WithSecure Elements

Administrator's Guide

目次

第
1
章

WithSecure Elementsソリューションの紹介

トピック：

このページでは、WithSecure Elementsソリューションの概要を説明します。

WithSecure Elementsの概要

「WithSecure Elements」は、エンドツーエンドのビジネスとクラウドに対応するサイバーセキュリティアプリケーションで構成された当社の単一モジュール型ソリューションです。本製品には、脆弱性管理、パッチ管理、エンドポイント保護、エンドポイントの検出および応答など、受賞歴のあるWithF-Secureの技術が含まれています。予測不可能で変化し続ける今日のビジネス環境において、当社のオールインワンセキュリティソリューションは、レジリエンス（回復力）のあるビジネスの構築と確保をサポートします。

WithSecure Elementsの特長

WithSecure Elementsは、外部の脅威だけでなく、変化するビジネスのニーズにも常に適応する必要がある、現代のアジャイルビジネス環境をサポートするために特別に設計されています。

主なメリット

- 生産性を向上させるためのサイバーセキュリティ管理の一元化と合理化
- 必要なソフトウェアコンポーネントを1つにまとめ、スムーズな導入を実現
- フルマネージドサービスとしても、セルフマネージドクラウドソリューションとしても利用可能

また、本ソリューションは柔軟なライセンスオプションを提供しており、ビジネスの必要性応じてWithSecure Elementsのアプリケーションを個別に選択することができます。

対応言語

Elementsのすべてのタッチポイントにおいて、言語サポートが合理化されました。これにより、すべてのElements製品および関連するサポートやドキュメントは、以下のように同じ言語セットを提供することになります。

- 英語（米国）、フィンランド語、フランス語、ドイツ語、イタリア語、日本語、ポーランド語、ポルトガル語（ブラジル）、スペイン語（ラテンアメリカ）、スウェーデン語

WithSecure Elementsのトレーニング

Elementsの入門的なトレーニングセッションを受けるには、パートナーポータルからWithSecureアカデミーにログインしてください。

WithSecure Elements Security Centerにアクセスする

次のURLからElements Security Centerにアクセスできます。
elements.withsecure.com

1.1 WithSecure Elements Security Centerにアクセスする

この章では、WithSecure Elements Security Center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WithSecure Elements Security Centerで表示される情報を設定できます。

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ー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。

1.1.1 ログイン

このセクションでは、WithSecure Elements Security Centerにログインする方法について説明します。

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。

非フェデレーションドメインにログインする

非フェデレーションドメインにログインする方法を説明します。

非フェデレーションドメインにログインするには、次の手順を実行します。

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。

   Elements Security Center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。

フェデレーションドメインへのログイン

フェデレーション ドメインにログインする方法を説明します。

フェデレーション ドメインにログインするには、次の手順を実行します。

注 : SSO による認証を試みる前に、Entra アカウントがあることを確認してください。新規ユーザーの場合は、アカウントを作成する必要があります。

1. Webブラウザで次のリンクを開きます。https://elements.withsecure.com/
   Microsoft ログイン ページにリダイレクトされます。
2. Entra の資格情報を入力し、[ログイン] を]選択します。

   重要 : 初めてご利用の場合、ドメイン連携前に WithSecure Business Accountをお持ちの場合は、Microsoftログインページにリダイレクトされ、認証用のMicrosoft認証情報を入力します。これにより、アカウントが連携シングルサインオンにリンクされます。次回以降のログインでは、Microsoft Entra IDアカウントを使用したSSO認証が行われます。

Elements Security Center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。

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 Security Center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。Elements Security Center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標準をサポートする セキュア**USB**キー（https://fidoalliance.org/fido2/）
- 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. 電子メール アドレスとパスワードを使用して、WithSecure Elements セキュリティ センターにログインします。
2. 選択右上隅にある [マイ設定]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。

デバイスの生体認証の使用

生体認証では、まず別の多要素認証 (MFA) 方法を使用する必要があります。

デバイスの生体認証を使用するには、次の手順を実行します。

1. Elements Security Centerで、右上隅にある [マイ設定]を選択します。
   「マイ設定」ウィンドウが開きます。
2. すでに 1 つ以上の MFA 方法が構成されている場合は、[変更]を選択します。
   「指紋認証または顔認証を使用してログインする」ウィンドウが開きます。
3. [別の方法を試すを]選択します。
4. 以前に設定した MFA 方法を使用して ID を確認し、[続行]を選択します。
   「このデバイスでより速くログイン」ウィンドウが開きます。
5. [続行]を選択します。
   「パスキーを保存」ウィンドウが開きます。
6. [続行]を選択してパスキーをデバイスに保存し、[**OK**]を選択します。
   デバイス登録成功ウィンドウが開きます。
7. [続行]を選択します。
   多要素認証設定ウィンドウに、新しいデバイスの生体認証キーが表示されます。
8. 画面下部の [戻る]を選択して ホームビューに戻ります

次回このデバイスで Elements Security Centerにログインする際は、生体認証キーを使用して認証を行うことができます。これにより、認証プロセスがより迅速かつ安全になります。

多要素認証を取り除く

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、[続行]を選択します。
3. 右上の を選択し、[設定] を選択します。
4. 多要素認証が有効の横にある [変更を]選択します。
   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. 削除する多要素認証方法の横にある [削除]を選択します。
7. メールアドレスとパスワードを入力してください。

1.1.2 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。

アクセス権について

エンドポイント保護（EPP）機能へのアクセスを許可された新規ユーザーは、拡張検出および対応（XDR）機能へのアクセスを自動的に許可されるわけではありません。管理者は、EPPとXDRの機能を別々のユーザーグループに割り当て、必要に応じて組み合わせることができます。

Exposure Managementへのアクセス権を付与された新規ユーザーには、スキャンの構成やレポートの実行など、脆弱性関連の問題を管理するための 脆弱性ロールも割り当てられる必要があります。

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、アクセス権を設定できます。

露出管理

サブカテゴリ	ロール	説明	監査ログエントリ
暴露	完全編集	次のエクスポージャー管理機能へのアクセスを許可します。 • 環境：デバイス、クラウド、ネットワーク、エクスポージャー、アイデンティティ • セキュリティ構成 • レポート • 管理 • クラウドオンボーディング 注：セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます（IAMロールに置き換えられます）	cspm: 管理者
脆弱性	管理	脆弱性管理ビュー、設定、および調査結果へのフルアクセスを許可します 注：セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます（IAMロールに置き換えられます）	vm: 管理者
脆弱性	チームメンバー	ユーザーとシステムを管理する権限なしで、脆弱性管理ビュー、設定、および結果にアクセスできます。	vm: チームメンバー

サブカテゴリ	ロール	説明	監査ログエントリ
脆弱性	読み取り専用	ユーザーを管理する権限のない、表示のみのアクセス。	vm: 読み取り専用チームメンバー

コラボレーション保護

サブカテゴリ	ロール	説明	監査ログエントリ
コラボレーション保護	管理者	コラボレーション保護ビューにアクセスし、次の保護機能を編集できます。 • 検出を処理する • Exchangeと共有ファイル設定を管理する • ポリシーの管理、ファイルの隔離、レポートの生成	cpo365:admin
コラボレーション保護	読み取り専用	Collaboration Protectionビューへの表示専用アクセスを許可します。	cpo: 読み取り専用
コラボレーション保護	検疫管理者	検出および隔離ファイルに関連するCollaboration Protectionビューへのアクセスを許可します。	cpo365:quarantine_mgr
管理	管理者	ユーザーの作成、ロールの管理、サブスクリプションの詳細、組織の設定などの管理機能へのアクセスを許可します。 注：セキュリティ管理者は追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てることができます（IAMロールに置き換えられます）	fusion_admin

エンドポイント保護

サブカテゴリ	ロール	説明	監査ログエントリ
	アクセス不可	以下のエンドポイント保護機能にはアクセスできません: • デバイス管理 • パッチ管理 • デバイスのセキュリティポスチャ • ソフトウェアの評価 • セキュリティイベント • プロフィール • ホーム/エンドポイント保護 • レポート 注: アクセスが他のロール(たとえば、Exposure)から行われない限り。	
コンピューターとモバイル	完全編集	次の機能へのアクセスを許可します: • セキュリティ構成/プロファイル • デバイスのステータス、ダッシュボード、セキュリティイベント、パッチ管理などのセキュリティ情報 • デバイスの削除や隔離、プロファイルの更新などのセキュリティ操作 • サブスクリプションを管理する • ユーザーアカウントの管理 • クラウドオンボーディングを行う 注: 追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てるには、セキュリティ管理者ロールと「サーバー - フル編集」ロールが必要です (IAM ロールに置き換えられます)。	epp:コンピュータとモバイルのみを管理する または epp: manage_all

サブカテゴリ	ロール	説明	監査ログエントリ
コンピューターとモバイル	読み取り専用	操作を実行したり、他のユーザーやプロファイルを管理したりする権限のない読み取り専用アクセス。	epp:サーバーのみを管理する または epp: 読み取り専用
サーバー	完全編集	次の機能へのアクセスを許可します: • セキュリティ構成/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 • デバイスの削除や隔離、プロファイルの更新などのセキュリティ操作 • サブスクリプションを管理する • ユーザーアカウントの管理 注: 追加の管理者を作成し、同じ組織内のユーザーにこのロールを割り当てるには、セキュリティ管理者ロールと「コンピューターとモバイル - フル編集」ロールが必要です (IAM ロールに置き換えられます)。	epp:サーバーのみを管理する または epp_manage_all
サーバー	読み取り専用	操作を実行したり、他のユーザーやプロファイルを管理したりする権限のない読み取り専用アクセス。	epp:コンピュータとモバイルのみを管理する epp: 読み取り専用

拡張検出および対応

サブカテゴリ	ロール	説明	監査ログエントリ
オフにする	アクセス不可	次の領域の拡張検出および対応(XDR)コンテンツを表示するためのアクセス権がありません。 • Broad Context Detection • 応答アクション • 自動化されたアクション • 検出と対応に関連するダッシュボードコンテンツ • ソフトウェアの評判 • 検出と対応に関連する組織設定 • 検出および対応レポート • イベント検索ページ • WithSecureに報告 • サブスクリプションビュー	

サブカテゴリ	ロール	説明	監査ログエントリ
Broad Context Detection	完全編集	管理権限: • 広範なコンテキスト検出（例：ステータスの変更やクローズ検出） • 私のレポート • ダッシュボード上の検出と対応に関するコンテンツ • 検出と対応に関連するソフトウェアの評判と組織の設定 • 該当する場合は WithSecure に昇格します • リクエスト アクセス制限: • デバイスビュー • クラウドビュー • サブスクリプションビュー クイックアクションを発行するには、応答の実行などの追加ロールが必要です。 注**:** この権限ではクラウドテナントを設定する権限は付与されません。このレベルのアクセスには、コンピューターとモバイルの完全な編集権限が必要です。	要素:xdr-incident-full

サブカテゴリ	ロール	説明	監査ログエントリ
Broad Context Detection	読み取り専用	拡張検出および応答(XDR)の場合の既定値。次の項目に対する読み取り専用アクセスが許可されます。 • Broad Context Detection • 私のレポート • ダッシュボード上の検出と対応に関するコンテンツ • ソフトウェアの評判 • 検出と対応に関連する組織設定 • 該当する場合はWithSecureに昇格します • デバイス • 雲の景色 • リクエスト サブスクリプションビューへのアクセスは制限されています。	要素:xdr-incident-read
応答	応答を実行する	実行するためのアクセス: • 対応措置 • 自動アクションを設定する クラウドビューへのアクセスが制限されています。	要素:xdr-response-full
応答	回答をリストする	レビューへのアクセス: • 実行された対応アクション • それぞれの結果が利用可能 アクセス制限: • デバイスビュー • クラウドビュー 応答結果をダウンロードするには、応答の実行権限が必要です。 サブスクリプションビューへのアクセスは制限されています。	要素:xdr-response-read

サブカテゴリ	ロール	説明	監査ログエントリ
応答	アクセス不可	実行またはレビューのアクセス権がありません: • 応答アクション • 自動化されたアクション	
イベント検索	読み取り専用	イベントデータの確認、フィルタリングされた検索の実行、カスタマイズされたビューの作成にアクセスします。 サブスクリプションビューへのアクセスは制限されています。	要素:xdrイベント検索
イベント検索	アクセス不可	イベントデータを確認するためのアクセス権がありません。	

要素管理

サブカテゴリ	ロール	説明	監査ログエントリ
	アクセス不可	新しいユーザーを作成したり、他のユーザーのアクセス権を管理したりする権限がありません。	
	アイデンティティとアクセス管理	すべての Elements ユーザーを作成、削除、管理する権限。	

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 Security Centerで表示される情報を設定できます。

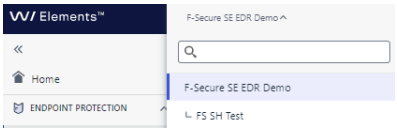
Elements Security Centerには、アクセス権を決定するさまざまなアカウントレベルがあります。

- 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。Elements Security Center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。Elements Security Center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Elements Security Center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、Elements Security Center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。

要素のアイデンティティとアクセス管理 (IAM) ロール

Identity and Access Management (IAM) ロールには、IAM 管理者自身の組織および関連エンティティ内のセキュリティ管理者のすべての Elements権限を付与および取り消す権限が付与されます。

概要

IAM ロールは、WithSecure Elements内の強力なロールです。セキュリティ機能とサービスの管理を合理化し、強化するように設計されています。

IAM 管理者には、自身の組織および関連エンティティ内のセキュリティ ロールを管理する権限があります。これには、セキュリティ管理者のロールの付与と取り消しが含まれます。

Elementsエコシステムが拡大するにつれて、IAM 管理者は新しい機能とサービスも管理できるようになり、面倒な自己登録プロセスが不要になります。

セキュリティ管理者は、Elements Security Centerビジネス アカウントを使用して WithSecureにアクセスします。アクセスは、特定の機能、能力、およびサービスに従って整理されます。IAM ロールにより、これまで複雑だったさまざまな機能にわたるロールの割り当てプロセスが簡素化されます。

利点

IAM ロールには、次のようないくつかの利点があります。

- WithSecure Elements全体での合理化された役割管理
- 集中管理によるセキュリティの強化
- 新しい機能やサービスを管理する能力で将来のニーズに適応する

IAM ロールの申請

IAMロールに権限のエスカレーションが含まれないユーザー(つまり、組織内のすべての従来のユーザーアクセス管理ロールを所有しているユーザー) の場合、セキュリティ管理者ビューには、新しい IAM 管理者ロールを要求する機会を提供するバナーが表示されます。IAM 関連の権限はセキュリティ管理ロールとは異なるため、すべての組織は IAM 関連の権限の管理方法を慎重に検討する必要があります。その結果、このオプションが利用できなかったときと比べて、IAM管理者として行動できる個人の数は少なくなります。

要素 IAM ロールのプロパティ

IAMロールの所有者(IAM管理者とも呼ばれます)は、組織内およびその子組織内の他の機能またはサービス固有のロールへのアクセスを許可または取り消すことができます。

IAM 管理者は次の操作を実行できます。

- 自分自身に他の役割を与え、それによってセキュリティ機能やサービスにアクセスできるようになる
- WithSecure for Elementsの機能またはサービスによって導入された新しいロールを付与または取り消す
- ロールを付与または取り消すことで、WithSecureビジネス アカウントを作成または削除します。
- 同じ組織内またはその子組織内の他のセキュリティ管理者に IAM 権限を譲渡します。

IAMロールの取得

独自のセキュリティを管理したり、他の組織にセキュリティ機能を提供したりしている組織には、少なくとも 1 人の IAM 管理者が必要です。IAM ロールは、次のいずれかの方法で取得できます。

- 同じ組織または親組織内の別のIAM管理者によってロールが付与されている
- 会社向けに発行された Elementsサブスクリプションによる自己登録
- 新規パートナーや顧客企業向けの WithSecureによるオンボーディング

既存の機能またはサービス固有のロールは引き続き有効ですが、最終的には IAM ロールを通じて管理されるようになります。IAM ロールは、API キーの構成など、現在他のロールによって管理されている機能へのアクセスも保護します。

IAM権限の移行

移行プロセスの目的は、従来の機能固有の IAM ロールから、より高い権限を付与する新しい Elements IAM ロールに移行することです。このプロセス中に、Elements適格なユーザーを識別し、新しい IAM ロールを要求するように促します。

IAMロールの候補者は、従来の機能固有のIAMロールの所有と、アクティブな会社のサブスクリプションの確認に基づいて特定されます。

- 顧客企業の場合: 以下の特定の従来の役割を持つセキュリティ管理者:
  - Elements Exposure Management：フル編集
  - Elements Collaboration Protection：管理管理者
  - Elements Vulnerability Management:管理者
  - Elements Endpoint Protection - コンピューター、サーバー、モバイル: 完全な編集
- ソリューション プロバイダーおよびサービス パートナー向け: 管理対象企業が使用するすべての機能とサービスに対する従来のロールを持つセキュリティ管理者

注 : パートナー向けのポリシーは顧客企業向けのポリシーとは異なり、資格のある管理者のみが IAM ロールを要求するようにします。

IAM管理者候補が特定できない場合

一部の組織では、セキュリティ管理者間で従来の機能固有のロールを割り当てると、IAMロールによって付与されるのと同じ有効なアクセス権を持つユーザーが1人もいない状況になることがあります。これは、たとえば、企業が Elements Endpoint Protectionと Elements Collaboration Protection両方の機能を採用しているが、これらの機能が2人の異なる個人によって個別に管理されており、同時に両方を監督する人がいない場合に発生する可能性があります。

IAM ロールに関するよくある質問

このトピックでは、IAM ロールに関するよくある質問に回答します。

パートナー(SOP/SEP)は、傘下のすべての企業に対して IAM ロールを作成できますか?	はい、パートナーレベルのIAM管理者は、XM/CP アクセスをSOPから分離することを選択した企業を除き、自身の組織とその傘下の組織を完全に管理できます。
企業が IAM 期限 (2025 年 4 月末) に間に合わなかった場合、企業管理者は何をすべきでしょうか?	会社の管理者は、サービス パートナーに問い合わせてサポートを受けるか、WithSecureサポートに連絡する必要があります。
セルフ登録ポータルを使用して新しいユーザーを作成すると、最初の管理者は IAM ロールを自動的に取得しますか?	はい、最初の管理者には IAM ロールが自動的に付与されます。
最高レベルの管理者ロールを要求するときに、誤って [拒否] を選択した場合はどうなりますか?	ユーザーが誤って IAM ロールの要求を拒否した場合でも、必要に応じて他の IAM 管理者が IAM ロールを割り当てることができます。
[拒否]を選択した Endpoint Protection 管理者ユーザーは、他の Endpoint Protection 管理者ユーザーを追加できますか?	はい、当面はまだ可能です。将来的には、すべてのユーザー管理アクション権限は IAM ロール所有者のみに制限されます。
1 つの組織に複数の IAM 管理者ユーザーを設定できますか?	はい、組織が持つことができる IAM 管理者の数に制限はありません。
一部の管理者ユーザーに請求および拒否のオプションが表示されないのはなぜですか?	最初の段階では、組織がサブスクリプションを所有しているすべての製品に対して完全な管理者権

	限を持つユーザーに [IAM Claim (IAM 要求)] ボタンが表示されます。たとえば、会社が Elements Endpoint Protection と Collaboration Protection のサブスクリプションを所有している場合、両方の製品に対して完全な管理者ロールを持つユーザーに [IAM Claim (IAM 要求)] ボタンが表示されます。
組織内で誰が IAM ロールを要求したかを確認するにはどうすればよいですか?	IAMロールが表示され、そのロールを持つユーザーは [管理] > [セキュリティ管理者]の下のテーブルでフィルタリングできます。

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 Security Centerにおいて必要な権限を付与することができます。

ソリューション プロバイダー、サービス パートナー、または会社のアカウントの管理者を追加できます。

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. [セキュリティ管理者] タブを選択します。

   注 : Elements Security Center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
3. スコープセレクターを使用して、新しい管理者アカウントを作成する組織レベルを選択します。
4. [管理者の追加を]選択します。
5. [管理者の追加] 画面で、次のように管理者の詳細を入力します。
   - メールアドレスを入力します。

     注 : メールアドレスは有効なもので、実際のアカウントユーザーがアクセスできるものである必要があります。共有アカウントは使用しないでください。
   - 新しい管理者に必要な言語を選択します。
6. [次へ] を選択します。
7. [ロール] 画面で、新しい管理者が持つ必要があるロールを選択します。

   注 : 新しい管理者に機能固有のロールでのフル クセスが許可されていない場合は、デフォルトの [アクセスなし] オプションをそのままにしておきます。
8. [次へ] を選択します。
   概要画面が開きます。
9. 選択したロールの管理者詳細が正しいことを確認し、[追加] を選択して新しい管理者の追加を完了します。

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。

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. [一般] タブを選択します。
3. ⋯ を選択し、次に [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 パートナーアカウントの作成] ビューが開きます。
4. 組織アカウントの名前を入力し、[保存]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。

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. [セキュリティ管理者] タブを選択します。
3. [メールアドレス] 列で、編集または削除する管理者アカウントのメールアドレスを選択します。
   概要画面が開きます。
4. 管理者アカウントを変更するには
   a) 管理者ロールに必要な変更を加えます。
   b) [保存] を選択します。
   管理者アカウントの情報が更新されます。
5. 管理者アカウントを削除するには、[削除] を選択します。

   注：管理者アカウントからすべてのアクセス権を削除すると、変更を保存するとアカウントは自動的に削除されます。

   管理者アカウントが削除されます。

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。

1.1.3 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。

顧客企業を追加する

WithSecure Elements セキュリティ センターアカウントに新しい *顧客会社* を追加するには、まずその会社を ***WithSecure*** *パートナー ポータル* アカウントに *新しい顧客* として追加し、その会社に対して少なくとも 1 つの WithSecure Elements製品を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。

新しい顧客企業でサブスクリプションとデバイスを管理する管理者が必要な場合は、Element Security Centerを通じて 管理者アカウントを作成する必要があります。

注：WithSecureパートナー ポータルは、Element Security Centerと連携して機能し、WithSecureソリューションの販売とサポートを促進するツール、資料、統合された電子注文システムを提供するオンライン サービスです。

新規顧客の注文書がパートナーポータルアカウントから正常に追加されると、Element Security Centerアカウントに新規顧客会社として自動的に追加されます。

その後、顧客企業のユーザーにWithSecure Elements製品を提供したり、購入した製品のサブスクリプションを管理したりできるようになります。

企業アカウントにサブスクリプションキーを割り当てる

企業アカウントにサブスクリプションキーを追加すると、WithSecure Elements Security Centerにコンピューターを割り当てることができます。

以下の点を考慮する必要があります。

- ソリューションプロバイダおよびサービスパートナーは企業アカウントにサブスクリプションキーを割り当てることができます。
- 企業ユーザーは、パートナーから提供された未使用のサブスクリプション キーを自社の組織に割り当てることができます。
- ユーザーには、Endpoint Protectionソフトウェアでの完全な編集ロールが付与されている必要があります（コンピューターとサーバーの両方に適用されます）。
- サブスクリプションはパートナーレベルで割り当てる必要があります（サブスクリプションキーが存在する必要があります）。パートナーは、サイドバーの[管理]の下の[サブスクリプション]ビューでサブスクリプションキーを見つけることができます。

