入力します。
このページには、デバイスIDが「USB」で始まるすべてのデバイスが表示されます。
5. リストに除外するすべてのデバイスが含まれていることを確認します
6. [**プロファイル**] で、プロファイルを選択してから、[**デバイス制御**] を選択します。
7. [**デバイスフィルタリングルール**] の [ルール] テーブルで、[**ルールを追加**] を選択します。
空の行が表示されます。
8. マスクを使用して新しいルールを追加します⊠例⊠*USB\"⊠。
9. [**保存して発行**] を選択します。

ルールテーブルにある「USB*」で始まるIDを持つすべてのデバイスは、接続されているデバイスのリストから除外されます。

ハードウェア デバイスをブロックする

プリセットのルールを使用してデバイスをブロックすることができます。

デフォルトでは、ルールはデバイスをブロックしません。デバイスをブロックするには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
「**プロファイル**」ページが開きます。
2. プロファイルを選択します。
3. 左のメニューから [**デバイス制御**] を選択します。
4. 「**デバイスのアクセスルール**」では、ルールを追加または削除して、デバイスを制御したり、デバイスへのアクセスを許可またはブロックしたりできます。次の方法でルールを追加できます。
   a) [**ルールを追加**] を選択します。
   b) デバイス名とハードウェア ID を入力します。
   c) デバイスへのアクセスを許可またはブロックするか選択します。
   [**アクセス レベル**] が [**ブロック**] に設定されているデバイスに該当するルールが有効な場合、デバイスにアクセスすることはできません。
   d) [**発行**] を選択して新しいルールを発行します。

デバイスのハードウェア ID を見つける

ブロック ルールでハードウェア ID を使用できます。

Windows デバイス マネージャを使用してハードウェア ID を確認するには

1. クライアント コンピュータで Windows **デバイス マネージャ**を開きます。
2. 一覧から正しいデバイスを見つけます。

ヒント : デバイスタイプを展開して、すべてのデバイスを表示します。

3. デバイスを右クリックして [**プロパティ**] を選択します。
4. [**詳細設定**] タブを開きます。
5. ドロップダウン メニューから次の ID を選択し、その値をメモします。
   - ハードウェア ID
   - 互換性 ID
   - デバイス クラス GUID
   - 親ID

注 : 外部ストレージデバイスの場合、これはデバイスの固有のシリアル番号を含む唯一のIDです。

注 : アイテムを右クリックすると、コンテキスト メニューが開き、ID がコピーされます。

4.1.17 ファイルウォールの構成

Windowsファイアウォールが有効の場合、対象のユーザとネットワーク ルールがデバイスに適用されます。

WithSecureのファイアウォール プロファイルは、Windowsファイアウォールのユーザ ルールおよびその他のドメイン ルールの上に追加のセキュリティ レイヤーを提供します。Windows ファイアウォールが無効の場合、WithSecure ファイアウォールのプロファイルまたはルールは適用されないため、ファイアウォールを常に有効にすることを推奨します。

注 : ドメイン ルールはこれらのルールを上書きする可能性があります。

注 : GPO またはサードパーティのファイアウォールを使用する場合、ほとんどの場合、競合を避けるために、WithSecureファイアウォール プロファイル(**WithSecureファイアウォール プロファイルの適用**設定)を無効にする必要があります。「Windowsファイアウォールを使用する」は、GPO またはサードパーティのファイアウォールに設定された固有の設定と一致する必要があります。

重要 : [**他のルールを許可する**] を有効にすると、WithSecure が作成していないファイアウォールルールも許可できます。このオプションを無効にすると、現在のプロファイルにはWithSecure ファイアウォール ルールのみ適用されます。このオプションを有効にしておくことを強く推奨します。

サイトごとに異なるファイアウォール プロファイルを使用するオプションがあります。カスタマイズ可能なルールを使用して、オフィスネットワークと外部ネットワークの間でファイアウォールプロファイルを変更できます。これを行うには、[**WithSecureファイアウォール プロファイル**] に移動し、ドロップダウン メニューから [**自動選択**] を選択して、ルールを追加します。これらのルールは、構成に基づいてファイアウォール プロファイルを自動的に選択するために使用されます。

ルールを追加する

ルルールを追加するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. プロファイルを選択します。
3. 左側のペインから [**ファイアウォール**] を選択します。
   「**ファイアウォール**」ページが開きます。
4. 編集するプロファイルまたは新しいルールを追加するプロファイルを選択します。
   「ファイアウォールルール」テーブルには、選択したファイアウォール プロファイルに対して作成されたルールが表示されます。

注： ルールの順序は影響ありませんが、ブロック ルールは許可ルールをオーバーライド (より優先される)します。

5. 次のいずれかを実行します。
   - 新しいルールを追加するには、テーブルの上部にある [**ルールを追加**] を選択します。
   - 既存のルールを編集するには、編集する行を選択します。

     注： ルールを削除するのではなく、不要と思われるルールを無効にすることを推奨します。

6. 次のフィールドにルールの値を入力するか、既存の値を編集します。
   - 新しいルールに名前と説明を指定します。

     [処理] と [方向] 列で、着信/発信トラフィックを許可またはブロックするか選択します。

     「属性」列で、次の操作を行います。
     - [プロトコル] を選択します。
     - ローカルとリモートのIPアドレスを入力します。

       注： 特定の IP アドレスまたは範囲を許可しない場合、これらの設定を空白のままにしてください。
     - ローカル ポート番号を入力すると、トラフィック (データ通信) が指定したポートを通過できることを許可します
     - リモート ポート番号を入力すると、指定したポートからのトラフィック⊠データ通信⊠を許可します。
     - サービスの名前を入力します。
     - アプリケーションのパスを入力します。
     - インターフェースのタイプを選択します。

       注： 複数のポート番号⊠カンマで区切る⊠またはポートの範囲⊠例⊠0⊠65535⊠を追加することができます。

注： 自動プロファイル選択ルールについては、[**ネットワークの場所の設定**] にアクセスしてください。たとえば、ノートパソコンをオフィスのネットワーク範囲外に持ち出す必要がある場合は、1つ以上のルールを追加して特定のファイアウォールプロファイルを割り当てることができます。

ネットワーク隔離プロファイルにファイアウォール ルールを追加する

コンピュータをネットワークから隔離すると、コンピュータがインターネットに接続するのを防ぐために、厳密なファイアウォール ルールセットが適用されます。

注： 隔離されたコンピュータは、ファイアウォール プロファイルを含むデバイス プロファイルを保持します。隔離ルールは適用されますが、プロファイル エディタには表示されません。

デフォルトでは、ファイアウォールプロファイルはすべてのネットワーク接続をオフにし、WithSecure のプロセスのみを許可します。また、選択したデバイスの他のすべてのファイアウォール ルールをオフにし、許可されていないすべての DNS アドレスの DNS 解決をブロックして、DNS クエリによる情報漏洩を防ぎます。隔離されたデバイスにはインターネットの接続がないため、外部からアクセスしたり、インターネットの検索に使用したりすることはできません。

管理者が追加のアクセスを提供する必要がある場合、デバイスが使用するファイアウォール プロファイルに追加のルールを追加できます。たとえば、サポート エンジニアがデバイスにアクセスして問題を調査できるように、デバイスへのリモートアクセスを許可できます。

注: デフォルトではすべてがすでにブロックされているため、追加のルールは通常「許可する」ルールになります。

注: 隔離ルールは、コンピュータが隔離されると、現在のファイアウォールプロファイルのファイアウォールルールを置き換えます。ネットワーク隔離が削除されると、以前のファイアウォール プロファイルが適用されます。

[ファイアウォールルール]テーブルの下にある[許可しているドメイン]フィールドでは、隔離されたデバイスの接続を許可するドメインを指定できます。

注： [許可しているドメイン] フィールドのドメインのみが DNS によって解決されます。

WithSecure Elements Endpoint Protectionのプロファイル設定でファイアウォールがオフになっていても、ネットワークの隔離機能は機能します。ネットワークの隔離モードは、ファイアウォールとネットワーク隔離プロファイルを強制的にオンにします。ただし、デバイスのGPO設定によりファイアウォールが強制的にオフになっている場合、ネットワーク隔離モードではファイアウォールはオンになりません。

不明な接続を許可する

不明なインバウンド (受信) およびアウトバウンド (送信) 接続を許可する方法について説明します。

デフォルトでは、[不明な受信接続を許可する] と [不明な送信接続を許可する] の設定は無効です。無効の場合、ファイアウォールは不明なトラフィック (データ通信) をブロックします。自動的に選択されたプロファイルを使用するか、プリセットの WithSecure ファイアウォール プロファイルを選択するか、必要に応じてプロファイルをカスタマイズできます。トラフィックをブロックまたは許可するルールが存在しない場合、デフォルトのルールが使用されるため、WithSecure ファイアウォールの一般設定が適用され、その後にファイアウォール ルール テーブルのルールが適用されます。他のルールが一致しない場合、フォールバック設定が適用されます。

注： フォールバック設定はプロファイルごとに設定されます。

たとえば、[不明な接続を許可する]を有効にして、すべてのファイアウォールルールを削除すると、すべてが許可されます。[不明な接続を許可する] を無効にすると、すべてがブロックされます。ファイアウォール ルールがない場合、すべてのトラフィックが不明になり、ブロックされます。特定のトラフィックを許可するルールを追加することができます。別の方法として、[不明な接続を許可する]を有効にすると、すべてを許可し、ブロックルールのセットを作成することで特定のトラフィックをブロックし、他のすべてを許可することができます。

不明な接続を許可する

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. プロファイルを選択します。
3. 左側のペインから [ファイアウォール] を選択します。
   「ファイアウォール」ページが開きます。
4. 編集するプロファイルを選択します。
5. 「フォールバック設定」で、次を設定します。
   - 不明な受信接続を許可する - 有効にすると、コンピュータに対する不明な受信接続が許可されます。無効にしておくことを推奨します。
   - 不明な送信接続を許可する-有効にすると、コンピュータからの不明な送信接続が許可されます。無効にしておくことを推奨します。
6. 現在のプロファイル ([保存して発行]) または複数のプロファイル ([複数のプロファイルに保存して公開]) の変更を保存して発行することができます。

4.1.18 自動タスクのスケジューリング

自動タスクでは、特定の時間にデバイス上で自動的に実行されるタスクをスケジュールすることができます。

ポータルのプロファイルエディターで自動化されたタスクを設定できます。選択したプロファイルを使用して、たとえば、次のようにスケジュールできます。

- マルウェアのクイック スキャンを実行する
- マルウェアのスケジュールスキャン
- フォルダ内のマルウェアをスキャンする
- 製品の更新を許可する

- 適用されていないソフトウェアアップデートをスキャンする
- クライアントアプリケーションをアップグレードする
- 適用されていないすべてのソフトウェアアップデートをインストールする
- すべてのセキュリティアップデートをインストールする
- 重大なセキュリティアップデートをインストールする
- 重大および重要なセキュリティアップデートをインストールする
- シャットダウンを強制する
- 必要に応じて強制的にシャットダウンする
- 再起動を強制する
- 必要に応じて、再起動を強制する
- 休止状態を強制する
- ワークステーションをロックする

自動タスクのスケジューリングでは、@daily、@midnight、@monthly、@away、@lockなどのマクロを使用できます。@awayを使用すると、ユーザが一定時間⊠分⊠不在のときに実行するタスクをスケジュールできます。例えば、[クイックマルウェアスキャン] または [ワークステーションのロック] を選択し、[@away 30] を選択すると、ユーザーが30分間不在のときにクイックマルウェアスキャンを実行するかワークステーションがロックされます。同様に、[ワークステーションのロック] タスクと [@daily <hours>] を選択すると、毎日特定の時間にワークステーションを自動的にロックするようスケジュールすることができます。@lockを使用すると、コンピュータがロックされると同時にタスクが実行されるようにスケジュールすることができます。

CRON式を使用することもできます。

注 : CRON式の詳細と例については、WithSecure Elements Endpoint Protectionポータルを参照してください。

注 : デバイスがインフラに負荷をかけないように、タスクの開始時刻は1時間の精度でランダム化されています。

注 : 自動タスクテーブルの [**スキップしない**] 列のスイッチをオンにすると、スケジュールされた時間に実行できなくても、タスクはできるだけ早く実行されます。それ以外の場合、タスクはスキップされます。

以下に、自動化されたタスクを設定する方法の例をいくつか示します。

スケジュール スキャン

定期的にウイルスやその他の有害なアプリケーションをスキャンするように製品を設定します。

スケジュール スキャンを設定するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. 目的のプロファイルを選択します。
3. [**自動タスク**] を選択します。
4. 自動化されたタスクがオンになっていることを確認してください。
5. [**タスクを追加**] を選択します。
6. [タイプ] 列で、[**マルウェアのスケジュールスキャン**] を選択します。
7. [スケジュール] 列で、スケジュール スキャンを実行する頻度を選択します。
8. [説明] ボックスに、選択したスキャンの説明を入力できます。
9. [利用可能] 列で、スイッチがオンになっていることを確認します。
10. [**保存して発行**] を選択します。
    変更が保存され、現在のプロファイルに公開されます。

特定のタイミングで製品を更新するためのタスクを設定する

たとえば、毎週土曜日の12:00に製品を更新する自動タスクを作成します。

注: このタスクでは、製品がアップデートされるタイミングを制御することができます。たとえば、メンテナンスのある週末にスケジュールを組んで、他の時間に更新されないようにすることができます。

特定のタイミングで製品を更新するためのタスクを設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [プロファイル] ページで、自動タスクを作成するプロファイルを選択します。
3. [自動タスク] を開き、オンになっていることを確認します。
4. [自動タスク] テーブルの上にある [タスクの追加] を選択し、次の操作を行います。
   a) [タイプ] ドロップダウン メニューから、[WithSecure Elements Agentのアップデートを許可する] を選択します。
   b) [スケジュール] フィールドに、次のCRON式を入力します。`* * 12 ? * 6`

      注 : CRON式の使用方法の詳細については、WithSecure Elementsポータルの関連ヘルプセクションを参照してください。

製品が毎週土曜日の12:00から13:00の間に新しいアップデートを確認します。

注 : 1時間は、こような自動タスクの一定期間で、製品が新しいアップデートを確認し、アップデートパッケージが利用可能な場合にアップグレードを実行するのに十分な時間を保証します。

適用されていない重大なおよびその他のセキュリティ アップデートをインストールするためのタスクの設定

適用されていない重要なセキュリティ アップデートやその他のセキュリティ アップデートを特定の時間にインストールするための自動タスクを作成します。

適用されていない重要なセキュリティ アップデート プログラム（たとえば、「毎日」）およびその他のセキュリティ アップデート プログラム（たとえば、「週1回」）をインストールするには、プロファイル エディターで2つの自動タスクを作成する必要があります。

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [プロファイル] ページで、自動タスクを作成するプロファイルを選択します。
3. [自動タスク] を開き、オンになっていることを確認します。
4. 重要なセキュリティアップデートを毎日インストールするタスクを作成するには、[自動タスク]テーブルの上にある [タスクの追加] を選択し、次の手順を実行します。
   a) [タイプ] ドロップ ダウン メニューから、[重大なセキュリティ アップデートをインストール] を選択します。
   b) [スケジュール] ドロップダウン メニューから、[@daily] を選択します。

      注 : [説明] フィールドで、新しいタスクの説明を追加できます（オプション）。
5. セキュリティ アップデートを週に一度インストールする タスクを作成するには、[タスクの追加] を選択し、次の手順を実行します。
   a) [タイプ] ドロップ ダウン メニューから、[すべてのセキュリティ アップデートをインストール] を選択します。
   b) [スケジュール] ドロップダウン メニューから、[@weekly] を選択します。

この2つの自動タスクを作成すると、本製品は毎日ランダムな時間に重要なセキュリティ アップデートをインストールし、特定の日にはランダムな時間にその他のセキュリティ アップデートをインストールします。

注： ネットワークの負荷を軽減するために、ランダム化を利用しています。

適用されていないセキュリティ アップデートをスキャンするためのタスクの設定

毎日更新されるセキュリティの欠落をスキャンするための自動タスクを作成します。

注： 欠落しているアップデートをスキャンするタスクを作成する場合は、[ソフトウェアアップデーター] ページで [**欠落しているアップデートを自動的にスキャンする**] をオフにできます。

注: 不足しているソフトウェアアップデートをインストールするタスクは、不足しているアップデートもスキャンします。アップデートを毎日インストールする場合、スキャンのための別のタスクは必要ありません。

適用されていないセキュリティ アップデートをスキャンするための自動タスクを作成するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. [プロファイル] ページで、自動タスクを作成するプロファイルを選択します。
3. [**自動タスク**] を開き、オンになっていることを確認します。
4. [自動タスク] テーブルの上にある [**タスクの追加**] を選択し、次の操作を行います。
   a) [タイプ] ドロップダウン メニューから [**適用されていないアップデートをスキャンする**] を選択します。
   b) [スケジュール] ドロップダウン メニューから、[**@daily**] を選択します。

本製品が毎日ランダムな時間に、適用されていないセキュリティ アップデートをスキャンします。

注： タスクの実行がスケジュールされているときにデバイスがオフになっている場合、[利用可能なときに開始] オプションをオンにしていると、デバイスが再びオンになるときにタスクは自動的に実行されます。

マルウェアをスキャンするタスクの設定

マルウェアを毎月スキャンする自動タスクを作成します。

マルウェアをスキャンする自動タスクを作成するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. [プロファイル] ページで、自動タスクを作成するプロファイルを選択します。
3. [**自動タスク**] を開き、オンになっていることを確認します。
4. [自動タスク] テーブルの上にある [**タスクの追加**] を選択し、次の操作を行います。
   a) [タイプ] ドロップダウン メニューから [**マルウェアをスキャンする**] を選択します。
   b) [スケジュール] ドロップダウン メニューから、[**@monthly**] を選択します。

この製品は毎月ランダムな時間にマルウェアをスキャンします。

4.1.19 ネットワークの場所を設定する

ネットワークロケーションを使用すると、選択したネットワークロケーションでデバイスがネットワークに接続されているときの設定を制御できます。

たとえば、デバイスが自宅にいるときはソフトウェアアップデーターとファイアウォールをオンにし、オフィスにいるときはソフトウェアアップデーターとファイアウォールを両方ともオフにするように、ネットワークの場所とルールを設定することができます。この設定には、2つの場所を追加し、4つのルールを作成する必要があります。

ネットワークの場所とルールを設定するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. ネットワークの場所を設定するプロファイルを選択し、ルールを作成します。

3. [ネットワーク場所の設定] を選択し、オンになっていることを確認します。
4. [ロケーションとルール] で [ロケーションを追加] を選択し、次のように操作します。
   a) [名前] 列に、場所のわかりやすい名前⊠例⊠ 自宅⊠を入力します。
   b) [トリガー] 列の [タイプ] ドロップダウンメニューから、[マイネットワーク] を選択します。
   c) [値] フィールドに、ネットワークマスク⊠例⊠`10.0.0.0/24`⊠を入力します。

      注: 場所には複数のトリガーを含めることができますが、少なくとも1つは必要です。

   d) [トリガーを追加] を選択します。
   e) [タイプ] ドロップダウンメニューから [DHCPサーバーのIPアドレス] を選択します。
   f) [値] フィールドに、デフォルトのDHCPサーバを入力します。

   両方のトリガーがアクティブになると、新しい場所がアクティブになります。
5. 別のロケーションを追加するには、[場所を追加] を選択し、次のように操作します。
   a) [名前] 列に、場所のわかりやすい名前⊠例⊠ 職場⊠を入力します。
   b) [トリガー] 列 の[タイプ] ドロップダウンメニューから、[デフォルトのIPアドレス] を選択します。。
   c) [値] フィールドに、デフォルトのゲートウェイIPアドレスを入力します。

      注: 場所の優先度を上げたり下げたりすることができます。優先度の高い場所は、優先度の低い場所よりも先に処理されます。たとえば、ネットワークの場所「自宅」を「常に」に設定し、別の場所「オフィス」を「デフォルトのゲートウェイIPアドレス」に設定している場合、「自宅」の場所の優先度を低くすることが重要です。それ以外の場合、デバイスの場所「自宅」は常に「オフィス」の場所よりも優先されます。

6. ルールを作成するには、ルールテーブルの上にある [ルールを追加] を選択し、次の手順を実行します。
   a) [場所] 列のドロップダウンメニューから、ルールが適用される場所⊠この例では [自宅]⊠を選択します。
   b) [設定] 列のドロップダウンメニューから、ルールによってオンまたはオフにされる製品機能⊠この例ではソフトウェアアップデーター⊠の1つ選択します。
   c) [値] 列で、スイッチが [オン] になっていることを確認します。
7. 別のルールを作成するには、[ルールを追加] を選択し、次の手順を実行します。
   a) [場所] 列のドロップダウンメニューから、[自宅で] を選択します。
   b) [場所] 列のドロップダウンメニューから、[ファイアウォール] を選択します。
   c) [値] 列で、スイッチが [オン] になっていることを確認します。
8. 最後の2つの手順を繰り返して、「オフィス」の場所にさらに2つのルールを作成します。
   a) 最初のルールで、[値] 列で [ソフトウェアアップデーター] を選択して、スイッチを [オフ] にします。
   b) 2つ目のルールで、[値] 列で [ファイアウォール] を選択して、スイッチを [オフ] にします。

      注: ルールを適用するには、場所がアクティブである必要があります。

4.1.20 ライセンスの有効期限通知を設定する

ライセンスの有効期限に関する通知を設定できます。

通知を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [Windowsコンピュータ用] または [Windowsサーバー用] タブを選択します。
   「プロファイル」ページが開きます。
3. 編集するプロファイルを選択します。
4. [一般設定] で、[ライセンスの有効期限] に移動します。
5. [通知を表示] で、通知をオンにします。

この設定がオンの場合、ユーザには、ライセンスの期限切れまたは期限切れに関する通知が表示されます。

6. [ライセンス満了の数日前] で、ライセンスの有効期限が切れる何日前に通知を表示するかを入力します。

   注： 負の値を入力すると、ライセンスの有効期限が切れた後に通知が表示されます。

7. [ライセンスの有効期限に関するカスタマイズされたメッセージ] フィールドには、ライセンスの有効期限が切れる前にユーザに表示するメッセージを入力できます。

   注： メッセージが通知領域に正しく表示されるようにするには、メッセージをできるだけ短くする必要があります。

4.1.21 改ざん防止を設定する

WithSecureインストーラとプロセスを保護するために、改ざん防止を設定することができます。

改ざん護は、エンドユーザやサードパーティの変更、およびF-Secureサービス、プロセス、ファイル、およびレジストリエントリを制御しようとする試みから WithSecureインストーラを保護します。