  注：企業ユーザーはパートナーにサブスクリプションキーを要求する必要があります。

サブスクリプションキーを割り当てるには

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。
2. スコープ セレクターで、サブスクリプションキーを割り当てる会社を選択します。
   選択した会社の現在のサブスクリプションの一覧表が開きます。
3. フィルターの上にある [サブスクリプションを割り当てる] を選択します。
   [サブスクリプションを割り当てる] ページが開きます。
4. 企業アカウントの新しいサブスクリプションキーを入力して [**OK**] を選択します。

新しいサブスクリプションキーが企業アカウントに追加されます。

顧客企業に製品を注文する

WithSecureパートナーポータルを通じて、顧客企業向けのWithSecure Elements製品を注文できます。

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 パートナー ポータルから WithSecure Elements製品を注文するには:

1. ウェブ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では、WithSecure Elementsセキュリティセンターとは別のログイン認証情報が必要です。ログイン情報がまだお手元にない場合は、ページ上の「認証情報のリクエスト」フォームにご記入の上、[送信」を]クリックしてください。アクセス認証情報が届くまで最大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。

   購入注文が完了すると、製品情報の変更が WithSecure パートナー ポータルと Elements Security Center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。

注文が完了すると、新しい顧客企業が、購入した製品とともにパートナー ポータルアカウントに表示されます。

注：新しい顧客会社が Elements Security Centerアカウントに表示されるまでには、しばらく時間がかかる場合があります。

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。

サブスクリプション キーを変更する

WithSecure Elements Security Center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。

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コンピューターに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。

1.1.4 フェデレーションシングルサインオン

このセクションでは、フェデレーション シングル サインオンについて説明し、その設定方法について説明します。

フェデレーション シングル サインオン (FSSO) は、ユーザーが異なるドメインや組織にまたがる複数のアプリケーションやサービスに、それぞれ個別にログインすることなく認証してアクセスできるようにするメカニズムです。ユーザーがログインすると、資格情報 (ユーザー名やパスワードなど) を ID プロバイダーに送信し、ID プロバイダーはこれらの資格情報を検証します。認証が成功すると、ID プロバイダーはユーザーの ID の証明として機能するデジタル署名されたトークンを生成します。ユーザーが別のドメインや組織にある他のアプリケーションやサービスにアクセスすると、ブラウザーは自動的にこのトークンを使用します。クラウド ID サービスはトークンを検証し、ユーザーに再度ログインを要求することなくアクセスを許可します。

FSSOは、ユーザーが一度認証すれば、さまざまなアプリケーションやサービス間をシームレスに移動できるようにすることで、さまざまなシステム間のアクセスを簡素化します。複数回のログインが不要になるため、セキュリティとユーザー エクスペリエンスが向上します。さらに、ユーザーが ID プロバイダーから削除されると、Elements Security Centerにログインする機能が自動的に失われるため、ユーザー アクセスの管理がより簡単かつ安全になります。

前提条件

Entra アカウントを WithSecure Elementsアカウントにリンクするには、Entra ID テナント アカウントに電子メール アドレスが設定されており、対応する Elementsアカウントの電子メール アドレスと一致している必要があります。

電子メール アドレスが設定されていないか、対応する Elementsアカウントの電子メール アドレスと一致しない場合、リンクは失敗し、ユーザーは WithSecure Elements Security Centerにアクセスできません。ユーザーの電子メール アドレス情報は Microsoft Entra Admin Centerの [連絡先情報] > [電子メール] に表示されます。

注：すべてのユーザーは Elementsアカウントを持っている必要があります。Microsoft Entra ID からの自動ユーザー プロビジョニングはありません。

シングルサインオン（SSO）を実装する前に

以下に、シングル サインオン (SSO) を実装する前に考慮する必要がある事項を示します。

プラスアドレス指定が問題となるのはなぜですか?

Microsoft Entra ID認証に電子メール エイリアスまたはプラス アドレスを持つ電子メール アドレスをサポートしていません。SSO を構成して使用を開始すると、プラス アドレスを持つすべての電子メール エイリアスと Elementsユーザー アカウントが機能しなくなります。

重要：

電子メール エイリアスまたはプラス アドレスを持つ Elementsユーザー アカウントを使用して SSO を設定しないでください。

ユーザーがフェデレーションを削除するためのアクセス権を失わないようにするにはどうすればよいですか?

フェデレーションを実装する場合は、プラス アドレスまたは電子メール エイリアスのないユーザー アカウントがあることを確認してください。そうしないと、Elements Security Centerにアクセスできなくなる可能性があります。

SSO はログインプロセスをどのように変更しますか?

フェデレーション後、ユーザーは Microsoft Entra IDを通じて認証されるため、Elements Security Center の個別のログイン フローは不要になります。

Elements Entra ID を持つユーザーは、どのくらいの頻度で Elements Security Center に対して認証する必要がありますか?

ユーザーに有効なフェデレーション認証セッションがない場合、Elements Security Centerログインと認証が要求されます。

SSOの世界的な影響

SSO を実装すると、フェデレーションされた電子メール ドメインのユーザー アカウントを持つすべての組織と階層に影響します。一部のユーザーは、さまざまなパートナー レベルおよびサービス パートナー レベルの階層にアカウントを持っているため、変更はこれらすべての階層に影響します。たとえば、パートナー A が独自のソリューション プロバイダー (SOP) を持ち、他のパートナーの SOP とドメインを共有している場合、SSO は特定の SOP だけでなく、要素レベルのすべてに影響します。電子メール ドメインは組織内で1回しかフェデレーションできませんが、そのドメインに関連付けられているすべてのユーザー アカウントに影響します。

階層レベルの考慮事項

SSO は適切な階層レベルからのみ変更できるため、必ず適切な階層レベルから生成してください。

Microsoft Entra ID アカウントの削除の処理

Microsoft Entra ID アカウントが削除された場合、Elements管理者は自動的に削除されませんが、アカウントは機能しなくなります。管理者は手動で削除する必要があります。

Microsoft Entra ID を使用したフェデレーション シングル サインオンの設定

Microsoft Entra ID フェデレーション シングル サインオンを設定する方法について説明します。

フェデレーション シングル サインオンを作成するには、次のものが必要です。

- 非フェデレーション ドメイン - Elements Security Centerとフェデレーションされていないドメイン名 (例: `yourcompanydomain.com`)
- Elements Security Centerアカウント - `Endpoint Protection` の完全編集権限が割り当てられた Elements Security Centerのアカウント。このアカウントは、フェデレーション ドメインを管理し、後で Entra ID アカウントを使用して Elements Security Centerに ログインするために必要です。

- Entra ID テナント アカウント - フェデレーションするドメインを管理する Entra ID テナント内のアカウント。このアカウントは Elements Security Centerにログインしてドメインをフェデレーションするために不可欠です。

  注: このシナリオでは、ドメインをフェデレーションするユーザーは、Entra IDテナントのグローバル管理者ロールを持っている必要があります。ドメインがフェデレーションされると、対応する Elements アカウントも持っている限り、Entra アカウントを持つすべてのユーザーがログインできるようになります。

1. ログインhttps://elements.withsecure.com。
2. [管理] > [組織の設定] > [セキュリティ管理者]で、[フェデレーション シングル サインオンの構成] を]選択します。
   シングル サインオン アクセス フェデレーションウィンドウが開き、電子メール アドレスに一致するドメインのステータスが表示されます。
3. [Microsoftにログインを]選択
4. 開いたポップアップ ウィンドウで、Entraテナントのパスワードを入力し、[サインイン]を選択します。
5. [組織を代表して同意する]を選択し、[同意する]を選択します。
   シングルサインオンアクセスフェデレーションウィンドウが更新され、検証が成功したことが表示されます。

   注: [キャンセル]を選択すると、ウィンドウに [検証に失敗しました]と表示されます。検証が失敗するその他の理由としては、プロセスに時間がかかりすぎることや、グローバル管理者のロールが不足していることなどが挙げられます。

6. ドメインをフェデレーションするには、[フェデレーション シングル サインオンを有効にする]を選択します。
   ドメインをフェデレーションすると、そのステータスが [ドメイン名] に対してフェデレーション シングル サインオンが有効に変わります。

ユーザーIDのリンク

Elements Security Center でユーザー ID をリンクする方法を説明します。

注: ドメイン内の電子メールアドレスを持つすべてのユーザーは、ドメインがフェデレーションされた後の最初のログイン時に、自分の ID を 1 回だけリンクする必要があります。

以下のものを用意してください。

- フェデレーションドメイン
- フェデレーションドメインに属する電子メールアドレスを持つElementsアカウントを持つユーザー

  注: これらのアカウントは他の管理者によって手動で作成されます。このフローは、ユーザーが初めてログインするときに発生します。

- ユーザーは現在ログインしていない必要があります
- Elements Security Centerへのログインに使用するアカウントは、以前にIDリンクが行われていない必要があります。

ID をリンクするには:

1. ログインhttps://elements.withsecure.com。
2. メールアドレスを入力し、[続行]を選択します。
3. 電子メールアドレスがドメインですでに認証されている場合は、IDリンクフローにリダイレクトされます。電子メールアドレスがドメインでまだ認証されていない場合は、ドメイン パスワードの入力を求められます。

   注: ドメインの構成によっては、多要素認証 (MFA) を実行する必要がある場合があります。

4. メールアドレスをもう一度入力し、[続行]を選択します。
5. 次に、Elementsアカウントのパスワードを入力し、[続行]を選択します。
   ビジネス アカウントが Entra ID アカウントにリンク (フェデレーション) されることを確認するウィンドウが開きます。
6. 続行するには [続行」を]選択してください。

ドメインからフェデレーションを削除する

ドメインからシングル サインオン フェデレーションを削除する方法について説明します。

ドメインからフェデレーションを削除する前に、次のものを用意してください。

- フェデレーションドメイン
- Endpoint Protection の完全な編集権限とフェデレーション ドメインの電子メール アドレスを持つ Elements Security Center のアカウント。

注：ドメインからフェデレーションが削除されると、そのドメインの電子メール アドレスを持つユーザーは、Elementの資格情報を使用してログインする必要があります。ただし、ドメインがフェデレーションされた後に Elements アカウントが作成された場合、ユーザーは初期パスワードが記載された電子メールを受信しておらず、Elementの資格情報がわかりません。その場合、ユーザーはパスワードをリセットする必要があります。

フェデレーションを削除するには:

1. ログインhttps://elements.withsecure.com。
2. [SSO アクセス フェデレーションを]選択します。
   フェデレーションシングルサインオンウィンドウが開き、電子メール アドレスに一致するドメインのステータスが表示されます。
3. [フェデレーションシングルサインオンの削除を]選択します。
   確認ウィンドウが開きます。
4. [OK]を選択します。
   シングル サインオン フェデレーションがドメイン アカウントから削除されます。

1.1.5 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ー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、まずコンピューター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WithSecure Elements Security Centerアカウントに追加されます。Elements Security Center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。
- ソフトウェアをElements Security Centerから直接ダウンロードし、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。

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。
  - WithSecure Elements EPP for Computers（WindowsおよびMac）
  - WithSecure Elements EDR and EPP for Computers（WindowsおよびMac）

  - コンピューター向けSecure Elements EDR（Windows、Mac、Linux）

    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 Elements EDRおよびEPP for Computers Premium (Windowsのみ)
  - セキュア要素露出管理（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（Windows/Linux）
  - WithSecure Elements EDR for Servers (Windowsのみ)
  - WithSecure Elements EPP for Servers Premium (Windowsのみ)
  - WithSecure Elements EDR and EPP for Servers Premium（Windows/Linux）
  - セキュア要素露出管理（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]の横にある[新しいデバイスを追加]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（19ページ）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、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。

Elements Security Center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 Security Center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. Elements Security Center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ー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。

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Elements Security Center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Elements Security Center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、そのコンピューター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。

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]の横にある[新しいデバイスを追加]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（19ページ）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、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 [デバイスの招待を管理します]。
   「デバイス招待の管理」ページが開きます。

   [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招待が一覧表示されます。[期限切れ]タブには、期限切れの電子メール招待が一覧表示されます。
3. 保留中の招待状については、インストール リンクが有効な間 (30 日間)、[リマインダーを送信]を選択してリマインダーを送信できます。その後、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、[新しい招待状を送信]を選択して別の招待リンクを送信できます。

   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、[保留中の削除] を]選択して、期限切れの招待状をテーブルから削除できます。

1.1.6 カスタムラベルによるデバイス管理の強化

ラベルを使用すると、カスタマイズ可能で柔軟なタグをデバイスに追加できます。

ラベルを追加すると、デバイスを任意の方法でグループ化できます。ラベルは、地域、オペレーティング システム、所有者、部門、ワークステーションとサーバー、またはニーズに合ったその他の基準に関する情報を提供するのによく使用されます。

ラベルは、より多くのコンテキストを提供することでアナリストを支援し、Elements Security Center 内でのデバイスの管理を容易にします。

関連タスク
デバイスラベルの追加（32ページ）
デバイス ラベルは 3 つの方法で追加できます。

デバイスラベルの追加

デバイス ラベルは 3 つの方法で追加できます。

- デバイスビューで手動で:
  - デバイスリストビュー
    1. デバイス リストビューで、ラベルを割り当てるデバイスを選択します。
    2. ページの下部にある [アクション]パネルで、[ラベルの管理] > [ラベルの追加]を選択し、既存のラベルを選択するか、新しいラベルを追加します。
    3. 選択したデバイスにラベルを割り当てるには、[追加] を]選択します。

- デバイスの詳細ビュー
  1. [アクション]パネルで、[ラベルの管理] > [ラベルの追加]を選択し、既存のラベルを選択するか、新しいラベルを追加します。
  2. 選択したデバイスにラベルを割り当てるには、[追加] を]選択します。

- プロファイルセクションのルールを使用する:
  1. Elements Security Centerで、[セキュリティ構成] > [プロファイル] > [プロファイル割り当てルール]に移動します。
  2. アウトブレイクルールとプロファイル割り当てルールのセクションでは、ルールごとに、ルールが一致したときにラベルを追加するオプションがあります。
- Elements エージェントのインストール プロセス中:
  - 詳細については、「デフォルト プロファイルとインストール タグの割り当て」セクションの手順 2 を確認してください。

注 : コマンドラインでは、ラベルはタグと呼ばれます。

1.1.7 Elements Security Centerでデバイスを管理する

選択したデバイスをWithSecure Elements Security Centerで管理する方法を説明します。

資産グループの管理

アセット グループは、組織内のデバイスを管理するための構造化された方法を提供します。

デバイスを資産グループに割り当てるには、次の 2 つの方法があります。

- 手動割り当て -デバイスページから管理グループにデバイスを割り当てます。
- 自動割り当て - プロファイル割り当てルールに基づいてデバイスをグループに割り当てます。

  注 : 1 つのルールでデバイスを複数のグループに割り当てることができます。

デバイスをグループに整理したら、次の操作を実行できます。

- グループ別にデバイスをフィルタリング
- 特定のグループに関連付けられたセキュリティイベントをフィルタリングする
- 各グループ内のデバイスのソフトウェア更新を一覧表示する

資産グループを活用することで、デバイスの可視性を高め、セキュリティ イベント管理を合理化し、組織内の高度なアクセス制御メカニズムを準備することができます。

資産グループの作成

資産グループを作成する手順。

注 : 資産グループは会社レベルでのみ作成できます。たとえば、パートナーの場合は、まず *スコープセレクター*から、または [管理] > [組織設定]の [全般]タブのリストから会社を選択する必要があります。

1. [管理]の下で、[組織設定] > [全般]を選択します。
2. [資産グループの作成を]選択します。
   資産グループの作成ペインが開きます。
3. 資産グループの名前を入力します。
4. [説明]ボックスに、資産グループの説明を入力できます。
5. [保存] を選択します。

次に、「デバイス」ページに移動して、作成した資産グループにデバイスを追加します。

資産グループへのデバイスの追加

資産グループにデバイスを追加する手順。

1. [環境]の下で、[デバイス]を選択します。
2. [デバイス]ページで、1 つ以上の資産グループに追加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、[資産グループの管理]>[資産グループへの割り当て]を選択します。
4. ドロップダウンメニューから、選択したデバイスを追加する1つ以上の資産グループを選択します。
5. [指定する] を選択します。

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 Security Center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]の横にある[新しいデバイスを追加]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（19ページ）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、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。
   - コンピューター - 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。

デバイスを自動的に削除する

WithSecure Elements Security Centerで、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できるように選択できます。

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。

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、そのコンピューター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。

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. 画面の左上にある 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顧客企業を確認できます。
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 構造は、会社のコンピューター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、そのドメイン内のコンピューターで WithSecure Elements EPP for Computersまたは WithSecure Elements EPP for Servers アクティブ化されるまで、WithSecure Elements Security Centerに表示されません。

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 : [すべてのフィルターをクリア]を選択すると、すべての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。
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. カスタマイズしたビューを保存するには、右上隅の [表示: 名前] > [を付けて保存]を選択します。

   注 : カスタマイズしたビューを削除するには、まず [ビューの削除]を選択し、次に [ビューの削除] ウィンドウで削除するビューを選択して [削除]を選択します。

診断ファイルを要求する

診断ファイルを WithSecureサポート チームにアップロードするようリモートでリクエストできます。

管理対象アカウント内のデバイスに問題が発生した場合、WithSecure Elements Security Center管理者は該当のデバイスを選択し、顧客にリクエストを送信します。顧客は診断ファイル（WSDIAG）を収集し、WithSecure Elements Security Centerにアップロードすることを許可します。診断ファイルは、問題の詳細とその根本原因を突き止める上で不可欠です。

注：この機能は、サーバーとワークステーションの両方の Elements Agent for Windowsと Elements Mobile Protectionで利用できます。

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は、Element Security Centerにログインし、関連する顧客アカウントに移動します。
2. 正しいアカウントにログインしたら、[環境]の [デバイス]を選択し、関連するデバイス (問題が発生しており、`wsdiag`ファイルが必要なデバイス) 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. ページ下部の 「アクション」パネルで、[診断ファイルの] > [リクエスト]を選択します。プライバシー保護のため、エンドユーザーには通知が表示されますが、サーバー側には表示されません。

   注：リクエストがユーザーに送信されたことを確認するには、顧客アカウントで [環境] > [デバイス] に移動し、右側にある3つのドットアイコンを選択して [操作の管理]を選択します。リストに [デバイスへの配信を待機中]というステータスのWSDIAG操作が表示されているかどうかを確認します。

4. ユーザーが診断ファイル（WSDIAG）の収集を許可していることを確認してください。許可するには、デバイスに通知が表示されたら [許可]を選択する必要があります。
5. ユーザーが診断 (WSDIAG) ファイルの収集を許可したら、顧客アカウントで [操作の管理]ページに戻り、ステータスが [成功、操作が実行されました]に変わっているかどうかを確認します。
6. 「操作の管理」ページで、作成されたWSDIAGファイルの参照番号を取得し、WithSecureサポートへのサポートチケットにこの番号を含めてください。サポートチケットで参照番号を確認すると、WithSecureがファイルをダウンロードして詳細な調査を行うことができます。[アクション]列の3つの点のアイコンをクリックすると、診断ファイルをダウンロードできます。

   注：WSDIAG ファイルはポータルから 2 週間後に自動的に削除されます。

1.1.8 要素データ復旧

WithSecureElementsサービスの可用性を維持し、必要なバックアップと必要な回復アクションを実行します。

あなたからのアクションは必要ありません。

重要：このバックアップには、WithSecure が提供するサービスに直接関連するデータのみが含まれます。ドキュメントやその他のデータをバックアップするのはお客様の責任となります。

第
2
章

Elements Endpoint Protectionの概要

トピック：

WithSecure Elementsは、コンピューターやモバイルのエンドポイントから、メールやサーバー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ー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サーバー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 サーバーにの強力なセキュリティ機能を提供します。

  注：すべてのサーバー製品は、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ー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 サーバー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。

2.1 製品を使用するには

WithSecure Elements Security Centerの使用を開始するには、次の手順に従ってください。

WithSecure Elements製品すべてを管理するための統合管理プラットフォームであるWithSecure Elements Security Centerにアクセスするには、WithSecure Business Accountが必要です。アクセスには2つのシナリオがあります。

- WithSecureのパートナーから製品をご購入いただくと、通常、パートナーは組織の最初の管理者用にビジネスアカウントを作成します。これに該当する場合は、WithSecureから一時パスワードとElements Security Centerへのログインリンクが記載されたメールが届いています。

  ヒント：電子メールメッセージが届かない場合は、まず迷惑メールフォルダを確認してください。

- 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は、そのサブスクリプションキーを使用して、組織の最初の管理者用のWithSecure Businessアカウントを作成できます。これを行うには、会社のセルフ登録リンクを使用してください。
  https://elements.withsecure.com/self-register

1. ビジネス アカウントの認証情報を使用して、https://elements.withsecure.com/にある WithSecure Elements セキュリティ センターにログインします。
2. 次のいずれかの方法で組織にデバイスを追加できます。
   - [電子メールによる招待を使用する]-少数のデバイスを手動でインストールする場合に適しています。
     a. [環境] > [デバイス]を選択し、3 つのドットのアイコンを選択して [新しいデバイスの追加] を選択します]。
     b. ウィザードの手順に従ってサブスクリプションを選択し、インストーラーのダウンロード リンクを含む電子メール招待状を 1 人以上のユーザーに送信します。
   - [インストーラーのダウンロード]- 多数のデバイスへの自動展開に適しています:
     a. サイドバーから [ダウンロード] を選択します。
     b. 必要なインストールパッケージを選択し、ツールとともに配布できるサブスクリプションキーが埋め込まれた製品を選択します。
3. [管理] > [組織設定] > [セキュリティ管理者] > [管理者の追加]を選択し、詳細を入力して管理者アカウントを作成します。
4. 次に、次のようにして、組織の特定のセキュリティ ニーズに合わせて独自のプロファイルを作成します。
   a) [セキュリティ構成] で、[プロファイル] を選択します。
   b) [**Windows**コンピューター用]または[**Windows**サーバー用]タブを選択し、[プロファイルを作成]を選択します。

      注：または、 次に、[プロファイルを複製して、]デフォルトのセキュリティ プロファイルの 1 つをベースとして使用します。

   c) 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。
   d) 設定を変更して、[保存して発行] を選択します。

      注：プロファイルを特定のデバイス タイプのデフォルトとして構成したり、Active Directory グループのメンバーシップに基づいて構成したりすることもできます。

5. プロファイルを作成したら、次のようにデバイスに割り当てる必要があります。
   a) [環境] > [デバイス]を選択します。
   b) プロファイルを割り当てるデバイスを選択します。
   c) ページの下で [プロファイルを指定する] を選択します。
   d) 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。
   e) [指定する] を選択します。

第
3
章

導入

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 Security Center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、Elements Security Center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、EXEファイルを使用した手動展開（41ページ）およびMSIファイルを使用した手動展開（46ページ）を参照してください。

製品をインストールするには

1. WithSecure Elements Security Center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サブスクリプションキー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。

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（55ページ）
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（51ページ）

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。

コマンドラインパラメータ

.exeインストーラを、あ環境に合わせた特別なニーズに合わせて設定することが可能です。

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 ファイルの場合、これはパラメータをコマンド ライン引数として追加することを意味します。たとえば、次の方法では、サブスクリプション キーを引数としてインストーラーに渡し、ユーザーがインストール中にそれを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。

.exeファイルを使用して製品をインストールする場合は、次のコマンドライン パラメータを使用できます。

EXEパラメータ	説明
--profile-id <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ー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`
--language <id> -l <ID>	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\<ユーザー名>\\Downloads>installer.exe --language ja`
--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ー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。

EXEパラメータ	説明
--voucher *<サブスクリプションキー>*	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、インストーラのファイル名に埋め込まれているかのように扱われます。ファイル名にサブスクリプションキーが存在し、コマンドラインにも追加されている場合、コマンドラインがファイル名のサブスクリプションキーを上書きします。例: `--voucher aaaa-bbbb-cccc-dddd-eeee`
--proxy <URL>	製品がインストールされている場合、すべてのリクエストはこのプロキシ経由で送信されます。例: `--proxy http://proxy.local:3128`
--skip-sidegrade *<スキップ オプション>*	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。 競合名の前に [skip-reboot] を追加することで、このサイドグレードは再起動を必要としない（ただし、サイドグレードは実行される）ことを示すこともできます。値（サイドグレードIDまたは名前）は「|」で区切ります。 • --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
--installation-tags *<タグ>*	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 Security Centerは、PSB=psb-tag1:psb-tag2:psb-tag3のタグをカンマ区切りの値として「ラベル」フィールドに保存します。文字列の最大長は255文字です。これらのタグにはカンマやコロンを含めることはできません。

EXEパラメータ	説明
--use_smbios_guid	このデバイスの一意の識別子として、SMBIOS GUID を使用してください。デフォルトでは、Elements Security Centerから削除されていないデバイスに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、新しいエントリが作成されないようにすることができます。 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、Element Security Centerに新しいデバイスが作成されます。 注：製品を通常通りアンインストールすると、Elements Security Center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と、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。
--use_ad_guid	このデバイスの一意の識別子として、Active Directory の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、Elements Security Centerから削除されていないデバイスに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、新しいエントリが作成されないようにすることができます。 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、Element Security Centerに新しいデバイスが作成されます。 注：製品を通常通りアンインストールすると、Elements Security Center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と、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	サーバー上のWindows Defenderを無効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は搭載されていますが、セキュリティセンターは搭載されていないため、他のセキュリティソフトウェアをインストールしてもWindows Defenderは自動的に無効になりません。通常は、GPOなどの標準的な方法でDefenderを無効にできます。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ご利用ください。
--skip-dotnet	インストール中に.NETをインストールしないでください。.NETを自分で管理するには、「プロファイル」>「全般設定」>「自動更新」で、「製品の更新中に [クライアントが.NETを管理することを許可する]をオフにしてください。
--connector-proxy <URL>	マルウェアシグネチャデータベースとソフトウェアアップデーターのアップデートをダウンロードする際の帯域幅使用量を最小限に抑えるには、コネクタを使用します。製品のインストール時には、すべてのリクエストが最終プロキシとしてコネクタ経由で送信されます。例： `--connector-proxy http://connector.local:80`

EXEパラメータ	説明
--upgrade-delay <分>	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。

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（55ページ）
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（51ページ）
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。

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: すべてのアンインストール試行がブロックされるため、製品をアンインストールする前に改ざん防止をオフにする必要があります。

注：オプションのパラメーターは [角括弧] 内にあります。

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、MSIプロパティ（46ページ）を参照してください。

製品をインストールするには

1. WithSecure Elements Security Center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、コマンドラインでプロパティを指定して、製品をセットアップできます。

   MSIファイルにプロパティを埋め込む手順については、次を参照してください。MSIプロパティ（46ページ）

   。

   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。

関連タスク

Active Directory GPOで展開する（51ページ）
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。

EXEファイルを使用した手動展開（41ページ）
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。

MSIプロパティ

MSIインストーラを、あ環境に合わせた特別なニーズに合わせて設定することが可能です。

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。

.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、引数を渡す方法の例は次のとおりです。

```
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、以下を参照してください。WithSecure MSI変換ツールを使用する（49ページ）。

.msiパッケージを使用して製品をインストールする場合、以下の MSI プロパティを使用できます。

MSIプロパティ	説明
PROFILE_ID	プロファイルIDの希望値を設定します。例：PROFILE_ID=180238。プロファイルIDを確認するには、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、ページ上部（割り当てられたコンピュータの番号と最終編集日の下）に表示されます。 MSIプロパティの例：PROFILE_ID=180238
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。 例えば、インストーラーコマンドで「LANGUAGE=<id>」MSIプロパティを指定しない場合、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またはC:\Users\<username>\Downloads>msiexec /i installer.msi
VOUCHER	サブスクリプションキーを設定します。例: --voucher aaaa-bbbb-cccc-dddd-eeee 注: 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_SERVER	製品のインストール時には、すべてのリクエストがこのプロキシ経由で送信されます。例：PROXY_SERVER=http://proxy.gtn:3128
SIDEGRADE_SKIPLIST	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「*」の値を指定します。例：SIDEGRADE_SKIPLIST=*
INSTALLATION_TAGS	ラベルを指定して、デバイスを好きなようにグループ化できます。ラベルは、地域、オペレーティングシステム、所有者、部門、ワークステーションとサーバーなど、ニーズに合った様々な基準に関する情報を提供するためによく使用されます。 例えば、INSTALLATION_TAGS=PSB=psb-tag1:psb-tag2:psb-tag3,RADAR=radar-tag1:radar-tag2:radar-tag3,department=accounting,role=secretary

MSIプロパティ	説明
UNIQUE_SIGNUP_ID=smbios	このデバイスの一意の識別子として、SMBIOS GUIDを使用してください。デフォルトでは、Elements Security Centerから削除されていないデバイスに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、新しいエントリが作成されないようにすることができます。 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、Element Security Centerに新しいデバイスが作成されます。 注: 製品を通常通りアンインストールすると、Elements Security Center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と、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。
UNIQUE_SIGNUP_ID=adguid	このデバイスの一意の識別子として、Active Directory の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、Elements Security Centerから削除されていないデバイスに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、新しいエントリが作成されないようにすることができます。 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、Element Security Centerに新しいデバイスが作成されます。 注: 製品を通常通りアンインストールすると、Elements Security Center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と、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	サーバー上のWindows Defenderを無効化してアンインストールするには、`DISABLE_DEFENDER=1` msiプロパティを使用します。バージョン2016以降のWindows ServerにはWindows Defenderは搭載されていますが、セキュリティセンターは搭載されていないため、他のセキュリティソフトウェアをインストールしてもWindows Defenderは自動的に無効化されません。通常は、GPOなどの標準的な方法でDefenderを無効化できます。それができない場合は、代わりに以下のインストールオプションをご利用ください。
CONNECTOR_PROXY	製品がインストールされると、すべてのリクエストは最終プロキシとしてコネクタを経由して送信されます。例 : `CONNECTOR_PROXY=http://proxy.gtn:3128`
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時間を分単位で指定します。このオプションは、即時のセルフアップグレードが望ましくない展開シナリオで役立ちます。既知のシナリオの1つは、Microsoft Intuneを使用した展開です。例: `UPGRADE_DELAY_MINUTES=5`

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（55ページ）
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（51ページ）
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。

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。

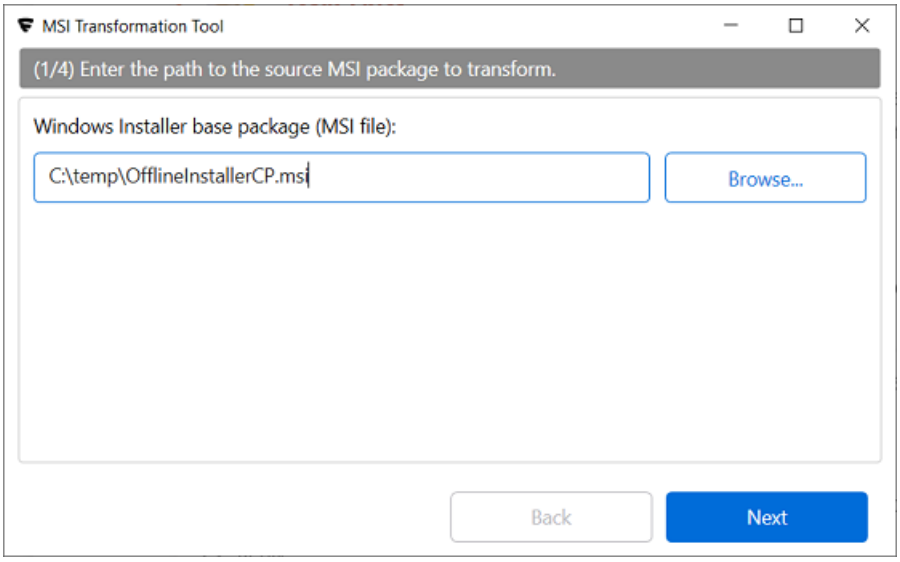
- WithSecure Elements Security Centerのダウンロードセクションから MSI形式のWithSecure Elements Agentの最新バージョンをダウンロードします。

  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。
- MSIプロパティ（46ページ）で利用可能なオプションをよく理解してください。

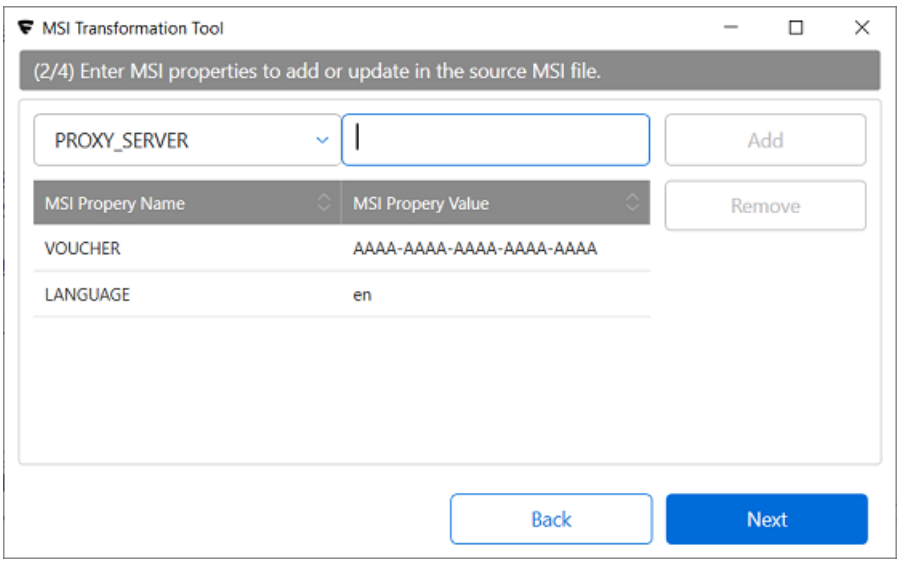
MSI変換ツールを使用するには

1. MSI 変換ツールを起動します。

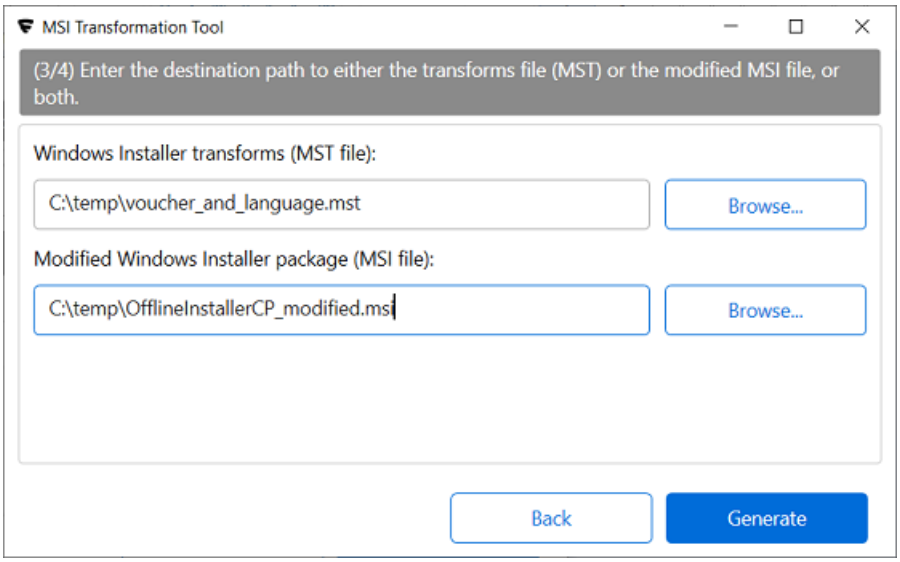
2. 開いたページで、Elements AgentのMSIインストーラーへのパスを指定し、[次へ] を選択します。



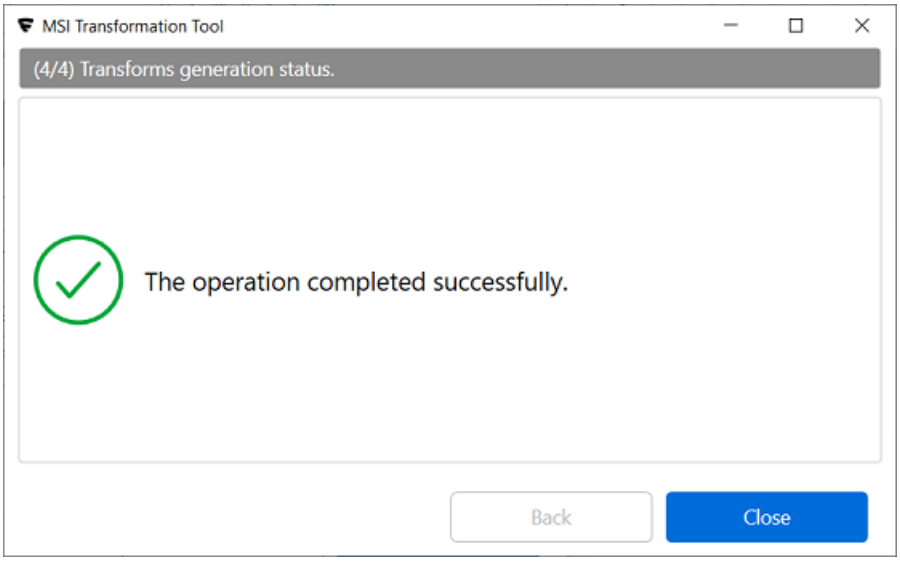
3. 追加する1つ以上のMSIプロパティを指定し、[次へ] を選択します。



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（42ページ）
.exeインストーラを、あ環境に合わせた特別なニーズに合わせて設定することが可能です。

3.1.3 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。

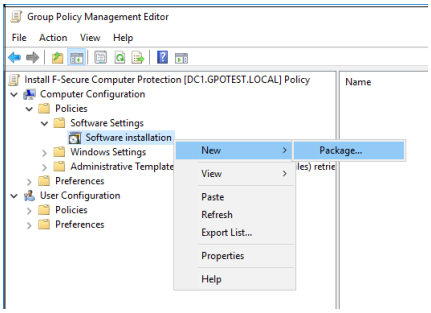
- Active Directory 環境
- 対象ドメインのすべてのメンバーにユニバーサルCRTがインストールされている必要があります。通常、これはWindowsのアップデートに付属しており、定期的にアップデートされるシステムに存在します。インストールで検出に失敗した場合、対応するエラー メッセージが対象システムのWindows イベントログに発行されます。手動でインストールまたは修復する必要がある場合、次のリンクをご覧ください。https://aka.ms/vs/16/release/vc_redist.x86.exe
- 対象ドメインのすべてのメンバーは、すべての UI 機能が正しく機能するために .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。

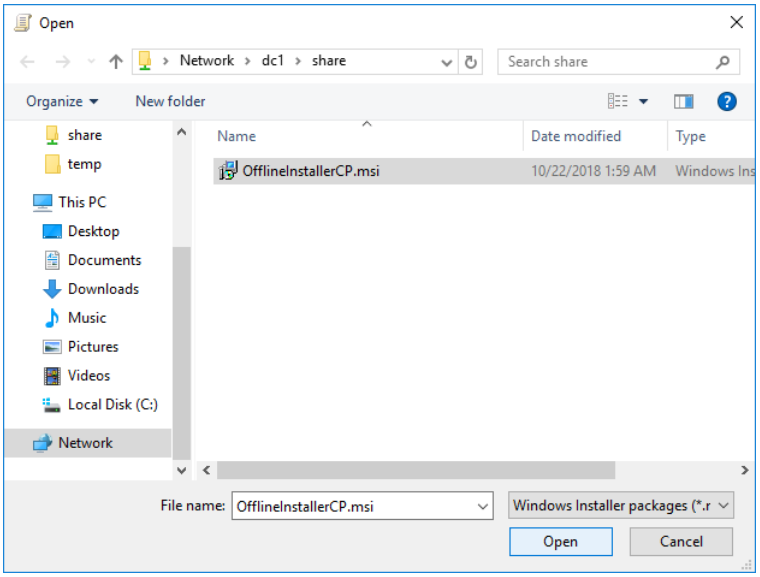
製品をインストールするには

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. コンピューター設定 > 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。

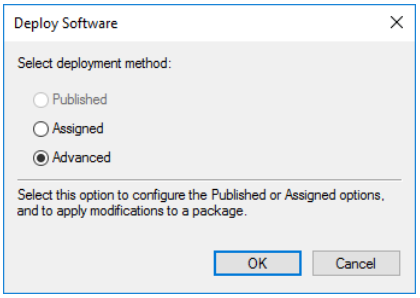
4. 右ペインを右クリックし、新規 > パッケージの順に選択します。



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。

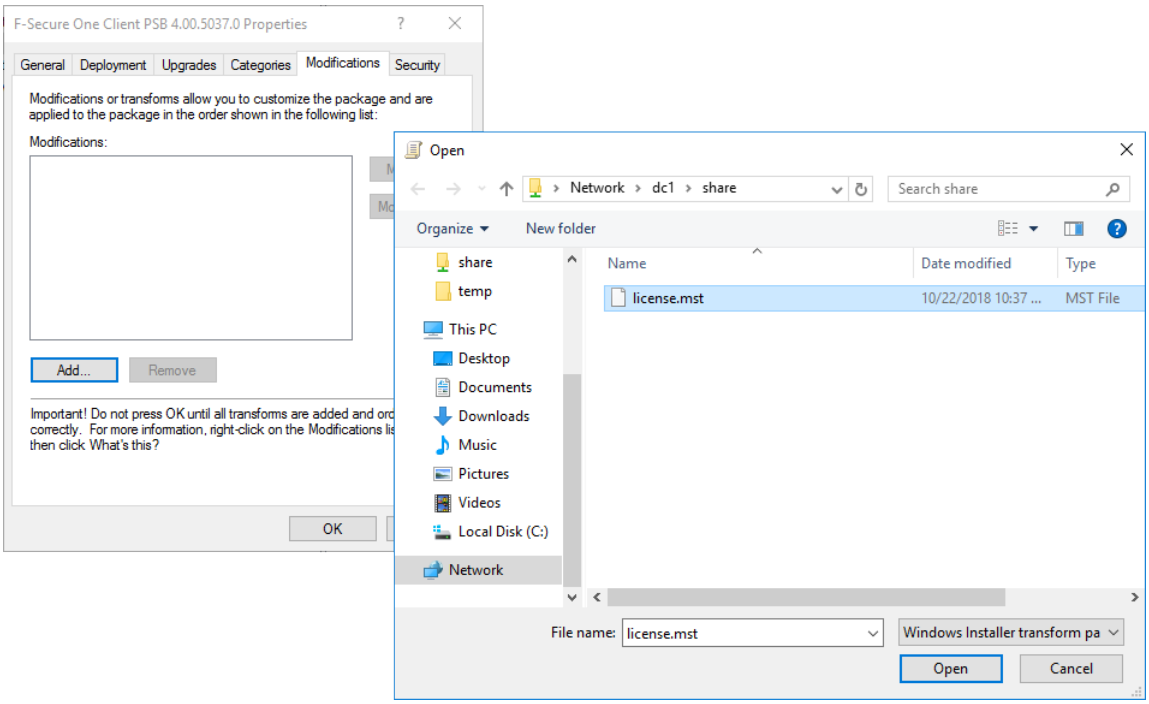


6. 「ソフトウェアの展開」ウィンドウで、[詳細設定]を選択してパッケージを構成し、[OK] を選択します。



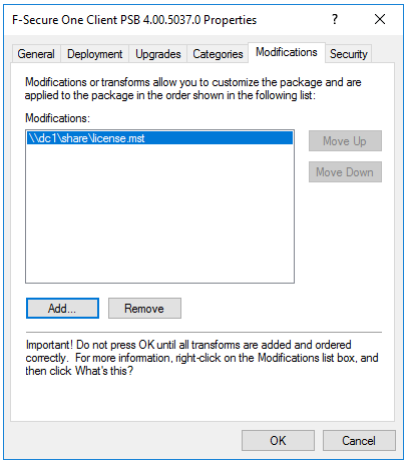
7. [変更] タブに移動し、[追加] を選択します。

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 コンピューターで GPO 設定が更新され、コンピューターが再起動されると、パッケージが展開されます。

3.1.4 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 Security Center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。

3.1.5 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 Security Center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\WOW6432Node\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。

3.1.6 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、MSIプロパティ（46ページ）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。

コンピューターシステム管理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コンピューター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、`--use_smbios_guid`の代わりに`--use_ad_guid`を使用して、デバイスをActive DirectoryコンピューターGUIDに関連付けることもできます。EXEファイルを使用した手動展開（41ページ）およびMSIファイルを使用した手動展開（46ページ）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. WithSecure Elements Security Centerでデバイスが正しく表示されていることを確認します。

   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. 以下のコマンドを実行し、WithSecure Elements Security Centerからログアウトします。

   ```
   "%ProgramFiles(x86)%\F-Secure\PSB\ws_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、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（57ページ）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. 以下のコマンドを実行し、WithSecure Elements Security Centerにログインします。

   ```
   "%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --keycode
   <subscription-key>
   ```
3. システムトレイ領域のWithSecure Elements Agentアイコンを右クリックしてコンテキスト メニューを開き、[更新プログラムの確認]を選択します。
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. 以下のコマンドを実行し、Elements Security Centerからイメージをログアウトします。

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_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. サーバーが再起動し、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\ws_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（サーバー）がWithSecure Elements Security Centerに作成されます。
3. サーバーが使用する通信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、それをサーバーに再展開する場合は、上記の手順1～3を繰り返します。
   サーバーは、Elements Security Center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、デバイスは、WithSecure Elements Security Center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、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\ws_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。

- ws_oneclient_logout.exeツールを実行する前に、デバイスを Active Directory グループに登録します。これにより、システムに登録するときに、デバイスは Active Directory グループに割り当てられている既定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、Elements Security Centerでプロファイルを手動で設定します。