改ざん防止を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [Windows 用のコンピュータ保護] または [サーバー保護] タブを選択します。
   「プロファイル」ページが開きます。
3. 編集するプロファイルを選択します。
4. [一般設定の] で、[改ざん防止] にスクロールします。
5. [リソース保護] をオンにします。

   重要： このオプションをオンにしておくことを強くお勧めします。

4.1.22 Server Protection

Server Share Protectionは、WithSecure Elements EPP for Serversサブスクリプションに付属するセキュリティ機能です。

Server Share Protectionは、リモートクライアント上で実行されるランサムウェアから共有ファイルを保護するのに役立ちます。悪意のあるファイルやプロセスがホスト上にない場合でも、ランサムウェアを識別します。共有ファイルやフォルダを操作しているユーザーセッションで行われるアクションを監視します。監視しながら、変更されたファイルをすべてバックアップします。Server Share Protectionは、ランサムウェアがユーザーになりすましてファイルを暗号化するケースを特定できます。ランサムウェアを検出すると、定義された時間（デフォルトでは30分）、ユーザーのさらなる変更をブロックし、すでに行われたすべての変更を元に戻し、ファイルシステムを元の状態に復元します。

注： ユーザーがファイルに変更を加えてもランサムウェアが検出されない場合、Server Share Protectionは変更を元に戻しません。

共有フォルダーとユーザーを除外できます。 Server Share Protectionは、除外されたフォルダとユーザーを監視しません。現在ブロックされているユーザーを除外した場合、そのユーザーは再び共有ファイルへのアクセスを許されます。

許可と報告モードをオンにする

許可と報告モードでは、Server Share Protectionランサムウェア攻撃を監視および識別します。

注： ただし、何かをブロックしたり、変更を元に戻したりすることはありません。

検出される可能性のある項目とその詳細は以下で確認できます。[イベント]>[セキュリティイベント]。

初めてテストを受ける際は、このモードをオンにしてテストすることをお勧めします。Server Share Protection機能を有効にしてください。モードをオンにしても保護されるわけではありませんが、オンにすると、たとえば、検出の観点からランサムウェアのように動作する有効なスクリプトがある場合などに、誤検知を識別するために使用できます。

注: このモードがオンの場合、暗号化されたファイルは復元されません。

許可と報告モードをオンにするには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。「プロファイル」ページが開きます。
2. を選択 [Windows サーバーの場合]タブをクリックし、編集するプロファイルを選択します。Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護]。
4. オンにします [許可と報告モード]設定。
5. [保存して発行] を選択します。

ユーザーが共有ファイルやフォルダに一時的にアクセスできないようにする

この設定がオンの場合、Server Share Protectionランサムウェアを検出した場合、ユーザーが共有ファイルやフォルダにアクセスできないようにする期間 (分単位) を定義できます。

ユーザーをブロックする期間を定義するには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。「プロファイル」ページが開きます。
2. を選択 [Windows サーバーの場合]タブをクリックし、編集するプロファイルを選択します。Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護]。
4. の中に [ユーザーアクセスをブロックする分]フィールドに時間を入力します。

   注: デフォルトの時間は 30 分です。
5. [保存して発行] を選択します。

共有フォルダを除外する

共有フォルダーを監視対象から除外する方法を説明します。

Server Share Protection は共有フォルダーを監視し、ランサムウェアによってネットワーク経由で変更されたファイルを復元できるようにします。監視したくない共有フォルダーがある場合は、除外フォルダーに追加できます。

注: 共有フォルダー全体を除外することしかできず、サブフォルダーの1つだけを除外することはできません。

共有フォルダを除外するには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。「プロファイル」ページが開きます。
2. を選択 [Windows サーバーの場合]tan をクリックし、編集するプロファイルを選択します。Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護]。
4. 選択する [除外されたフォルダ]を選択し、[除外フォルダを追加]。
5. 除外する共有フォルダーへのパスを入力します。
6. [保存して発行] を選択します。

ユーザーを除外する

ユーザーを監視対象から除外する方法の説明。

ユーザーを除外すると、マルウェアが検出されても監視やブロックは行われず、共有フォルダ内のファイルの編集も許可されます。

完全修飾形式でユーザー名を追加できます `domain_name\user_name`またはユーザー SID (セキュリティ識別子)。

> **注 :** ユーザー名またはユーザー SID は、Windows サーバーで使用されているものと同じである必要があります。

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
「**プロファイル**」ページが開きます。
2. を選択 [**Windows サーバーの場合**]タブをクリックし、編集するプロファイルを選択します。
Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [**サーバー共有保護**]。
4. 選択する [**除外されたユーザー**]を選択し、[**ユーザーを追加する**]。
5. ユーザー名またはユーザー SID のいずれかを入力します。

> **注 :** ユーザー名またはユーザー SID は、Windows サーバーで使用されているものと同じである必要があります。

6. [**保存して発行**] を選択します。

4.1.23 ランサムウェアからファイルを保護する

ランサムウェアからファイルとシステム設定を保護する方法を説明します。

ランサムウェア攻撃による可能性があるファイルまたはシステム設定の変更が製品によって検出された場合、変更内容は自動的に元に戻され、隔離領域に保存されます。変更内容が有効であり、ランサムウェアによるものでない場合は、自動的に元に戻された変更内容を隔離領域から復元できます。

製品がランサムウェアからファイルを自動的に保護できるようにするには:

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
「**プロファイル**」ページが開きます。
2. を選択 [**Windows コンピューターの場合**]または [**Windows サーバーの場合**]タブをクリックし、編集するプロファイルを選択します。
3. 左側のメニューから [**ロールバック**]そして次の操作を行います。
   - オンにする [**ロールバック**]。
   - 消す [**許可と報告モード**]。
   - オンにする [**元に戻したファイルの復元を許可する**]。

> **注:** まず、許可と報告モードを1週間オンにしておくことをお勧めします。誤検知がない場合は、許可と報告モードをオフにして、[**元に戻したファイルの復元を許可する**]隔離されたファイルを復元する設定。

> **注 :** デフォルトでは、許可とレポート モードはオンになっています。このモードでは、製品はランサムウェアが行った変更を検出しますが、元に戻すことはありません。変更されたファイルは、許可とレポート モードをオフにした後にのみ自動的に復元されます。

変更されたファイルとシステム設定が復元されます。

4.1.24 ローカルに除外されたパスを削除する

ポータルを使用すると、組織にとって危険であると考えられる除外をローカル除外リストからリモートで削除できます。

ローカルに除外された 1 つ以上のパスを削除するには:

1. [**環境**] のサイドバー から [**デバイス**] を選択します。

「デバイス」画面が表示されます。
2. 除外パスを削除するデバイスの名前を選択します。
デバイスの詳細ページが開きます。
3. 下部のアクションメニューから、[ローカルに除外されたパスを削除する]。
除外されたパスのリストが表示されます。
4. 削除する除外パスを１つ以上選択します。
5. 選択する [削除].

選択されたローカル除外パスが削除されます。

4.1.25 ポータルからElements Agentを再起動する

ポータルを使用すると、再起動できます [エレメントエージェント]システム全体を再起動することなく、選択したデバイス上で実行できます。

再起動します [エレメントエージェント]ポータルから:

1. [環境] のサイドバー から [デバイス] を選択します。
「デバイス」画面が表示されます。
2. 再起動するデバイスを選択します。
3. 下部のアクションメニューから、[再起動] > [Secure Elements Agentで再起動]。

[エレメントエージェント]選択したデバイスで再起動します。

4.2 プレミアム製品でプロファイルを管理する

WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversに、WithSecure Elements EPP for Computers PremiumおよびWithSecure Elements EPP for servers Premiumの製品バリエーションが加わりました。

高度なセキュリティ機能が含まれています。そのうちの一つである「データガード」は、ランサムウェアなどの脅威に対する特別なセキュリティ機能を提供します。

4.2.1 データガードを使用する

WithSecure Elements EPP for Computers Premium およびWithSecure Elements EPP for Servers Premiumのサブスクリプションは、予期しないアプリケーションによるデータの変更を防ぐWithSecure DataGuard機能を追加します。

注 : データガードは、WithSecure Elements EPP for ComputersとWithSecure Elements EPP for ServersのPremium (プレミアム) バージョンで利用できます。Premiumのサブスクリプションがない場合、データガード機能はグレーアウトされます。

データガードは、ディープガードを強化し、ユーザのコンテンツ フォルダを監視する追加機能です。フォルダは自動的に検出され、例外は手動で追加できます。信頼できるアプリケーションは、フォルダにアクセスして変更することができます。データガードは、WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversが提供するすべてのセキュリティ レイヤを迂回する新しいランサムウェアの管理に特に役立ちます。

重要 : データガードが機能するには、ディープガードを有効にする必要があります。

DataGuard を設定する

管理対象コンピュータ上で DataGuard が保護するフォルダを定義し、DataGuard でブロックしたくない信頼性の高いアプリケーションを追加できます。

DataGuardを有効にすると、信頼できないアプリケーションやマルウェア (ランサムウェアを含む) は、保護されているフォルダ内のファイルを変更することはできません。

DataGuard を使用するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。

「プロファイル」ページが開きます。

2. プロファイルを選択します。
3. DataGuardを使用するには、DataGuard で[DataGuardの高度な動作ブロック] を有効にします。
4. [監視対象のユーザ データ フォルダを自動的に検出する] を有効にすると、DataGuard は文書、画像、またはその他のエンドユーザーのコンテンツを含むフォルダを自動的に確認します。
5. [手動で含めたフォルダ] と [手動で除外したフォルダ] で、、次の方法でエンドユーザ コンピュータのDataGuard保護からフォルダを追加または除外できます。
   - [手動で含めたフォルダ] から [パスを追加] を選択します。

     注 : パスを追加すると、指定したパスとすべてのサブフォルダが追加されます。たとえば、C:\Documents を追加すると、DataGuard は C:\Documents の下にあるすべてのファイルとフォルダを監視します。
   - [手動で除外したフォルダ] から [パスを追加] を選択します。

     注 : パスを除外すると、指定したパスとすべてのサブフォルダが除外されます。たとえば、C:\Documents を除外すると、DataGuard は C:\Documents の下にあるすべてのファイルとフォルダに対して監視を停止します。
6. [アクセス制御] を有効にして、DataGuard が保護するファイルとフォルダを変更するためにアクセスできる信頼済みのアプリケーションを定義します。
   - [信頼できるアプリケーションを自動的に検出する] を有効にすると、DataGuard は信頼できるアプリケーションを自動的に検索できます。
   - 信頼できるアプリケーションを手動で追加する場合は、[信頼できるアプリケーションとフォルダを手動で追加] で [パスを追加] を選択します。

     注 : パスを追加すると、指定したパスとすべてのサブフォルダが追加されます。たとえば、C:\Documents を追加すると、DataGuard は C:\Documents の下にあるすべてのファイルとフォルダを監視します。

ボールトの追加

ボールトを追加する方法の説明 DataGuard。

ボールトとは、そのボールト用に設定されたアプリケーションのみがファイルやサブフォルダの書き込み、作成、名前変更を行えるフォルダです。ボールトを使用すると、特定の場所をロックダウンするための特定のルールを作成できます。たとえば、Windowsエクスプローラを使用してボールトにサブフォルダを作成する場合は、次のものを追加する必要があります。`%windir%\explorer.exe`信頼できるアプリケーションのリストに追加します。または、SQLサーバー実行可能ファイルのみがローカルデータベースを使用するアプリケーションのファイルを変更できるようにするには、それを許可するボールトを作成します。

各ボールトには監視機能があります。アプリケーションがボールト内のファイルにアクセスしようとすると、DataGuardセキュリティ イベントにログが作成されます。

ボールトを追加するには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. 編集するプロファイルを選択します。
   「プロファイル」ページが開きます。
3. 左側のメニューから [プレミアム]、 選択する [データガード]。
4. 下にスクロール [金庫]を選択し、[金庫を追加する]。
5. の中に [金庫への道]フィールドにパスを入力します。
6. 選択する [信頼できるアプリケーションを追加する]。
7. の中に[アプリケーションへのパス]フィールドに、ボールトにアクセスできるようにするアプリケーションへのパスを入力します。

   注 : 信頼できるアプリケーションを追加するには、[信頼できるアプリケーションを追加する]。

8. [保存して発行] を選択します。

4.2.2 データガードの使用に関するヒント

プログラムが「プログラム ファイル」から実行される場合、プログラムはブロックされません。たとえば、AppData\Localから同じプログラムが実行されている場合、DataGuardによってブロックされています。したがって、Windows では、プログラム ファイルの下にソフトウェア プログラムをインストールすることを推奨します。Windows にはセキュリティ対策が組み込まれているため、マルウェア ディストリビューターがその場所に侵入することは困難です。

ユーザが安全でない場所を許可するように頼んだ場合、許可した後、DataGuardはその特定の場所のすべてを許可します。これは指定されたファイル名にも適用されます。たとえば、特定の場所にあるファイルが同じ名前の別のファイルに置き換えられた場合、DataGuardはそのファイルを自動的に許可します。

有効にすると、データガードはドキュメントなどのユーザ コンテンツを含むフォルダを自動的に確認します。データガードのフォルダを手動で追加して確認することもできます。個々のユーザの要求に基づいてパスを追加することはできますが、Windows環境変数を使用することを推奨します。たとえば、c:\user\JohnSmith を追加する代わりに、環境変数 %HOME% を使用します。

4.2.3 アプリケーション制御

アプリケーション制御は、アプリケーションの実行とインストールを防ぎ、スクリプトの実行を阻止します。

注： アプリケーション制御は、WithSecure Elements EPP for Computers PremiumとWithSecure Elements EPP for Servers Premiumでのみ利用可能です。

「アプリケーション制御」は、悪意のある、違法な、不正なソフトウェアが企業環境にもたらすリスクを軽減します。以下の機能を提供します。

- セキュリティ⊠WithSecureの侵入テスト担当者が設計した事前設定のセキュリティルールは、企業環境への侵入に使用される攻撃ベクトルをカバーしています。
- ポリシーの適用⊠シンプルなルールエディタに基づき、管理者はどのアプリケーションをブロック、許可、または監視するかを定義することができます。
- セキュリティ イベントでルールがトリガーされたすべてのケースを一元的に可視化

アプリケーション制御を使用する

アプリケーション制御を使用すると、実行できるアプリケーションに対して制限を設定できます。

アプリケーション制御を使用するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. プロファイルを選択します。
3. 「プロファイル」ページで、[アプリケーション制御] を選択します。
4. [アプリケーション制御] をオンまたはオフにします。

注： デフォルトでは、アプリケーション制御は有効です。

5. 「グローバル ルール」で次のいずれかのオプションを選択します。
   - すべてのアプリケーションを許可 - いずれの除外ルールがアプリケーション、インストーラ、スクリプトをブロックしない場合、許可されます。
   - 信頼できないすべてのアプリケーションをブロックする - いずれの除外ルールがアプリケーション、インストーラ、スクリプトを許可しない場合、ブロックされます。
   - すべてのアプリケーションを許可および監視する - いずれの除外ルールがアプリケーション、インストーラ、スクリプトをブロックしない場合、許可されます。また、動作が監視され、必要に応じて報告されます。

注： グローバル ルールは、すべてのアプリケーションに適用される最後のルールを定義します。

6. 変更を現在のプロファイルまたは複数のプロファイルに保存して公開することを選択できます。

> **注：** 複数のプロファイルに保存して公開するように選択した場合、変更を保存しないでウィンドウを閉じる場合、現在のプロファイルに適用されません。

アプリケーション制御ルールを追加する

独自のアプリケーション制御ルールを追加できます。

ルールとトップルールを追加できます。ルールは優先順位で適用されます-テーブルの上から下にチェックされます。アプリケーションを許可するかブロックするかの決定は、最初の一致ルールによって行われます。一致するルールがない場合は、グローバルルールが使用されます。

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
「**プロファイル**」ページが開きます。
2. プロファイルを選択します。
[**プロファイル**] ページが開きます。
3. 左のメニューから [**アプリケーション制御**] を選択します。
4. 追加するルールの種類に応じて、[**新しいトップルールを追加する**] また [**新しいルールを追加する**] を選択します。
5. ルールの名前を入力します。
6. [イベント] ドロップダウン メニューから、ルールを適用するイベントを選択します。

次の表は、利用可能なイベントの種類とそれらがいつ発生されるかを示します。

イベント	説明
アプリケーションの起動	実行可能ファイルまたはスクリプトが起動されたときに発生されます。
モジュールの読み込み	DLL がプロセスにロードされるときに発生されます。
インストーラの開始	`msiexec.exe` が MSI パッケージをコマンドライン パラメータとして使用して起動されたときに発生されます。
ファイル アクセス	ファイルにアクセスするとトリガーされます。
アプリケーションの起動とモジュールの読み込み	⊠つのイベント タイプの組み合わせ。実行可能ファイルまたはスクリプトが起動された際、および DLL がプロセスにロードされるときに発生します。

7. [アクション] ドロップダウンメニューから、[**許可**]、[**ブロック**]、または [**許可して監視**] を選択します。
8. ルールの説明を入力します。
9. 新しいルールを有効にする条件を1つ以上追加します。
   a) [**条件を追加**] を選択します。
   b) [属性] ドロップダウン リストから属性を選択します。
   c) [条件] ドロップダウン リストから属性の条件を選択します。
   d) 条件の値を入力します。

ルールに属性と条件を使用する

次の表は、条件値に一致するように選択できる属性について説明します。

選択した属性	説明
対象	実際のアプリケーションの値。たとえば、[Target file name (対象ファイル名)] は、ブロックする実際のファイルです。
ペアレント	アプリケーションを起動するプロセスの値。たとえば、[Parent file name (親ファイル名)] は、ブロックするアプリケーションを起動するファイルです。
インストーラ	インストーラの値 (MSI インストーラ パッケージ)。

注: たとえば、Internet Explorer をブロックする場合、`iexplore.exe` が対象となり、`explorer.exe` (Windows Explorer) が親になります。

次の表は、条件と入力する値がどのように機能するかを説明しています。

選択した条件	説明
に等しい	値が選択した属性と同じである必要があります (例: `iexplore.exe`)。
に等しくない	値が選択した属性と違う値である必要があります。
未満	数値は、選択した属性よりも小さいものである必要があります。
より大きい	数値は、選択した属性よりも大きいものである必要があります。
以下	数値は、選択した属性よりも小さい、またはまったく同じものである必要があります。
以上	数値は、選択した属性よりも大きい、またはまったく同じものである必要があります。
を含む	選択した属性が値を含めている必要があります (例: `explore`)。
開始値	選択した属性が指定した値で始まる必要があります (例: `ie`)。
終了値	選択した属性が指定した値で終わる必要があります (例: `explore.exe`)。

注: 各パラメータの内容に関する情報は、**プロファイル** > **アプリケーション制御**の横にあるヘルプアイコンを選択すると表示されます。各条件の種類ごとの条件値について説明されます。たとえば、ターゲットファイルサイズは、起動したアプリケーションまたはロードしたモジュールのバイト数で表示されます。

ルールに条件を追加するときに次の点に注意してください:

- ルールの条件に `Target SHA1` または `Parent SHA1` の属性を使用する場合、イベント タイプとして [**アプリケーションの起動**] を使用する必要があります。
- ダイナミックリンクライブラリ (.dll) がブロックされていて、アプリケーション制御でリストに登録する場合、ルールで [**モジュールの読み込み**] のイベントタイプを使用する必要があります。このような場合、ルールに `Target SHA1` と `Parent SHA1` の属性は使用できません。

- [ターゲットファイル名の不一致]と[親ファイル名の不一致]の属性は、バイナリのファイル名がファイルの [プロパティ] > [詳細] にある [元のファイル名] と異なる場合に発生します。

例: 脆弱性のあるバージョンの実行を阻止する

アプリケーション制御を使用して、脆弱なアプリケーションが実行されないようにするには(たとえば、パッチのないバージョンをブロックするなど)、対象ファイルのバージョン属性を使用します。

たとえば、プログラムがバージョン1.2.4で重大な脆弱性を修正している場合、次の方法で1.2.4以前の古いバージョンをブロックすることができます。

1. 次の除外ルールを作成します。
   a) ルールに名前を指定します: パッチされていないプログラムをブロックする
   b) [イベント] ドロップダウン メニューから、[アプリケーションの開始 (`Application start`)] を選択します。
   c) [処理] ドロップダウン メニューから [ブロック] を選択します。
2. 除外ルールに最初の条件を追加します。
   a) [属性] ドロップダウン リストから [対象ファイルの説明 (`Target file description`)] を選択します。

      注 : ファイルの説明を見つけるには、ファイル エクスプローラでファイルを右クリックし、[プロパティ] を選択します。

   b) [条件] ドロップダウン メニューから [含む] を選択します。
   c) [値]フィールドに、ファイルの説明で表示されているように、パッチされていないプログラムの名前を入力します (例: Internet Explorer)。

      注 : 「Internet Explorer」が対象ファイルの説明にあるため、プログラムがファイル名またはパスに関係なくブロックされるようになります。

3. 除外ルールに2つ目の条件を追加します。
   a) [属性] ドロップダウン リストから [対象ファイルの説明 (`Target file version`)] を選択します。
   b) [条件] ドロップダウン メニューから [以下] を選択します。
   c) [値] フィールドで「`1.2.3.*.*`」を入力します。

      注 : 対象ファイルのバージョンの条件は「1.2.3.*.*」「以下」です。アスタリスクは、メジャーフィールドとマイナー フィールドのみが比較に使用されることを示します。

4.2.4 システムイベントの検出

システムイベント検出は、WithSecure Elements EPP for Computers Premiumそしてその WithSecure Elements EPP for Servers Premiumサブスクリプション。

データが複数の場所に分散しているため、潜在的に危険なアクティビティを認識することが困難な場合があります。システムイベント検出を使用すると、セキュリティ関連のWindowsイベントログエントリをシステムイベントログで直接認識できます。WithSecure Elements EPPポータル。これらのイベントは、何かが起こっている可能性を示す潜在的な兆候です。正当な理由がないかどうかを確認するために、さらに調査することをお勧めします。

次のイベントはデフォルトでオンになっています。

- [**イベント ID: 認証失敗 ("アカウントのログインに失敗しました")**] - 認証が失敗するのはよくあることですが、単一のユーザーまたはエンドポイント デバイスをターゲットにした認証の試行が突然複数回発生する場合、攻撃者がエンドポイント デバイスにアクセスするためにユーザー アカウントの資格情報を複数送信していることを示している可能性があります。
- [**イベント ID: ユーザーがロックされました ("ユーザー アカウントがロックアウトされました")**] - これは、認証の試行が複数回失敗したため、ユーザー アカウントがロックされたことを示します。繰り返し発生するイベントは、スクリプト エラーまたは進行中の攻撃の強力な指標です。