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。

3.1.7 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
   ```

   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。

注：MozillaFirefoxのブラウザ保護拡張機能を有効にするかどうかを尋ねるウィンドウが表示されたら、[許可]を選択します。拡張機能は自動的に有効になりますが、ウィンドウの表示を防ぐ方法はありません。

ブラウザ保護拡張機能をインストールするには

1. 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。

3.2 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。

WithSecure Elements Endpoint Protection for Computers (Mac)の配布方法、自動インストールと設定、サブスクリプションの有効化について説明します。

WithSecure Elements Endpoint Protectionソフトウェアを配布する一般的なシナリオを以下に示します。

以下の方法で製品を配布することができます。

- 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。

3.2.1 ssh を使用した配布

ssh 経由で製品を配布する方法の説明。

1. 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。
2. 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。

3. 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。

3.2.2 MDMを使用した配布

モバイル デバイス管理 (MDM) または別のソフトウェア配布ソリューション (Munki など) を通じて製品を配布するには、さまざまな方法があります。

製品を手動でアクティブ化して構成することも、カスタム パッケージを使用して製品をアクティブ化して構成することも、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ブ化の両方を行うこともできます。

手動での有効化と設定

手動でアクティベートおよび構成して製品を配布する方法に関する手順。

1. 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。
2. sshを使用して、対象のコンピューター上で必要な構成パラメータを指定してactivatorを実行します。
3. コンピュータをアクティブ化し、WithSecure Elements Security Centerに接続します。

カスタムパッケージの使用

アクティベーションと構成用のカスタム パッケージを使用して製品を配布する方法について説明します。

1. 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コンピューターに製品をインストールできるようにします。
2. 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/WithSecure/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.withsecure.elements.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) 。

3. 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。

特別な製品パッケージの使用

製品のインストールとアクティベーションの両方に1つのパッケージを使用して製品を配布する方法について説明します。

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。

3.2.3 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。

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システム拡張を許可する

```
<?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'>

'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>V928P8X763</string>

</array>

<key>RemovableSystemExtensions</key>

<dict>

<key>V928P8X763</key>

<array>

<string>com.withsecure.wsagent.wssystemextension</string>

</array>

</dict>

<key>PayloadDescription</key>

<string>Allows WithSecure System Extension</string>

<key>PayloadDisplayName</key>

<string>WithSecure System Extension</string>
```

```
<key>PayloadIdentifier</key>
<string>com.apple.system-extension-policy.213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadType</key>
<string>com.apple.system-extension-policy</string>
<key>PayloadUUID</key>
<string>213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent 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>WithSecure Firewall</string>

<key>PluginBundleID</key>

<string>com.withsecure.wsagent</string>

<key>FilterDataProviderBundleIdentifier</key>

<string>com.withsecure.wsagent.wssystemextension</string>

<key>FilterDataProviderDesignatedRequirement</key>

<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor
apple generic and certificate leaf[subject.OU] = "V928P8X763"</string>

<key>FilterSockets</key>

<true/>

<key>FilterPackets</key>

<false/>

<key>FilterBrowsers</key>

<false/>

<key>FilterType</key>

<string>Plugin</string>

<key>PayloadDescription</key>

<string>Allow WithSecure Firewall to filter network traffic</string>

<key>PayloadDisplayName</key>

<string>WithSecure 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>WithSecure Oyj</string>
```

```
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent 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 WithSecure processes</string>
<key>PayloadDisplayName</key>
<string>Grant Full Disk Access to WithSecure 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>WithSecure Oyj</string>

<key>Services</key>

<dict>

<key>SystemPolicyAllFiles</key>

<array>

<dict>

<key>Identifier</key>

<string>com.withsecure.wsagent</string>

<key>IdentifierType</key>

<string>bundleID</string>

<key>CodeRequirement</key>

<string>identifier "com.withsecure.wsagent" and anchor apple generic and
certificate leaf[subject.OU] = "V928P8X763"</string>

<key>Allowed</key>

<true/>

<key>Comment</key>

<string>Grant Full Disk Access to WithSecure processes</string>

</dict>

<dict>

<key>Identifier</key>

<string>com.withsecure.wsagent.wssystemextension</string>

<key>IdentifierType</key>

<string>bundleID</string>

<key>CodeRequirement</key>

<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor
apple generic and certificate leaf[subject.OU] = "V928P8X763"</string>

<key>Allowed</key>

<true/>

<key>Comment</key>

<string>Grant Full Disk Access to WithSecure's System Extension'</string>

</dict>
```

```
</array>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent 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.withsecure.wsagent</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 WithSecure products</string>
<key>PayloadDisplayName</key>
<string>Allow notifications for WithSecure 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>WithSecure Corporation</string>
</dict>
</array>
```

```
<key>PayloadDisplayName</key>
<string>WithSecure Agent 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。

3.2.4 Microsoft Intune の MDM プロファイルの作成

デバイスのネットワークを管理する場合、すべてのデバイスが組織のセキュリティ標準に準拠していることを確認することが重要です。

Microsoft Intuneは、MDMプロファイルを使用することでこのプロセスを簡素化します。これらのプロファイルは、デバイスのセキュリティと機能のさまざまな側面を制御する設定のパッケージです。

このセクションでは、コンテンツ フィルタリング、通知、フルディスク アクセス、システム拡張設定を含む Microsoft Intune MDM プロファイルを作成する方法について説明します。

コンテンツフィルタリング設定を含むMDMプロファイルの作成

コンテンツ フィルタリング設定を使用して MDM プロファイルを作成する方法について説明します。

1. Microsoft Intuneポータルにログインします。
2. [デバイス] > [デバイスの管理] > [構成]
3. 新しいポリシーを作成するには、次の手順を実行します。
   a) [新しいポリシー][の作成]を選択します。
   b) [macOS]プラットフォームを選択します。
   c) プロファイルタイプとして、[設定カタログ]を選択します。
   d) [新規作成] を選択します。
4. プロファイルの名前を入力し、[次へ]を選択します。
5. 構成設定タブで、[+ 設定の追加を]選択します。
6. 検索バーに「Web コンテンツ フィルター」と入力します。
7. [Web] > [Web コンテンツ フィルター]を選択し、次の設定を選択します。
   - フィルターデータプロバイダーバンドル識別子
   - ユーザー定義名

- フィルターグレード
- ユーザー名
- フィルターソケット
- パケットをフィルタリングする
- プラグインバンドルID
- フィルターデータプロバイダー指定要件
- 組織
- フィルタータイプ

8. 設定ピッカーウィンドウを閉じます。
9. 次の値を入力します。
   - フィルターデータプロバイダーのバンドル識別子：`com.withsecure.wsagent.wssystemextension`
   - ユーザー定義名:`WithSecure Firewall`
   - フィルターグレード:ファイアウォール
   - ユーザー名:`WithSecure Element Content Filter`
   - フィルターソケット：`True`
   - パケットをフィルタリング：`False`
   - プラグインバンドル ID:`com.withsecure.wsagent`
   - フィルター データ プロバイダー指定の要件:識別子 `"com.withsecure.wsagent.wssystemextension"`、アンカー `apple generic`、証明書 `leaf[subject.OU] = "V928P8X763"`
   - 組織:`WithSecure`
   - フィルタータイプ:プラグイン
10. [次へ] をクリックします。
11. [割り当て]タブで、このプロファイル構成を適用するグループ、ユーザー、およびデバイスを追加します。
12. [次へ] を選択します。
13. [レビュー+作成] タブで 、[作成] を選択します

通知設定を含むMDMプロファイルの作成

通知設定を含む MDM プロファイルを作成する方法について説明します。

1. Microsoft Intuneポータルにログインします。
2. [デバイス] > [デバイスの管理] > [構成]
3. 新しいポリシーを作成するには、次の手順を実行します。
   a) [新しいポリシー][の作成]を選択します。
   b) [**macOS**]プラットフォームを選択します。
   c) プロファイルタイプとして、[設定カタログ]を選択します。
   d) [新規作成] を選択します。
4. プロファイルの名前を入力し、[次へ]を選択します。
5. 構成設定タブで、[+ 設定の追加を]選択します。
6. 検索バーに 「通知」と入力します。
7. [ユーザーエクスペリエンス] > [通知を]選択
8. [通知設定]オプションを選択します。
9. 設定ピッカーウィンドウを閉じます。
10. [+インスタンスの編集を]選択します。
11. 次の設定の値を入力します。

    注：その他の設定のデフォルト値は変更しないでください。

    - アラートの種類:永続バナー

- バンドル識別子：com.withsecure.wsagent

12. [次へ] をクリックします。
13. [割り当て]タブで、このプロファイル構成を適用するグループ、ユーザー、およびデバイスを追加します。
14. [次へ] を選択します。
15. [レビュー+作成] タブで 、[作成] を選択します

フルディスクアクセス設定を持つ MDM プロファイルの作成

フルディスク アクセス設定で MDM プロファイルを作成する方法について説明します。

1. Microsoft Intuneポータルにログインします。
2. [デバイス] > [デバイスの管理] > [構成]
3. 新しいポリシーを作成するには、次の手順を実行します。
   a) [新しいポリシー][の作成]を選択します。
   b) [macOS]プラットフォームを選択します。
   c) プロファイルの種類として、[テンプレート]を選択し、[デバイスの制限]を選択します。
   d) [新規作成] を選択します。
4. プロファイルの名前を入力し、[次へ]を選択します。
5. 構成設定タブで、[プライバシー設定]を選択します。
6. [アプリとプロセス]の下で [追加]を選択し、次の値を入力して選択します。
   - 名前：WithSecure Elements
   - 識別子タイプ:[バンドルIDを]選択
   - 識別子: com.withsecure.wsagent
7. [次へ] をクリックします。
8. [割り当て]タブで、このプロファイル構成を適用するグループ、ユーザー、およびデバイスを追加します。
9. [次へ] を選択します。
10. [レビュー+作成] タブで 、[作成] を選択します

システム拡張設定を含むMDMプロファイルのインポート

システム拡張設定を含む MDM プロファイルをインポートする方法について説明します。

1. Microsoft Intuneポータルにログインします。
2. [デバイス] > [デバイスの管理] > [構成]
3. 新しいポリシーを作成するには、次の手順を実行します。
   a) [新しいポリシー] > [の作成]を選択します。
   b) [macOS]プラットフォームを選択します。
   c) プロファイルタイプとして、[設定カタログ]を選択します。
   d) [新規作成] を選択します。
4. プロファイルの名前を入力し、[次へ]を選択します。
5. 構成設定タブで、[+ 設定の追加を]選択します。
6. 検索ボックスに「System Extensions」と入力します。
7. [システム構成] > [システム拡張機能]を選択します。
8. [許可されたシステム拡張機能]オプションを選択します。
9. 設定ピッカーウィンドウを閉じます。
10. [+インスタンスの編集を]選択します。
11. [許可されたシステム拡張機能]で、次の操作を行います。
    a) チェックボックスの横に、以下を入力します:com.withsecure.wsagent.wssystemextension
    b) チーム識別子として V928P8X763を入力します

12. [次へ] をクリックします。
13. [割り当て]タブで、このプロファイル構成を適用するグループ、ユーザー、およびデバイスを追加します。
14. [次へ] を選択します。
15. [レビュー+作成] タブで 、[作成] を選択します

3.2.5 Jamf管理システムのMDMプロファイルの作成

Jamfポータルのシステム拡張設定を使用してMDMプロファイルを作成する方法について説明します。

Jamf のシステム拡張設定を使用して MDM プロファイルを作成することで、Apple デバイスの管理を効率化できます。この統合により、デバイスの構成とセキュリティ保護を一元的に行えるようになり、組織全体の一貫性が確保されます。システム拡張により、標準のオペレーティング システムには含まれていない追加のセキュリティ機能が提供されます。これらを Jamf に作成すると、管理対象デバイスすべてにこれらの強化されたセキュリティ対策を展開できます。

MDM プロファイルを作成するには:

1. Jamfポータルにログイン
2. [コンピューターの] > [構成プロファイル]を選択します。
   構成プロファイルページが開きます。
3. 新しいプロファイルを作成するには、まず [新規]を選択します。
4. 新しい **macOS** 構成プロファイルページで、[オプション] > [一般]を選択します。
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] ドロップダウン メニューから、[コンピューター レベル]を選択します。
   c) [配布方法] ドロップダウン メニューから、[自動的にインストール]を選択します。
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) [オプション]で、[システム拡張機能]を選択します。
   b) [表示名]ボックスに「 `WithSecure` 」と入力します。
   c) 「システム拡張タイプ」ドロップダウン メニューから、[許可されたシステム拡張]を選択します。
   d) チーム識別子ボックスに「`V928P8X763`」と入力します。
   e) [許可されたシステム拡張機能]で、以下を入力し、[保存]を選択します。

      ```
      com.withsecure.wsagent.wssystemextension
      ```

   f) [+ を]選択して、新しい [許可されたシステム拡張機能と **Teams ID** を]追加します。
   g) 「表示名」フィールドに「`WithSecure Elements System Extension Allow Removal`」と入力します。
   h) システム拡張機能の種類のドロップダウン メニューから、[リムーバブル システム拡張機能]を選択します。
   i) チーム識別子フィールドに V928P8X763と入力します。
   j) [リムーバブル システム拡張機能]の下で、[追加]を選択し、以下を入力します。

      ```
      com.withsecure.wsagent.wssystemextension
      ```

7. [保存] を選択します。

macOS Sequoiaのシステム拡張機能の変更

macOS Sequoia (15.x) 以降では、管理者権限を持つユーザーはシステム設定からシステム拡張機能をオフにすることができます。

ユーザーが特定のシステム拡張機能をオフにできないようにするには、システム設定 UI からこの機能を削除する構成プロファイルを適用できます。

重要: プロファイルのスコープを macOS Sequoia 以降を搭載したデバイスに設定する必要があります。プロファイルのスコープを以前のバージョンに設定すると、アップグレード後に設定は適用されません。

Jamf を使用して UI プロファイルから削除不可能なシステム拡張機能を作成する

macOS Sequoia 以降を搭載したデバイス用に、Jamf を使用して UI 構成プロファイルから削除不可能なシステム拡張機能を作成する方法について説明します。

1. [コンピューターの] > [構成プロファイル]に移動し、[新しい]プロファイルを作成します。
2. [全般]カテゴリで、新しいプロファイルにわかりやすい名前を付けます。
3. [システム拡張]ペイロードを選択し、[構成]を選択します。
4. プロファイルを識別できるように、[表示名]フィールドに名前を入力します (例: `WithSecure UI Non-Removable`)。
5. ユーザーがシステム設定アプリから拡張機能を無効にできないようにするには、[システム拡張機能の種類]ドロップダウンから、[UI から削除できないシステム拡張機能]オプションを選択します。
6. チーム識別子フィールドに、次のように入力します : `V928P8X763`。
7. [+ 追加]ボタンを選択し、次の拡張機能名を入力します: `com.withsecure.wsagent.wssystemextension`。
8. テキスト フィールドの右側にある [保存]を選択します。
9. 「スコープ」タブで、macOS Sequoia 以降を搭載したデバイスを含む [スマート コンピュータ グループを]選択します。既存のスマート グループがない場合は、「macOS Sequoia 以降を搭載したデバイスのスマート グループを作成する」を参照してください。
10. プロファイルを保存します。
11. 構成プロファイルをターゲットデバイスに展開します。
12. システム設定でシステム拡張機能が削除不可能であることを確認します。

macOS Sequoiaでデバイスのスマートグループを作成する

macOS Sequoia を搭載したデバイスのスマート グループを作成する方法について説明します。

重要 : これらの手順は、macOS Sequoia (15.x) 以降のバージョンにのみ適用されます。

1. Jamf ポータルにログインします。
2. [コンピューター] > [スマート コンピューター グループ] > [新規]を選択します。
3. 表示名として、`macOS 15` 以降を入力します。
4. [条件]タブで、[追加]を選択します。
5. 基準として、[オペレーティング システムのバージョン]を選択します。
6. [演算子]ドロップダウン メニューから [以上]を選択し、[値]フィールドに `15` と入力します。
7. [保存] を選択します。

3.2.6 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。コマンドラインインターフェース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。

3.2.7 MPKG ファイルを使用して製品を手動でインストールする

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すると、インストーラーファイルをダウンロードして製品をインストールします。

製品をインストールするには

1. https:elements.withsecure.comで WithSecure Elements Security Center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. [**WithSecure Elements Agent for Computers**]の下で、[**.mpkg のダウンロード**]を選択します。

   注 : .mpkg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. インストールする製品を選択し、[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. ダウンロードしたインストール ファイル (.mpkg) を見つけてダブルクリックし、インストールを開始します。
   「**Install WithSecure Elements**」ウィザードが開きます。
6. ウィザードの指示に従います。
7. インストールが完了したら、[概要]画面で [閉じる]を選択します。

3.2.8 フルディスクアクセスの許可

macOS でフルディスク アクセスを許可する方法を説明します。

WithSecure Elements Endpoint Protection with EDR for Macおよび Client Security for Macコンピューターをスキャンし、実行できるようにする必要があります。

1. メニューバーの左上隅にある Apple アイコンを選択し、[システム設定...」を]選択します。
2. [プライバシーとセキュリティ]を選択します。
3. [プライバシー]の下で、[フル ディスク アクセス]を選択します。
4. [**WithSecure Agent**]オプションをオンにします。

3.2.9 WithSecureシステム拡張を許可する

macOS で WithSecure システム拡張機能を許可する方法を説明します。

1. 製品をインストールすると、「システム拡張機能がブロックされました」というポップアップが表示されます。
2. WithSecureシステム拡張機能を許可するには、ポップアップで[システム設定を開く]を選択します。

   注 : [**OK**]を選択すると、ポップアップが閉じます。続行するには、[システム設定]を開きます。

3. [アプリケーション **WithSecure Agent** のシステム ソフトウェアの読み込みがブロックされました]の下で、[許可]を選択します。

3.2.10 WithSecure Agent通知の許可

WithSecure Agent 通知を許可する方法を説明します。

通知を許可するには:

1. 製品をインストールすると、WithSecure Agent Notifications ポップアップが開きます。
2. ポップアップで、[オプション] > [許可]を選択します。

3.2.11 ネットワークコンテンツのフィルタリング

ネットワーク コンテンツをフィルタリングする方法について説明します。

ネットワークコンテンツをフィルタリングするには:

1. Apple メニューから、[システム設定]を開きます。
2. [スクリーンタイム] > [コンテンツとプライバシー]を選択します。
3. [ストア、ウェブ、**Siri** および **Game Center** コンテンツ]を選択します。
4. ネットワーク コンテンツをフィルターするには、次のいずれかを実行します。
   - 多くのアダルトWebサイトへのアクセスを自動的に制限するには、[**Web**コンテンツへのアクセス]ドロップダウン メニューから [アダルト **Web** サイトの制限]を選択します。

     注 : [カスタマイズ]を選択すると、許可または制限される Web サイトを追加できます。
   - 特定の Web サイトへのアクセスを制限するには、[**Web** コンテンツへのアクセス]ドロップダウン メニューから、[許可された **Web** サイトのみ]を選択します。

     注 : [カスタマイズ]を選択すると、+ アイコンと - アイコンを使用して許可された Web サイトを追加または削除できます。リストから許可されたWebサイトを選択し、3つのドットのアイコンを選択すると、Web サイトのタイトルまたは URL を編集できます。
5. [完了] を選択します。

3.2.12 ブラウザ拡張機能が使用されているかどうかを確認する

ブラウザ保護には、Webブラウジング、オンラインバンキング、ショッピングを保護し、インターネット閲覧中にセキュリティ情報を表示できるブラウザ拡張機能が必要です。

製品をコンピュータにインストールしたら、使用するWebブラウザのブラウザ拡張機能をインストールして有効にする必要があります。

この製品はSafariのブラウザ拡張機能を自動的にインストールするので、拡張機能がオンになっていることを確認するだけで済みます。

Chromeの場合、インターネットを安全に閲覧するには、ブラウザ拡張機能をインストールして有効にする必要があります。また、拡張機能のインストールには、アクセスしたウェブアドレスに関する情報へのアクセス許可が必要です。より詳細な情報については、関連情報を参照してください。

Safariのブラウザ拡張機能を有効にする

ブラウザを安全に使用するには、Safariのブラウザ拡張機能を有効にする必要があります。

この製品はブラウザ拡張機能を自動的にインストールするので、拡張機能がオンになっていることを確認するだけで済みます。

Safariのブラウザ拡張機能がオンになっていることを確認するには

1. メニューバーの製品アイコンを選択します。
2. メニューから [設定...] を選択します。
3. [セキュア ブラウジング] タブを開きます。
4. [ブラウザ拡張機能のインストール] を選択します。
5. ポップアップウィンドウで、[**Safari**] を選択し、[有効にする] を選択します。
6. [拡張機能] ダイアログで、次の操作を行います。
   a) [ブラウザ保護] が選択されていることを確認してください。
   b) [プライベートブラウジング]で、[プライベートブラウジングの許可] を選択します。
   c) [権限] の下で、[すべての **Web** サイトで許可] を選択します。

Safariを使用して安全にインターネットを閲覧できるようになりました。

ブラウザ拡張機能が動作しているかどうかをテストするには、ブラウザで次のテストページを開きます : `https://unsafe[.]fstestdomain[.]com`。製品ブロックページが表示されるはずです。

Google Chromeのブラウザ拡張機能をインストールして有効にする

Chromeブラウザを安全に使用するには、Google Chrome用のブラウザ拡張機能をインストールして有効にする必要があります。

Google Chromeのブラウザ拡張機能を設定するには

1. メニューバーの製品アイコンを選択します。
2. メニューから [設定...] を選択します。
3. [セキュアブラウジング] タブを開きます。
4. [ブラウザ拡張機能のインストール] を選択します。
   [ブラウザ保護のインストール] ウィンドウが開きます。
5. ドロップダウンから [**Chrome**] を選択し、[今すぐインストール] を選択します。
6. [**Chromeに追加**] > [**拡張機能を追加**] を選択します。
   拡張機能がインストールされると、ユーザー同意ダイアログが開きます。このブラウザ拡張機能は、アクセスしたWebアドレスに関する情報にアクセスする許可を必要とします。
7. [承諾] を選択します。
   注：許可を拒否すると、拡張機能を使用できなくなり、ブラウザ保護機能によって有害なWebサイトをブロックしたり、検索結果の評価を表示したりできなくなります。また、拡張機能はブラウザから削除されます。
8. 拡張機能の設定を完了するには、[**OK**] を選択します。

Chromeを使用して安全にインターネットを閲覧できるようになりました。

ブラウザ拡張機能が動作しているかどうかをテストするには、ブラウザで次のテストページを開きます：`https://unsafe[.]fstestdomain[.]com`。製品ブロックページが表示されるはずです。

3.2.13 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/WithSecure/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/WithSecure/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/WithSecure/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.
```

3.2.14 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 Security Center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：`ElementsAgentInstaller[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：`ElementsAgentInstaller__XXXX-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/WithSecure/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。

3.2.15 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。

3.3 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。

この展開方法は、Linuxデバイスを使用していて、WithSecure Elements Agentを展開したい企業に適しています。

WithSecure Elements Agent for Linux 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、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。

ダウンロード可能なバージョンはAMD64とARM64の2つです。イメージのアーキテクチャに合ったバージョンを選択してください。

いずれのインストーラーを使用する場合も、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。その後、コマンドを実行して製品をアクティベートします。

製品をWithSecure Elementsの管理モードでインストールすると、WithSecure Elements Security Centerポータルを使用して製品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ています。本製品は、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を2週間以上認証できない場合、製品は動作しなくなります。

3.3.1 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。

注：プラットフォームアーキテクチャ固有のインストーラーがあります。適切なものをダウンロードしてください。

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) WithSecure Elements Security Centerにログインします。
   b) [管理]の下で、[ダウンロード]を選択します。
   c) **WithSecure Elements Agent for Servers**で、DEBまたはRPMインストーラ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 Protection システム要件」を参照してください。
   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。
      - AMD64 バージョンを使用するか ARM64 バージョンを使用するかに応じて、DEB ベースのディストリビューションで、次のいずれかのコマンドを実行します。

```
dpkg -i linuxsecurity-installer_amd64.deb
```

```
dpkg -i linuxsecurity-installer_arm64.deb
```

- AMD64 バージョンを使用するか ARM64 バージョンを使用するかに応じて、RPM ベースのディストリビューションで次のコマンドのいずれかを実行します。

```
rpm -Uvh linuxsecurity-installer.x86_64.rpm
```

```
rpm -Uvh linuxsecurity-installer.aarch64.rpm
```

2. 製品をアクティベートするには、以下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、WithSecure Elements Security Center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: `--override-distro`オプションを使用すると、正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できます。たとえば、`--override-distro rhel:8.6`を使用します。WithSecure 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=host:port`: 認証を必要とせずに、指定されたホストと ポートをネットワーク プロキシとして使用するように製品を構成します。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=username:password@host:port`: 指定されたホストとポートをネットワーク プロキシとして使用するように製品を設定し、指定されたユーザー名とパスワードを認証資格情報として使用します。ユーザー名またはパスワードの特殊文字には 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`。

3.3.2 tar パッケージを使用して製品をインストールする

tar 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。

注：プラットフォームアーキテクチャ固有のインストーラーがあります。適切なものをダウンロードしてください。

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) WithSecure Elements Security Centerにログインします。
   b) [管理]の下で、[ダウンロード]を選択します。
   c) **WithSecure Elements Agent for Servers**の下にある汎用インストーラ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 Protection システム要件」を参照してください。
   f) AMD64 バージョンを使用するか ARM64 バージョンを使用するかに応じて、ダウンロードした汎用インストーラー ファイルで次のいずれかのコマンドを実行します。

```
tar -xf linuxsecurity-installer.amd64.tar
```

```
tar -xf linuxsecurity-installer.arm64.tar
```

2. 製品をアクティベートするには、以下のコマンドを実行します。

```
./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、WithSecure Elements Security Center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: `linuxsecurity-installer` プログラムを実行する前に、`linuxsecurity-installer`プログラムの名前を次のいずれかのパターンに一致するように変更して、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 を提供することもできます: linuxsecurity-installer-[SUBSCRIPTION-KEY] または `linuxsecurity-installer-[SUBSCRIPTION-KEY]-[profile=PROFILE-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: `--override-distro`オプションを使用すると、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できます (例: `--override-distro rhel:8.6`)。WithSecure 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=host:port`: 認証を必要とせずに、指定されたホストと ポートをネットワーク プロキシとして使用するように製品を構成します。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=username:password@host:port`: 指定されたホストとポートをネットワークプロキシとして使用するように製品を設定し、指定されたユーザー名とパスワードを認証資格情報として使用します。ユーザー名またはパスワードの特殊文字には 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。

- WithSecure Elements Security Centerを通じてインストールメールを送信してユーザーを招待する
- 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アカウントに表示されます。

この展開方法を使用すると、WithSecure Elements Mobile Protectionをダウンロードするためのリンクを含む電子メール メッセージをユーザーに送信して招待します。

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 Security Center。

WithSecure Elements Mobile Protectionエンドポイント デバイスにインストールするには、新しいデバイスを Elements Security Centerに追加し、電子メール アドレスや名、姓などのユーザー情報を入力する必要があります。

注: Elements Security Center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、電子メール アドレスとエイリアスがチェックされます。情報が何もない場合は、UUID が表示されます。

MDM を使用した展開

MDM を使用して WithSecure Elements Mobile Protectionを導入することは、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 デバイスのみ ）
- VMware Workspace ONE（ 旧称 AirWatch ）
- Microsoft Intune
- IBM Security MaaS360
- Ivanti Endpoint Management（ 旧称 MobileIron Cloud ）
- Miradore
- Samsung Knox (Android デバイスのみ)

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 :

- アプリを構成しない場合は、Elements Security Centerのデバイス名の下に表示される UUID が使用されます。
- 電子メール アドレスを設定すると、Elements Security Center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、重複が作成されるため、まず Elements Security Centerからデバイスを削除し、MDM エージェントからもアプリを削除する必要があります。

診断とデータ収集の自動許可

MDM プロファイル経由で WithSecure Elements Mobile Protection有効にする場合、診断とデータ収集が自動的に許可されるようにするには、アプリ構成に以下を追加する必要があります。

- データ収集:「data_usage_permission」
- 診断コレクション:「diagnostic_usage_permission」

3.4.1 Google Chromeのブラウザ拡張機能のインストール

Chromeブラウザを安全に使用するには、GoogleChromeのブラウザ保護拡張機能をインストールして有効にする必要があります。

注 : これらの手順は Chrome OS に適用されます。Android 上の Chrome ブラウザは現在、ブラウザ拡張機能をサポートしていません。

1. Google Chrome ブラウザを開きます。
2. 右上隅にある 3 つのドットのメニューから、[拡張機能] > [拡張機能の管理]選択します。
3. 検索ボックスに「`Browsing Protection by WithSecure`」と入力します。
4. 結果から必要な拡張機能を選択します。

インストールが完了すると、ChromeOS 上の Chrome ブラウザは、ChromeOS の Android コンテナにインストールされている WithSecure Elements Mobile Protection使用して、開いた URL の検証を開始します。

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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

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ますが、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 WithSecure Elements Security Centerに表示されます。メール アドレスを空のままにすると、WithSecure Elements Mobile Protectionがインストールされているデバイスがデバイス UUID で表示されます。

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 [管理] > [サブスクリプ] > [ション] [サブスクリプション]にあります。
   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

VMware Workspace ONE (旧称 AirWatch) 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。

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

WithSecure Elements Mobile Protection iOS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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注 : WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定するか、

1. VMware Workspace ONE管理ポータルで、[リソース] > [アプリ]に移動します。
2. [パブリック] タブを選択します。
3. [アプリケーションの追加を]選択します。
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: [WithSecure Mobile Protection)]。
   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]をクリックします。
   「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 [名前]の下に、デフォルトで検出されない場合は WithSecure Mobile Protectionと入力し、[保存して割り当て]を選択します。

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

WithSecure Elements Mobile Protection iOSアプリをVMware Workspace ONE MDMに設定する方法を説明します。

1. [割り当ての] > [配布]で、次の内容を入力します。
   - 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 [(自動]または [オンデマンド)]を選択します。
2. 「制限]タブを選択し、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]タブを選択し、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. [構成の送信]オプションをオンにして、次の操作を行います。
   a) 次に、「追加]を選択して、アプリの自動アクティベーションを可能にするための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。
      - ***fate_registration_key*** - サブスクリプションキー
      - ***first_name*** (オプション) - WithSecure Elements Security Centerでデバイスを識別しやすくする名前
      - ***last_name*** (オプション) - WithSecure Elements Security Centerでデバイスを識別しやすくする名前
      - ***email*** - ユーザーのメールアドレス
      - ***alias*** （ 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]を選択します。
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]を選択します。
9. メイン ビューで、[デバイス][リスト ビュー]を選択します。
   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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。
- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

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 [アプリケーションの追加]を選択します。
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. [WithSecure Elements Mobile Protection] ビューで、[承認] > [選択] を選択します。
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. [SDK]ドロップダウン メニューから、[MP strings@ WithSecure を]選択します。
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. VMware Workspace ONEコンソールウィンドウで、[アプリとブック]を選択し、[アプリケーション]の下で [リストビュー]を選択します。
   [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。

   WithSecure Elements Mobile Protectionアプリは、VMware Workspace ONE管理ポータルのアプリリストに表示されます。

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 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。

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. [WithSecure Elements Mobile Protection] ビューで、[承認] > [選択] 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。
6. [SDK]タブを選択し、[アプリケーション プロファイル]ドロップダウン メニューから [MP 文字列 @ WithSecure を]選択します。
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]の下にあります。

   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) - WithSecure Elements Security Centerでユーザーを識別しやすくする名前
   - last_name (オプション) - WithSecure Elements Security Centerでユーザーを識別しやすくする名前

   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：これを行うには WithSecure Elements Mobile Protection with External MDMのサブスクリプションが必要です。

証明書を使用してデバイスを登録するには

1. 会社の管理者アカウントで WithSecure Elements Security Centerにログインします。
2. [サブスクリプション]の下で、
   
   次に [外部MDMサーバー構成を]選択します
3. 証明書ファイルをダウンロードして保存します。
4. VMware Workspace ONE管理ポータルで、[[リソース] > [プロファイルとベースライン] > [新しいプロファイルの追加]に移動します。

   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. [資格情報]の下で [追加]を選択し、WithSecure Elements Security Centerからダウンロードした証明書をアップロードします。
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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定するか、

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（88ページ）
   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。

ヒント：デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

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。

WithSecure Elements Mobile Protectionライセンスのアクティベーションには、次のキーと値が必須です。

キー	種類	説明	値	参考
fate_registration_key	文字列	クライアントが使用する登録キーまたはアクティベーションキー	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、WithSecure Elements Mobile Protectionアプリから VPN をオフにしたり、個々の保護機能を無効にしたり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」を参照してください。

以下のオプションキーは WithSecure Elements Security Center上のデバイスを識別するのに役立ちます。適切な値を取得するには、Microsoft Intune動的変数を使用してください。

キー	種類	説明
email	文字列	ユーザーのアクティベーションメールを指定します
env	整数	アプリケーションがアクティベートされる環境を指定します。本番環境でご利用の場合は、この値を「2」に設定してください。
data_usage_permission	ブール値	管理者がデータ収集を許可する場合は true に設定し、そうでない場合は false に設定します。
diagnostic_usage_permission	ブール値	管理者が診断情報の収集を許可する場合は true に設定し、許可しない場合は false に設定します。
create_vpn_profile	ブール値	VPNプロファイルの作成を許可するにはtrueに設定し、そうでない場合はfalseに設定します。

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

Microsoft Intune MDM を使用して WithSecure Elements Mobile Protectionアプリを展開する方法について説明します。

MDM管理対象デバイスの場合、WithSecure Elements Mobile Protectionはサイレントアクティベーションをサポートし、必要なすべてのシステムおよび機能権限を自動的に付与し、ユーザーの介入なしにVPNプロファイルを展開します。これにより、ユーザーが各権限リクエストを手動で承認してVPNプロファイルをインストールする必要がある標準的な展開とは異なり、真のゼロタッチ展開エクスペリエンスを実現します。

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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

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 Android デバイスに WithSecure Elements Mobile Protection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]または [完全に管理された専用および企業所有の仕事用プロファイル] の]いずれかを選択します。
   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: 値の型:[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 セキュリティ センターの [管理] > [サブスクリプション]」にあります。

- 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. Microsoft Endpoint Manager管理センターにログインします。
2. [アプリ]、] > [アプリ構成ポリシー] > [管理対象デバイス] > [の追加]の順に選択します。

   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することを選択できます。詳細については、「アプリ構成をサポートするアプリ」を参照してください。

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]です
4. [プラットフォーム]で、[**Android Enterprises**]を選択します。
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. [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、[**OK**]を選択します。
7. [次へ] > [追加] を選択します。
   「権限の追加」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

IBM MaaS360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。

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 Protection iOS アプリを IBM MaaS360 MDM に追加し、展開する方法について説明します。

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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

ヒント：デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

統合は次のものから構成されます。

- 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ーで設定するか、

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. 「アプリの詳細」タブで、[WithSecure Mobile Protection]アプリを検索して選択します。
   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。

WithSecure Elements Mobile Protectionアプリはアプリリストにあります。

iOSアプリの配布

WithSecure Elements Mobile Protection iOS 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アプリを追加する必要があります。

WithSecure Elements Mobile Protectionアプリを追加する

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

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]を選択して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] ウィンドウの [構成]タブで、[アプリ設定の構成]を選択し、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 [WithSecure Elements Mobile Protection]で、[表示]を選択します。
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

Ivanti Endpoint Management (旧称 MobileIron Cloud MDM) を使用した 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。

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

Ivanti Endpoint Managementを使用して iOS アプリを展開する方法を説明します。

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

WithSecure Elements Mobile ProtectioniOSアプリをIvanti Endpoint Managementに追加する方法を説明します。

WithSecure Elements Mobile Protection をMDM に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定するか、

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

1. Ivanti Endpoint Managementの管理ポータルで、[アプリ] ページに移動し、[追加] を選択します。
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。

ヒント：デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

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) この構成の名前を入力します (例: `WithSecure Elements Mobile Protection` ライセンス構成)。
   b) [fate_registration_key]フィールドに、WithSecure Elements Endpoint Protectionライセンスキーを入力します。
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、WithSecure Elements Security Center上のデバイスを識別するのに役立ちます。

ヒント：デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

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`
email	`$(userEmailAddress)`
first_name	`$(userFirstName)`
last_name	`$(userLastName)`
alias	`$(userDisplayName)`

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

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

Ivanti Endpoint Managementの [アプリ構成] > [][Android 向け管理構成]でサブスクリプション キーとその他の変数を追加することで、WithSecure Elements Mobile Protection手動で構成できます。

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

WithSecure Elements Mobile ProtectionAndroidアプリをIvanti Endpoint Managementに追加する方法を説明します。

WithSecure Elements Mobile Protection をMDM に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

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

1. Ivanti Endpoint ManagementのMDM管理ポータルで、[アプリ] に移動し、[追加] を選択します。
2. メニューから [Google Play]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、[選択]をクリックします。
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、[次へ]を選択します。
8. 優先する配布グループを選択し、[次へ]を押します。

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. [アプリ構成] > [Android 向け管理構成]で、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) [管理対象構成]で、[インストール時に自動起動]を選択します。
   c) [値が定義されたプッシュ設定のみが]選択されていることを確認します。
   d) [登録キー]の横に、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 Security Centerで確認できます。

   e) 電子メール アドレス フィールドに、値として `${userEmailAddress}`を入力します。
   f) [権限の管理]を]選択します。
      「権限の選択」ウィンドウが開きます。
   g) すべてのオプションを選択し、[選択]をクリックします。
   h) [ランタイム権限]の下で、すべてのドロップダウン メニューを確認し、[自動付与]を選択して、[次へ]を選択します。
      [アプリ設定] ページが開きます。
3. [デバイスにインストール]の横にある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) [デバイスのインストール構成を]オンにします。
   c) [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 [高優先度]を選択します。
   d) [次へ] を選択します。
      [構成設定] ページが開きます。
4. [プロモーション]の横にある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) [注目リスト]を選択します。
   c) [次へ] を選択します。
5. [委任されたデバイスの権限]の横にある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) [アプリ構成の管理」を]選択します。
   c) [次へ] を選択します
6. [完了] を選択します。
   WithSecure Elements Mobile Protectionがアプリ カタログに追加されました。

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. Ivanti Endpoint Managementの管理ポータルで、[構成] ページに移動し、[追加] を選択します。
2. [証明書] を選択します。
3. 証明書の名前を入力します。
4. WithSecure Elements Mobile Protectionの WithSecure Elements証明書をアップロードします。

   注 : 証明書は、WithSecure Elements Security Centerで見つかります。

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 : WithSecure Elements Mobile Protection有効にするには、証明書を手動または自動でデバイスに展開する必要があります。

Ivanti Endpoint Management を使用した Android Enterprise の導入

ここでは、Ivanti Endpoint Managementを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。

WithSecure Elements Mobile Protectionアプリを追加する

WithSecure Elements Mobile ProtectionアプリをIvanti Endpoint Managementに追加する方法を説明します。

1. Ivanti Endpoint Management管理ポータルで、[管理者] > [Google] > [Android Enterprise]を選択します。
   [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. [選択] ビューで、ドロップダウン メニューから [Google Play]を選択します。
6. [Google Playストアを検索] ボックスに「`WithSecure Elements Mobile Protection`」と入力します。
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、[次へ]を選択します。
10. 代理人ビューで、[次へ]を選択します。
11. 配布ビューで、希望するオプションを選択し、[次へ]を選択します。
12. [構成] ビューで、[Android 向けの管理対象構成]の横にあるプラス 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] フィールドに名前を入力し、[管理対象構成]で次の操作を行います。
    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。

       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 ProtectionApp Catalogページに表示されます。

3.4.7 Miradore MDMを使用した展開

Miradore 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。

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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定するか、

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

WithSecure Elements Mobile Protection iOSアプリをMiradore MDMに設定する方法を説明します。

ヒント：デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

1. Miradore管理ポータルで、アプリケーション リストの `WithSecure Elements Mobile Protection`エントリをダブルクリックします。
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。

キー	種類	説明
email	文字列	ユーザーのアクティベーションメールを指定します
env	整数	アプリケーションがアクティブ化される環境を指定します。本番環境でご利用の場合は、この値を「2」に設定してください。

キー	種類	説明
data_usage_permission	ブール値	管理者がデータ収集を許可する場合は true に設定し、そうでない場合は false に設定します。
diagnostic_usage_permission	ブール値	管理者が診断情報の収集を許可する場合はtrueに設定し、許可しない場合はfalseに設定します。
create_vpn_profile	ブール値	VPNプロファイルの作成を許可するにはtrueに設定し、そうでない場合はfalseに設定します。

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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

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、WithSecure Elementsサービスから見つけられるインストールリファラー文字列を使用します。WithSecure WithSecure Elements Mobile Protectionアクティベーション文字列を含む [**Google Play ダウンロード URL**]を探します。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 Jamf Pro MDMを使用した展開

WithSecure Elements Mobile Protection MDM を使用して Jamf Proアプリを iOS および iPadOS デバイスに展開する手順。

デバイスのライセンスを購入する

デバイスのライセンスを購入するための手順。

WithSecure Mobile Protectionアプリは、App Storeから無料で入手できます。Jamf Jamf Pro MDM 経由でアプリを配布するには、WithSecure Mobile Protectionアプリをインストールするデバイスの Volume Purchase Program (VPP) ライセンスを購入する必要があります。このライセンスの数は、WithSecure Mobile Protectionから購入した WithSecureライセンスの数と同じである必要があります。

必要なライセンスを購入するには:

1. Apple Business Managerポータルにログインします。
2. [アプリとブック]に移動して、WithSecure Mobile Protectionを検索します。
3. [ライセンスの購入]で、WithSecure Mobile Protectionから購入した WithSecureライセンスの数を入力し、[取得]を選択します。

   購入は 15 分以内に Jamf Pro と同期されます。

iOSおよびiPadOSデバイス用のアプリの設定

Jamf Pro MDM で iOS および iPadOS デバイス用の With Secure Mobile Protectionアプリを構成する手順。

ヒント: デフォルトでは、インストールプロセスでは、データ収集（Appleの規定による）、VPNプロファイルのインストールとアクティベーション、診断情報の収集へのユーザーの同意が必要です。構成キーを使用して事前にMDMを設定しておくことで、ユーザーの承認は不要になります。

アプリを構成するには:

1. Jamf Proにログインします。
2. [デバイス] > [モバイル デバイス アプリ、] > [セキュア モバイル保護] > [の編集]。
3. [全般] タブで、以下を構成します。
   a) [配布方法]で、希望する方法を選択します。
   b) [アプリの更新を自動的に強制する]オプションを選択します。
   c) ユーザーが WithSecure Mobile Protection削除できないようにするには、「ユーザーにアプリの削除を許可する (iOS 14 以降)]オプションをオフにすることをお勧めします。
4. [管理配布]タブで、[一括購入コンテンツの割り当て]を選択します。

   ユーザーが WithSecure Mobile Protection削除できないようにするには、「ユーザーにアプリの削除を許可する (iOS 14 以降)]オプションをオフにすることをお勧めします。

   注: 「場所」は、WithSecure Mobile Protectionアプリを購入した VPP の場所と一致する必要があります。

5. [アプリ構成]タブで、次の操作を行います。
   a) 次の設定を 「設定」ボックスにコピーします。

```
<dict>
 <key>fate_registration_key</key>
 <string>ENTER-THE-SUB-KEY-HERE</string>
 <key>email</key>
 <string>$EMAIL</string>
 <key>alias</key>
 <string>$USERNAME</string>
 <key>env</key>
 <string>2</string>
</dict>
```

注：「ENTER-THE-SUB-KEY-HERE」を WithSecure Mobile Protectionサブスクリプション キーに置き換えます。WithSecure Mobile Protection のサブスクリプション キーは、WithSecure Elements セキュリティ センターで確認できます。

注：「エイリアス」キーは WithSecure Elements Security Centerでデバイスを識別するのに役立ちます。「エイリアス」に別の値を使用する場合、Jamf では考慮すべき他の変数を提供しています。詳細については、Jamf Pro ユーザー ガイドの「管理対象アプリの構成変数」を参照してください。ただし、エイリアスを使用しない場合は、オプションの設定であるため、そのキーと関連する文字列を構成から削除できます。

b) With Secure Mobile Protectionインストールするデバイスが含まれるようにスコープを構成します。

アプリの通知の設定

構成プロファイルを使用して通知の表示方法を設定できます。

注：デバイスの通知の構成はオプションです。

WithSecure Mobile Protectionの通知を構成するには:

1. Jamf Proで、[デバイス] > [構成プロファイル] > [新規]を選択します。
2. 名前フィールドに「`WithSecure Mobile Protection Notifications`」と入力します。
3. [通知ペイロードの] > [追加を]選択し、次の操作を行います。
   - アプリ名：`WithSecure Mobile Protection`
   - バンドル**ID**: `com.f-secure.mobileprotection`

組織の設定に合わせてアラート設定を構成し、それに応じてポリシーの範囲を設定します。

3.4.9 Samsung Knoxを使用した展開

Samsung Knoxを使用してWithSecure Elements Mobile ProtectionアプリをAndroid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 に統合する前に、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
- プロファイルにポリシー制限を設定しました

  注：WithSecure は、特に明記されていない限り、プロファイルおよびポリシーに関連するサポートや指示を提供しません。

- 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サブスクリプション

統合は次のものから構成されます。

- 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ーで設定します

Android アプリを Samsung Knox に追加するには:

1. Samsung Knoxコンソールにログインします。
2. [アプリケーションを]選択します。
   [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 Managed Google Play]を選択し、[OK]を選択します。
5. 「アプリケーションの追加」ページで、「`WithSecure Elements Mobile Protection`」と入力し、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]の横にあるチェックボックスをオンにして、国を選択します。