注： 実際の試行回数は、GPO のユーザー ロックアウトしきい値で定義されます。

- [**イベント ID: 監査ログがクリアされました ("監査ログがクリアされました")**] - 攻撃者がデバイスにアクセスすると、監査ログを消去して痕跡を隠そうとする可能性があります。このような場合は、正当な行為によるものではないことを確認する必要があります。

注： デフォルトでオフになっているイベントがいくつかあります。通常、これらは、SIEM または SOAR ソリューションに関連データを収集したいプロのセキュリティ運用管理チームにとって興味深いイベントです。このようなイベントはアクティビティの間接的な指標であるため、デフォルトではオフになっています。

システムイベント検出の設定

必要なWindowsシステムイベントを選択する方法の説明 WithSecure Elements Agent監視してセキュリティ イベントに送信します。

システム イベント検出を設定するには:

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. を選択 [**Windows サーバーの場合**]または [**Windows コンピューターの場合**]タブをクリックし、編集するプロファイルを選択します。
   [**プロファイル**] ページが開きます。
3. 左側のメニューから [**システムイベント検出**]。
4. の中に **アクティブ**列で、製品で監視するイベントのスイッチをオンにします。
5. [**保存して発行**] を選択します。

4.2.5 デバイスドライブの暗号化

Elements Endpoint encryptionデバイスの暗号化の状態とそれを管理するためのツールの概要を示します。

暗号化は、データの機密性を確保するために不可欠なツールです。デバイスを暗号化することで、デバイスが紛失または盗難にあった場合でも、第三者がデバイスに保存されているデータにアクセスできないようにすることができます。ディスク暗号化のステータスは、デバイスの詳細、デバイス リストのコンプライアンス ビュー、およびデバイス レポートで確認できます。

注： ドライブを暗号化する Elements Endpoint encryptionWindows 10 以降のオペレーティング システムが必要です。さらに、デバイスには Trusted Platform Module (TPM) バージョン 2 以上が搭載されている必要があります。デバイスの TPM バージョンに関する情報は、デバイスの詳細ページの左側のメニューで確認できます。

回復キーは、ディスク暗号化の管理において重要な役割を果たします。正当なユーザーがデバイスからロックアウトされた場合、または別のデバイスを使用して暗号化されたドライブからデータを復元する必要がある場合、データにアクセスするために回復キーが必要になります。これらのキーを収集するツールは多数ありますが、その1つを使用することが重要です。WithSecure Elements Endpoint Protection必要に応じて回復キーを収集できます。設定は [**一般的な**]下のタブ [**プロフィール**]。

注: 回復キーを収集するには、Elements Endpoint Protectionインストールされ、Bitlockerで「回復パスワードプロテクター」を使用して暗号化されたディスク。この機能をオンにした後、回復キーが正常に収集され、キーが Elements Endpoint Protectionポータル。

デバイスドライブの暗号化

ドライブの暗号化のオン/オフは、WithSecure Elements EPP for Computers PremiumおよびWithSecure Elements EPP for Servers Premiumサブスクリプションに付属する高度なセキュリティ機能です。

Elements Endpoint Protectionがインストールされ たWindowsデバイスと、BitlockerまたはFilevaultを使用して暗号化されたディスクが必要です。

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   「**デバイス**」画面が表示されます。

2. ドライブを暗号化するデバイスを選択します。
3. ページの下部にあるアクションメニューから、[システムドライブの暗号化] > [ドライブを暗号化]をクリックし、次のいずれかを選択します。
   - 使用済みのディスク領域のみを暗号化する□新しいPCやドライブにはより高速で最適です□
   - ドライブ全体を暗号化する□遅くなりますが、使用中のPCやドライブには最適です□
4. [暗号化] を選択します。

4.3 Elements EPP for Computers□Mac□でプロファイルを管理する

ここでは、WithSecure Elements EPP for Computers (Mac)でプロファイルを管理する方法を説明します。

4.3.1 新しいコンピュータ プロファイルを作成する

特定のコンピュータに指定できるプロファイルを作成することができます。

新しいプロファイルを作成するには

1. プロファイル > Mac用 から既存のプロファイルの横にある を選択し、[プロファイルをクローン] を選択します。
   [Mac用プロファイル] ページが開きます。
2. 新しいプロファイルの名前と説明を入力してください。新しいプロファイルのラベルを選択することもできます。
3. 設定を変更して、[保存して発行] を選択します。
   新しいプロファイルが作成されます。

4.3.2 アンインストールを許可する

この設定がオンになっている場合にのみ、ユーザはコンピュータで製品をアンインストールできるようになります。

アンインストールを許可するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [Mac用] タブを選択します。
3. いずれかのプロファイルを選択します。
   [Mac用プロファイル] ページが開きます。
4. 左のメニューから [一般設定] を選択します。
5. [製品のアンロードをユーザに許可] を有効にします。

4.3.3 早期アクセスを有効にする

早期アクセス設定をオンにする方法の説明。

デバイスにプロファイルを割り当てた後、[早期アクセス]オンにすると、デバイスは、一般向けに公開され、サイレント アップグレード用にチャネルにリリースされる前に、最新の製品バージョンを受信します。アップグレードはサイレントに実行され、通常の更新と同じです。

注: 新しいバージョンをすべてのクライアント ソフトウェアにプッシュする前に、早期アクセスで新しいバージョンが利用可能になるまで最大2週間の猶予を設けています。リリースに緊急の脆弱性修正が含まれている場合は、早期アクセスステージを最小限に抑える場合があります。

重要: 新しい機能や今後の機能をテストできるように、この設定をオンにすることを強くお勧めします。

早期アクセス設定をオンにするには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。

「プロファイル」ページが開きます。
2. [Mac用] タブを選択します。
3. いずれかのプロファイルを選択します。
[Mac用プロファイル] ページが開きます。
4. 左のメニューから [一般設定] を選択します。
5. ターン [クライアントソフトウェアへの早期アクセス]設定オン。
6. [保存して発行] を選択します。

4.3.4 自動更新の設定

WithSecure Elementsのプロファイルでは、製品が自動更新をどのように処理するかを設定できます。

ポータルには、HTTPプロキシ接続を設定するための以下のオプションがあります。

- プロキシを使用しない
- システム設定からのHTTPプロキシ
- リモートで管理されたHTTPプロキシを使用する

注： このオプションを選択する場合、[リモートで管理されるプロキシアドレス] フィールドにプロキシアドレスを指定する必要があります。

製品の社内 GUTS2 サーバー アドレスを設定して、そこから更新を取得できます。ローカル サーバーがセットアップされていて利用可能な場合、製品は最初にローカル サーバーからアップデートをダウンロードしようとします。そうでない場合、[セキュリティ構成] > [プロファイル] > [一般設定] の下にある [グローバルな WithSecure 更新サーバーへのフォールバック] オプションをオンにしている場合に製品はグローバル WithSecure サーバーからアップデートをダウンロードします。サーバーごとに、製品は許可された HTTP プロキシ オプションを次の順序で通過します。[リモートで管理された HTTP プロキシを使用する] > [システム設定の HTTP プロキシ] > [プロキシを使用しない] (HTTP プロキシなしの直接接続)。

4.3.5 リアルタイム スキャンを設定する

この設定は、エンドユーザーがアクセスするすべてのアイテムに対してリアルタイムマルウェアスキャンを有効にします。

リアルタイム スキャンを設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. [Mac 用] を選択し、プロファイルを選択します。
[Mac用プロファイル] ページが開きます。
3. 左のメニューから [リアルタイム スキャン] を選択します。
4. 次のことを実行します。
   a) リアルタイム スキャンを有効にします。

注： この設定を有効にしておくことを強く推奨します。

   b) [Security Cloud (ORSP)] が有効であることを確認してください。

注： ***Security Cloud*** は、未知のアプリケーションや Web サイト、悪質なアプリケーションや Web サイトの悪用に関するセキュリティ データを収集します。この設定を有効にしておくことを強く推奨します。

   c) [XFence] が無効であることを確認してください。

注： XFence は、高度な機能であり、通常の環境では使用しないことを推奨します。

4.3.6 スケジュール スキャン

定期的にウイルスやその他の有害なアプリケーションをスキャンするように製品を設定します。

スケジュール スキャンを設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. プロファイルを選択します。
3. 手動スキャン > スケジュールスキャンの順に選択します。
4. スケジュール スキャン スキャンを有効にします。
5. スケジュール スキャンを実行する頻度を選択します。
   - 日単位 - スキャンを毎日実行します。
   - 週単位 - 毎週、選択した曜日にスキャンを実行します
   - 月単位 - 毎月スキャンを実行します
6. 「スキャン開始」 で次のいずれかのオプションを選択します。
   - 時間 - スキャンを開始する時間を選択します。コンピュータを使用する予定のない時刻を選択してください。
   - 分 - スキャンを開始する分を選択します。

4.3.7 スキャン除外の設定

ファイルまたはフォルダをスキャンから除外するように製品を設定します。

注: フォルダとファイルの除外機能は、クライアントバージョン17.7以降にのみ適用されます。

スキャンの除外を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. Mac 用選択し、プロファイルを選択します。
[Mac用プロファイル] が開きます。
3. [一般設定] を選択します。
4. [すべてのセキュリティスキャンからフォルダやファイルを除外する] で、[除外を追加する] リンクを選択します。
5. [パス]列で、除外するファイルまたはフォルダへのパスを追加します。
指定されたパスにあるフォルダとファイルは、すべてのセキュリティスキャンと対策から除外され、WithSecureによって保護されていません。これは、指定されたフォルダ内のすべてのサブフォルダに適用されます。たとえば、`/Users/*/folder-to-exclude/*`はすべてのユーザに対して「folder-to-exclude」にあるすべてのものを除外します。

   重要: これは、スキャンから絶対に除外する必要があるファイルまたはフォルダにのみ使用してください。たとえば、スキャンから「/*」を除外すると、システムボリューム全体と、その中のすべてのフォルダ、サブフォルダ、およびファイルがすべてのセキュリティ対策から除外されます。

4.3.8 ブラウザ保護を設定する

ブラウザ保護は、銀行サイトへのアクセスを保護し(接続制御)、ブロックされたサイトへのアクセスを阻止します (Web コンテンツ制御)。

ブラウザ保護を設定するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. [Mac 用] を選択し、プロファイルを選択します。
[Mac用プロファイル] ページが開きます。

3. 左のメニューから [ブラウザ保護] を選択します。
4. 次のことを実行します。
   a) ブラウザ保護を有効にします。

      注： この設定を有効にしておくことを推奨します。

   b) [Web コンテンツ制御] を有効にできます。

      注： この設定は、コンテンツ (「憎悪表現」や「違法」など) に基づいて Web サイトをブロックします。「不明」は、評価が不明なサイトへのアクセスをブロックします。通常、「不明」なサイトは人気がなく、他のサイトと比べてアクセス数が低いです。

   c) [接続制御] が有効であることを確認します。

      注： この設定は、オンライン バンキング サイトや機密情報を処理するサイトに対して安全な接続が確立されている場合にユーザを通知します。この設定を有効にしておくことを推奨します。

4.3.9 Mac ファイアウォールを有効にするには

Mac ファイアウォールを有効にすると、侵入者がコンピュータにアクセスすることを阻止できます。

注: デフォルトでは、Appleファイアウォールは製品でオンになっています。 Elementsプロファイルで変更できます。

Firewall が有効であることを確認するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。
2. [Mac 用] を選択し、プロファイルを選択します。
   [Mac用プロファイル] ページが開きます。
3. 左のメニューから [ファイアウォール] を選択します。
4. [Appleファイアウォール] ドロップダウンメニューから次のいずれかのオプションを選択します。
   - オン - Appleファイアウォールをオンにします
   - オフ - Appleファイアウォールをオフにします
   - 外部管理 - 外部管理されている場合、ファイアウォール設定は変更されません

   注： 管理対象のMontereyデバイスで `/usr/libexec/ApplicationFirewall/socketfilterfw`を実行すると、「管理対象のMacコンピュータのコマンドラインからファイアウォール設定を変更できません。」というメッセージが表示されます。そのメッセージが表示された場合は、Appleファイアウォールオプションとして [外部管理] を選択します。

4.3.10 WithSecureアプリ層ファイアウォールプロファイルを使用する

WithSecureアプリ層ファイアウォールプロファイルを使用すると、アプリケーション固有のルールを使用して、着信および発信ネットワークトラフィックを制御できます。

注： WithSecureファイアウォールは、ここでは「WithSecureアプリ層ファイアウォール」と呼ばれます。

プロファイルエディタで、以下を切り替えることができますWithSecureファイアウォールオンまたはオフにし、ファイアウォールプロファイルを編集し、ファイアウォールルールを作成、エクスポート、およびインポートします。

注： 現在、WithSecureアプリ層ファイアウォールプロファイルは、WithSecure Elements EPP ポータルでのみ設定できます。

WithSecureアプリ層ファイアウォールとは何ですか

WithSecureのアプリ層ファイアウォールでは、特定のクライアントデバイスの受信および送信ネットワーク接続を制御することができ、ネットワークトラフィックの保護に役立ちます。これらの設定は、特定のカテゴリに属するアプリケーションのセットに対して定義することも、特定のアプリケーションに適用することもできます。設定可能なファイアウォールプロファイルと呼ばれる事前定義されたルールのセットを使用して、特定のアプリケーションセットに対する受信または送信のネットワーク接続を許可またはブロックすることができます。また、特定のアプリケーションに特定のファイアウォールルールを定義することで、そのアプリケーションのネットワークトラフィックを許可またはブロックすることができます。

macOSのファイアウォールを使用すると、特定のアプリケーションまたはすべてのアプリケーションの受信接続を許可またはブロックすることができます。F-Secureファイアウォールでは、受信接続と送信接続の両方を許可またはブロックすることができるなど、より幅広い可能性があります。また、単一のアプリケーションや、署名付きアプリケーションなど特定のカテゴリに属するアプリケーションのセットに対して指定できます。

Trusted by WithSecure設定とは何ですか

この設定を使用して、WithSecureが信頼するベンダーまたは開発者によって署名された、許可されたすべてのアプリケーションの受信および送信接続を許可またはブロックすることができます。

ファイアウォール ルールを追加する

ファイアウォール プロファイルに新しいルールを追加できます。

ファイアウォール ルールを追加するには

1. [**セキュリティ構成**] で、サイドバーの [**プロファイル**] を選択します。
   「**プロファイル**」ページが開きます。
2. [**Mac 用**] タブを選択し、変更するプロファイルを選択します。
3. [**ファイアウォール**] を選択します。
4. ルールを追加する WithSecure ファイアウォール プロファイルを選択します。
5. [**WithSecure プロファイルのファイアウォール ルール**]で、[**ルールを追加**] を選択し、次の操作を行います。
   a) [**有効**] 列のスイッチがオンになっていることを確認します。
   b) ルールの名前と説明を入力します。
   c) 上部のドロップダウンメニューから、ルールのアクション(**許可**または**ブロック**)を選択します。
   d) 真ん中のドロップダウン メニューから、トラフィックの方向を選択します。

方向	説明
受信/送信	トラフィックは、双方向でコンピュータとの間で許可またはブロックされます。この方向を使用するアプリケーションの例: オーディオ/ビデオ コール機能とトレント クライアントを備えたメッセンジャー。
受信	定義されたリモートホストまたはネットワークからコンピュータへのトラフィックは、許可またはブロックされます。この方向を使用するアプリケーションの例: sshd (ssh サーバ)、ScreenSharing (vnc サーバ)、Apache、Nginx などのサーバ アプリケーション。
送信	コンピュータから定義されたリモート ホストまたはネットワークに向いている場合、トラフィックは許可またはブロックされます。この方向を使用するアプリケーションの例: Web ブラウザ、wget、curl、ftp クライアント、ssh クライアント、vnc クライアントなどのクライアント アプリケーション。

e) 下部のドロップダウンメニューから、アラートのアクション[警告なし]または [アラートを送信する] のいずれかを選択します。
f) [属性で] で、1つ以上の署名識別子を入力します。
署名識別子は、アプリケーション署名に埋め込まれた一意の識別子です。通常、`com.apple.Safari` などのバンドル識別子と一致します。

> **注:** 複数の識別子を入力する場合、カンマを使用して区切ることができます。または、最後の文字としてワイルドカード (*) を使用できます。たとえば、`com.google.Chrome*` または `com.apple.Safari,com.google.Chrome*`

g) 1つ以上のチーム識別子を入力します。
チーム識別子は、Apple が macOS のアプリケーションを提供するベンダーに割り当てられた一意の識別子です (例: APPLE または EQHXZ8M8AV)。複数の識別子を入力する場合、カンマを使用して区切ることができます: APPLE、EQHXZ8M8AV

ファイアウォール ルールのエクスポートとインポート

ファイアウォールルールを .json ファイルにエクスポートしたり、.json ファイルからインポートしたりできます。

ファイアウォール ルールをエクスポートまたはインポートするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. [Mac 用] タブを選択し、変更するプロファイルを選択します。
3. [ファイアウォール] を選択します。
4. [ファイアウォール ルール] テーブルの横にある ••• を選択します。
5. 実行する内容に応じて、オプションのいずれかを選択します。
   - ルールをエクスポートするには、[ファイルにエクスポート (JSON)] を選択し、FirewallRules.json ファイルを開くか保存します。
   - ルールをインポートするには、[ファイルからインポート (JSON)] を選択し、ルールのインポート元の .json ファイルを選択します。
   - テーブル内のルールを置換するには、[ファイルから置換] を選択し、置換する.jsonファイルを選択します。

署名とチーム識別子の取得

Apple `codesign` ユーティリティを使用して、アプリケーションの署名とチーム識別子を取得できます。

> **注:** `codesign` ユーティリティは、サポートされているすべての macOS バージョンに含まれています。

アプリケーションの識別子を取得するには

1. アプリケーションのパスを見つけます。
2. `Terminal.app` を開きます。
3. 次のコマンドを入力し、Enter ををを押します:
   `codesign -dv "<アプリケーションへのパス>"`
4. 出力で、Identifier および TeamIdentifier フィールドを見つけます。

```
Executable=###
Identifier=<Signing Identifier>
Format=###
CodeDirectory ###
Signature size=###
Timestamp=###
```

```
Info.plist entries=#
TeamIdentifier=<Team Identifier>
Runtime Version=###
Sealed Resources version=###
Internal requirements ###
```

Apple が提供する一部のアプリケーションでは、TeamIdentifier 値が設定されていません。

```
Executable=###
Identifier=com.apple.###
Format=###
CodeDirectory ###
Signature size=###
Timestamp=###
Info.plist entries=#
TeamIdentifier=not set
Runtime Version=###
Sealed Resources version=###
Internal requirements ###
```

そのような場合、次のチーム識別子を使用できます。

```
APPLE
```

注： 識別子に「com.apple」のプレフィックスが含まれていることを確認します。

例

Google Chrome

- アプリケーションのパス: `"/Application/Google Chrome.app"`
- `codesign` コマンド:

```
codesign -dv "/Applications/Google Chrome.app"
```

- `codesign` の出力:

```
Executable=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome
Identifier=com.google.Chrome
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20500 size=1789
flags=0x12a00(kill,restrict,library-validation,runtime) hashes=47+5
location=embedded
Signature size=9043
Timestamp=11 Feb 2020 at 4.12.31
Info.plist entries=36
TeamIdentifier=EQHXZ8M8AV
Runtime Version=10.14.0
Sealed Resources version=2 rules=13 files=60
Internal requirements count=1 size=204
```

注： 上記の例では、署名識別子は「com.google.Chrome」であり、チーム識別子は「EQHXZ8M8AV」です

Apple Safari:

- アプリケーションのパス: `"/Applications/Safari.app"`
- `codesign` コマンド:

```
codesign -dv "/Applications/Safari.app"
```

- `codesign` の出力:

```
Executable=/Applications/Safari.app/Contents/MacOS/Safari
Identifier=com.apple.Safari
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20100 size=321 flags=0x2000(library-validation) hashes=3+5
 location=embedded
Signature size=4547
Info.plist entries=41
TeamIdentifier=not set
Sealed Resources version=2 rules=13 files=2227
Internal requirements count=1 size=64
```

注: 上記の例では、署名識別子は「com.apple.Safari」です。チーム識別子は設定されていませんが、組み込みの Apple アプリケーションであるため (つまり、識別子に「com.apple。」プレフィックスが付いているため)、「APPLE」を使用できます。

第 章
5

セキュリティを監視する

トピック :

WithSecure Elements EPPポータルを通じて保護しているコンピュータとモバイル デバイスのセキュリティ ステータスを監視できます。

ソリューション プロバイダまたはサービス パートナーとして、デバイスは組織または一覧ビューから表示できます。組織ビューでは会社別のデバイスがすべて表示され、一覧ビューでは該当するソリューション プロバイダまたはサービス パートナーの管理下にあるデバイスがすべて表示されます。

注 : 会社ビューで新しいデバイスを追加またはモバイル デバイスをインポートできます。

特定のデバイスのステータスに関する詳細情報を表示することができます。

- デバイスがマルウェアとブラウザ保護を最後にアップデートした日時
- デバイスが使用しているライセンス キーコードと有効期限
- ブロックしたマルウェア、危険なサイト、追跡試行の履歴

また、特定のデバイスに特定の操作を行うように指示することもできます。

- ステータス アップデートを送信 - 1つまたは複数のデバイスからステータスのアップデートを要求して、ポータルに最新のステータス情報があることを確認します。
- ソフトウェア アップデートをインストール - 選択したデバイスにインストールするソフトウェア アップデートを選択します
- スキャン(マルウェアまたはアップデート) - 1つまたは複数のデバイスで手動スキャンを遠隔から実行します。
- プロファイルの割り当て - 選択したデバイスにプロファイルを指定します
- ラベルの管理 - 選択したデバイスへのラベルの追加、置換、削除
- サブスクリプションの変更 - 選択したデバイスの既存のサブスクリプションを変更します。
- リモート デバイス - システムから1つ以上のデバイスを削除します
- ネットワーク隔離 -1つ以上のデバイスをネットワークから隔離します (例: ネットワーク攻撃の場合など)。

  重要 : このオプションを使用する場合には十分注意してください。

  注 : WithSecure Elements Endpoint Detection and Response ポータルからもデバイスを隔離することができます。
- システムの再起動 - システムを自動的に再起動します。ユーザはデバイスの再起動を止めることはできませんが、すべてのデータを保存するために5分与えられます。
- システムドライブの保護 - システムドライブの暗号化または復号化

- 診断操作 - [診断ファイルを要求] を選択すると、診断データを WithSecureにアップロードすることを許可するリクエストをユーザに送信します。プライバシー保護のため、ユーザには承諾を求めます。また、デバッグロギングをオンにし、自動的にオフになる時間を選択することができます。
- デバイスにメッセージを送信する-選択されたデバイスにメッセージを送信します。ログインしているすべてのユーザにメッセージが表示されます。
- セキュリティ機能をオフにする - オフにするセキュリティ機能 (ファイアウォール、ディープガード、リアルタイム スキャン、リソース保護) を選択するか、すべてのセキュリティ機能をオフにします
- アンインストール - デバイスからソフトウェアをアンインストールします。アンインストールすると、サブスクリプションが解放され、デバイスに関するすべての情報がシステムから削除されます。

5.1 デバイスのセキュリティを監視する

WithSecure Elementsポータルを使用して、保護しているコンピュータとモバイルデバイスのセキュリティステータスを監視できます。

👉 **注：** *スコープセレクタ*を使用してポータルで表示する内容を設定できます。次の情報を切り替えできます。

- 顧客企業の概要または
- 特定の企業に関する詳細情報

5.1.1 デバイスのセキュリティ概要を表示する

WithSecure Elementsポータルに登録されているすべてのデバイスのセキュリティステータスの概要は、[**ホーム**] ページで確認できます。

登録したデバイスのセキュリティ ステータスを表示するには

1. サイドバーから [**ホーム**] を選択します。

   [**ホーム**] 画面が表示されます。

   ホームページには次のタブがあります。

   - [**概要**] は以下を示します。
     - 検出と対応
     - 予測する
     - 防ぐ
     - 危険にさらされている上位 5つのデバイス
     - 影響を受ける上位5つのメールボックス
     - 最も一般的な検出事項
     - 最もリスクにさらされている組織
   - [**Endpoint Protection**] は以下を示します。
     - ワークステーションの保護ステータス
     - サーバーの保護ステータス
     - ソフトウェアのアップデート状況
     - モバイル保護ステータス
     - 対処する問題のリスト問題の種類、重大度、影響を受けるデバイスの数
   - [**検出と対応**] は以下を示します。
     - 危険にさらされているデバイス
     - 概要
     - リスクごとのオープン検出
     - ステータス別の検出
     - 種類別の検出
     - デバイス数別のOS

2. 選択した会社の詳細な [**会社ステータス**] 情報を [**ホーム**] ページに表示するには、 *スコープセレクター* を使用します。

5.1.2 デバイスをフィルタする

WithSecure Elementsポータルからフィルタリング機能を使用して、デバイスを見つけることができます。

フィルタ機能を使用するには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   「**デバイス**」画面が表示されます。

2. フィルタのドロップダウン メニューからデバイスのフィルタ対象となるカテゴリを選択します。
3. 「価値」ドロップダウン メニューから対象のカテゴリに対する値を選択し、[適用] を選択します。

注： たとえば、カテゴリとして [接続ステータス] を選択し、値として [接続済み] を選択すると、現在接続されているすべてのデバイスが表示されます。

ヒント： フィルタと同時に検索機能も活用できます。

4. 選択したフィルタのカテゴリと値をリセットする場合、[フィルタを消去] を選択します。

注： フィルターの横にある X を選択すると、フィルターを削除できます。

指定したフィルタの条件に一致するデバイスが一覧に表示されます。

5.1.3 モバイル デバイスを検索する

検索機能を使用してモバイル デバイスを検索することができます。

次の情報を検索キーワードとして利用できます。

- デバイスUUID
- 装置名
- ラベル
- 最後のユーザー
- 上場企業
- IPアドレス
- ライセンス キーコード

モバイル デバイスを検索するには

1. [環境] のサイドバー から [デバイス] を選択します。
「デバイス」画面が表示されます。
2. を選択 [モバイルデバイス]タブ。

ヒント： フィルタ機能はデバイスの検索にも活用できます。

3. 検索文字列を入力してください [検索]分野。
検索に一致するモバイル デバイスが一覧に表示されます。

5.1.4 デバイスの保護ステータスを表示する

WithSecure Elements Endpoint Protectionアカウントに追加した個別のコンピュータまたはモバイル デバイスに関する情報 (保護ステータス、ライセンス情報、デバイス情報、インストールしたソフトウェアと統計情報) を確認できます。

デバイスの保護ステータスの詳細情報を表示する

[デバイス] ページでは、デバイスの保護ステータスのさまざまな詳細を表示できます。

特定のデバイスの詳細情報を表示するには

1. [環境] のサイドバー から [デバイス] を選択します。
「デバイス」画面が表示されます。
2. [デバイス] ページで、[コンピュータ]、[モバイルデバイス]、[コネクター]、 または [保護されていないデバイス] タブを選択します。
選択したタイプに一致するデバイスの詳細を含むテーブルが表示されます。デフォルトでは、[全体的なステータス] ビューが表示されます。
3. 他のデバイスの詳細を表示するようにビューを変更するには、[ドロップダウンリストの表示] の横にある矢印を選択します。
メニューが開き、使用可能なビューが一覧表示されます。
4. 該当するビューを選択してデバイスの追加情報を確認できます。

コンピュータの場合、次のビューを使用できます。

- 全体的なステータス
- 構成の詳細
- コンプライアンス
- ハードウェア情報
- 再起動が必要
- 容量不足
- すべてのフィールド
- EDR ステータス
- Vulnerability management

モバイルデバイスの場合、次のビューを使用できます。

- セキュリティ概要
- すべてのフィールド

コネクターの場合、次のビューを使用できます。

- コネクターすべて

選択した情報が表に反映されます。

5.2 セキュリティイベントを表示する

[セキュリティイベント] ページには、システム内のすべてのセキュリティイベントが表示されます。

注 : この機能はパイロットの段階にありますがが、すべてのユーザが利用できます。

セキュリティイベントを表示するには

注 : スコープセレクタを使用して、セキュリティイベントを表示する会社を選択できます。

1. [イベント] で [セキュリティイベント] を選択します。
   [セキュリティイベント] ページが開き、次の情報が表示されます。
   - 日時
   - 重大度
   - ソース
   - デバイス
   - 説明
   - 承認済み
2. セキュリティイベントの詳細を表示するには、詳細を表示するイベントの前にある ˅ を選択します。
   [詳細] ビューには次の情報が表示されます。
   - インシデントID
   - リスク
   - 解決方法
   - フィンガープリント
   - 初期検出タイムスタンプ
   - ユーザー名
   - クライアントのタイムスタンプ
   - トランザクションID
   - デバイスUUID

5.2.1 セキュリティイベントをフィルタする

表示されるセキュリティイベントをフィルタリングできます。**セキュリティイベント**ページ。

セキュリティイベントをフィルタするには

1. [**イベント**] で [**セキュリティイベント**] を選択します。
   [**セキュリティイベント**] ページが開きます。
2. ドロップダウンメニューから選択 [**デバイスタイプ**]。
3. から **値を選択**ドロップダウンメニューで、次のフィルタリングオプションのいずれかを選択します
   - Active Directory 組織単位

     注 : このオプションは会社レベルでのみ使用できます。

   - デバイスラベル
   - デバイス タイプ
   - デバイスUUID
   - イベントID
   - ソース
   - 対象
   - 日時
   - メールアドレス
4. から [**値を選択**] ドロップダウン メニューで、いずれかのオプションを選択します。

   注 : ドロップダウン メニューに検索語を入力することもできます。

   注 : 関連するイベントの前にある矢印を選択すると、セキュリティ イベントの詳細が表示されます。
5. 選択する [**適用する**]。
   セキュリティ イベント テーブルには、フィルターされたイベントが表示されます。

5.3 Active Directory で保護されていないデバイスをスキャンする

会社の Active Directory をスキャンして保護されていないデバイスを検出する方法を説明します。

保護されていないデバイスとは、会社のActive Directoryでまだ管理されていないコンピュータまたはサーバーのことです。WithSecure保護されていないデバイスは、新しいデバイスか、ポータルから完全に削除されたデバイスのいずれかです。

スキャンが開始されると、ポータルは各Active Directoryノードでスキャン操作を実行する1つ以上のデバイスを自動的に選択します。これらのデバイスはWithSecure管理対象デバイスは、**デバイス**ページ。スキャン操作の場合、ポータルは常に最近ポータルに接続したデバイスを選択します。

保護されていないデバイスに関する情報は、特にトラブルシューティングに役立ちます。たとえば、スキャンが失敗した場合、その理由はデバイスの 1 つにあります。他のデバイスで操作を実行する場合は、新しいスキャンを開始する必要があります。

保護されていないデバイスをスキャンするには

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   「**デバイス**」画面が表示されます。
2. を選択 [**保護されていないデバイス**]タブ。
3. 選択する [**スキャン開始**].
   システムは、会社の Active Directory をスキャンして、保護されていないデバイスを探します。スキャンが完了すると、ページの上部に、スキャンに使用されたノード名とデバイスが表示されます。保護されていないデバイスは、以下の情報を示す表にリストされます。
   - DNS名
   - デバイスが Active Directory に作成された日付

- 最終ログイン日
- Active Directory コメント
- オペレーティング·システム
- Active Directory 組織単位
- Active Directory GUID
- コメント
- 状態
- コラム アイコンには次のオプションがあります: 信頼済みとしてマーク、コメント

注: 保護されていないデバイスのリストは、スキャンが終了してから 24 時間以内にクリーンアップされます。

注: 保護されていないデバイスをポータルに追加するには、手動でインストールする必要があります。WithSecure Elements Agentその上に。

4. 保護されていないデバイスでも信頼する場合は WithSecure Elements Agent信頼できるものとしてマークすることができます。そのためには、 デバイスの行で、[**信頼できるものとしてマーク**]。
5. 保護されていないデバイスについてコメントを残すこともできます。その手順は次のとおりです。
   a) 選択する デバイスの行で、[**コメント**]。
   b) コメントを入力して選択してください [**保存**]。

5.4 ネットワークからデバイスを隔離する

ネットワークからデバイスを隔離することができます。

注: ネットワークの分離は、モバイルデバイスには適用されません。

デバイスをネットワークから隔離するには

注: ネットワークの隔離機能は、ネットワークが攻撃の対象となる場合にのみ使用してください。

1. [**環境**] のサイドバー から [**デバイス**] を選択します。
   「**デバイス**」画面が表示されます。
2. ネットワークから隔離するホストを選択します。
3. ページ下部のアクションメニューから、**ネットワーク分離** > **ネットワークから分離**を選択します。
   選択したデバイストがネットワークから隔離されます。
4. 隔離されたデバイスをネットワークに接続し直すには、**ネットワークの隔離** > **解除** を選択します。

5.5 デバイスを削除する

デバイスを削除する方法について説明します。

デバイスを削除すると、サブスクリプションが解放されます。ポータルから削除されたデバイスが再びアクティブになり、サブスクリプションに空きシートがある場合、そのデバイスはEPPポータルに再び表示されます。サブスクリプションに空きシートがない場合、デバイスは管理ポータルに表示されず、デバイスは保護されません。

[**デバイスの復帰をブロック**] オプションをチェックすると、デバイスがブロックリストに移動されます。

注: [**デバイス**] の横にある アイコンを選択し、ドロップダウンメニューから [**削除されたデバイスの管理**] オプションを選択すると、デバイスを再び追加することができます。デバイスが再接続され、サブスクリプションに空きシートがある場合、デバイスはデバイスリストに再び表示されます。

デバイスを削除するには

1. [環境] のサイドバー から [デバイス] を選択します。
   「デバイス」画面が表示されます。
2. ポータルから削除するデバイスを1つ以上選択します。
3. ページ下部のアクションメニューから、[デバイスの削除] を選択します。
4. 次のいずれかを実行します。
   - 選択したデバイスを削除するには、[デバイスを削除] を選択します。
   - 選択したデバイスをブロックリストに移動するには、[デバイスの復帰をブロック] > [デバイスを削除] を選択します。

選択内容に応じて、選択したデバイスはポータルから削除されるか、ブロックリストに移動されます。

注: 管理 > サブスクリプションの [ブロックリストからデバイスを復元] を使用すると、ブロックリストに移動したデバイスを元に戻すことができます。この場合、デバイスは再接続時にデバイスリストに再び表示され、サブスクリプションに空きライセンスがある場合に表示されます。

5.6 サードパーティ RMM ツールを使用する

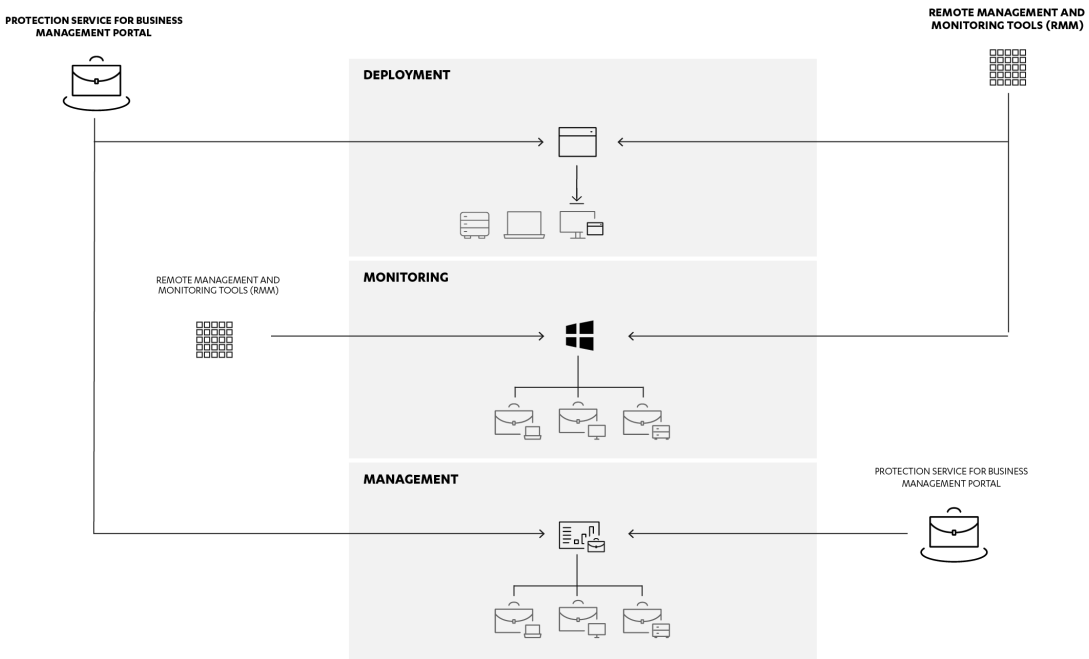
WithSecure Elements EPPは、サードパーティ製の Remote Monitoring and Management (RMM) ツールの連携に対応しています。

注: WithSecure Elements EPPの現在のバージョンは、Datto、Kaseya、およびSolarWinds RMMツールをサポートしています。他のRMMツールでWindows Management Instrumentation (MI) APIを使用します。

ポータルを使用してシステムを導入、監視、および管理できます。また、以下の方法で、RMM ツールを使用できます。

- MSIパッケージを展開し、RMMツールを介してシステムを監視し、ポータルを介してシステムを管理します。
- ポータルを介してシステムを導入および管理し、RMM ツールを介してシステムを監視します。

注: システムの管理は、ポータルを通してのみ可能です。



5.6.1 Kaseya RMM との連携 (Windows)

管理方法の説明 WithSecure Elements EPP for Computersそしてその WithSecure Elements EPP for Servers Kaseya ポータルを使用してソフトウェアをインストールします。

監視と管理を簡素化するために WithSecure Elements EPP for Computersそして WithSecure Elements EPP for Servers Kaseya ポータルから、事前に作成された次のエージェント プロシージャ セットを使用できます。https://download.withsecure.com/PSB/RMM/Kaseya/Kaseya_F-Secure.xml

Agent Procedure モジュールに移動して、`Kaseya_F-Secure.xml`ファイルを Kaseya ポータルにインポートする必要があります。それから「Manage Procedures」セクションの下にある「Schedule / Create」ページを選択します。「Shared」フォルダを右クリックしてコンテキスト メニューから[Import Folder/Procedure]を選択すると、アップロードするXMLファイルを指定できます。次のAgent Procedure が利用可能になります。

注 : ニーズに応じて、Kaseya の標準的な方法を使用して、Procedure (手順) の一部または全部をスケジュールすることができます。

CheckProductInstalled 検出する WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversソフトウェアがインストールされていない場合は、警告が発行されます。このプロシージャは、他のすべてのプロシージャによって呼び出されます。これは、他のすべてのプロシージャが機能するには製品のインストールが必要であるためです。

CheckWmiProviderEnabled WMI プロバイダ モジュールが有効になっているか検出します。モジュールが無効の場合、警告が発行されます。WMI プロバイダ モジュールが機能するために必要であるため、このプロシージャは他のすべてのプロシージャ(CheckProductInstalledを除く) によって呼び出されます。

注 : WMIプロバイダーをオンにするには、WithSecure Elements EPPプロフィール設定のポータル。

CheckLicenseStatus 製品のサブスクリプション ステータスを確認します。サブスクリプションが失効しているか、インストールされていない場合、警告が発行されます。

CheckDefinitionsAreUpToDate ウイルス対策定義が更新されているか確認します。7日以上経過している場合、警告が発行されます。インターネット接続または他の障害に関する問題が発生している可能性があります。

CheckConnectivityTo ManagementPortal 接続性をチェックします WithSecure Elements EPPポータル。ポータルへの接続が24時間以上前に成功した場合、アラートが発行されます。これは、インターネット接続の問題またはその他の障害を示している可能性があります。

RunFullComputerScan フル コンピュータ スキャンを実行します。感染したオブジェクトが検出されると、警告が発行されます。

CheckRealTimeScanning リアルタイム スキャンが有効になっているか確認します。無効の場合、警告が発行されます。

CheckDeepGuard ディープガードモジュールが有効になっているか確認します。無効の場合、警告が発行されます。

CheckFirewall ファイアウォール モジュールが有効になっているか確認します。無効の場合、警告が発行されます。

CheckBrowsingProtection ブラウザ保護モジュールが有効になっているか確認します。無効の場合、警告が発行されます。

CheckSoftwareUpdater ソフトウェア アップデーター モジュールが有効になっているか確認します。無効の場合、警告が発行されます。

5.6.2 Kaseya RMM との連携 (Mac)

管理方法の説明 WithSecure Elements EPP for Computers (Mac) Kaseya ポータルを使用するソフトウェア。

Kaseya エージェントをリモート コンピュータに手動でインストールするには

1. Kaseya ポータルにログインします。
2. **エージェント** > **パッケージ** > **パッケージを管理** を選択して、エージェント パッケージをダウンロードします。

   注： Macintosh エージェント インストール パッケージのフル ファイル名は `KcsSetup.app` です。パッケージは、Agent と言うフォルダにある `KcsSetup.app` を含む `KcsSetup.zip` としてダウンロードされます。

3. `KcsSetup.zip` ファイルを展開するために選択して、Agent フォルダを開いて `KcsSetup.app` ファイルを実行します。
4. インストールするには WithSecure Elements EPP for Computers (Mac) ソフトウェアをインストールするには、オフライン PKG パッケージ (ファイル名にライセンス キーが埋め込まれている) をアップロードし、エージェント プロシージャを作成して、リモート デバイスにアプリをインストールします。次の手順を実行します。
   a) エージェント手順モジュールにナビゲートして、PKG ファイルをアップロードします。
   b) **Schedule/Create (スケジュール/作成)** > **Manage Files (ファイルの管理)**を選択します。
   c) サーバ上のファイルをアップロードします。

      注： サーバに保存されているファイルはスクリプトを介してエージェントに送信できます。

   d) 新しいエージェント手順を作成するには、**Agent Procedures (エージェント手順)** > **Schedule/Create (スケジュール/作成)** > **New Procedure (新規手順)** を選択します。

      注： Kaseya が提供する OS X 用のエージェント手順モジュールは限られています。

      注： `writeFile` モジュールを使用して PKG ファイルをリモート マシンの場所に書き込みできます。パッケージをインストールするには、`installPKG` モジュールを使用してください。例:

      ```
      writeFile(“F-Secure_PSB_Mac_Installer[License key].pkg”, “/tmp/ F-Secure_PSB_Mac_Installer[License key].pkg”, “Mac OS X”, “Halt on Fail”)
      installPKG (“/tmp/ F-Secure_PSB_Mac_Installer[License key].pkg”, "Mac OS X”, “Halt on Fail”)
      ```

   e) エージェント手順を実行またはスケジュールするには、エージェント手順のリストから新しく作成したエージェント手順を選択します。次に、エージェント手順をスケジュールする、または実行するターゲット デバイスを選択します。

モニタリング用のエージェント手順をインポートする

WithSecure リモート クライアントが Kaseya RMM ポータルにステータスを報告する方法を説明します。

監視を簡素化するために WithSecure Elements EPP for Computers (Mac) Kaseya ポータルから、事前に作成されたエージェント プロシージャのセットを含む xml ファイルをインポートできます。xml ファイルは次のリンクから入手できます。Kaseya_F-Secure_Mac_プロシージャ.xml

エージェント手順をインポートするには

1. エージェント手順モジュールに移動して、 **Kaseya_F-Secure_Mac_Procedures.xml** ファイルを Kaseya ポータルにインポートします。
2. [**手順の管理**] で [**スケジュール/作成**] を選択します。
3. [**共有**] フォルダを右クリックします。

4. メニューから [フォルダ/手順のインポート] を選択して、アップロードする XML ファイルを指定します。

次のエージェント手順を使用できます。

注 : 必要に応じて、Kaseya の標準的な方法を使用して、Procedure (手順) の一部または全部をスケジュールすることができます。

- ***Mac**にインストールされている製品を確認する*- 検出する WithSecure Elements EPP for Computers (Mac)ソフトウェアがインストールされていない場合は、警告が発行されます。このプロシージャは、他のすべてのプロシージャによって呼び出されます。これは、他のすべてのプロシージャが機能するには製品のインストールが必要であるためです。
- ***Mac** 向けライセンス有効性チェック*- 製品のサブスクリプション ステータスを確認します。サブスクリプションの有効期限が切れているか、インストールされていない場合は、アラートが発行されます。
- ***CheckRealTimeScanningForMac*** - リアルタイムスキャンがオンになっているかどうかを確認します。オフになっている場合は、アラートが発行されます。
- ***Mac**向けファイアウォールの確認*- ファイアウォール モジュールがオンになっているかどうかを確認します。オフになっている場合は、アラートが発行されます。
- ***CheckDatabaseUptoDateforMac*** - ウイルス対策定義が最新かどうかを確認します。定義が 7 日以上古い場合は、警告が発行されます。これは、インターネット接続の問題またはその他の障害を示している可能性があります。
- ***Mac**のブラウジング保護を確認する*-ブラウジング保護モジュールがオンになっているかどうかを確認します。オフになっている場合は、警告が発行されます。