6. 検索結果で、まず追加するアプリケーションを選択し、次に [選択します]。
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。[カテゴリの管理]を選択すると、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。
   - [保存して割り当て]を選択して情報を保存し、[続行]を選択してアプリケーションの割り当てに進みます。
   - [保存]を選択して情報を保存し、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. [アプリケーションを]選択します。
   [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 - [Android Enterprise]、[Android Legacy]、または [Android Enterprise + Legacy]のいずれかのオプションを選択できます。
   - 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。
     - [手動]- 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します
     - [自動 (削除可能)] - 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 (非リムーバブル、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 - 使用可能なオプションは [、デフォルトの更新]、[高優先度]、[延期 (90 日)]です。
4. [管理された構成] の横にある [構成の設定]を選択し、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 (例 : `Work`) を入力します。
   - 「登録キー」フィールドに、WithSecure Elements Mobile Protectionサブスクリプション キーを入力します。
   - エイリアスフィールドに「`$username$`」と入力します。
   - メールアドレスフィールドに「`$emailaddress$`」と入力します。
   - [環境] フィールドに、「2」と入力します。

注：値 `$ emailaddress$`を設定すると、WithSecure Elements に登録されたデバイスが電子メール アドレスとともに表示されます。

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 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。

WithSecure Elements Security Centerダウンロードするためのリンクを含む電子メール メッセージをユーザーに送信することで、WithSecure Elements Agentを通じてユーザーを招待できます。

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]の横にある[新しいデバイスを追加]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（19ページ）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、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。

3.5.1 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。

3.5.2 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

ユーザーに、次の手順に従ってiOSデバイスにWithSecure Elements Mobile Protectionインストールするように指示します。

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. 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。

第
4
章

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。

コンピューター、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。
- コンピューターのタイプ、「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 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。

4.1.1 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、WithSecure Elements Security Center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コンピューター。
   - 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。

4.1.2 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) [セキュリティ構成]で [プロファイル]を選択し、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。

4.1.3 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 Security Centerにログインします。
2. [環境] で、[デバイス] を選択し、1つ以上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。

4.2 プロファイルの管理

プロファイルは、エンドポイントに適用できる構成設定を定義します。プロファイルを管理することで、管理者は複数のデバイス間でセキュリティポリシーを効率的に標準化できます。

プロファイルは、エンドポイントの動作を制御し、セキュリティポリシーを適用する定義済みの設定の集合です。プロファイルを使用することで、以下のことが可能になります。

- 複数のクライアントに一貫した構成を適用します。
- ポリシーの更新を簡素化し、手動による構成エラーを削減します。
- 環境間で再利用できるようにプロファイルをエクスポートおよびインポートします。

4.2.1 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、WithSecure Elements Security Center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。

4.2.2 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ー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。

4.2.3 プロファイルをエクスポートする

WithSecure Elements Security Center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。

4.2.4 プロファイルをインポートする

WithSecure Elements Security Center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。

4.2.5 プロファイルを削除する

プロファイルを削除すると、WithSecure Elements Security Centerから削除されます。

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 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。
   プロファイルは Elements Security Centerから削除されます。

4.2.6 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。

4.2.7 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コンピューター用] または [Windowsサーバー用] タブを選択します。
3. 選択 比較するプロファイルの横にある をクリックし、[プロファイルの比較と編集]を選択します。
4. [比較するプロファイルの選択]ページで、比較する１つ以上のプロファイルを選択し、[次へ]を選択します。
   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。

4.2.8 エンドユーザによるコンピューター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. 選択 右上隅にある をクリックし、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。

4.2.9 テーブルの管理

選択したプロファイル内のテーブルからデータをエクスポートし、それをWithSecure Elements Security Center内の別のプロファイル内の同じテーブルまたは別の類似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。

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たり、データをエクスポートしたり、エクスポートしたファイル内のデータをテキスト エディターで編集したり、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したりできます。

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. 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、[アプリケーションコントロールの] > [除外]を選択します。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。

[ファイルからインポート (JSON)]オプションを使用すると、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. 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 コントロールの] > [除外]を選択します。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. 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 テーブル内のデータを置き換えるには、[アプリケーション コントロールの] > [除外]を選択します。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。

4.3 Elements EPP for Computers および Elements EPP for Servers (Windows) でのプロファイルの管理

このセクションでは 、WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversソフトウェアでプロファイルを管理する方法について説明します。

4.3.1 新しいコンピューター プロファイルを作成する

特定のコンピューター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 セキュリティ センターにログインします。
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コンピューター用] または [Windowsサーバー用] タブを選択し、[プロファイルを作成] を選択します。
   [Windowsコンピューター用プロファイル] または [Windowsサーバー用プロファイル] 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。

4.3.2 Windowsの一般設定を構成する

全般設定では、ユーザー インターフェイスの表示、統合機能、BitLocker 管理、ライセンス通知、ユーザー権限など、Windows エンドポイント クライアントのグローバル動作を制御します。

「全般」設定には、管理対象デバイスにおけるエンドポイント保護クライアントの動作を定義する構成オプションが含まれています。これらの設定により、機能の可用性、クライアントアプリケーションに対するユーザー操作、オペレーティングシステムのセキュリティ機能との統合を制御できます。

これらのオプションは通常、ポリシーの作成時で構成され、ポリシーに割り当てられているすべての Windows デバイスに適用されます。

Windowsの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。

[早期アクセス]がオンになっているプロファイルをデバイスに割り当てると、デバイスは、一般公開される前に最新の製品バージョンを受信し、サイレントアップグレード用の標準チャネルを通じてリリースされます。

アップグレード プロセスはサイレントのままで、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. [Windows コンピューター用]または [Windows サーバー用]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。
4. 左のメニューから [一般設定] を選択します。
5. [クライアント ソフトウェアへの早期アクセス]設定をオンにします。
6. 変更を適用するには、[プロファイルの保存]を選択します。

Windows への EDR センサーの統合

Windows エンドポイントに EDR センサーを統合するための設定を構成します。

WithSecure Elements Connector を使用して EDR センサーを有効にして構成するには、次の手順に従います。

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用]タブを選択します。
3. 編集するプロフィールを選択します。
   Windows の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. [EDR センサーを]オンにして、EDR サブスクリプションを持つデバイスでエンドポイントの検出と応答を有効にします。

   注：この設定はオンのままにすることを強くお勧めします。無効にすると、EDRはエンドポイントへの攻撃を検知または警告しません。

6. EDR で高度な応答モジュールを有効にする場合は、[高度な応答]をオンにします。

   高度なレスポンス機能を使用すると、機密データを含む可能性のある詳細なシステム情報にアクセスできます。この機能を有効にする前に、適用される労働者プライバシー法および関連する顧客要件または契約要件に準拠していることを確認してください。

   。

   注：この機能を使用することにより、お客様は法的に許可されており、適用法に基づいて必要なすべての同意を得ていることを確認します。

7. 外部ツールまたはスクリプトで Windows Management Instrumentation (WMI) を介して WithSecure Elements Agent の状態を照会する場合は、[WMI プロバイダーを]オンにします。

   WMI クエリに依存する監視ツールや管理ツールを使用しない場合は、この設定をオフのままにしておきます。

8. 変更を適用するには、[プロファイルを保存]を選択します。

Windows での BitLocker の管理

BitLocker 管理オプションを構成して、回復キーを収集し、管理対象デバイスでディスク暗号化をオンにします。

BitLocker 管理設定を使用して、Windows デバイスでのディスク暗号化と回復キーの収集を制御します。

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用]タブを選択します。
3. 編集するプロフィールを選択します。
   Windows の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. デバイスで使用可能なすべての [BitLocker 回復キーを収集するには、「BitLocker 回復キーの収集] をオンにします。

   注：回復キーが正常に収集され、管理ポータルに表示されることを確認します。

6. [BitLocker 保護]で、BitLocker 保護が適用されるディスクを選択します。
   - [変更なし]: デバイスの BitLocker 設定は変更されません。
   - [システムのみ]: BitLocker はシステム ディスクのみを保護します。
   - [すべて固定]: システム内のすべての固定ディスクに対して BitLocker がオンになっています。

7. デバイスの保護を [強化するために、PIN コードを設定するようリクエスト]をオンにします。

   PIN は、システムの起動時に PIN を要求することで、保護の層を追加します。

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コンピューター用] 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。

Windows のセキュリティ機能の管理

ユーザーが WithSecure Elements Agent をアンインストールしたり、デバイスのセキュリティ機能をオフにしたりできるかどうかを制御します。

これらの設定を使用して、ユーザーが製品をアンインストールしたり、セキュリティ機能をオフにしたりできるかどうかを制御します。

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用]タブを選択します。
3. 編集するプロフィールを選択します。
   Windows の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. [ユーザーに製品のアンインストールを許可する]は、ユーザーが WithSecure Elements Agent をアンインストールできるかどうかを制御します。

   この設定をオンにすると、ユーザーはデバイスからエージェントをアンインストールできます。パスワードが設定されている場合は、製品をアンインストールする際にパスワードを入力する必要があります。

   重要 : ユーザーがエージェントを削除できないように、この設定はオフにしておくことをお勧めします。

6. [ユーザーがすべてのセキュリティ機能をオフにできるようにするは、]ユーザーが WithSecure セキュリティ機能をオフにできるかどうかを制御します。

   この設定をオンにすると、ユーザーはデバイスの WithSecure 保護機能をオフにすることができます。

   重要 : セキュリティ機能を常に有効な状態に保つために、この設定をオフのままにしておくことを強くお勧めします。

7. [パスワード]フィールドにパスワードを指定します。

   この設定はオプションです。パスワードが設定されている場合、製品のアンインストールやセキュリティ機能の無効化など、制限された操作を実行するには、ユーザーはパスワードを入力する必要があります。

パスワードが指定されていない場合、設定がオンになっていると、ユーザーは認証なしでこれらのアクションを実行できます。

4.3.3 Windows の通信設定の構成

通信設定は、Windows エンドポイント クライアントがサービスに接続する方法、更新プログラムをダウンロードする方法、およびプロキシ サーバーまたは WithSecure Elements コネクタを介してネットワーク トラフィックをルーティングする方法を制御します。

通信設定は、管理対象Windowsエンドポイントクライアントがサービスインフラストラクチャへのネットワーク接続を確立する方法を定義します。これらの設定により、クライアントがクラウドサービスに直接接続するか、設定されたプロキシサーバーまたはWithSecure Elementsコネクタを介してトラフィックをルーティングするかが決まります。

これらのオプションを使用すると、特に送信インターネット アクセスを制御または特定のゲートウェイ経由でルーティングする必要がある環境で、エンドポイント通信を組織のネットワーク ポリシーに合わせることができます。

プロキシ設定の構成

Windows エンドポイント クライアントが HTTP プロキシ経由でネットワーク トラフィックをルーティングする方法と、更新プログラムをダウンロードする方法を構成します。

Windows クライアントのプロキシ設定を構成するには、次の手順に従います。

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 コンピューター用] を**]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[コミュニケーション]を選択します。
4. 通信設定を構成するポリシーを開きます。
5. [通信設定]に移動します。
6. クライアントの通信をプロキシ サーバー経由でルーティングするには、[**HTTPプロキシを使用する**] を選択します。

   HTTPプロキシが使用されている場合、製品コンポーネントによるすべての接続はHTTPプロキシを使用します。プロキシに接続できない場合、クライアントは自動的に直接接続にフォールバックします。

   この設定は、スタンドアロンの Endpoint Detection and Response エージェントにも適用されます。

   注：ユーザーのブラウザ設定からプロキシを使用するには、ユーザーがログインしている必要があります。プロキシ設定はユーザーが変更することもできます。プロキシはログインしているユーザーによって選択され、ユーザーがログインしていない場合は検出できないため、ユーザーのブラウザ設定からサーバーへのプロキシ設定を使用することはお勧めしません。

7. クライアントが [プロキシ接続を優先するようにしたい場合は、「プロキシ経由の接続を優先する] を選択します。

   デフォルトでは、クライアントは前回の接続で成功した接続方法を使用します。プロキシが失敗した場合、クライアントは直接接続に切り替え、利用できなくなるまで直接接続を継続することがあります。

   この設定により、クライアントはすべての接続でプロキシの使用を強制されます。

8. ローカル クライアント インターフェイスからプロキシ設定を非表示にするには、[プロキシ構成を非表示]を選択します。

   非表示にすると、プロキシ構成パネルはエンドポイント デバイスのローカル ユーザー設定インターフェイスに表示されなくなります。

9. 暗号化された接続経由で更新をダウンロードするには、[**HTTPS を使用して更新をダウンロードする**]を選択します。

HTTPSはプライバシーを向上させ、特定のコンプライアンス要件を満たすのに役立ちます。ただし、HTTPSトラフィックはプロキシによってキャッシュできないため、更新キャッシュが使用されている環境ではネットワークトラフィックが増加する可能性があります。

ソフトウェア アップデータ通信設定の構成

HTTP プロキシまたは WithSecure Elements Connector を使用して、Software Updater が更新サービスに接続する方法を構成します。

ソフトウェア アップデーターの通信設定は、ソフトウェア アップデーター コンポーネントが更新サービスに接続する方法を決定します。専用の HTTP プロキシを使用するか、WithSecure Elements コネクタを介してトラフィックをルーティングするようにコンポーネントを設定できます。

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 コンピューター用**] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[コミュニケーション]を選択します。
4. [**HTTP プロキシを使用する**]ようにソフトウェア アップデーターを構成するには、「HTTP プロキシを使用する」を選択します。

   HTTPプロキシを使用する場合、ソフトウェア アップデータは設定されたHTTPプロキシを介してアップデートサービスへの接続を試みます。プロキシに接続できない場合、ソフトウェアアップデータは自動的に直接接続にフォールバックします。

5. ElementsConnector経由でSoftwareUpdaterトラフィックをルーティングするには、[**UseWithSecure Elements Connector**]を選択します。

Windowsコンピュータープロファイルで 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:「Windows に Elements Connector をインストールする」の手順に従ってください。
   - Linux の場合:「Linux に Elements Connector をインストールする」の手順に従ってください。

   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。

ログ	説明
`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使用するようにプロファイルを構成します。
   a) [セキュリティ構成] で、[プロファイル] を選択します。
   b) 編集するプロファイルを選択します。
   c) [全般]で、[**WithSecure Elements** コネクタ]設定を編集し、インストールしたコネクタ サーバーのアドレスを指定します。

      注 : デフォルトでは、WithSecure Elements Connectorはポート80を使用します。HTTPSアドレス/ポートを使用するには、「Elements Connectorをプロキシとして設定する」の手順に従ってTLS証明書を設定してください。ポートがWindowsファイアウォールでブロックされていないことを確認してください。

   d) ソフトウェア アップデーターを使用する場合は、[ソフトウェア アップデーター]タブを開き、**WithSecure Elements** コネクタ設定を編集して、インストールしたコネクタ サーバーのアドレスを指定します。

      注 : デフォルトでは、WithSecure Elements Connector は TLS とポート 443 を使用します。TLS 証明書を設定するには 、「Elements Connector をプロキシとして設定する」の手順に従ってください。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。

   e) エンドポイントコンピュータが直接インターネットに接続できない場合は、Elements Connectorを最終プロキシとして設定します。「全般]タブを開き、[手動で定義したプロキシアドレス]を編集し、インストールしたコネクタサーバーのアドレスを指定します。

      注: 究極モードでは、HTTPホストインターフェース (デフォルトはポート80) が拡張されます。このポートが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。

3. プロファイルを割り当てたら、クライアントで確認します。
   a) トレイ アイコンからクライアントを右クリックし、[更新プログラムの確認]を選択します。
   b) 設定ウィンドウが開いたら、[接続] > [更新サーバー]フィールドに WithSecure Elements Connector アドレス値が指定されていることを確認します。
   c) [今すぐ確認を]選択します。

      チェックはエラーなしで実行されるはずです。

4.3.4 Windowsのスキャン設定の構成

スキャン設定では、エンドポイント保護クライアントがマルウェアを検出して処理する方法、リムーバブル メディアのスキャンを管理する方法、セキュリティ スキャン全体にグローバル除外を適用する方法を定義します。

スキャン設定は、Windowsクライアントがファイルやシステムアクティビティを悪意のあるコンテンツの有無について監視する方法を制御します。これらの設定により、脅威の検出方法、リムーバブルストレージデバイスの処理方法、ユーザーへのスキャン通知の表示方法が決まります。

Windows での一般的なスキャン設定の構成

Windows エンドポイント クライアントがマルウェアを監視し、リムーバブル メディアを処理し、通知を表示する方法を構成します。

共通スキャン設定は、エンドポイントクライアントがシステムアクティビティをマルウェアの有無で監視する方法と、管理対象デバイスにスキャン関連の動作を適用する方法を制御します。これらの設定は、マルウェア検出の動作、リムーバブルメディアの処理、ユーザーへの通知、スキャン中のディスク容量の使用状況に影響します。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[スキャン設定]を選択します。
4. [共通スキャン]で、[マルウェア監視モード]を構成します。

   マルウェア監視モードは、検出された脅威をクライアントが処理する方法を決定します。

   注 : [ブロック]以外のモードでは、Windows Elements エージェントはオペレーティング システムを積極的に保護せず、検出された脅威を報告するだけです。

   - 有害なアイテムを自動的にブロックするには、[ブロック (推奨)]を選択します。

     これはデフォルトのモードです。有害なアイテムが検出された場合は、製品の設定に従って処理されます。

   - マルウェアをブロックせずにアクティビティを監視するには、[許可]を選択します。

     このモードではマルウェアはブロックされません。すべてのプロセスとアクションを監視すると、コンピューターのパフォーマンスに影響する可能性があります。

     注 : このオプションはテスト目的でのみ使用してください。

   - 強化された検出機能を使用してアクティビティを監視するには、[許可 (強化された脅威検出)]を選択します。

     このモードではマルウェアはブロックされません。拡張監視によりすべてのプロセスとシステムアクションが分析されるため、システムパフォーマンスが大幅に低下する可能性があります。

     注 : このオプションはテスト目的でのみ使用してください。

   重要 : WithSecure サポートから別途指示がない限り、デフォルトの [ブロック]モードを維持することを強くお勧めします。

5. [USB ストレージ デバイスが接続されたときのアクション]を設定します。

   この設定は、USBストレージデバイスがコンピューターに接続されたときにクライアントがどのように反応するかを制御します。

   - [何もしない]: USB ストレージ デバイスが接続されたときに、クライアントはスキャンを実行しません。
   - [USB のスキャンをユーザーに要求]: 接続されている USB ストレージ デバイスのスキャンを開始するようにユーザーに要求します。
   - [USB をサイレントスキャン]: ユーザーに通知せずに USB ストレージ デバイスが自動的にスキャンされます。
   - [USB をスキャンして結果をユーザーに表示]: USB ストレージ デバイスが自動的にスキャンされ、スキャン結果がユーザーに通知されます。
   - [USBを強制スキャンして結果をユーザーに表示] : USBストレージデバイスが自動的にスキャンされ、その結果がユーザーに表示されます。ユーザーはスキャンをスキップできません。

6. [通知の表示]を構成して、再起動要求、検出された脅威、エラー通知などのクライアント通知を表示できるユーザーを選択します。
7. スキャン中に使用される [一時ファイルの最大サイズ]を設定します。

   この設定は、アーカイブやその他の複雑なファイルを分析するときに、スキャン プラットフォームが一時ファイルを保存するために使用できるディスク領域の量を定義します。

   注 : 使用可能なディスク容量が不足している場合、または解凍されたファイルが設定された制限を超えている場合、スキャンは失敗します。

スキャン除外の設定

選択したファイル、フォルダー、ファイル ハッシュがセキュリティ スキャンに含まれないように除外を設定します。

グローバル除外設定では、すべてのセキュリティスキャンと保護対策から除外するファイル、フォルダ、およびSHA-1またはSHA-256チェックサムを定義します。除外されたコンテンツはWithSecureの保護の対象外となるため、必要な場合にのみ除外設定を使用してください。

注：これは EDR センサー スキャンには適用されません。

重要：ファイルまたはフォルダの除外は、絶対に必要な場合のみ行ってください。たとえば、`C:\`を除外すると、デフォルトのシステムドライブ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。

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. [**Windows** コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. [スキャン設定]を選択します。
4. Elements Agent またはスキャン レポートでユーザーに除外を表示したくない場合は、[すべてのセキュリティ スキャンからのグローバル除外]で [クライアントから除外を非表示にする]を選択します。

   非表示にすると、構成された除外リストはクライアント ユーザー インターフェイスおよびユーザーに表示されるスキャン レポートに表示されなくなります。

5. [グローバル除外]の下に必要なエントリを追加します。

   フォルダ、ファイル、SHA-1またはSHA-256チェックサムを除外できます。設定されたすべての除外は、すべてのセキュリティスキャンと保護対策に適用されます。

   パスにはワイルドカード (*) とシステム環境変数を使用できます。

   注：フォルダーの除外は、バックスラッシュ (\) で終わる必要があります。

   - [ファイル パスは]特定のファイルを除外します (例: `C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE`)。
   - [フォルダー パスでは]、フォルダーとそのすべてのサブフォルダーおよびファイルが除外されます (例: `C:\Program Files (x86)\Microsoft Office\ `)。
   - [ワイルドカード パスは]、一致するパスを除外します (例: `C:\Program Files*\Microsoft*`)。
   - [環境変数パスに]は、システム環境変数を使用するパス (例: `%ProgramFiles%\Java`)は含まれません。
   - [**SHA-1** または **SHA-256** チェックサムは]、チェックサムによってファイルを除外します (例: `3395856ce81f2b7382dee72602f798b642f14140`)。

Windows での検疫設定の構成

隔離またはブロックされたアイテムを解放する方法と、アイテムを隔離エリアに保持する期間を構成します。

隔離設定は、エンドポイントクライアントがブロックまたは隔離されたファイルを管理する方法を制御します。ユーザーが隔離されたアイテムを復元できるようにしたり、解放操作をパスワードで保護したり、古い隔離アイテムを自動的にクリーンアップするように設定したりできます。

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** コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[スキャン設定]を選択します。

4. ユーザーが隔離またはブロックされたファイルを復元できるようにする場合は、[隔離]の下で、[ブロックおよび隔離されたアイテムの解放をユーザーに許可する]を選択します。

   この設定をオンにすると、ユーザーはクライアント インターフェイスから隔離されたアイテムを解放したり、ブロックされたアイテムを許可したりできるようになります。

5. このアクションを制限する場合は、[ブロックまたは隔離されたアイテムを解放するためのパスワード]を設定します。

   パスワードが定義されている場合、ユーザーは隔離されたアイテムを解放したり、ブロックされたアイテムを許可したりする前にパスワードを入力する必要があります。

   パスワードが設定されていない場合、ユーザーは追加の認証なしでアクションを実行できます。

6. 隔離されたファイルを自動的にクリーンアップするには、[古い隔離アイテムを自動的に削除する]を選択します。

   選択すると、隔離領域に保存されたアイテムは、設定された保持期間後に自動的に削除されます。

7. [アイテムを検疫に保持する日数]を設定します。

   この値は、隔離されたアイテムが自動的に削除されるまでの保持期間を定義します。

   許容範囲は `1 ~ 1095` 日です。

改ざん防止の設定

改ざん防止を設定して、エンドポイント保護クライアントの不正な変更を防ぎ、必要に応じて特定のアプリケーションが改ざん防止イベントを生成しないように除外します。

改ざん防止機能は、不正なアプリケーションやユーザーが管理対象デバイス上のWithSecureサービス、プロセス、ファイル、レジストリ エントリを変更することを防ぎます。