5.6.3 Kaseya RMM との連携 (Linux)

Kaseyaポータルを使用して、WithSecure Linux Protectionを管理する方法について説明します。

インストールと監視を簡素化するために WithSecure Linux ProtectionKaseya ポータルを使用すると、事前に作成された次のエージェント プロシージャ セットを使用できます。
https://download.withsecure.com/PSB/RMM/Kaseya/Kaseya_F-Secure_Linux_Procedures.xml。

エージェント手順をインポートする

インポート方法の説明 WithSecure Linux ProtectionKaseya ポータルを使用したインストールおよび監視手順。

エージェント手順をインポートするには

1. Kaseya ポータルにログインします。
2. [エージェント手順] モジュールを開きます。
3. [手順の管理] で [スケジュール/作成] を選択します。
4. 右側のペインで、[共有] を右クリックします。
5. 開いたメニューから、[フォルダ/手順をインポート] を選択して、アップロードするXMLファイル `KaseyaF-SecureLinuxProcedures.xml`を指定します。

エージェント手順

WithSecureリモートクライアントのステータスを確認し、KaseyaRMMポータルに報告するために、次のエージェント手順を使用できます。

- ***CheckProductInstalledForLinux*** - WithSecure Linux Protectionソフトウェアがインストールされているか検出します。製品がインストールされていない場合、警告が発行されます。この手順は、機能させるために製品のインストールが必要なため、他のすべての手順によって呼び出されます。
- ***CheckLicenseValidForLinux*** - 製品のサブスクリプションステータスを確認します。製品の電源がオフになると、アラートが発行されます。サブスクリプションの有効期限が切れているか、インストールされていない場合、アラートが発行されます。機能チェックを動作させるために製品をアクティブにする必要があるため、この手順は他のすべての手順`CheckProductInstalledForLinux`を除くによって呼び出されます。
- ***CheckRealTimeScanningForLinux*** - リアルタイム スキャンが有効になっているか確認します。無効の場合、警告が発行されます。

- ***CheckIntegrityCheckingForLinux*** - 完全性検査がオンになっているかどうかをチェックします。オフの場合、アラートが発行されます。
- ***CheckDatabaseUpToDateForLinux*** - ウイルス対策定義が更新されているか確認します。7日以上経過している場合、警告が発行されます。インターネット接続または他の障害に関する問題が発生している可能性があります。

注： 必要に応じて、Kaseya の標準的な方法を使用して、Procedure (手順) の一部または全部をスケジュールすることができます。

Kaseyaエージェントをリモートコンピュータにインストールする

ここでは、Kaseyaエージェントをリモートコンピュータにインストールする方法について説明します。

Kaseyaエージェントをインストールするには

1. Kaseyaポータルで、**エージェント** > **パッケージ** > **パッケージを管理** を選択して、エージェントパッケージ`KcsSetup.sh`をダウンロードします。
2. ダウンロードしたファイルを実行します。

WithSecure Linux Protectionをインストールする

Kaseyaポータルを使用して、WithSecure Linux Protectionをインストールする方法について説明します。

WithSecure Linux Protectionをインストールするには

1. WithSecure Elements Endpoint Protectionポータルで [**ダウンロード**] ページを開きます。
2. Linuxで、[**Generic**] を選択して、`f-secure-linuxsecurity-installer.tar`アーカイブをダウンロードします。
3. tarアーカイブから`f-secure-linuxsecurity-installer`ファイルを抽出します。
4. リモートデバイスにソフトウェアをインストールするためのエージェント手順を作成するには

   注： Kaseyaが提供するLinux用のエージェント手順モジュールは限られています。

   a) [**エージェント手順**] モジュールを開き、抽出したインストーラファイルをKaseyaポータルにアップロードします。
   b) **Schedule/Create (スケジュール/作成)** > **Manage Files (ファイルの管理)** を選択します。
   c) サーバ上のファイルをアップロードします。

      注： サーバに保存されているファイルはスクリプトを介してエージェントに送信できます。

   d) ソフトウェアのインストール手順に、サンプルエージェントの手順を参考にします。

      `Linux Protection`をインストールする 使用前に編集 手順を編集して、WithSecure Linux Protectionのサブスクリプションキーを含め、アップロードされたインストーラへのパスを修正します。

      注： 実際に製品をインストールする前に、リモートデバイスにWIthSecure Linux Protectionの依存関係ディストリビューションに固有がインストールされていることを確認してください。`executeShellCommand`または`executeShellCommandToVariable`ステートメントを使用して、必要なパッケージのインストールをサンプル手順に追加できます。詳細については、こちらを参照してください。

   e) エージェント手順を実行またはスケジュールするには、最初に使用可能な手順のリストからエージェント手順を選択し、次にターゲットデバイスを選択して、[**エージェント手順のスケジュール**] または [**今すぐ実行**] を選択します。

5.6.4 SolarWinds MSP RMM との連携 (Windows)

管理できるのは WithSecure Elements EPP for Computersそして WithSecure Elements EPP for Servers SolarWinds MSP を使用したソフトウェア。

詳細については、SolarWinds MSP の公式ドキュメントを参照してください。
https://secure.n-able.com/webhelp/NC_11-0-0_en/Content/Help_20/Services/FSecure/Services_FSecureCentralMgmt.htm
/
https://secure.n-able.com/webhelp/NC_11-0-0_en/Content/Help_20/Automation/Policies/F_Secure/pol_FSecure_AV_Protection.htm

5.6.5 SolarWinds MSP RMM との連携 (Mac)

管理方法の説明WithSecure Elements EPP for Computers (Mac) SolarWinds MSP を使用するソフトウェア。

MSP N-Centralを使用してリモートデバイスに製品をインストールする

1. MSP N-Central にログインします。
2. macOS エージェントをリモート macOS デバイスにダウンロードします。

   注: デバイスが「**すべてのデバイス**」ビューで表示されていることを確認して、[**リモート制御**] オプションが選択したリモート デバイスで有効であることを確認してください。

   注: また、次のものも必要になります。
   - 製品のサブスクリプション キー
   - パッケージ WithSecure Elements Agent for Computers(Mac)、ローカルまたはネットワーク共有

3. 使用 [**リモコン**]コピーする WithSecure Elements Agent for Computers(Mac) パッケージをリモートデバイスに送信します。
4. リモート デバイスで install_mac_client.sh スクリプトを実行するために Mac スクリプト タスクを実行します。

   注: スクリプトを実行するには管理者権限が必要です。このスクリプトは、リモートデバイスのパッケージパス、パッケージ名、および製品のサブスクリプションキーの各コマンドライン引数を受け入れます。

   ```
   sh install_mac_client.sh -p
   /Users/Shared/F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg -n
   F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg -k
   4T16-E2VW-U2U9-J5V8-9Z0F
   ```

レポート用のカスタム サービスをインポートする

WithSecure リモート クライアントが SolarWind RMM ポータルにステータスを報告する方法を説明します。

カスタム サービスをインポートするには

1. 必ず WithSecure Elements EPP for Computers (Mac) ソフトウェアがリモート コンピュータにインストールされます (詳細については、前のセクションを参照してください)。
2. **管理** > **サービス管理** > **カスタム サービス** > **インポート** の順に選択します。
3. レポート用のカスタム サービスを含むすべての XML ファイルを参照してインポートします。

   注: xml ファイルは次のリンクから入手できます。
   https://download.withsecure.com/PSB/RMM/Solarwinds/Solarwind_F-Secure_Custom_services_for_Mac.

4. モニタリング用のカスタム サービスを追加するには
   a) **ビュー** > **すべてのデバイス** を開き、カスタム サービスをモニタリングするデバイスを選択します。
   b) **デバイスの詳細** > **モニタリング** > **追加** の順に選択します。
   インポートしたすべてのカスタム サービスを表示できます。

c) 次の各カスタム サービスを追加して、変更を適用します。

サービスが更新され、リモート マシン上の WithSecure クライアントの個々の設定のレポートが表示されます。各設定の状態に基づいて、レポートには、期待される動作と一致しない場合は失敗または警告が表示されます。

Mac コンピュータで利用できるカスタム サービス

要件に応じて、関連するカスタム サービスをインポートできます。

- WithSecure アンチウイルス データベース ステータス (Mac用) - データベースのステータスを表示します。データベースが最新でない場合、警告が表示されます。
- WithSecure アンチウイルス ファイアウォール管理 (Mac 用) - システム ファイアウォールのステータスを表示します。ファイアウォールがオフの場合、警告が表示されます。
- WithSecure アンチウイルス保護 (Mac 用) ステータス - リアルタイム スキャンのステータスを表示します。リアルタイム スキャンがオフの場合、エラーが表示されます。
- WithSecure アンチウイルス Safari 拡張機能 (Mac 用) - Safari 拡張機能がオンになっている場合に表示されます。オフにすると、警告が表示されます。
- WithSecure アンチウイルス ウイルス保護 (Mac 用) - ウイルス保護のステータスを表示します (「ライセンスの有効期限が切れました」、「OASが無効」、「OASエラー」、「古いアップデート」など)。
- WithSecure ブラウザ保護 (Mac 用) ステータス - ブラウザ保護のステータスを表示します。オフにすると、警告が表示されます。

5.6.6 SolarWinds MSP RMM との連携 (Linux)

管理方法の説明 WithSecure Linux ProtectionSolarWinds MSP を使用します。

Linuxデバイスとそのステータスの監視 WithSecure Linux Protectionこのソフトウェアを使用するには、SolarWindsのLinuxエージェントがデバイス上で動作している必要があります。インストール手順はLinuxエージェントセクションのインストールN-Central ユーザー ガイドの。

注 : インストールの自動化 WithSecure Linux ProtectionMSP N-CentralではLinuxデバイスのサポートが限られているため、リモートデバイスにソフトウェアをインストールすることはできません。WithSecure Linux Protectionソフトウェアは利用可能ここ。

ソフトウェアをインストールした後、rootユーザとして次のコマンドを実行して、RMMアップストリームレポートサービスをオンにします。

```
/opt/f-secure/linuxsecurity/bin/setup-rmmd.sh install
```

注 : サービスが不要になった場合は、アンインストールオプションを使用して削除できます。

レポート用のカスタム サービスをインポートする

WithSecure リモート クライアントのステータスを SolarWinds RMM ポータルに報告する方法について説明します。

カスタムサービスをインポートするには

1. インストールされていることを確認してください WithSecure Linux Protectionリモート コンピューターにソフトウェアをインストールし、rmmd サービスをオンにします (詳細については、前のセクションを参照してください)。
2. **管理** > **サービス管理** > **カスタム サービス** > **インポート** の順に選択します。
3. レポート用のカスタム サービスを含むすべての XML ファイルを参照してインポートします。

   注 : xml ファイルは次のリンクから入手できます。
   https://download.withsecure.com/PSB/RMM/Solarwinds/SolarWinds_F-Secure_Custom_Services_for_Lin

4. モニタリング用のカスタム サービスを追加するには

a) **ビュー** > **すべてのデバイス** を開き、カスタム サービスをモニタリングするデバイスを選択します。
b) **デバイスの詳細** > **モニタリング** > **追加** の順に選択します。
インポートしたすべてのカスタム サービスを表示できます。
c) 次の各カスタム サービスを追加して、変更を適用します。

サービスが更新され、リモート マシン上の WithSecure クライアントの個々の設定のレポートが表示されます。各設定の状態に基づいて、期待される動作と一致しない場合は、レポートに失敗または警告が表示されます。

利用可能なカスタムサービス

要件に応じて、監視用の関連するカスタムサービスを追加できます。

Linuxコンピュータで利用可能なカスタムサービスは次のとおりです。

- WithSecureアンチウイルスデータベースのステータス(Mac用)-データベースのステータスを表示します。データベースが最新でない場合、警告が表示されます。
- WithSecureアンチウイルス Linux用 完全性チェックの保護ステータス-完全性チェックのステータスを表示します。完全性チェックがオフの場合、エラーが表示されます。

  注: 整合性チェック用にファイルパスが追加されていない場合も、この機能はオフになっていると見なされます。

- WithSecureアンチウイルス Linux用 のライセンスステータス-製品ライセンスのステータスを表示します。ライセンスが無効な場合は、エラーが表示されます。
- WithSecure AV製品 Linux用 のステータス - 製品のマスタースイッチのステータスを表示します。製品の電源が切れている場合は、エラーが表示されます。
- WithSecureリアルタイムアンチウイルス保護 Linux用 のステータス - リアルタイム スキャンのステータスを表示します。リアルタイム スキャンがオフの場合、エラーが表示されます。

  注: スキャン用のディレクトリが含まれていない場合も、この機能はオフになっていると見なされます。

5.6.7 Datto RMM との連携 (Windows)

Datto プラットフォームを使用してWithSecure Elements EPP for Computersをインストールおよび管理するために使用できるコンポーネントに関する情報。

Datto のオンライン コンポーネント リポジトリ (ComStore) には、次の WithSecure コンポーネントが含まれています。

WithSecure Elements Agent [WIN]で展開する	このスクリプト コンポーネントを使用して、WithSecure Elements EPP for Computersを対象のコンピュータにインストールしてください。有効なライセンスキーコードを提供し、実行時にリストから正しい地域を選択する必要があります。
WithSecure Elements Agentのタスク[WIN]	このスクリプト コンポーネントを使用して、WithSecure Elements EPP for Computersがインストールされているエンドポイントでタスクを実行してください。使用可能なタスクには、完全スキャンとセキュリティ アップデートのインストール (重大なアップデート、重要なアップデート、またはすべてのアップデート) が含まれます。
WithSecure Elements Agentモニター[WIN]	この監視コンポーネントを使用して、現在のステータスを確認してください。WithSecure Elements EPP for Computersがインストールされているか、現在のライセンスステータス、さまざまなセキュリティ コンポーネントのステータス、パターンファイルの有効期間、および不足している重大なアップデートを確認できます。各項目をオンまたはオフにできます。

すべてのコンポーネントの詳細については、Datto RMM 管理ポータルの説明を参照してください。すべての構成変数にはヘルプ テキストが含まれています。

コンポーネントの最新バージョンは、次のリンクからも入手できます
https://download.withsecure.com/PSB/RMM/Datto/Components_For_Datto_RMM.zip

5.6.8 Datto RMM との連携 (Mac)

インストールと管理方法の説明 WithSecure Computer Protection for MacDatto プラットフォームを使用します。

WithSecure Elements EPP for Computers (Mac)をインストールする

インストール方法の説明 WithSecure Elements EPP for Computers (Mac)Datto プラットフォームを使用します。

製品をインストールするには

1. Datto ポータルの [**コンポーネント**] メニューの [アクション] で、[**新しいコンポーネント**] を選択します。
2. [**カテゴリ**] ドロップダウンメニューから、[**アプリケーション**] を選択します。
3. 名前フィールドに、[**Secure Elements EPP for Computers (Mac) を使用**]。
4. [**説明**] ボックスに、アプリケーションの説明 (オプション) を入力し、[**保存**] を選択します。
   [**コンポーネント アプリケーション**] ページが開きます。
5. [**インストールコマンド**] ドロップダウン メニューから、[**Unix (Linux、Mac OSX)**] を選択し、テキスト フィールドに次のファイルのスクリプトを入力します:
   deploy_f-secure_computer_protection_Mac.sh
6. 選択する [**ファイルを追加...**]そして、[**Secure Elements EPP for Computers (Mac) を使用**]パッケージ名にキーが埋め込まれたインストーラー。
7. [**保存**] を選択します。
   インストーラ ファイルが新しいコンポーネントにアップロードされます。
8. [**サイト**] メニューから [**サイト**] を選択し、[マネージド] または [オンデマンド] の下で [**デバイス**] を選択します。
9. [**アクション**] で、[**ジョブのスケジュール**] を選択します。
10. スケジュール ジョブの名前を入力します。
11. [**スケジュール**] 、[**即時**] を選択します。

    注 : 別のオプションを選択するには、[**クリックして変更...**] を選択します。

12. 次に、[**コンポーネント名**] で、[**コンポーネントを追加**] を選択します。
    開いたページに、作成したコンポーネントが表示されます。
13. コンポーネントを選択し、[**保存**] を選択します。

製品を監視する

監視方法の説明 WithSecure Elements EPP for Computers (Mac)Datto プラットフォームを使用します。

製品を監視するには

1. [**コンポーネント**] メニューの [アクション] で、[**新しいコンポーネント**] を選択します。
2. [**カテゴリー**] の [**コンポーネント**] メニュー から、[**デバイスのモニタリング**] を選択します。
3. 名前フィールドに、[**コンピューター用のSecure Elements EPP (Mac)**]。
4. [**説明**] ボックスに、説明 (オプション) を入力し、[**保存**] を選択します。
   [**コンポーネント モニター**] ページが開きます。
5. [**スクリプト**] ドロップダウン メニューから、[**Unix (Linux、Mac OSX)**] を選択し、テキスト フィールドに次のファイルのスクリプトを入力します: monitor_f-secure_computer_protection_Mac.sh
6. [**保存**] を選択します。
7. [**サイト**] メニューから [**マネージド**] または [**オンデマンド**] の下で [**サイト**] を選択します。
8. 開いたページで、監視するデバイスを選択します。
9. ≡ を選択してから、[**監視**] を選択します。
10. ページの右側で、[**モニタリング**] オプションを選択します。
    「デバイス」ページが開きます。
11. [**モニタリングの追加...**] を選択します。

12. [モニターの追加] ページで、ドロップダウン メニューから [コンポーネント モニター] を選択し、[次へ] を選択します。
13. [コンポーネント モニターの実行] のドロップダウン メニューを実行し、作成したばかりのコンポーネントを選択し、次へ > 次へ 選択します。
    警告は、リアルタイムスキャン、ファイアウォール、ブラウザ保護など、コンポーネントの1つがデバイスでオフになったときに生成されます。

5.6.9 Datto RMM との連携 (Linux)

インストールと管理方法の説明 WithSecure Linux ProtectionDatto プラットフォームを使用します。

WithSecure Linux Protectionをインストールする

インストール方法の説明 WithSecure Linux ProtectionDatto プラットフォームを使用します。

WithSecure Linux Protectionをインストールするには

1. 最新のジェネリックをダウンロード WithSecure Linux Protectionソフトウェアインストーラーから WithSecure Elements Endpoint Protectionポータル。
2. Datto ポータルの [コンポーネント] メニューの [アクション] で、[新しいコンポーネント] を選択します。
3. [カテゴリ] ドロップダウンメニューから、[アプリケーション] を選択します。
4. 名前フィールドに、[セキュアな Linux 保護を導入する [LIN]]。
5. [説明] ボックスに、アプリケーションの説明 (オプション) を入力し、[保存] を選択します。
   [コンポーネント アプリケーション] ページが開きます。
6. [インストールコマンド] ドロップダウン メニューから、[Unix (Linux、Mac OSX)] を選択し、テキスト フィールドに次のファイルのスクリプトを入力します:
   `deploy_f-secure_linux_protection.sh`

   注 : デプロイメントスクリプトは以下からダウンロードできます。
   https://download.withsecure.com/PSB/RMM/Datto/deploy_f-secure_linux_protection.sh。
7. 必要に応じて、実際のインストール手順の前に依存関係のインストールを含めるようにスクリプトを編集します。必要な依存関係を確認します。ここ。
8. スクリプトの有効なサブスクリプションキーを編集します。
9. 選択する [ファイルを追加...]そして、[セキュアなLinux保護]インストーラ。
10. [保存] を選択します。
    インストーラ ファイルが新しいコンポーネントにアップロードされます。
11. [サイト] メニューの [管理対象] で [デバイス] を選択します。
12. インストールするデバイスを確認してください。
13. ジョブをスケジュールするには、⚙ を選択します。
    a) スケジュール ジョブの名前を入力します。
    b) [スケジュール] 、[即時] を選択します。

       注 : 別のオプションを選択するには、[クリックして変更...] を選択します。
    c) [コンポーネント名] で、[コンポーネントを追加] を選択します。
       開いたページに、作成したコンポーネントが表示されます。
    d) コンポーネントを選択し、[保存] を選択します。
    e) [保存] を選択して、ジョブを開始します。

WithSecure Linux Protectionを監視する

監視方法の説明 WithSecure Linux ProtectionDatto プラットフォームを使用します。

WithSecure Linux Protectionを監視するには

1. 次のリンクから、事前に作成された Linux 監視コンポーネントをダウンロードします。
   https://download.withsecure.com/PSB/RMM/Datto/F-Secure_Linux_Protection_Monitor_LIN.cpt

次のコンポーネントが含まれています。F-Secure Linux Protection Monitor [LIN]この監視コンポーネントを使用して、現在のステータスとWithSecure Linux Protectionがインストールされ、有効になっているかどうかを確認できます。また、現在のライセンス ステータス、さまざまな保護コンポーネントのステータス、ウイルス対策定義の有効期限も確認できます。個々のチェックをオンまたはオフにすることができます。

注: コンポーネントの詳細については、DattoRMM管理ポータルの説明を参照してください。

すべての構成変数には、ヘルプテキストが含まれています。

2. Dattoポータルの [**コンポーネント**] ページにコンポーネントファイル.cpt をインポートします。
3. インポートしたコンポーネントを使用して、次のようにコンポーネントモニターを作成します。
   a) [サイト] メニューの [管理対象] で [**デバイス**] を選択します。
   b) 開いたページで、監視するデバイスを選択します。
   c) アイコンを選択してから、[**監視**] を選択します。
   d) ページの右側で、[**モニタリング**] オプションを選択します。[デバイス] ページを開きます。
   e) [**モニタリングの追加...**] を選択します。
   f) [**モニターの追加**] ページで、ドロップダウン メニューから [**コンポーネント モニター**] を選択し、[**次へ**] を選択します。
   g) [コンポーネント モニターの実行] のドロップダウン メニューを実行し、作成したばかりのコンポーネントを選択します。
   h) 必要に応じてパラメータを調整し、**次へ** > **次へ** > **次へ**を選択して、作成を完了します。

      アラートは、デバイスでコンポーネントの1つがオフになっている場合に生成されます。たとえば、リアルタイムスキャンや整合性チェックなどです。最初に失敗したチェックはアラートを生成します。1つのモニターから同じデバイスに対して新しいアラートが生成される前に、アラートを解決する必要があります。

第 章
6

登録したデバイスでレポートを表示する

トピック :

[**レポート**] ページでは、WithSecure Elementsに登録しているコンピュータとモバイル デバイスに関するセキュリティ ステータスを監視するための指標データが記録されます。

[**レポート**] セクションでは、次の操作を実行および表示できます。

- ウィジェットを追加して独自のレポートを作成する
- 指定したメールアドレスに配信されるアラートとスケジュールされたカスタムメールレポートを構成する
- スケジュールされたEndpoint Detection and Responsレポートを構成する
- 感染情報と登録したデバイスの保護ステータスに関する統計情報を表示する
- クライアント・バージョン、メーカー、オペレーティング・システム、ドライブ暗号化ステータス、その他の変数によるデバイスの統計を表示する
- 上位の感染、感染によってブロックされた上位のコンピュータ、これまでに検出および処理された感染など、セキュリティイベントの詳細を表示します。
- ソフトウェアアップデートに関する統計を表示する

6.1 セキュリティ概要

[レポート] の [デバイス] タブのグラフには、感染に関する情報と登録したデバイスの保護ステータスが表示されます。

チャートには次の情報が表示されます。

- [コンピュータの保護ステータス] - 保護されていてセキュリティに影響する問題がないコンピュータ、重要でない問題があるコンピュータ、重要な問題があるデバイス、および2週間以上サーバーに接続していないコンピュータの数を示します。
- クライアントバージョン別のWindowsデバイス - インストールされているクライアントバージョンに基づいてWindowsデバイスの数を表示します
- クライアントバージョン別のMacデバイス-インストールされているクライアントバージョンに基づいてMacデバイスの数を表示します
- クライアントバージョン別のLinuxデバイス - インストールされているクライアントバージョンに基づいてLinuxデバイスの数を表示します
- クライアントバージョン別のモバイルデバイス-インストールされているクライアントバージョンに基づいてモバイルデバイスの数を表示します
- クライアントバージョン別のConnectorデバイス - インストールされているクライアントバージョンに基づいてConnectorデバイスの数を表示します
- メーカー別の最も人気のあるコンピューター-コンピュータのメーカーに基づくコンピューターの数
- オペレーティングシステム別のコンピューター-オペレーティングシステムに基づくコンピューターの数
- オペレーティングシステム別のモバイルデバイス-オペレーティングシステムに基づくモバイルデバイスの数
- パスワードポリシー最小長 - デバイスに設定されているパスワードの長さに基づくデバイスの数
- ドライブ暗号化ステータス別のコンピューター- ドライブの暗号化ステータス有効または無効に基づくコンピューターの数
- コンピューターのデフォルトのブラウザ-コンピューターで使用されているデフォルトのブラウザに基づくコンピューターの数
- アカウント ロックアウトしきい値別のコンピューター - アカウントロックアウトしきい値が構成されているコンピュータと構成されていないコンピュータの数

すべてのチャートは、過去28日間のアクティビティの要約を提供します。

6.1.1 ステータスチャートを表示する

[レポート]セクションには、[デバイス]、[セキュリティイベント]、[ソフトウェアアップデート] タブの保護ステータスやその他のグラフが表示されます。

保護ステータス チャートを表示するには

1. サイドバーから [レポート] を選択します。
   [レポート] ページが開きます。
2. [デバイス] タブを選択します。
   コンピュータの保護ステータスを示すグラフが表示されます。
3. 全体のセキュリティ情報、感染・脅威の一覧、ソフトウェア アップデートの一覧を表示するサマリ レポートをエクスポートできます。次の方法でサマリをエクスポートできます。

   注: ソフトウェア アップデーター機能が無効な場合、サマリにアップデートは表示されません。

   a) レポートの横にある アイコンをクリックします。
   メニューが表示されます。
   b) メニューから [サマリ レポートを次のユーザに送る...] をクリックします。
   システムがログインしているユーザのメール アドレスへサマリ レポートをエクスポート・送信します。

6.1.2 レポートをエクスポートする

コンピュータ、モバイルデバイス、適用されているソフトウェアアップデートに関するレポートをCSVファイルにエクスポートすることができます。

また、*スコープセレクタ*を使用して企業アカウントを表示したり、企業アカウントに関連しているデバイスと適用されているソフトウェア アップデートのレポートをエクスポートしたりできます。

1. サイドバーから [**デバイス**] を選択します。
2.  を選択します。
   メニューが開きます。
3. 次のいずれかのレポートを選択します。
   - 検出したコンピュータ レポートをエクスポート

     注 : たとえば、[プロファイル フィルター] ドロップダウン メニューから、プロファイル フィルターオプションのいずれかを選択し、選択したプロファイルが割り当てられているデバイスの表示を選択できます。 [デバイス] ページで、[**検出したコンピュータ レポートをエクスポートする**] オプションを選択して、フィルター (または検索) 結果に基づいて検出したデバイスのみをエクスポートできます。
   - コンピュータ レポートをすべてエクスポート
   - ソフトウェア アップデート操作をすべてエクスポート
   - モバイル レポートをエクスポート

   レポートはブラウザのデフォルトのダウンロード場所にダウンロードされます。その後、レポートを開くか保存することができます。

6.2 ライセンスの使用量レポート

[**サブスクリプションの使用量**] レポートは登録しているデバイス上のElements EPP製品が使用しているサブスクリプションの概要を提供します。

注: ライセンスの使用量レポートは月額ライセンスのユーザにのみ表示されます。月額ライセンスを有効にする場合、WithSecureの担当者にお問い合わせください。

6.2.1 ライセンスの使用量レポートを表示・エクスポートする

特定の企業に対してWithSecure Elements Endpoint Protectionソフトウェアのライセンスを使用しているデバイスの数をまとめたライセンス使用量レポートを表示・ダウンロードできます。

レポートを表示・ダウンロードするには

次のいずれかを実行します。

- *スコープセレクタ*が特定の企業を表示している場合、**レポート** > **ライセンスの使用量** を開きます。[**エクスポート**]ボタンおよび企業のライセンス使用量を示すグラフ形式のレポートが表示されます。[**エクスポート**] ボタンをクリックすると CSV ファイルがダウンロードされます。
- スコープ セレクタが **レポート** > **ライセンスの使用量** を開きます。[**ダウンロード**] ボタンが表示されます。[**ダウンロード**] ボタンをクリックするとすべての顧客企業の CSV ファイルを含めた ZIP ファイルがダウンロードされます。

注 : **管理** > **サブスクリプション**の下で、ソリューションプロバイダー ユーザはすべての企業と使用中のサブスクリプションを表示するサブスクリプションレポートを確認できます。

6.3 セキュリティイベントレポート

[レポート] ページの [セキュリティイベント] タブのグラフには、セキュリティイベントの概要が示されています。

チャートには次の情報が表示されます。

- [感染をブロックした上位コンピュータ] - 感染をブロックした上位1コンピュータの名前、および過去30日間にブロックされた感染の総数。
- [上位の感染] - 過去30日間の上位10件の感染者の名前と数。感染の名前を選択して、WithSecure Labs Threat Descriptionsデータベースからの感染に関する詳細を表示するWebブラウザページを開くことができます。バーを選択すると、[セキュリティイベント] ページを開くことができます。
- [リアルタイムスキャンで処理された感染] - リアルタイムスキャンで処理された1日あたりの感染数、および過去30日間に処理された感染の総数。
- [手動・スケジュールスキャンで処理された感染] - 手動・スケジュールスキャンで処理された1日あたりの感染数、および過去30日間に処理された感染の総数。
- [改ざんの試みが最も多いコンピューター] - 過去30日間に改ざん試行のターゲットに最もなったコンピュータの名前。
- [レピュテーションベースのブラウジングによって最もブロックされたWebサイト] - 過去30日間に最もブロックされたWebサイトのURLと、レピュテーションベースのブラウジングによってブロックされた回数。
- [適用回数が最も多いアプリケーション制御ルール] - アプリケーションを最も多くブロックしたアプリケーション制御ルールと、過去30日間にそのルールに基づいてアプリケーションがブロックされた回数。
- [ブロックされたWebサイトのアクセスが最も多いコンピューター] - 上位のコンピューターの名前と、過去30日間にブロックされたWebサイトにアクセスしようとした回数。
- [上位ソース] - セキュリティイベントをトリガーした上位のソースの名前と、過去30日間に各ソースがトリガーしたイベントの数。
- [Webコンテンツ制御 - 最もブロックされたカテゴリ] - 過去30日間に最もブロックされたWebコンテンツカテゴリの名前。
- [DataGuard - 最もブロックされたアプリケーション] - 過去30日間にDataGuardがアクセスを最もブロックしたアプリケーション。
- [デバイス制御 - ルールを最もブロックしたデバイス] -...過去30日間。
- [改ざん防止 - 最も発生したアラートタイプ] -...過去30日間。
- [システムイベント - 最も発生したイベントタイプ] - 過去30日間のタイプ別の上位システムイベントの数。

6.3.1 セキュリティイベントに関するカスタマイズされた電子メールレポートの作成

「レポート」の「電子メール通知とレポート」機能を使用すると、カスタマイズされた電子メール レポートを作成して自動的に送信できます。

カスタマイズされたメールレポートを作成する前に、セキュリティイベントページ。その後、そのビューを電子メール レポートのテンプレートとして使用できます。

カスタム ビューを作成するには:

1. 下 [イベント]、 選択する [セキュリティイベント]。
2. 開く [ビュー]右上隅のドロップダウンメニューをクリックし、システムビューの1つを選択します。
3. 選択する [名前を付けて保存]カスタム ビューの名前を入力します。
4. 選択する [保存]. カスタムビューは、[私の意見]。

カスタム ビューを作成したら、セキュリティ イベントに関する電子メール レポートを作成できるようになります。

1. サイドバーから [レポート] を選択します。
2. 上の レポートページで、[メール通知とレポート]タブ。
3. 選択する [メールレポートを追加]。
   の 新しいメールレポートを追加ペインが開きます。
4. レポートの名前を入力します。
5. から 情報元ドロップダウンメニューで選択 [セキュリティイベント]。
6. から テンプレート ドロップダウンメニューで、以前に作成したテンプレートを選択します。セキュリティイベントページ。
7. レポートに使用する言語を選択します。

8. 下 [**スケジュール**]セキュリティ イベントに関するレポートの頻度は継続的であり、新しいレポートが 10 分ごとに送信されます。

   注： 生成される最初のレポートには、過去 24 時間のデータが表示されます。後続のレポートには、過去 10 分間のデータが表示されます。

9. の [**レポートにコンテンツがある場合にのみ送信**]オプションはデフォルトでオンになっています。オフにすると、イベントがない場合でもレポートを受信します。
10. の中に [**受信者**]ボックスに受信者のメールアドレスを入力します。

    注： 複数のメールアドレスがある場合は、カンマで区切ってください。

6.4 監査ログレポート

監査ログレポートを使用すると、プロファイルに関するイベントを表示およびフィルタリングできます。

監査ログレポートページには、イベントのタイムスタンプ、イベントの説明、およびトランザクション IDが表示されます。

次のイベントを表示できます。

- プロファイルが作成されました
- プロファイルが更新されました

  注： イベントの下にある [**詳細を見る**] を選択すると、プロファイルに設定された新しい値の一覧が表示されます。

- プロファイルが削除されました

また、時間帯でイベントをフィルタリングすることもできます。選択した日付の前後に行われたイベントを表示するように選択できます。

第 章
7

サードパーティのソフトウェアを最新の状態に保つ

トピック :

ネットワーク内の管理対象コンピュータに対するソフトウェア アップデートの管理とインストールを行うことができます。

ソフトウェアの開発ベンダーは、ソフトウェアの改善やセキュリティの問題を解決するためにソフトウェアのアップデートを定期的に発行します。ソフトウェアのアップデートによりセキュリティの脆弱性は解決することがよくあるため、管理対象コンピュータにインストールされているソフトウェアが最新のアップデートを適用していることは重要です。

WithSecure Elementsポータルを使用して、選択したプログラムのソフトウェアアップデートを、アカウントに登録されているコンピュータやモバイル デバイスにインストールできます。セキュリティ アップデートをコンピュータに自動的にインストールするようにプロファイル エディタを設定できます。また、ソフトウェア アップデートのステータスを確認してソフトウェアアップデートを手動でインストールすることも可能です。

注: ソフトウェアアップデーターは、実行中のアプリケーションを更新できません。[**実行中のアプリケーションを強制終了**] オプション[**パッチ管理**]でアップデートを選択したときに開くアクションメニューをオンにして、すべてのソフトウェアアップデートをインストールできることを確認します。

注 : 登録しているデバイスのセキュリティを最善の状態にするためにデバイスが最新のソフトウェア アップデートを導入していることを推奨します。

7.1 適用できるソフトウェアアップデートをすべて表示する

WithSecure Elementsポータルでダウンロードおよびインストールできるソフトウェアアップデートの情報を確認できます。

適用されていないアップデートに加えて、[**パッチ管理**]ページにはインストールログも表示されます。

情報を表示するには

1. 適用されていないアップデートを表示するには
   a) [**環境**] のサイドバー から [**パッチ管理**] を選択します。
   [**パッチ管理**] ページが開きます。
   a) [**適用されていないアップデート**] タブを選択します。
2. インストールログを表示するには
   a) [**環境**] のサイドバー から [**パッチ管理**] を選択します。
   [**パッチ管理**] ページが開きます。
   a) 「**インストールログ**」タブを選択します。

7.2 ソフトウェア アップデートを個別またはカテゴリ別でインストールする

特定のデバイスに対してソフトウェア アップデートをすべて、個別 (ベンダー別に) またはカテゴリ別にインストールすることができます。

注 : ソフトウェア アップデートは「*重大*」、「*重要*」、「*中*」、「*低*」、「***Unclassified***」、「*未分類*」および「*サービスパック*」に分類化されます。

1. 次のいずれかを選択することでアップデートをインストールできます。
   - 利用可能なアップデートをすべてインストールするには、**パッチ管理**ページで、テーブルヘッダーの横にあるチェックボックスを選択します。最初の50ベンダー対して利用可能なアップデートが表示されます。
   - ソフトウェアアップデートを個別にインストールする場合、[**パッチ管理**] ページでインストールするアップデートを選択します。
2. ページの下にあるメニューから [**アップデートするデバイスの選択**] を選択します。

   注 : [**実行中のアプリケーションを強制的に閉じる**] を選択して、インストールが失敗するのを防ぐために実行中のアプリケーションを閉じることができます。

   注 : ドロップダウンメニューから、アップデートをすぐにインストールするか、アップデートをインストールする時間を選択するかを選択できます。これはWindowsデバイスにのみ適用されます。

   [**デバイスの選択**] パネルが開きます。
3. ソフトウェア アップデートをインストールするコンピュータ (複数選択可能) を選択します。
4. [**アップデート**] を選択します。
   アップデートをインストールする確認の通知が選択したデバイスに送られます。

7.3 ソフトウェア アップデートを自動的にインストールする

ネットワーク内の管理対象コンピュータのソフトウェアに対するセキュリティ アップデートを自動的にインストールするようにWithSecure Elements EPPポータルを設定できます。

注 : ソフトウェア アップデートの自動インストールを許可することを推奨します。

注 : Windows 機能の更新とサービス パックが自動的にインストールされることはありません。

セキュリティ アップデートの自動インストールを有効にするには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. 編集するプロファイルを選択します。

   注： プロファイルの変更は作成されたレベルで可能です。

3. [自動タスク] を選択します。
4. [自動化されたタスク] をオンにします。
5. [自動化されたタスクのリスト] で、[タスクを追加] を選択して、以下の操作を行います。
   a) [有効] 列のスイッチがオンになっていることを確認します。
   b) [タイプ] 列のドロップダウンメニューから、次のいずれかのオプションを選択します。
      - 重大なセキュリティアップデートをインストールする
      - 重大で重要なセキュリティアップデートをインストールする
      - すべてのセキュリティアップデートをインストールする
      - すべてのアップデートをインストールする

   c) [スケジュール] 列のドロップダウンメニューから、アップデートをインストールする間隔を選択します⊠例⊠1時間ごと、毎日、平日⊠。また、CRON式を使って独自のスケジュールを作成することもできます。
   d) [説明] 列に、自動化されたタスクの説明を入力します。
   e) [スキップしない] 列のスイッチがオンの場合、アップデートはスケジュールされた時間にインストールされます。スケジュールされた時間にインストールできない場合は、利用可能なときにインストールされます。このスイッチがオフの場合、アップデートはスケジュールされた時間にのみインストールされます。

      注： デフォルトでは、スイッチはオンになっています。

      注： セキュリティ構成 > プロファイル > ソフトウェア アップデーターでは、[新しいアップデートを通知する] オプションをオンにして、ソフトウェアアップデートが利用可能になったときに通知を表示できます。

6. [保存して発行] を選択してポリシーを配信します。

7.3.1 ソフトウェアアップデートを含める/除外する

ソフトウェアアップデーターを自動的に更新する、または更新しないソフトウェアの名前、セキュリティ情報ID、ベンダー名、重大度、およびソフトウェア名を入力できます。

[含める] と [除外] は、管理されているホストによって報告されたアップデートのインストール状況に基づいています。含める場合は、[アップデートを自動的にインストールする] で選択した内容に応じて、重大度に基づいてアップデートがチェックされます。次に、除外されたものを除くすべてのアップデートがインストールされます。

除外は、管理されているホストから報告されたアップデートのインストール状況に基づいています。管理対象ホストが報告するインストールステータスによってアップデートの除外が判断されます。アップデートのインストール開始時に除外されているインストールの確認が行われ、管理者に除外されたアップデートが通知されます。ホストはインストールステータスのみ通知するため、除外されたアップデートは「ソフトウェアアップデート」タブにある一覧からすぐに非表示になりません。

ソフトウェアアップデートを含める/除外するには

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
「プロファイル」ページが開きます。
2. 編集するプロファイルを選択します。

   注： プロファイルの変更は作成されたレベルで可能です。

3. [ソフトウェア アップデート] を選択します。
4. 含める、または除外するソフトウェア アップデートの詳細を手動で入力するには

a) 次のいずれかを実行します。

- 「**ソフトウェアを自動インストール煮含める**」で [**ルールを追加**] を選択します。
- 「**ソフトウェアを自動インストールから除外**」で [**ルールを追加**] を選択します。

b) [**ルール**]列のドロップダウンメニューから、条件の1つを選択し、含めるまたは除外する更新の詳細を入力します。

次の詳細情報を入力できます。

- 更新名は次を含む - アップデートの名前またはその一部
- ソフトウェア名は次を含む - ソフトウェアの名前またはその一部

> **注:** たとえば、「mozilla」と入力すると、「MozillaFirefox」と「MozillaThunderbird」の両方が含まれるか、除外されます。

- ベンダー名は次を含む - ソフトウェアベンダーの名前またはその一部
- 重大度は次に等しい - 重大度のレベルを示します⍰重大、重要、中程度、低、評価されていない⍰
- Bulletin IDは次の値に等しい - ソフトウェアアップデートのセキュリティ情報ID

5. [**保存して発行**] を選択してポリシーを配信します。

7.3.2 スキャン結果にアップデートを含める

スキャン結果に含むソフトウェアアップデートを指定できます。

スキャン結果にソフトウェアアップデートを含めるには

1. サイドバーから [**プロファイル**] を選択します。
[プロファイル] ビューが開きます。
2. 編集するプロファイルを選択します。
3. [**ソフトウェアアップデーター**] で、**アップデートをスキャン結果に含める**を開きます。
[ルールの追加] テーブルが表示されます。
4. [**ルールを追加**] を選択します。
[有効] 列のスイッチがオンになります。
5. [ルール] 列のドロップダウンメニューから、条件の1つを選択し、スキャンの結果に含めるアップデートの詳細を入力します。
次のパラメータを使用できます。
   - 更新名は次を含む - アップデートの名前またはその一部
   - ソフトウェア名は次を含む - ソフトウェアの名前またはその一部。

   > **注:** たとえば、「mozilla」と入力すると、「MozillaFirefox」と「MozillaThunderbird」が含まれます。

   - ベンダー名は次を含む - ソフトウェアベンダーの名前またはその一部
   - 重大度は次に等しい - 重大度のレベルを示します⍰重大、重要、中程度、低、評価されていない⍰
   - Bulletin IDは次の値に等しい - ソフトウェアアップデートのセキュリティ情報ID

   > **注:** 条件を満たさないソフトウェアアップデートは除外され、結果には表示されません。

6. 現在のプロファイルの保存を変更するために [**保存して発行**] を選択します。

7.3.3 セキュリティ以外のアップデートをスキャンから除外する

セキュリティに関連しないソフトウェアアップデートをスキャンから除外することを選択できます。

1. サイドバーから [**プロファイル**] を選択します。
[プロファイル] ビューが開きます。
2. 編集するプロファイルを選択します。
3. [**ソフトウェアアップデーター**] で、[**アップデートをスキャン対象外にする**] を開きます。
4. **セキュリティ以外のアップデート** をオンにします。

セキュリティに関連しないアップデートはスキャンから除外されます。

7.3.4 スキャン結果からアップデートを除外する

スキャン結果から除外するソフトウェアアップデートを指定できます。

スキャン結果からソフトウェアアップデートを除外するには

1. サイドバーから [**プロファイル**] を選択します。
   [プロファイル] ビューが開きます。
2. 編集するプロファイルを選択します。
3. [**ソフトウェアアップデーター**] で、[**アップデートをスキャン対象外にする**] を開きます。
   [ルールの追加] テーブルが表示されます。
4. [**ルールを追加**] を選択します。
   [有効] 列のスイッチがオンになります。
5. [ルール] 列のドロップダウンメニューから、条件の1つを選択し、スキャンの結果から除外するアップデートの詳細を入力します。
   次のパラメータを使用できます。
   - 更新名は次を含む - アップデートの名前またはその一部
   - ソフトウェア名は次を含む - ソフトウェアの名前またはその一部

     注: たとえば、「mozilla」と入力すると、「MozillaFirefox」と「MozillaThunderbird」が除外されます。
   - ベンダー名は次を含む - ソフトウェアベンダーの名前またはその一部
   - 重大度は次に等しい - 重大度のレベルを示します。重大、重要、中程度、低、評価されていない。
   - Bulletin IDは次の値に等しい - ソフトウェアアップデートのセキュリティ情報ID
6. 現在のプロファイルの保存を変更するために [**保存して発行**] を選択します。

7.4 デバイスに対して適用されていないソフトウェア アップデートをスキャンする

ポータルを通じて、デバイスに適用されていないソフトウェア アップデートをスキャンすることができます。

特定のデバイスをスキャンするには

1. サイドバーから [**デバイス**] をクリックします。
   「**デバイス**」ページが表示されます。

   スコープセレクタ が顧客企業をすべて表示されるようになっている場合、管理する企業を選択してください。
2. デバイスの名前の横にあるチェック ボックスを選択します。
   ページの下にメニューが表示されます。
3. メニューから [**適用されていないソフトウェアのアップデートをスキャン**] をクリックします。
   インストールしているElements Endpoint Protectionソフトウェアにデバイスのスキャンを指示するコマンドが送られ、適用されていないソフトウェア アップデートを検出します。

スキャンが完了したらポータルに適用されていないソフトウェア アップデートの一覧が表示され、デバイスにインストールするソフトウェア アップデートを選択できます。

7.5 特定のデバイスでソフトウェア アップデートを表示・インストールする

特定のデバイスで利用できるソフトウェア アップデートの情報を確認できます。

注: 適用されていないソフトウェア アップデートは「**ホーム**」ページにある問題のテーブル (「*重大*」、「*重要*」、「*情報*」で分類化) でも一覧表示されます。[**表示**] ボタンをクリックすると、利用できるアップデートがあるデバイスを確認できます。

特定のデバイスで利用できるアップデートを表示するには

1. サイドバーから [**デバイス**] をクリックします。
   「**デバイス**」画面が表示されます。
2. デバイスの名前をクリックします。
   デバイスの詳細情報を示すページが開きます。
3. 「保護ステータス」テーブルで [ソフトウェア アップデート] の横にある » をクリックします。
   利用できるアップデートがドロップダウン メニューで表示されます。
4. [**アップデートを選択してインストール**] ボタンをクリックします。
   「**ソフトウェア アップデートをインストール**」ページには特定のソフトウェアに対する利用可能なアップデート (カテゴリ、CVE ID、Bulletin ID (セキュリティ番号)、アップデートの詳細が記載されている外部リンクを含む) が表示されます。「*すべてのアップデート*」、「*すべてのセキュリティ アップデート*」、「*重大なセキュリティ アップデート*」、「*重要なセキュリティ アップデート*」、「*セキュリティに関連しない更新*」または「*サービス パック*」をクリックすると表のアイテムを個別に表示できます。
   「**ソフトウェア アップデートをインストール**」ページが表示され、適用されていないアップデートを確認できます。
5. 該当するアップデートを選択して [**インストール**] ボタンをクリックします。
   選択したアップデートがデバイスにインストールされます。

7.6 ソフトウェア アップデーターに HTTP プロキシを設定する

インターネットのトラフィック (データ通信) を減らすためにソフトウェア アップデーターに HTTP プロキシを設定できます。

「プロファイル」ページにあるプロキシのアップデート設定は設定することが可能です。

1. **プロファイル** > **ソフトウェア アップデータ** で [**通信**] を選択します。
2. 「**HTTP プロキシを使用**」ドロップダウン メニューから次のいずれかのオプションを選択します。
   - なし - インターネットへ直接接続します
   - 製品構成から、製品のプロキシ設定を使用します
   - [ユーザ定義] - [代理のプロキシ URL] (ユーザ定義) を指定します
3. [**リモート管理**] を選択した場合、[リモート管理]-[プロキシ フィールド] フィールドで HTTP プロキシ アドレスを次の形式で入力します: `http://[ユーザ[:パスワード]@]ホスト:ポート`

7.7 ソフトウェア アップデータ用の Secure Elements コネクタの設定

ソフトウェアアップデーターは、以下の方法でアップデートを受け取るように設定できます。WithSecure Elements Connector。

「プロファイル」ページにあるプロキシのアップデート設定は設定することが可能です。

1. **プロファイル** > **ソフトウェア アップデータ** で [**通信**] を選択します。
2. から **セキュアエレメントコネクタの使用** ドロップダウン メニューで、次のいずれかのオプションを選択します。
   - 常に - 常に使用する WithSecure Elements Connector
   - 可能であれば、WithSecure Elements Connectorいつでも可能なとき
   - なし - インターネットへ直接接続します

7.8 ソフトウェア アップデータとWindows Server Update Serviceを使用してMicrosoftの更新プログラムをインストールする

WithSecure Elementsで、ソフトウェアアップデーター（SWUP）は、常にWindows Updateをインストールします。

Windowsの更新プログラムのインストールをオフにすることはできません。[**WSUSを使用している場合、ソフトウェアアップデーターとWSUSの両方がMicrosoftの更新プログラムをインストールする**]の設定は、ソフトウェアアップデーター(SWUP) とWindows Server Update Services (WSUS) によるWindows Updateを同時にインストールすることを防ぎます。

注： ソフトウェアアップデーターは、Windowsのオプションの更新プログラムをサポートしていません。

WSUSを使用していて、その設定をオンにすると、Windowsアップデートのインストール中に、SWUPはWSUSをオフにします。その後、インストール開始前にWSUSがオンになっている場合、SWUPはWSUSをオンに戻します。

重要: この設定がオフの場合、SWUPはWSUSをオフにしません。これにより、WSUSとSWUPが同時に更新プログラムをインストールしようとし、重大なクライアント側の更新プログラムエラーが発生する可能性があります。

注： アクティブに管理されたWS USを使用している場合は、この設定をオフにすることをお勧めします。WS USをアクティブに管理しない場合は、この設定をオンのままにしてください。

付録
A

ポータルとソフトウェアのカスタマイズ

トピック :

この章では、顧客会社の追加方法、サブスクリプション キーの追加方法、顧客会社の製品の注文方法、範囲セレクタを使用してWithSecure Elements EPPポータルに表示される情報の範囲を変更する方法およびポータルとElements Endpoint Protectionソフトウェアのカスタマイズ方法について説明します。

注 : **プロファイル** > **一般設定**で、Pilot クライアントの設定をオンにできます。このオプションがオンの場合、該当するプロファイルに割り当てられているデバイスは事前に新機能をテストできるようになります。パイロット コンピュータは、他のユーザよりも数日前にソフトウェア アップデートを受け取ります。 この機能を使用することで、新機能のプレビューを取得し、顧客にそれを伝達できるようになります。

A.1 顧客企業を追加する

新しい「*顧客企業*」をWithSecure Elementsポータルのアカウントに追加するにはまず*規顧客*」を***WithSecure***パートナーポータルのアカウントに追加し、WithSecure Elementsを1つ以上購入する必要があります。

注: ソリューションプロバイダおよびサービスパートナーのみ企業アカウントを追加できます。

新しい顧客企業でライセンス・デバイスを管理する管理者アカウントが必要な場合、PSB ポータルを通じて管理者アカウント作成してください。

注: エフセキュア「パートナー ポータル」はWithSecure Elementsポータルと連携したオンライン サービスで、販売活動を支援するツール、資料、統合したオンライン注文システムおよびエフセキュア ソリューションのサポートを提供します。

パートナー ポータルのアカウントから新規顧客の発注書を追加したらWithSecure Elementsポータルのアカウントに新規顧客として自動的に追加されます。

以後、WithSecure Elements製品を顧客企業のユーザに提供できるようになり、購入した製品のライセンス管理も可能になります。

A.2 企業アカウントに新しいライセンス キーコードを追加する

企業アカウントに新しいライセンス キーコードを追加すると、WithSecure Elementsポータルにコンピュータを追加できます。

新しいライセンス キーコードを追加するには

注: ソリューション プロバイダおよびサービス パートナーのみ企業アカウントに新しいライセンス キーコードを追加できます。

1. [**管理**] で、 サイトバーの **サブスクリプション**] を選択します。
2. [**Endpoint Protectionのサブスクリプション**] タブを選択します。
3. 新しいライセンス キーコードの対象となる企業アカウントの名前の横で ··· を選択し、[**ライセンス キーコードを追加**] を選択します。
   「**ライセンス キーコードを追加する**」ページが開きます。
4. 企業アカウントの新しいライセンス キーコードを入力して [**追加**] を選択します。

新しいライセンス キーコードが企業アカウントに追加されます。

A.3 顧客企業に製品を注文する

顧客企業向けのWithSecure Elements製品は、WithSecureパートナーポータルから注文することができます。

注: ソリューション プロバイダおよびサービス パートナーのみが、顧客企業向けの製品を注文できます。

WithSecure Partner Portal経由でWithSecure Elements製品を注文するには

1. Webブラウザで次のリンクを開いて、ポータルにログインします。パートナーポータル

   注: WithSecure パートナー ポータルには、WithSecure Elementsポータルからの別のログイン資格情報が必要です。ログインの詳細がまだない場合は、ページ上の**認証情報のリクエスト**フォームに入力し、[**送信**] をクリックします。アクセス認証情報を受け取るまでに最大24時間かかります。

   「**オンライン注文**」ページが表示されます。
2. 既存の顧客企業に製品を注文するには
   a) メインページで [**顧客**] をクリックし、製品を注文する顧客企業名を選択します。

b) 「[注文] 列で、[新規SaaS注文] または [新規年間注文] を選択します。
[注文] ウィンドウが開きます。
c) [新規注文] の下に、注文の参照番号を入力します。
d) [製品の注文] で、[製品を追加] を選択します。
e) 必要な製品を選択して注文の指示に従います。

発注が完了すると、製品情報の変更は、WithSecure パートナーポータルおよびWithSecure Elements ポータル アカウントで更新されます。

3. 新規顧客企業に製品を注文するには
a) メイン ページで、[新規注文] を選択します。
b) 新規顧客企業の名前を入力し、[新規追加] 選択します。
[新規顧客] ウィンドウが開きます。
c) 顧客の詳細を入力し、[保存] を選択します。
d) [新規注文] の下に、注文の参照番号を入力します。
e) [製品の注文] で、[製品を追加] を選択します。
f) 必要な製品を選択して注文の指示に従います。

発注が完了すると、新規顧客企業が購入した製品と一緒にパートナーポータルアカウントにリストされます。

注: 新規顧客企業がWithSecure Elementsポータルアカウントに表示されるまでに時間がかかる場合があります。

A.4 管理ポータルをカスタマイズする

WithSecure Elementsポータルは、お客様のロゴやサポートリンクでカスタマイズできます。

管理ポータルをカスタマイズするには

1. [管理] で、 サイトバーの [サブスクリプション] を選択します。
[組織の設定] ページが開きます。
2. [Endpoint Protectionのアカウント] タブを選択します。
[アカウント] ページが開きます。
3. ••• アイコンを選択して、[ポータルのカスタマイズ] を選択します。
「ポータルのカスタマイズ」ページが開きます。
4. [サポート URL] フィールドに、サポート サイトの URL を入力します。
指定したリンクは、デフォルトの WithSecure サポート リンクに代わるものです。
5. ロゴを[ポータルと概要レポートのロゴ] ボックスにドラッグアンドドロップしてアップロードします。

注 : ログは PNG 形式にして、60 x 60 ピクセルのサイズにしてください。

6. 変更を保存します。

カスタマイズすると、ポータルの左下隅にロゴが表示されます。

A.5 WithSecure Elementsソフトウェをカスタマイズする

ロゴとサポートリンクを使用して、WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversソフトウェアをカスタマイズできます。

注 : ロゴまたは URL、あるいは両方をソフトウェアで表示するには、カスタム プロファイルを割り当て、使用する必要があります (WithSecure のデフォルト プロファイルではありません)。

ソフトウェアををカスタマイズするには

1. [管理] で、 サイトバーの [サブスクリプション] を選択します。
[組織の設定] ページが開きます。
2. [Endpoint Protectionのアカウント] タブを選択します。

[アカウント] ページが開きます。

3. アイコンを選択して、[クライアントのカスタマイズ] を選択します。
「クライアントのカスタマイズ」ページが開きます。
4. [URL] フィールドにリンクを入力します。
提供するリンクはロゴのための任意のリンクです。たとえば、パートナー サポート サイトへのリンクを指定したらデフォルトの WithSecure サポート リンクの代わりになります。
5. ロゴを [クライアントロゴ] ボックスにドラッグアンドドロップしてアップロードします。

注 : ロゴの必要寸法は128 x 128ピクセルです。見栄えを良くするために余白を追加することもできます。

アップロードしたロゴは、WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversに表示されます。

このURLはロゴのための任意のリンクです。たとえば、パートナー サポート サイトを指定できます。

付録
B

Windows Management Instrumentation

トピック：

WithSecure Elementsは、Windows Management Instrumentation ⊠WMI⊠統合を提供します。これを使用して、たとえばリモート監視および管理⊠RMM⊠ツールを統合できます。

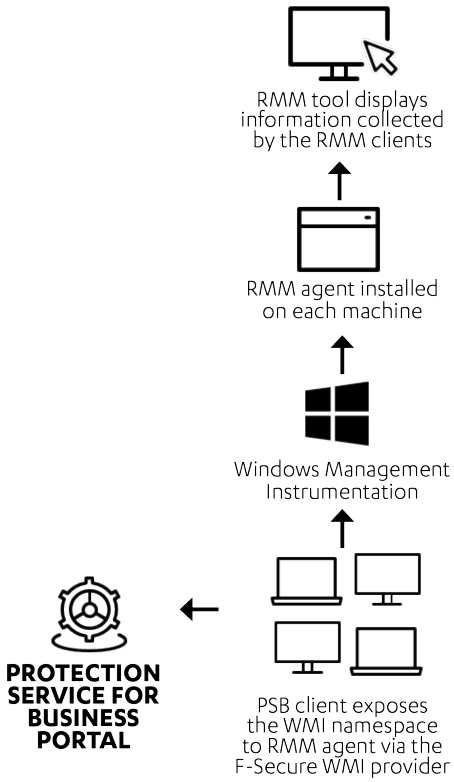
サービス プロバイダの多くはアセット (資産) ディスカバリー、管理、設定、プロセス・サービスの自動化、セキュリティ サービス、バックアップなどの管理機能を強化するためにWMIの連携を使用します。

B.1 WMI の連携

WithSecure Elements Windows Management Instrumentation (WMI) インターフェイスを使用して、WithSecure クライアント アプリケーションの読み取り専用ステータス情報を収集します。

WMI インターフェースはホストにインストールされているベンダー固有のエージェントを使用して収集した情報を管理コンソール サーバに転送します。構成オプションまたは一般的なセキュリティ管理機能は WMI インターフェースを通して通知されることはありません。

管理者は WMI インターフェースを使用してホスト コンピュータに対してフル スキャンをリモートから開始することもできます。



WMI インターフェースを通じて Windows のクライアントとサーバから次の情報を取得できます。

- 製品のバージョン
- リアルタイム スキャンのステータス
- マルウェア定義ファイルのデータベース情報
- ファイアウォールのステータス
- ファイアウォールのセキュリティ レベル (プロファイル)
- ファイアウォールのバージョン
- アプリケーション制御のステータス
- WithSecure Elements Endpoint Protectionポータルへの最後の接続時間
- WithSecure Elements Endpoint Protectionポータルへの最後のポリシー更新時間
- 使用しているWithSecure Elements Endpoint Protectionプロファイルの名前
- ディープガードのステータス
- ブラウザ保護のステータス
- メール フィルタのステータス
- ソフトウェア アップデーターのステータス (セキュリティ アップデートの自動インストール ステータス、インストールされていないアップデート (タイプ別: 重大、重要、その他))
- サブスクリプションステータス
- 前回の手動スキャンおよびスケジュールス キャンに関する情報

B.1.1 WMI を通じてプロパティを取得する

WMI を使用してプロパティを取得する方法を説明します。

1. WMI プロバイダの設定を有効にするには
   a) WithSecure Elementsにログインします。
   b) [**セキュリティ構成**] で、[**プロファイル**] を選択します。
   a) [**一般設定**] を選択します。
   b) 「**連携**」で [**WMI プロバイダ**] を有効にします。
   c) [**保存して発行**] を選択します。
   d) [**環境**] で、[**デバイス**] を選択し、デバイスを選択します。
   e) [**プロファイルを指定する**] を選択します。
   f) ドロップダウンメニューで、プロファイルを選択し、[**プロファイルを指定する**] をクリックします。
2. 管理者権限で **Windows PowerShell** を開きます。
3. コマンドプロンプトで、以下のコマンドを入力して、次のクラスとプロパティなどの情報を取得します。
   - シングルトンインスタンスをすべて含むリストをリクエストする

     ```
     Get-WmiObject -Namespace root/fsecure -List | where {
     $_.Qualifiers["Singleton"].Value }
     ```

   - 製品のバージョンを取得する

     ```
     $product = Get-WmiObject -Namespace "root/fsecure" -Class Product
     Write-Host Version: $product.Version
     ```

     結果:

     ```
     Version: 18.15
     ```

   - リアルタイム スキャンのステータス:

     ```
     $av = Get-WmiObject -Namespace "root/fsecure" -Class AntiVirus2
     Write-Host "Is real-time scanning enabled: " $av.RealTimeScanningEnabled
     ```

     結果:

     ```
     Is real-time scanning enabled: True
     ```

   - AvDefinitions

     ```
     $av = Get-WmiObject -Namespace "root/fsecure" -Class AntiVirus2
     $status = if ($av.AvDefinitionsAgeInHours -lt 7*24){
     "up to date" } else { "outdated" }
     Write-Host "AV definitions are" $status
     ```

     結果:

     ```
     Av definitions are up to date
     ```

   - ファイアウォールのステータス

     ```
     $fw = Get-WmiObject -Namespace "root\fsecure" -Class Firewall
     Write-Host "Is firewall enabled: " $fw.Enabled
     ```

     結果:

     ```
     Is firewall enabled: True
     ```

- WithSecure Elementsポータルへの最後のポリシー接続時間

```
$cm = Get-WmiObject -Namespace "root\fsecure" -Class CentralManagement2
$status = if ($cm.LastConnectionTimeInHoursAgo -lt 24) { "OK" } else {
"Connectivity issues" }
Write-Host "PSB Portal connection status: " $status
```

結果:

```
PSB Portal connection status: OK
```

- WithSecure Elementsポータルへの最後のポリシー更新時間

```
$cm = Get-WmiObject -Namespace "root\fsecure" -Class CentralManagement
Write-Host "PolicyUpdateTime: " $cm.PolicyUpdateTime
```

結果:

```
PolicyUpdateTime: 20181001144235.000000+000
```

- ディープガードのステータス:

```
$av = Get-WmiObject -Namespace "root\fsecure" -Class AntiVirus2
Write-Host "Is DeepGuard enabled:" $av.DeepGuardEnabled
```

結果:

```
Is DeepGuard enabled: True
```

- ブラウザ保護のステータス:

```
$inet = Get-WmiObject -Namespace "root\fsecure" -Class Internet2
Write-Host "Is Browsing Protection enabled:"
$inet.BrowsingProtectionEnabled
```

結果:

```
Is Browsing Protection enabled: True
```

- ソフトウェア アップデーターのステータス (セキュリティ アップデートの自動インストール ステータス、インストールされていないアップデート (タイプ別: 重大、重要、その他))

```
$su = Get-WmiObject -Namespace "root\fsecure" -Class SoftwareUpdater
Write-Host "Enabled: " $su.Enabled
Write-Host "InstallSecurityUpdatesAutomatically: "
$su.InstallSecurityUpdatesAutomatically
Write-Host "MissingCriticalUpdatesCount: " $su.MissingCriticalUpdatesCount
Write-Host "MissingImportantUpdatesCount: "
$su.MissingImportantUpdatesCount
Write-Host "MissingOtherUpdatesCount: " $su.MissingOtherUpdatesCount
```

結果:

```
Enabled: True
```

```
InstallSecurityUpdatesAutomatically : 0
```

```
MissingCriticalUpdatesCount : 2
```

```
MissingImportantUpdatesCount : 1
```

```
MissingOtherUpdatesCount : 1
```

- サブスクリプション ステータス

```
$license = Get-WmiObject -Namespace "root\fsecure" -Class LicenseStatus
Write-Host "License status: " $license.Valid "; End date: "
$license.EndDate
```

結果:

```
License status: True ; End date: 20191231235959.000000+000
```

- 前回の手動スキャンのレポート情報

```
$report = Get-WmiObject -Namespace "root\fsecure" -Class
LastManualScanReport

Write-Host "HarmfulItemsFound: " $report.HarmfulItemsFound
```

結果:

```
HarmfulItemsFound: False
```

- 前回の手動スキャンのレポート情報

```
$report = Get-WmiObject -Namespace "root\fsecure" -Class
LastScheduledScanReport

Write-Host "HarmfulItemsFound: " $report.HarmfulItemsFound
```

結果:

```
HarmfulItemsFound: True
```

B.2 連携用の WMI クラス

この付録では、Windows Management Instrumentation (WMI)統合に使用されるクラスの詳細について説明します。WithSecure Elements。

B.2.1 WMI クラス

ここでは、WithSecure ElementsポータルのWMI統合に使用されるクラスの詳細について説明します。

一部のクラスはシングルトンインスタンスとして使用でき、一部は補助型としてのみ使用されます。詳細については、WMI を通じてプロパティを取得するページ158 の例を参照してください。

AntiVirus

アンチウイルスモジュールに関する情報を提供し、コンピュータの完全スキャンを実行できます。

プロパティ名	説明	種類
CheckRealTimeScanning	リアルタイムスキャンのステータス情報	***component***
DeepGuard	*ディープガード*のステータス情報	***component***
AvDefinitionsUpdateTime	アンチマルウェア定義ファイルの前回のアップデート時間	***datetime***
AvDefinitions	インストールされているアンチウイルス エンジンの一覧	***AvDefinitions***

メソッド名	説明	戻り型
ScanComputer	フル コンピュータ スキャンの開始と完了までの待機	***AvScanResult***

AntiVirus2

アンチウイルス モジュールに関する情報を提供する簡易クラス。

プロパティ名	説明	種類
RealTimeScanningEnabled	リアルタイムスキャンのステータス情報	***boolean***
DeepGuardEnabled	*ディープガード*のステータス情報	***boolean***
AvDefinitionsAgeInHours	アンチウイルス定義が発行されてからの経過時間	***uint32***

API

WithSecure WMIネームスペースAPIの基本情報。

プロパティ名	説明	種類
バージョン	APIの実バージョン	*文字列*

AvDefinition

アンチウイルス エンジンの情報。

プロパティ名	説明	種類
EngineId	該当するエンジンの一意識別子	***uint32***
EngineName	該当するエンジンのユーザフレンドリ名	*文字列*
EngineVersion	該当するエンジンのバージョン	*文字列*
UpdateSerialNumber	インストールしたアップデートの一意識別子	*文字列*
UpdateTime	アップデートがインストールされた時間	***datetime***

AvScanResult

ウイルス スキャンの結果。

プロパティ名	説明	種類
StartTime	スキャンが開始された時間	***datetime***
EndTime	スキャンが終了した時間	***datetime***
InfectedFilesCount	スキャン中に検出した感染ファイルの数	***uint32***
InfectedSectorsCount	スキャン中に検出した感染セクターの数	***uint32***
ScanningReportFilePath	スキャンレポートのパス	*文字列*

CentralManagement

プロテクション サービスの相互作用に関する情報。

プロパティ名	説明	種類
LastConnectionTime	プロテクション サービスの前回の接続時間。	***datetime***
PolicyUpdateTime	前回のポリシー アップデート時間。	***datetime***
プロフィール	インストールされているプロファイル。	*プロフィール*

CentralManagement2

プロテクション サービスの相互作用に関する情報を提供する簡易クラス。

プロパティ名	説明	種類
LastConnectionTimeInHoursAgo	プロテクションサービスの前回の接続時間	***uint32***

CentralManagement3

ホストIDとそのタイプに関する情報を提供します。

プロパティ名	説明	種類
HostIdentityType	ホスト ID タイプ ☒SMBIOSGUID/RANDOMGUID/WINS/MAC、またはホスト IDが定義されていない場合は空☒。	*文字列*
HostIdentity	ホストID	*文字列*

Component

製品コンポーネントの概要情報。

プロパティ名	説明	種類
Enabled	コンポーネントのステータス	***boolean***

Firewall : Component

WithSecure Firewallに関する情報を提供します。

プロパティ名	説明	種類
Enabled	WithSecureファイアウォールの現在のステータス	***boolean***
SecurityLevel	WithSecureファイアウォールの現在のセキュリティレベル	*文字列*
ApplicationControl	アプリケーション制御の現在のステータス	***component***
バージョン	WithSecureファイアウォールのバージョン	*文字列*
Build	WithSecureファイアウォールのビルド	*文字列*

Internet

インターネット セキュリティのコンポーネントの情報。

プロパティ名	説明	種類
BrowsingProtection	ブラウザ保護のステータス	***component***
EmailFiltering	メールフィルタのステータス	***component***

Internet2

インターネット セキュリティ コンポーネントに関する情報を提供する簡易クラス。

プロパティ名	説明	種類
BrowsingProtectionEnabled	ブラウザ保護のステータス	***boolean***

LastManualScanReport

ユーザーが最後に手動で実行したスキャンに関する情報を提供します。

プロパティ名	説明	種類
Valid	レポートが正常に検出およびロードされたか示します	***boolean***
StartTime	スキャンが開始された時間	***datetime***
EndTime	スキャンが終了した時間	***datetime***
StartTimeInHoursAgo	スキャンが開始された時刻⊠何時間前⊠	***uint32***

プロパティ名	説明	種類
EndTimeInHoursAgo	スキャンが終了した時刻⊠何時間前⊠	***uint32***
InfectedFilesCount	スキャン中に検出した感染ファイルの数	***uint32***
TotalScannedFilesCount	スキャンされたファイルの総数	***uint32***
HarmfulItemsFound	有害なアイテムが見つかったかどうかを示します	***boolean***
ScanningReportFilePath	スキャンレポートのパス	*文字列*

LastScheduledScanReport

スケジュールに従って実行された最後のスキャンに関する情報を提供します。

プロパティ名	説明	種類
Valid	レポートが正常に検出およびロードされたか示します。	***boolean***
StartTime	スキャンが開始された時間	***datetime***
EndTime	スキャンが終了した時間	***datetime***
StartTimeInHoursAgo	スキャンが開始された時刻⊠何時間前⊠	***uint32***
EndTimeInHoursAgo	スキャンが終了した時刻⊠時間単位⊠	***uint32***
InfectedFilesCount	スキャン中に検出した感染ファイルの数	***uint32***
TotalScannedFilesCount	スキャンされたファイルの総数	***uint32***
HarmfulItemsFound	有害なアイテムが見つかったかどうかを示します	***boolean***
ScanningReportFilePath	スキャンレポートのパス	*文字列*

LicenseStatus

現在使用されているライセンスに関する情報を提供します。

プロパティ名	説明	種類
Valid	ライセンスの有効性ステータス	***boolean***
EndDate	サブスクリプションの終了日	***datetime***
DaysTillEndDate	サブスクリプションの終了日までの日数	***uint32***
SubscriptionName	製品のサブスクリプション名	*文字列*

Product

インストールされているセキュリティ製品の情報。

プロパティ名	説明	種類
名前	製品の名前	*文字列*
バージョン	製品のバージョン	*文字列*
Build	製品のビルド	*文字列*

Profile

インストールされているプロファイルの情報。

プロパティ名	説明	種類
ProfileName	プロファイルのユーザフレンドリ名	*文字列*
ProfileVersion	プロファイルパッケージのバージョン	*文字列*
SeriesName	プロファイルパッケージの名前	*文字列*
InstallationTime	プロファイルがインストールされた時間	***datetime***

RebootStatus

再起動ステータスに関する情報を提供します。

プロパティ名	説明	種類
Pending	再起動が保留中かどうかを示します	***boolean***
Reason	再起動が保留されている理由。可能な値: • ***swup***ソフトウェアアップデーター • ***update***自己更新 • ***virus*** • ***spyware*** • ***critical***自己更新に失敗した • ***malfunction***	*文字列*

SimpleComponent : Component

ベース クラスのデフォルト導入。

プロパティ名	説明	種類
Enabled		***boolean***

SoftwareUpdater : Component

WithSecureソフトウェア アップデーターに関する情報を提供します。

プロパティ名	説明	種類
Enabled	WithSecureソフトウェア アップデーターの状態	***boolean***
InstallSecurityUpdatesAutomatically	ソフトウェアアップデーターにより自動的にインストールされたアップデートの種類 • 0: なし • 1: 重大 • 2: 重大および重要 • 3: すべて	***uint32***
MissingCriticalUpdatesCount	インストールされていない重大なアップデートの数	***uint32***
MissingImportantUpdatesCount	インストールされていない重要なアップデートの数	***uint32***
MissingOtherUpdatesCount	インストールされていないアップデート⊠重大・重要なアップデートを除く⊠の数	***uint32***

B.2.2 Windows レジストリの WMI クラス

ここで説明するすべての WMI クラスは、Windows レジストリにも反映されます。

クラスは次のパスにあります。

64ビット システムの場合: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\F-Secure\Monitoring`

32ビット システムの場合: `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\Monitoring`

注: このレジストリ キーを表示するには、WithSecure Elementsポータルで WMI プロバイダ設定を有効にする必要があります。

付録 C

望ましくない Web コンテンツをブロックする

トピック :

Web コンテンツ制御を使用することで不適切なコンテンツを含む Web ページのアクセスをブロックすることができます。

「Web コンテンツ制御」は、WithSecure の評価分析データを使用して Web サイトを分類し、ポリシーで特定されている禁止コンテンツを含むサイトのアクセスをブロックします。

C.1 Web コンテンツ カテゴリ

以下のカテゴリを指定することで WithSecure Network Reputation Service (NRS) コンテンツ分析の結果に応じて Web サイトをブロックできます。

注 : ini ファイルで使用されているカテゴリ名は括弧で区切られています。

中絶	中絶に関する情報⊠中絶について議論し、促進し、奨励し、中絶の手順⊠を提供、または中絶を得るもしくは回避するためのサポートを提供するWebサイト。
広告配信	広告やその他の販促用コンテンツを表示するファイルのダウンロードを提供するWebサイト。たとえば、有害な可能性のあるブラウザプラグインブラウザをインストールするWebサイト。
成人	成人向けなページや性的な要素があるページ。例:アダルトグッズショップや性的描写。
お酒とタバコ	お酒とたばこ製品、および製造者、製造所、ブドウ園、醸造所などを紹介する Web サイト。例: ビールの祭り (ビアガーデンなど) を紹介するサイトやバーやナイトクラブの Web サイトなど。
アノニマイザ	ネットワークのフィルタを回避する方法を説明する Web サイト、Web ベースの翻訳サイトを含む。例: 公開プロキシの一覧を記載しているサイト。
オークション	オンライン オークションなど、ユーザがインターネットで製品やサービスを売買できるWebサイト。製品やサービスの取引が実際には別の場所で行われるサイトも含まれる。
バンキング	銀行預金、銀行口座間の電子送金、通貨換算などのオンライン バンキング機能を提供するWebサイト。
ブログ	ブログを作成および維持するための無料または有料のサービスを提供するブログサイトまたはフォーラム/掲示板。
チャット	テキストベースのインスタントメッセージやチャットのためのWebベースのサービスやダウンロード可能なソフトウェアを提供し、同じサイト上でリアルタイムにオンラインチャットができるようにするWebサイト。
出会い系	出会い系の Web サイト。例: 出会い系サイトや結婚相談所サイト。
不適切	本質的に望ましくないコンテンツ (画像、説明、ビデオ ゲームなど) を含むWeb サイト。
麻薬	麻薬の使用を推奨するサイト。例:違法薬物の購入、栽培、販売に関する情報を提供するサイト。
芸能	さまざまな映画、音楽、本、テレビ、または雑誌に関する情報を宣伝または提供するWebサイト
ファイル共有	ファイル共有アプリケーションを提供するWebサイト。
ギャンブル	ギャンブルに関する情報を宣伝または提供し、実際のお金や何らかのクレジットを使ってオンラインで賭けをすることができるWebサイト。例: オンライン ギャンブル、宝くじサイトのWeサイト
ゲーム	オンラインで他の人と対戦するゲームなどへのアクセスを提供するWebサイト。
ハッキング	ウイルスの作成、パスワードのハッキング、他のコンピュータへのアクセスを目的として、デバイスやソフトウェアの疑わしい、または違法な利用を指示または促進するWebサイト。
憎悪表現	宗教、人種、国籍、性別、年齢、障害、性的指向などに対して差別を行っているWeb サイト。例: 人権侵害、動物虐待などに関する情報や暴行を想起させるサイト。

不正	性的行為における未成年の画像や情報を含むアダルト サイト、および未成年を悪用しようとする Web サイト。
就活	求職、求人情報、履歴書交換を専門とするヘッドハンティングまたは人材紹介会社のWebサイト。
支払いサービス	オンライン決済に特化したサービス、またはオンラインウェブストア向けに、オンライン決済方法なや金融サービスを提供するサービス。
詐欺	ユーザのコンピュータを攻撃し、個人情報を取得するために使用される悪意のあるソフトウェアが含まれている違法または詐欺的なWebサイト。
ショッピング	オンライン ショッピング向け商品カタログを掲載しており、ユーザがオンラインで商品やサービスを購入できるWebサイト。もしくはオンラインで注文や購入できる商品の情報を提供しているサイト。
SNS	一般ユーザ同士を結びつけたり、特定のグループのメンバー間の交流、ビジネス交流などを助けるネットワーク ポータル。例えば、自分の個人的、仕事上の関心事などをシェアするためのメンバー プロファイルを作成できるようなサイト。Twitter などのソーシャルメディア サイトがこれに含まれる。
ソフトウェア ダウンロード	無料、試用、または有料のソフトウェアダウンロードを提供するWebサイト。
スパム	スパムメールに記載されているアドレスのWebサイト。
ストリーミング メディア	音楽や映像のダウンロードおよび映像や音声のストリーミングコンテンツを提供するWebサイト。
原因は不明です。	評判が不明な Web サイト (評判が悪く、アクセス頻度が低いことが主な原因)、または安全の評価があっても分類されていない Web サイト。
暴力	暴力を扇動したり、陰惨で暴力的な画像もしくは動画を含むWebサイト。例えば、レイプ、ハラスメント、スナッフ、爆弾、暴行、殺人あるいは自殺についての情報を含むサイト。
ウェアーズ(不正なダウンロード)	ユーザがソフトウェアを無料または使用料なしでダウンロードできるWebサイト。また、ダウンロードを実現するために多数のユーザの間のファイル共有、無許可のファイル共有またはソフトウェアの違法コピーを無料または利益を得るために配布する Web サイト。
武器	人間、もしくは動物に害を与える武器等に使用可能な情報、画像、もしくは動画などを含む、または推進んする Web サイト。これには狩猟や射撃クラブなど、これらの武器の普及を援助している組織が含まれる。またこのカテゴリにはペイントボール ガンや BB ガンなどのおもちゃの武器も含まれる。
Web メール	任意のインターネットブラウザを使用してアクセスできる無料のWebベースのメールサービスをユーザに提供するWebサイト。

信頼済みの/拒否したサイトの校正

信頼済みのサイト	信頼済みのサイトのパターンの一覧を含めています。
拒否したサイト	拒否されているサイト パターンの一覧を含めています。
不審なサイト	不審なサイトのパターンの一覧を含めています。
禁止サイト	禁止サイトのパターンの一覧を含めています。

C.2 ブロックするコンテンツを選択する

Webコンテンツ制御の設定からブロックするWebコンテンツの種類を選択できます。

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
   「プロファイル」ページが開きます。

2. [**コンピュータプロファイル**] タブで、編集するプロファイルを選択します。
3. [**ブラウザ保護**] を選択します。
4. [**Webコンテンツ制御**] を有効にします。
5. [**Webコンテンツ制御**] の横にある を選択します。
   Webコンテンツカテゴリー一覧が開きます。
6. [**拒否**] で管理対象ホストに対してブロックするタイプを選択します。
7. [**保存して発行**] をクリックします。

C.3 Web サイトがブロックされた場合

「危険」として評価されている Web サイトにアクセスするとブラウザ保護のブロック ページが表示されます。

ブラウザ保護のブロック ページが表示した場合

1. Web サイトにアクセスする場合、[**このコンピュータでWebサイトのアクセスを許可する**] をクリックしてください。
   Windows ユーザー アカウント制御 (UAC) が操作の確認を尋ねます。
2. 必要に応じて管理者アカウントの情報を入力し、変更を確認します。

付録 D

ポリシーマネージャコンソールを使用して移行する

トピック：

ポリシーマネージャを使用した場合は、以下の手順に従って、ポリシーマネージャの.jarファイルを使用してコンピュータを移行します。

D.1 コンピュータを移行する

コンピュータをWithSecure Client SecurityからWithSecure Elements EPP for Computers、およびServer SecurityをWithSecure Elements EPP for Serversに移行する方法。

`.jar`ファイルを適用して移行するには、Policy Managerコンソールと、次のリンクからダウンロードできる`.jar`ファイルが必要です。https://download.withsecure.com/PSB/bs2cp/bs2elements.jar。

コンピュータを移行するには

1. ポリシー マネージャ コンソールを開き、移行するコンピュータ グループを選択します。
2. 「**インストール**」タブを選択します。
   「**インストール**」ページが開きます。
3. 「ポリシー ベース インストール」の下で [**インストール...**] を選択します。
   「**インストール パッケージの選択**」ウィンドウが開きます。
4. [**インポート...**] を選択すると、インストール パッケージをインポートします。
   利用できる`.jar`ファイルが表示されます。
5. `.jar`ファイルを選択し、[**インポート**] を選択します。
   ポリシー マネージャが`.jar` ファイルをインポートし、パッケージの詳細が表示されます。
6. [**OK**] を選択すると、`.jar` ファイルを適用します。
7. 表示される「**インストール オプション**」ウィンドウで次を行います。
   a) サブスクリプション キーを入力します。
   b) インストールで使用する言語を選択し、[**完了**] を選択します。
8. 「**インストール**」ウィンドウで、左上隅の  アイコンを選択して、指定したコンピュータにポリシーを配布します。
   選択したコンピュータが移行され、ポリシーも配布されます。

インストールを完了するために選択したコンピュータを再起動する必要があるかもしれません。

付録 E

FAQ

トピック :

このトピックでは、FAQ (よくあるご質問と回答) を紹介します。

お探しの情報が見つからない場合は、エフセキュアのサポートにお問い合わせください。

注 : ディスカッションや製品の最新情報については、WithSecureコミュニティページもご覧ください。

E.1 ポータルの言語を変更するにはどうすればいいですか

言語を変更するには、まずWithSecure Elements EPPポータルにログインし、右上の を選択し、[設定]を選択します。[言語] ドロップダウンメニューから、ポータルで使用する言語を選択し、[保存]を選択します。

E.2 WithSecure Email and Server Securityのメール設定はポータルのどこにありますか

WithSecure Elements EPPのポータルでは見つけることができません。ローカルのElements Endpoint Protection管理コンソールから設定を表示・変更することができます。

E.3 ポータルで新しいサブスクリプションキーを注文するにはどうすればよいですか

の WithSecure Elements Endpoint Protectionポータルサブスクリプションはパートナーポータルから注文できます。注文の詳細については、ここ。

E.4 ポータルで現在のサブスクリプションキーを更新または拡張するにはどうすればよいですか

注 : これはパートナーにのみ適用されます。

WithSecure Elements Endpoint Protectionサブスクリプション キーは、パートナー ポータルを通じて更新および拡張されます。

E.5 ポータルから削除したコンピュータの一覧を消去するにはどうすれば良いですか

WithSecure Elements EPPポータルからコンピュータを削除すると、対象のコンピュータはブロックリストに追加され、コンピュータはポータルに再接続することができなくなります。これにより、WithSecure Email and Server Security (ESS) は、ブラックリストに含まれているコンピュータを同じコンピュータ (該当するライセンス キーコードで) に新しくインストール することを拒否します。新しいまたは異なるサブスクリプションキーはこのコンピュータ上で動作するため、このコンピュータは特定のサブスクリプションキーに関連付けられている場合にのみ、ポータルへの接続がブロックされます。

E.6 セキュリティ プロファイルはどのような場合に作成する必要がありますか

WithSecure Elements EPP for ComputersおよびWithSecure Elements for ServersではWithSecureの事前定義されたプロファイルの中にエンドユーザのニーズに合うものがない場合、新しいセキュリティ プロファイルを作成する必要があります。たとえば、リアルタイムのスキャン操作によって動作が遅くなるプログラムがコンピュータ上にある場合、そのプログラムをスキャン対象から除外するプロファイルを作成する必要があります。また、VPNクライアントのようなネットワークソフトウェアが、デフォルトのファイアウォールルールではインターネットに接続できない場合、そのソフトウェアに特化したファイアウォールルールを持つ新しいセキュリティプロファイルを作成する必要があります。

E.7 WithSecure Server Securityのインストール中に SQL について尋ねられます。なぜですか?

間違ったライセンス キーコードを入力した可能性があります。たとえば、WithSecure Server Security をインストールしているのにWithSecure Email and Server Securityのライセンス キーコードを使用した場合など。ライセンス キーコードのタイプはWithSecure Elements EPPポータルの「ライセンス」タブで確認できます。

注 : WithSecure Server Securityソフトウェアは、2020年2月にサポート終了になりました。

E.8 インストールしたソフトウェアを再初期化する方法を教えてください。

`fs_oneclient_logout`ツールを使用すると、WithSecure Elements EPP for Computersからログアウトできるため、サブスクリプションキーを再入力して、デバイスを管理ポータルの正しい会社に接続できます。

このコマンドラインツールは、WithSecure Elements EPP for Computersから現在のサブスクリプションを削除し、サブスクリプションキーが使用される前の初期状態に戻します。

ヒント : これは、たとえば、メインの画像から新しいCitrixインスタンスを複製する場合に便利です。

製品を再初期化するには

1. 管理者権限でコマンド プロンプトを開きます。
2. 次のコマンドを実行して、WithSecure Elements EPPクライアントのインストールディレクトリに移動します。

```
c: && cd %ProgramFiles(x86)%\F-Secure\PSB
```

3. 製品からログアウトしてWithSecure Elements Endpoint Protectionポータルに自動的に登録するには、次のコマンドを入力します。

```
.\fs_oneclient_logout.exe
 --keycode <subscription-key>
```

製品からログアウトされ、入力したサブスクリプションキーを使用するようになります。

製品を再初期する際に次のコマンドラインパラメータを使用できます。

パラメータ	説明
--psb1, --psb2, --psb3, --psb4, --psbsmieu	ポータル間で登録されたクライアントの切り替えを許可します。 **注:** クライアントを別のポータルに切り替える場合にのみ、ポータル名を指定します。同じポータル内でサブスクリプションキーを切り替える場合は、これらのコマンドパラメータを追加しないでください。
--nokeycode	現在のサブスクリプションキーを削除します。製品 WithSecure Elements EPP for Computers が動作を停止し、アプリケーションのメインビューを開くと、新しいサブスクリプションキーを手動で入力するように求められます。

パラメータ	説明
--profile-id <profileId>	任意のプロファイルを強制的に割り当てることができます。デバイスを再登録すると、デフォルトのプロファイルがデバイスに割り当てられます。このパラメータを使用して、デバイスに目的のプロファイルを割り当てることができます。例 `"%ProgramFiles(x86)%\F-Secure\PSB\fs_oneclient_logout.exe" --keycode <サブスクリプションキー> --profile-id profileId` **注:** 目的のプロファイルが製品に保存されます。--profile-idコマンドラインパラメータを追加せずに`fsoneclientlogout.exe`ツールを再度使用すると、同じプロファイルが再度割り当てられます。
--proxy	ログインの処理中に使用するプロキシを指定します。例 `--proxy your.proxy:80` **注:** プロキシは、proxy:portの形式にする必要があります。
--wait-uuid-changed	クローン作成の直後にSMBIOS UIDが変更されない場合は、クローン作成された仮想マシンで使用できます。`fs_oneclient_logout.exe`ツールをこのオプション `fs_oneclient_logout.exe --wait_uuid_changed` と一緒にに使用する場合、システムはUUIDが変更されるまで待機し、デバイスがWithSecure Elements EPPポータル上で正しい一意のIDで登録されていることを確認します。 このオプションは、SMBIOSを使用してデバイスを識別する場合にのみ機能します。他の識別方法が使用されている場合は効果がありません。

ツールが正常に実行されると、`0`が返されます。他の場合、たとえば、ネットワークが利用できない場合、または誤ったサブスクリプションキーを入力した場合、WithSecure Elements EPP for Computersは「失効」状態のままで、新しいサブスクリプションキーを手動で入力するように求めます。

E.9 WithSecure Elements Mobile Protection を WithSecure Mobile Security または WithSecure FREEDOME と並行して実行できますか?

技術的には可能ですが、レガシーソリューションを削除することを強くお勧めします WithSecure Mobile Security または WithSecure FREEDOME をインストールした後 WithSecure Elements Mobile Protection 追加の価値がないからです。