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 用のコンピューター保護] 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. [スキャン設定]の下で、[改ざん防止]まで下にスクロールします。
5. [改ざん防止をオンにする]を選択します。

   選択すると、改ざん防止により、外部のアプリケーションまたはユーザーが WithSecure のサービス、プロセス、ファイル、またはレジストリ エントリを制御できなくなります。

6. 特定のアプリケーションが改ざん防止イベントを生成しないようにする場合は、[除外の追加]を選択して、[改ざん防止イベントを除外」にエントリを追加します。

   特定のアプリケーションを改ざん防止イベントの生成から除外することで、信頼されたアプリケーションが保護されたコンポーネントと頻繁に対話する環境で生成される改ざん防止イベントの数を減らすことができます。

   不正なアクセス試行は引き続きブロックされますが、イベントは送信されません。

   アプリケーション パスではワイルドカード (*) とシステム環境変数を使用できます。

   - [アプリケーション パスは、]特定のアプリケーションを改ざん防止イベントの生成から除外します。
   - [ワイルドカード パスは、]指定されたパス パターンに一致する複数のアプリケーションを除外します。
   - [環境変数パスは、]パス内のシステム環境変数を使用するアプリケーションを除外します。

4.3.5 Windows のリアルタイムスキャンの設定

リアルタイム スキャンは、システム アクティビティとファイル操作を継続的に監視し、エンドポイントに影響を与える前に悪意のあるコンテンツや疑わしいコンテンツを検出してブロックします。

リアルタイムスキャンは、管理対象デバイス上のファイル、プロセス、システムアクティビティを監視することで、継続的な保護を提供します。リアルタイムスキャンがオンになっている場合、エンドポイント保護クライアントは、Webトラフィックやネットワークドライブなどのサポートされているチャネルを介してファイルがアクセス、実行、または転送されたときに、ファイルを分析します。

脅威の検出方法、疑わしい動作の処理方法、保護エンジンがオペレーティングシステムのセキュリティ機能と対話する方法を構成できます。

マルウェア対策スキャンインターフェースの使用

AntiMalware Scan Interface (AMSI) 統合により、オペレーティング システムは WithSecure 保護エンジンを使用して、スクリプトやその他のサポートされているコンテンツをスキャンできるようになります。

AntiMalware Scan Interface (AMSI) 統合により、オペレーティング システムは WithSecure 保護エンジンを使用して、スクリプトやその他の潜在的に悪意のあるコンテンツを実行前に分析できます。

たとえば、Windowsは、インストールされているマルウェア対策ソリューションを使用して、PowerShell スクリプトと Microsoft Office VBA マクロをスキャンするために AMSI を使用します。

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 コンピューター用] を**]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[リアルタイム スキャン]を選択します。
4. [**AMSI を有効にする**]を選択します。

   この設定を選択すると、サポートされているアプリケーションとオペレーティング システム コンポーネントは、実行前にセキュリティ分析のためにスクリプトやその他のコンテンツをWithSecure保護エンジンに送信できます。

ファイルスキャン設定の構成

リアルタイム スキャンで感染したファイルを処理する方法、ネットワーク ドライブをスキャンする方法、ファイルの種類を分析する方法を構成します。

ファイルスキャン設定は、エンドポイント保護クライアントがリアルタイム保護中にファイルをスキャンする方法を定義します。さまざまな脅威の種類への対応方法を設定したり、ネットワークドライブやファイルの種類に対するスキャン動作を制御したり、クラウドベースの分析を有効にして脅威検出能力を向上させたりすることができます。

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 コンピューター用] を**]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[リアルタイム スキャン]を選択します。
4. [感染時のアクション]を構成して、感染していると検出されたオブジェクトをクライアントがどのように処理するかを決定します。
5. [リスクウェアに対するアクション]を構成して、リスクウェアとして分類されたオブジェクトをクライアントがどのように処理するかを決定します。
6. [スパイウェアに対するアクション]を構成して、スパイウェアとして分類されたオブジェクトをクライアントがどのように処理するかを決定します。
7. リアルタイム スキャン中にネットワーク ドライブ上にあるファイルをどのようにスキャンするかを制御するには、[ネットワーク ドライブのスキャン]のスキャン動作を選択します。
   - [ファイル アクセスごとにスキャンを実行すると、]ファイルが開かれたり、変更されたり、アクセスされたりするたびにファイルがスキャンされます。

- 実行 [時にスキャンすると]、アプリケーションの起動時など、ファイルが実行されるときにのみファイルがスキャンされます。

注: ファイルにアクセスするたびにネットワークドライブ上のファイルをスキャンすると、パフォーマンスが大幅に低下する可能性があります。

8. スキャンを特定のファイルタイプに制限する場合は、[特定の拡張子のファイルのみをスキャンする]を選択します。

   選択すると、スキャンエンジンは保護エンジンによって定義された拡張子を持つファイルのみを分析します。このリストは自動的に管理されます。

   注 : [除外される拡張子]設定を使用して、追加のファイル拡張子を除外することもできます。

9. [疑わしいサンプルを **WithSecure Security Cloud** にアップロード]を選択します。

   選択すると、ローカル保護エンジンによって認識されない疑わしいファイルが、さらに分析するために WithSecure Security Cloud にアップロードされる可能性があります。

   ドキュメントにユーザーデータが含まれる可能性がある場合は、個人情報が含まれないファイル部分のみがアップロードされます。

   注 : ゼロデイマルウェアの検出と誤検知の削減に役立つため、この設定をオンのままにしておくことを強くお勧めします。

10. [保護ホスト ファイル]を構成します。

    この設定により、システムの `Hosts`ファイルの保護が有効になります。

    hostsファイルが保護されている場合でも、ファイルは編集可能です。ただし、製品の機能に支障をきたす可能性のあるリダイレクトが検出された場合、変更内容はファイルのクリーンなバージョンに戻されます。

11. 特定のファイルタイプのスキャンをスキップするには、[次の拡張子を持つファイルを除外する]を選択します。

    [除外拡張子]リストを使用して、スキャンしないファイル拡張子を定義します。

    ファイル拡張子は先頭にピリオドを付けずに入力してください (例 : `.JPG`ではなく `JPG`) 。複数の拡張子を入力する場合は、スペースで区切ってください。

除外の設定

特定のファイル、フォルダー、プロセス、または脅威カテゴリがリアルタイム保護によってスキャンされないように除外を設定します。

除外設定を使用すると、選択したファイル、フォルダー、プロセス、または特定の脅威カテゴリをリアルタイム保護によるスキャンから除外できます。保護対象ファイルとやり取りする信頼できるアプリケーションや特殊なワークロードでは、除外設定が必要になる場合があります。

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. [**Windows** コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[リアルタイム スキャン]を選択します。
4. オブジェクトの除外を使用するには、「オブジェクトの [除外を許可する]を選択します。

   選択すると、リアルタイム スキャンから除外するファイルとフォルダーを定義できます。

5. [除外オブジェクト]の下に除外エントリを追加します。

   スキャンから除外するファイルまたはフォルダのフルパスを指定します。パスにはワイルドカード (`*`) とシステム環境変数を使用できます。

   注 : フォルダーの除外は、バックスラッシュ (\) で終わる必要があります。

   - [ファイル パス](例: `C:\Program Files\Application\app1.exe`) では、指定されたファイルが除外されます。

- [フォルダー パス](例: `C:\Folder1\`) は、指定されたフォルダー内のすべてのファイルを除外します。
- [ワイルドカード パス](例: `C:\Program Files (x86)\Microsoft*`)は、ワイルドカード パターンに一致するすべてのファイルとフォルダーを除外します。
- [環境変数パス](例:`%ProgramFiles%\Java\`)は、システム環境変数を使用するファイルを除外します。

6. プロセスの [除外を使用するには、「プロセスの除外を許可する]を選択します。

   選択すると、特定のプロセスをリアルタイム スキャンから除外できます。

   注 : 除外されたプロセスは監視されず、セキュリティ リスクが発生する可能性があります。

7. [除外プロセス]の下に除外エントリを追加します。

   スキャンから除外するプロセスのフルパスを指定します。パスにはシステム環境変数を使用できます。

   - [プロセス パス](例: `C:\Program Files\Application\app1.exe`)。
   - [環境変数パス](例: `%ProgramFiles%\Application\app1.exe`)。

8. [すべてのリスクウェアのスキャンをスキップするには、「すべてのリスクウェアを除外]を選択します。
9. すべてのスパイウェアのスキャンをスキップするには、[すべてのスパイウェアを除外する]を選択します。
10. 特定の検出に対してカスタム除外を使用するには、[リスクウェア/スパイウェアの除外を許可する]を選択します。

    選択すると、リアルタイム スキャンから除外する特定のリスクウェアまたはスパイウェアの検出を定義できます。

11. [除外されたリスクウェア/スパイウェア]の下に除外されたエントリを追加します。

    スキャンから除外する検出名または検出名の部分文字列を指定します。ワイルドカード (*) がサポートされています。

ウェブトラフィックスキャンの設定

HTTP Web トラフィック スキャンを設定し、Web トラフィック検査から除外するアプリケーションを定義します。

Webトラフィックスキャンは、HTTP接続を介して転送されるファイルを分析して、エンドポイントに到達する前に悪意のあるコンテンツを検出し、削除します。Webトラフィック検査を有効にしたり、スキャンするコンテンツの種類を制御したり、必要に応じて特定のアプリケーションをスキャンから除外したりできます。

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** コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[リアルタイム スキャン]を選択します。
4. [**Web** トラフィック スキャンを有効にする]を選択します。

   この設定は、HTTP 接続経由の Web トラフィックのスキャンをオンにします。

5. [**Web** トラフィックをスキャンし、見つかったマルウェアを削除するよう]設定します。

   この設定では、スキャンされる Web コンテンツの種類と、検出されたマルウェアを自動的に削除するかどうかを決定します。

   - [**Web**トラフィックをスキャンして、見つかったマルウェアを削除します。**Web**]トラフィックをスキャンし、検出された悪意のあるファイルを自動的に削除します。
   - [含まれている拡張子のみ、]保護エンジンによって定義された拡張子に一致するファイルのみをスキャンします。

6. 特定のアプリケーションがWebトラフィック検査をバイパスする必要がある場合は、[Webトラフィックスキャンから除外されるアプリケーション]にエントリを追加します。

   このリストを使用して、特定のアプリケーションをウェブトラフィックスキャンから除外します。各エントリは、SHA-1ハッシュを使用してアプリケーションを定義します。

   - [有効にすると、]除外ルールがオンまたはオフになります。
   - [アプリケーションSHA-1は]除外する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ハッシュを生成します。

     注：アプリケーションをアップグレードする場合は、新しいハッシュを計算する必要があります。

   - [メモは]、アプリケーション名やその他の識別情報を保存するために使用できます。このフィールドはユーザーには表示されません。

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。

DeepGuardは実行中のすべてのアプリケーションを継続的に監視し、異常な動作やシステムへの有害な変更を検出します。

重要:DeepGuardを常に有効にしておきましょう。ランサムウェアなどの高度な脅威に対する重要な保護を提供します。

DeepGuardがアクティブな場合、次の保護が有効になります。

- 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

DeepGuard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. [DeepGuard設定]で、[まれなファイルや疑わしいファイルをブロックするを]選択します。

   この設定により、DeepGuardは動作分析と評価情報に基づいて、まれなファイルや疑わしいファイルをブロックできるようになります。

   この機能をオンにすると、疑わしいプログラムの検出が改善され、ゼロデイ攻撃に対する保護が強化されます。

   注：一般的でないソフトウェアや社内で開発されたソフトウェアを使用する環境では、この設定によって誤検知が発生する場合がありますが、有効にしておくことを強くお勧めします。

3. 特定のアプリケーションを信頼またはブロックする必要がある場合は、[保護ルール]にエントリを追加します。

   保護ルールを使用すると、信頼できるアプリケーションをDeepGuardのスキャンから除外したり、明示的にブロックしたりできます。DeepGuardはランサムウェアなどの高度な脅威に対する重要な保護を提供するため、この機能は必要な場合にのみ使用してください。

   - [有効にすると、]保護ルールがオンまたはオフになります。
   - [アプリケーションSHA-1/SHA-256は、]SHA-1またはSHA-256ハッシュを使用してアプリケーションを識別します。ハッシュ計算機を使用してハッシュを生成します。

注：アプリケーションをアップグレードする場合は、新しいハッシュ値を計算する必要があります。

- [メモは]、アプリケーション名やその他の識別情報を保存するために使用できます。このフィールドはエンドユーザーには表示されません。
- [Trusted は]、DeepGuard がアプリケーションを処理する方法を定義します。

  アプリケーションが信頼されている場合、DeepGuard はアプリケーションのすべての操作を許可します。

  アプリケーションが信頼されていない場合、DeepGuard は常にアプリケーションの実行を防止します。

4. 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：絶対に必要な場合のみアプリケーションを除外することをお勧めします。

   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。

4.3.6 Windows の手動スキャンの設定

手動およびスケジュールされたスキャン設定では、オンデマンドまたはスケジュールされた間隔でエンドポイント デバイスをマルウェア スキャンする方法を定義します。

手動スキャンとスケジュールスキャンは、リアルタイム保護の枠外でファイルやシステム領域をスキャンし、悪意のあるコンテンツを検出することで、さらなる保護を提供します。スケジュールスキャンは、指定した間隔で自動的に実行されるように設定でき、手動スキャンの実行時の動作を制御することもできます。

スケジュールスキャンの設定

スケジュールされたスキャンの実行頻度を設定し、スケジュールされたスキャン中に使用される条件とパフォーマンス設定を定義します。

スケジュールスキャンにより、エンドポイント保護クライアントは、指定された時間にシステムを自動的にスキャンしてマルウェアを検出できます。スキャン頻度、開始時刻、システム状態、パフォーマンス設定を調整することで、保護とシステムへの影響のバランスを取ることができます。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから [手動スキャン]を選択します。
4. [スケジュールされたスキャン]で、[スキャンの頻度]とスケジュールされたスキャンが実行される日を構成します。

   これにより、スケジュールされたスキャンの実行頻度と、スキャンが実行される曜日が定義されます。

5. [スキャンの開始]でスケジュールされたスキャンの開始時刻を構成します。

   時間と分を定義して、スケジュールされたスキャンを開始する時刻を指定します。

6. [システムがアイドル状態になった後にスキャンを開始するを]設定します。

   スケジュールされたスキャンは、コンピューターが指定された期間アイドル状態になった後にのみ開始されます。

7. スキャンで使用するシステム リソースを少なくしたい場合は、[スキャンを低優先度で実行]を選択します。

   低い優先度でスキャンを実行するとシステムへの影響は軽減されますが、スキャンを完了するのに必要な時間は長くなります。

8. スキャンでアーカイブの内容を分析する場合は、[圧縮ファイル内をスキャン]を選択します。

選択すると、スキャン エンジンは ZIP、7Z、RAR などのアーカイブ内のファイルを分析します。

注：この設定を無効にすると、圧縮ファイル内にマルウェアが隠れている可能性があるため、検出機能が低下する可能性があります。

9. スキャンを危険度の高いファイル タイプに制限するには、[スケジュールされたスキャン中に既知のファイル タイプのみをスキャンするを]選択します。

   選択すると、実行可能ファイルやスクリプトなど、マルウェアによく関連付けられるファイルの種類のみがスキャンの焦点になります。

   注：スキャンを既知のファイル タイプに制限するとパフォーマンスは向上しますが、検出範囲が狭まる可能性があります。

10. [デバイスが電源に接続されているときのみスキャンを実行する場合は、[デバイスがバッテリで動作している間はスケジュールされたスキャンをスキップする]を選択します。
11. [ユーザーへの通知を表示するよう]設定します。

    この設定をオフにすると、スケジュールされたスキャンの通知がユーザーに表示されなくなります。

手動スキャンの設定

手動スキャンでシステム リソースを使用する方法、検出された脅威を処理する方法、スキャンに含めるファイルと除外するファイルを定義する方法を設定します。

手動スキャン設定は、オンデマンドスキャンの実行方法を定義します。これらの設定は、スキャンの優先度、脅威の処理方法、スキャン範囲、除外対象を制御します。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから [手動スキャン]を選択します。
4. [手動スキャン]の下で、[スキャンの優先順位]を構成します。

   これにより、手動スキャンで使用できるシステム リソースの量を定義します。

   - [通常の優先度では、]通常のシステム リソースを使用してスキャンが実行されます。
   - [バックグラウンドスキャンは]、リソース使用量を抑えながらスキャンを実行します。このオプションはパフォーマンスへの影響を最小限に抑えますが、スキャンの完了にかかる時間が長くなる可能性があります。

5. [感染時のアクション]を設定して、手動スキャン中に感染していると検出されたオブジェクトを製品が処理する方法を定義します。
6. アーカイブに含まれるファイルを分析する場合は、[圧縮ファイル内をスキャン]を選択します。

   選択すると、スキャン エンジンは ZIP ファイルなどのアーカイブ形式内にあるファイルを分析します。

7. 電子メールのメールボックスファイルをスキャンする場合は、[メールボックスファイル内のスキャン]を選択します。

   選択すると、スキャナーはサポートされているメールボックスファイル形式を分析します。メールボックスファイル内で検出された脅威に対するデフォルトのアクションは、メールボックスデータの破損リスクを回避するため、「報告のみ」です。

   サポートされているメールボックスの形式は次のとおりです。

   - BSD mbox形式
   - Netscape/Mozilla メールボックス
   - Eudora メールボックス
   - ペガサスメールボックス
   - Outlook メールボックス

8. [スキャンするファイル]でスキャンするファイルを構成します。

すべてのファイルをスキャンすることも、特定のファイル拡張子のみをスキャンすることもできます。すべてのファイルをスキャンする場合でも、除外設定を使用して選択したファイル拡張子を除外することができます。

9. スキャンが特定の [拡張子に限定されている場合は、「含まれる]拡張子」でスキャンするファイルの種類を指定します。

   ファイル拡張子は先頭のピリオドなしで入力してください（例：.EXEではなくEXE）。複数の拡張子を入力する場合は、スペースで区切ってください。

10. 特定のファイルタイプのスキャンをスキップするには、[次の拡張子を持つファイルを除外する]を選択します。

    [除外拡張子]で定義されたファイル拡張子は、手動スキャン中にはスキャンされません。

11. [除外する拡張子]で除外するファイルの種類を指定します。

    ファイル拡張子は先頭のピリオドなしで入力してください（例：.EXEではなくEXE）。複数の拡張子を入力する場合は、スペースで区切ってください。

12. ファイルとフォルダーの除外を有効にするには、[除外オブジェクトを有効にする]を選択します。
13. [除外オブジェクト]の下にエントリを追加します。

    スキャンから除外するファイルまたはフォルダのフルパスを指定します。パスにはワイルドカード（*）とシステム環境変数を使用できます。

    注：フォルダーの除外は、バックスラッシュ (\) で終わる必要があります。

    - [ファイル パス](例: `C:\Program Files\Application\app1.exe`)。
    - [フォルダー パス](例: `C:\Folder1\`) では、フォルダー内のすべてのファイルが除外されます。
    - [ワイルドカード パス](例: `C:\Program Files (x86)\Microsoft* `)。
    - [環境変数パス](例: `%ProgramFiles%\Java\`)。

4.3.7 Windows のブラウジング保護の設定

ブラウジング保護設定は、Windows エンドポイント クライアントが Web トラフィックを監視およびフィルター処理して、悪意のある Web コンテンツ、疑わしい Web コンテンツ、または不要な Web コンテンツをブロックする方法を制御します。

ブラウジング保護は、アクセスしたウェブサイトを分析し、ウェブコンテンツをフィルタリングし、有害または不適切なリソースへのアクセスを防止することで、ウェブベースの脅威からユーザーを保護します。ブラウジング保護を設定することで、危険なウェブサイトをブロックしたり、セーフサーチを強制したり、特定のカテゴリのウェブコンテンツへのアクセスを制御したりできます。

ブラウジング保護の設定

ブロックされたページへのユーザー アクセス、ブラウザー拡張機能のリマインダー、セーフサーチの適用、イベント レポートなど、一般的なブラウジング保護の動作を構成します。

ブラウジング保護の共通設定では、ブロックされたページの処理方法、ブラウザ保護拡張機能についてユーザーに通知する方法、ブロックされた Web サイトに関連するセキュリティ イベントに含める情報を制御します。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[ブラウジング保護]を選択します。
4. [ユーザーがブロックされたページを続行できるようにする設定を行います]。

   選択すると、管理者権限を持つユーザーは警告ページをバイパスして、ブロックされたWebサイトに進むことができます。

   注：これをオフのままにしておくことをお勧めします。

注：ページがブロックされたときにブラウザに [この Web サイトを許可する]リンクが表示されるようにするには、[Web サイトの例外が]オンになっており、許可/拒否サイトのテーブルが編集モードになっている必要があります。

5. [ブラウザ拡張機能を有効にするようユーザーに通知するを]選択します。

   選択すると、ブラウザ保護拡張機能が見つからない場合はインストールするように、また、ブラウザ保護拡張機能がインストールされているがサポートされているブラウザで無効になっている場合はアクティブ化するようにというリマインダーがユーザーに送信されます。

6. [セーフサーチモードを強制するを]選択します。

   この設定により、サポートされている検索エンジンでSafeSearch厳格モードが強制され、検索結果からアダルトコンテンツや不適切なコンテンツがフィルタリングされます。

   注：この機能が正しく動作するには、ブラウザ拡張機能をインストールして有効にする必要があります。

7. [ブロックされた URL をすべてのセキュリティ イベントに含めるように]設定します。

   選択すると、ブロックされた Web サイトの URL が、セキュリティ イベントビューに表示される関連セキュリティ イベントに含まれます。

   注：ユーザーのウェブアクティビティの監視に関する地域の法律により、この機能の使用が制限される場合があります。この設定を有効にする際は、適用される現地の法律および組織のポリシーに準拠していることを確認してください。

8. [ブロックされた悪意のある URL をすべてのセキュリティ イベントに含めるよう]に設定します。

   選択すると、ブロックされた Web サイトの悪意のある URL が、セキュリティ イベントビューに表示される関連セキュリティ イベントに含められます。

   注：ユーザーのウェブアクティビティの監視に関する地域の法律により、この機能の使用が制限される場合があります。この設定を有効にする際は、適用される現地の法律および組織のポリシーに準拠していることを確認してください。

9. [サンプル送信 URL を]指定します。

   この URL はブロック ページでユーザーに表示され、分析用に URL を送信するための手順が記載されたカスタム ページにユーザーを誘導できます。

   URL にはプロトコルを含める必要があります (例:`https://example.com/SampleSubmission`)。

Windows での評価ベースのブラウジングの使用

レピュテーションベースブラウジングは疑わしい、または悪意のあることがわかっているWebサイトをブロックします

Windows エンドポイントでレピュテーションベースのブラウジングを有効にするには:

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. [Windows用]タブを選択します。
3. 編集するプロファイルを選択します。
   Windows のプロファイルページが開きます。
4. 左側のメニューから、[ブラウジング保護]を選択します。
5. [レピュテーションベースのブラウジングを有効にする]をオンにして、Web サイトをフィルタリングします。
6. [評判に基づくブラウジング]では、以下をオンにできます。
   - [有害と評価されたウェブサイトへのアクセスをブロックする]
   - [疑わしいと評価されたウェブサイトへのアクセスをブロックする]
   - [禁止されていると評価されたウェブサイトへのアクセスをブロックする]
   - [ウェブサイトで見つかったトラッカーをブロックする]
   - [最近作成されたドメインへのアクセスをブロックする]

7. [検索結果のリンクの評判を表示する]を選択すると、検索結果の評判に基づく情報が表示されます。

   注: ブラウザ拡張機能をインストールして有効化する必要があります。

ウェブコンテンツの制御

Webコンテンツ コントロールをオンにすると、コンテンツ カテゴリに基づいてWebサイトをブロックできます。

Webコンテンツ制御を使用すると、違法コンテンツ、ヘイトコンテンツ、ギャンブル、ファイル共有など、事前に定義されたコンテンツカテゴリに基づいてWebサイトへのアクセスを制限できます。これにより、利用規約を遵守し、危険または不適切なWebコンテンツへのアクセスを減らすことができます。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[ブラウジング保護]を選択します。
4. [Webコンテンツ コントロール]の下で、[Webコンテンツ コントロールを有効にする]を選択します。

   選択すると、コンテンツ カテゴリに基づいて Web サイトへのアクセスがブロックされます。

   注:「不明」カテゴリを選択すると、評判がまだ確定していないウェブサイトへのアクセスがブロックされます。これらのウェブサイトは通常、あまり人気がない、または新しく作成された、あまりアクセスされていないウェブサイトです。

コンテンツタイプのフィルタリング

コンテンツ タイプ フィルタリングをオンにして、インターネット メディア タイプまたはファイル名に基づいてダウンロードをブロックするフィルタを構成します。

コンテンツタイプフィルタリングを使用すると、インターネットメディアの種類やファイル拡張子に基づいて、特定の種類のウェブコンテンツをブロックできます。これにより、実行ファイル、スクリプト、その他の高リスクコンテンツなど、潜在的に危険なファイルタイプのダウンロードを防ぐことができます。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[ブラウジング保護]を選択します。
4. [コンテンツ タイプ フィルタリング]の下で、[コンテンツ タイプ フィルタリングを有効にする]を選択します。

   選択すると、[コンテンツ タイプ フィルター]リストで定義されたルールに基づいて Web コンテンツがブロックされます。

5. [コンテンツ タイプ フィルター]でルールを構成します。

   このリストでは、ブロックするコンテンツの種類を定義します。提案されたフィルターをオン/オフにしたり、[コンテンツタイプフィルターの追加]を選択して新しいフィルターを追加したりできます。

   [安全なサイトをフィルタリング」が]無効になっている場合、フィルタリングは、セキュリティ クラウドによって不明または安全でないと判断されたサイトにのみ適用されます。

   - [Active は]フィルタルールを有効または無効にします。無効なルールは無視されます。
   - [安全なサイトをフィルタリング」は]、すべてのウェブサイトにフィルタリングを適用します。無効にすると、不明なウェブサイトまたは安全でないウェブサイトにのみフィルタリングが適用されます。
   - [コンテンツタイプは]、ブロックするインターネットメディアの種類を指定します。ワイルドカード (*、?) がサポートされています。例： `application/*zip*`。

- [ファイル名/拡張子は、]ブロックするファイル名または拡張子をスペース区切りで指定します。ワイルドカードがサポートされています。例：`*.exe *.do? viewcard*.asp.scr`
- [説明には、]管理参照用のフィルタ ルールの説明が保存されます。

ウェブサイトの例外の設定

指定されたドメインへのアクセスを常に許可またはブロックする Web サイトの例外ルールを構成します。

ウェブサイトの例外設定では、レピュテーションに関わらず、常に許可またはブロックするドメインを定義できます。これらのルールは、信頼できるサービスへのアクセスを確保したり、特定のウェブサイトをブロックしたりするために使用できます。

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 コンピューター用] を**]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[ブラウジング保護]を選択します。
4. [**Web サイトの例外を有効にする**]を選択します。

   有効にすると、[許可サイト]と [拒否サイト]のリストが使用され、通常のブラウジング保護の動作が上書きされます。

   ユーザーは、[許可されたサイト]にリストされているサイトには常にアクセスできますが、[拒否されたサイト]にリストされているサイトへのアクセスは常にブロックされます。

5. 明示的に許可されたWebサイトへのアクセスのみを許可する場合は、[許可されたサイト以外はすべてブロック」を]選択します。

   有効にすると、[許可されたサイト]にリストされているサイトを除くすべての Web サイトがブロックされます。

6. より厳格なフィルタリング ルールを適用するには、[リファラーベースの許可を無効にする]を選択します。

   有効にすると、リファラーに基づいてページが許可されなくなります。通常、ホワイトリストに登録されたウェブサイトに埋め込まれたコンテンツが正しく機能するように、承認されたリファラーから読み込まれたページは許可されます。

   注：この設定を有効にすると、一部の Web サイトに埋め込まれたコンテンツやリンクされたリソースが正しく読み込まれなかったり、まったく表示されなかったりする可能性があります。

7. [拒否されたサイトへのアクセスに関するセキュリティ イベントを送信するよう]に構成します。

   有効にすると、ユーザーが [拒否されたサイト]にリストされているサイトにアクセスしようとするたびに、セキュリティ イベントが生成されます。

   無効にすると、サイトへのアクセス試行が拒否されてもイベントは生成されません。

8. [許可サイト]または [拒否サイト]にエントリを追加します。

   これらのリストを使用して、常に許可するドメインまたは常にブロックするドメインを定義します。

   - [アドレスは]ドメイン名を指定します。例： `www.example.com`または `example.com`。ルートドメインを使用すると、ルールはすべてのサブドメインに適用されます。
   - [メモを]使用して、ドメインまたはルールに関する追加情報を保存できます。

接続制御の使用

接続制御を構成して、機密性の高いオンライン セッションを保護し、信頼できないアプリケーションからのネットワーク アクティビティを制限します。

接続制御は、信頼できないアプリケーションからのネットワークアクティビティを制限することで、オンラインバンキングなどの機密性の高いウェブセッションを保護します。この機能を使用すると、機密性の高いウェブサイトへの接続を監視し、追加のセキュリティ制限を適用することで、不正アクセスやデータ漏洩を防止します。

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 コンピューター用] を]選択し、プロファイルを選択します。
   Windows コンピューターのプロファイルが開きます。
3. 左側のメニューから、[ブラウジング保護]を選択します。
4. [許可サイト]または [拒否サイト]にエントリを追加します。

   これらのリストを使用して、常に許可するドメインまたは常にブロックするドメインを定義します。

   - [アドレスは]ドメイン名を指定します。例： `www.example.com`または `example.com`。ルートドメインを使用すると、ルールはすべてのサブドメインに適用されます。
   - [メモを]使用して、ドメインまたはルールに関する追加情報を保存できます。

5. [接続制御]の下で、[接続制御を有効にする]を選択します。

   選択すると、接続制御は、ユーザーがオンライン バンキング サイト (HTTPS のみ) などの機密性の高い Web サイトや、機密情報を扱うその他の定義済みサービスにアクセスしたことを検出します。

6. [信頼できないアプリのアクティブな接続をブロックしないように]構成します。

   この設定は、接続制御が有効になっているときに、信頼されていないアプリケーションからの既存のネットワーク接続をどのように処理するかを制御します。

   - この設定をオンにすると、既存のアクティブな接続は引き続き正常に動作します。
   - この設定をオフにすると、信頼されていないアプリケーションのアクティブなインターネット接続は更新時に機能しなくなります。

   注：信頼できないアプリケーションからの新しい接続は常にブロックされます。

7. 保護されたセッション後にクリップボードの内容を削除するに[は、「完了時にクリップボードをクリア]を選択します。

   選択すると、ユーザーがオンラインバンキングセッションなどの保護されたセッションを終了した後にクリップボードの内容がクリアされます。これにより、機密情報がクリップボードに残るのを防ぐことができます。

8. [コマンドラインおよびスクリプト ツールをブロック]を選択します。

   選択すると、接続制御は、保護されたセッション中にコマンドラインおよびスクリプトツールによって開始されたネットワーク接続をブロックします。

9. [リモート アクセスをブロック]を選択します。

   選択すると、保護されたセッションがアクティブな間、接続制御によってリモート アクセス ツールがブロックされます。

   サポートされるツールには、リモート デスクトップ、TeamViewer、LogMeIn、VNC などのアプリケーションが含まれる場合があります。

10. 追加の保護された Web サイトを定義する場合は、[接続制御サイト]にエントリを追加します。

    サイトをリストに追加すると、そのサイトを機密性の高いサービスとしてマークできます。ユーザーがこれらのサイトにアクセスすると、接続制御によってセッションの強化された保護が有効になります。

4.3.8 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。

ファイアウォールルールのアラートの設定

ファイアウォール ルールのアラートを設定する手順。

注: アラートは、ルールのアクションとして「ブロック」を選択した場合にのみ機能します。

ファイアウォール ルールのアラートを設定するには:

1. WithSecure Elements Security Centerにログインします。
2. [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。
3. [**Windows コンピューターの場合**] タブを選択し、編集するプロファイルを選択します。
4. [ファイアウォール] を選択します。
5. アラートを設定する WithSecure ファイアウォール プロファイルを選択します。
6. 次のことを実行します。
   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) 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として [ブロック]を選択します。
   c) 中央のドロップダウン メニューから、トラフィックの方向として [**In**]または [**Out**]を選択します。
   d) 下部のドロップダウン メニューから、[アラートを送信]を選択します。

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

コンピューターをネットワークから隔離すると、コンピューター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ーは、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、コンピューターが隔離されると、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、コンピューター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、コンピューター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。

4.3.9 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ーに接続すると、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 コンピューターで 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。

4.3.10 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。

WithSecure Elements Security Center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、コンピューター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 Security Center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 Security Center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。

4.3.11 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サーバーを入力します。

   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。

4.3.12 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って引き起こされた可能性のあるファイルやシステム設定の変更を検出した場合、製品は自動的にその変更を元に戻し、検疫に保存します。変更が有効で、ランサムウェアによるものでない場合は、隔離から自動的に戻された変更を復元できます。

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. [Windowsコンピューター用] または [Windowsサーバー用] タブを選択し、変更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] を選択し、次の操作を実行します。
   - [ロールバック] をオンにします。
   - [許可と報告モード] をオフにします。
   - [元に戻したファイルの復元を許可する] をオンにします。

   注：まず、[許可と方奥モードモード] を1週間オンのままにする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、[元に戻したファイルの復元を許可する] 設定をオンにして、隔離からファイルを復元します。

   注：デフォルトでは、許可および報告モードが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、許可および報告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。

ローカルに除外されたパスを削除する

WithSecure Elements Security Center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、[ローカルで除外されたパスを削除]を選択します。
   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. [削除]を選択します。

選択されたローカル除外パスが削除されます。

4.3.13 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。

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ー上で 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ーの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

DataGuardにボールトを追加する方法を説明します。

ボールトとは、そのボールト用に構成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、または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 エクスプローラーを使用してボールト内にサブフォルダを作成する場合は、信頼できるアプリケーションの一覧に`%windir%\explorer.exe`を追加する必要があります。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したい場合は、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たびに、セキュリティ イベントに DataGuard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. 左側のメニューの [**Premium**]の下で、[**DataGuard**]を選択します。
4. [**Vaults**]まで下にスクロールし、[**Add a vault**]を選択します。
5. [ボールトへのパス]フィールドにパスを入力します。
6. [信頼できるアプリケーションの追加を]選択します。
7. [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さらに追加するには、[信頼できるアプリケーションの追加]を選択します。

8. [保存して発行] を選択します。

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。

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。

イベント	説明
アプリケーションの起動とモジュールの読み込み	2 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。

選択した条件	説明
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ついては、[プロファイル] > [アプリケーション制御] に移動し、[アプリケーション制御ルール] の横にあるヘルプアイコンを選択してください。各条件タイプごとの条件値が説明されています。例えば、[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され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。

カスタム侵害指標の提出

カスタムの侵害指標（IOC）を送信することで、ファイルハッシュ、IPアドレス、またはホスト名に基づく検出ルールを作成し、これらが検出された場合にシステムがどのような対応を行うかを定義できます。これにより、WithSecureの検出機能とお客様独自の脅威インテリジェンスを組み合わせることで、よりプロアクティブで柔軟性が高く、協調的なサイバーセキュリティアプローチが可能になります。

IOCは、組織が最新のサイバーセキュリティ基準に準拠し続けるのに役立ちます。組織固有の環境に合わせて、カスタム検知機能と自動レスポンスを作成できます。また、知識共有コミュニティ、脅威インテリジェンス出版物、社内調査など、信頼できる情報源から得られる脅威データを活用することで、よりプロアクティブな防御アプローチを実現できます。

IOC検出ルールの作成

侵害指標（IOC）は、組織が最新のサイバーセキュリティ基準に準拠し続けるのに役立ちます。組織固有の環境に合わせて、カスタム検出機能と自動応答を作成できます。また、知識共有コミュニティ、脅威インテリジェンス出版物、社内調査など、信頼できる情報源から得られる脅威データを活用することで、よりプロアクティブな防御アプローチを実現できます。

セキュリティプラットフォームインターフェースを通じて、カスタムIOCルールを定義および管理できます。プラットフォームは3種類のIOCをサポートしています。

- ファイルハッシュ（SHA1またはSHA256）
- IPアドレス
- DNSホスト名

各IOCタイプごとに、検出を生成するか、脅威をブロックするか、またはその両方のアクションを実行するようにシステムを設定できます。デフォルトでは、検出とブロックの両方が有効になっています。

注: ファイルハッシュベースのルールはWindowsシステムでサポートされており、特定のネットワークプロトコルに依存しません。IPアドレスベースのルールもWindowsでサポートされており、送信TCPトラフィックにのみ適用されます。DNSホスト名については、プラットフォームはWindows上でプレーンDNSクエリをサポートしますが、DNS over HTTPS（DoH）はサポートしません。

プロファイルエディターを使用してカスタムの侵害インジケーター(IOC)を追加するには、次の手順に従います。

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. 編集するプロファイルを選択します。
   プロファイル エディターが開きます。
3. [アプリケーション制御]タブを開きます。
4. 新しい IOC ルールを追加します。
   a) [イベント タイプ]フィールドで、ハッシュベースの IOC の場合は [**IOC - ハッシュ**]を選択し、IP ベースの IOC の場合は [**IOC - IP] を**]選択します。
   b) [条件]フィールドに、選択した IOC タイプに応じて、SHA1 または SHA256 ハッシュ値、または IP アドレスを入力します。
   c) [ルール名]フィールドに、後でルールを簡単に識別して追跡できるカスタム名を入力します。
   d) [ルールの説明]フィールドに、ルールがトリガーされたときに検出コンテキストに表示される簡単な説明を入力します。
   e) IOC の潜在的な影響に基づいて、ルールの適切な [重大度]レベル（[重大]、[高]、[中]）を選択します。
   f) [アクション タイプ]フィールドで、IOCが検出されたときに実行するアクションを選択します([検出の生成]、[ブロック]、または [検出の生成とブロック)]。
5. 変更を保存して公開します。

カスタムIOCがトリガーされると、プラットフォームはBroad Context Detection（BCD）を生成します。これらのBCDは標準的な検出と同様に機能し、メールアラートの送信、ダッシュボードへの表示、インシデントタイムラインへの表示などが可能で、イベントの完全な可視性を提供します。

IOCルールを設定したら、保存して公開し、組織内のすべてのプロファイルに適用できます。これにより、環境全体でカスタム脅威インテリジェンスを一貫して適用できます。

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。

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WithSecure Elements Security Centerで直接認識できます。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指標です。さらに調査して、正当な理由がないかどうかを確認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 アカウントの複数の資格情報を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、監査ログをクリアして痕跡を隠そうとする可能性があります。このようなイベントでは、正当なアクションが原因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

WithSecure Elements Agentで監視し、セキュリティ イベントに送信する Windows システム イベントを選択する方法について説明します。

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. [**Windows**コンピューター用] または [**Windows**サーバー用] タブを選択し、変更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]を選択します。
4. [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。

デバイスドライブの暗号化

Elements Endpoint encryptionデバイス上の暗号化の状態の概要と、それらを管理するためのツールが提供されます。

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 : Elements Endpoint encryption使用してドライブを暗号化するには、Windows 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要素です。有効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です。これらのキーを収集するツールは多数あり

ますが、そのうちの１つを使用することが重要です。Secure WithSecure Elements Endpoint Protection必要に応じて回復キーを収集できます。設定は、[プロファイル]の下の [全般]タブにあります。

注: 回復キーを収集するには、Elements Endpoint Protectionインストールされた Windows デバイスと、「回復パスワードプロテクター」を使用して BitLocker で暗号化されたディスクが必要です。この機能を有効にした後、回復キーが正常に収集され、WithSecure Elements Security Centerでキーが表示されていることを確認することをお勧めします。

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。

4.3.14 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

許可とレポート 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イベントとその詳細は [、[イベント] > [セキュリティ イベント]で確認できます。

Server Share Protection機能を初めて使用する場合、テストの一環としてこのモードをオンにすることをお勧めします。モードをオンにしても保護は行われませんが、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. [Windowsサーバー用] タブを選択し、変更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、[Server Share Protection] を選択します。
4. [許可と報告モード]設定をオンにします。
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

この設定がオンになっていて、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ー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. [Windowsサーバー用] タブを選択し、変更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、[Server Share Protection] を選択します。
4. [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. [Windowsサーバー用] タブを選択し、変更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、[Server Share Protection] を選択します。
4. [除外フォルダー]を選択し、[除外フォルダーの追加]を選択します。
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 `domain_name\user_name`のユーザー名またはユーザー SID (セキュリティ識別子) のいずれかを追加できます。

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。

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サーバー用] タブを選択し、変更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、[Server Share Protection] を選択します。
4. [除外ユーザー]を選択し、[ユーザーの追加]を選択します。
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。

4.3.15 ポータルからElements Agentを再起動する

WithSecure Elements Security Centerを使用すると、システム全体を再起動せずに、選択したデバイス上の [Elements Agent を]再起動できます。

Elements Security Centerから [Elements Agent を]再起動するには:

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. 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]を選択します。

選択したデバイスで [Elements Agent が]再起動します。

4.4 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。

4.4.1 新しいコンピューター プロファイルを作成する

特定のコンピューター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. [セキュリティ構成] > [Mac用] > [プロファイル]で、  既存のプロファイルの横にある をクリックし、[プロファイルの複製]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。

4.4.2 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ー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。

4.4.3 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。

[早期アクセス]が有効になっているプロファイルをデバイスに割り当てると、デバイスは、一般提供用に公開され、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け取ります。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. [クライアント ソフトウェアへの早期アクセス]設定をオンにします。
6. [保存して発行] を選択します。

4.4.4 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。

WithSecure Elements Security Centerには、HTTPプロキシ接続を設定するための次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)。

4.4.5 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。

4.4.6 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。コンピューター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。

4.4.7 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。

4.4.8 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。

4.4.9 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ー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コンピューター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。

4.4.10 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 Security Center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ー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ー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 サーバー)、ScreenSharing (vnc サーバー)、Apache、Nginx などのサーバー アプリケーション。

方向	説明
送信	コンピューター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。

4.5 F-Secure Elements EPP for Linux でのプロファイルの管理

このセクションでは WithSecure Elements EPP for Linux ソフトウェアでプロファイルを管理する方法について説明します。

4.5.1 Linux用の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ー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. [セキュリティ構成] > [Linux用] > [プロファイル]で、  既存のプロファイルの横にある をクリックし、[プロファイルの複製]を選択します。
   Linux の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. 設定に必要な変更を加え、[プロファイルの保存]を選択します。
   新しいプロファイルが作成されます。

4.5.2 Linuxのプロキシ設定を構成する

Linux Protection の更新と Security Cloud (ORSP) 接続のプロキシ設定を構成します。

更新と安全な接続を有効にするには、次の手順で Linux システムのプロキシ設定を構成します。

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. [Linux 用]タブを選択し、プロファイルを選択します。
   Linux のプロファイルページが開きます。
3. 左側のメニューから、[全般]を選択します。
4. プロキシ設定を定義する

   Linux Protection の更新 (製品およびマルウェア定義) および Security Cloud (ORSP) のプロキシ設定を構成します。

   a) 更新と Security Cloud 接続にプロキシを使用するには、[HTTP プロキシを使用する]をオンにします。
   b) HTTP プロキシ [ホスト フィールドに HTTP プロキシ]ホスト アドレスを入力します。

      受け入れられる形式: `domain.com`、`127.0.0.1`、`localhost`。

c) HTTP プロキシ [ポート フィールドに **HTTP** プロキシ]ポート番号を入力します。
有効な範囲: `0` ~ `65535`。
d) [**HTTP** プロキシ ユーザー名]フィールドにプロキシ認証のユーザー名を入力します。
e) [**HTTP** プロキシ パスワード]フィールドにプロキシ認証のパスワードを入力します。

5. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.3 WithSecure Elementsコネクタの使用

WithSecure Elements Connector の使用方法の説明。

WithSecure Elements Connector 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. [**Linux**向け]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。
Linux の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. [**WithSecure Elements Connector**]で。

受け入れられる形式: `domain.com`、`127.0.0.1`、`localhost`。

複数のコネクタをセミコロンで区切って指定できます。例: `http://myconnector.local; http://myproxy2.com:8080`

複数のコネクタが指定されている場合、クライアントは最初のコネクタを使用し、最初のコネクタが使用できなくなった場合は次のコネクタに切り替えます。

6. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.4 自動更新の設定

Linux 上の WithSecure 製品とマルウェア定義の自動更新を構成します。

これらの設定は、管理対象ソフトウェアがWithSecure製品およびマルウェア定義の更新をどのように処理するかを制御します。Linuxシステムの自動更新を有効にして設定するには、以下の手順に従ってください。

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. [**Linux** 用]タブを選択し、編集するプロファイルを選択します。
Linux のプロファイルページが開きます。
3. 左側のメニューから、[全般]を選択します。
4. [自動更新を有効にするを]オンにすると、更新が自動的にダウンロードされてインストールされます。
5. [更新プログラムの適用]で、更新プログラムをいつインストールするかを選択します。
   - [到着時]: 更新プログラムをダウンロードしたらすぐにインストールします。
   - [一度] : 特定の日時にアップデートをインストールします。インストールする日付と時刻の両方を設定します。
   - [スケジュール] : 定期的に更新をインストールします。インストールする曜日と時刻を指定します。
6. 更新が適用されたときに管理者に通知するには、[更新後にアラートを送信する」を]オンにします。
7. [**HTTPS** を使用して更新をダウンロードする」を]オンにして、HTTPS経由で更新のダウンロードを安全に行います。

注 : HTTPSを使用するとプライバシーが強化され、特定の認証のコンプライアンス要件を満たすことができます。ただし、プロキシサーバーではHTTPSトラフィックをキャッシュできないため、プロキシを使用する場合はネットワークトラフィックが増加する可能性があります。

8. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.5 Linuxの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。

[早期アクセス]がオンになっているプロファイルをデバイスに割り当てると、デバイスは、一般公開される前に最新の製品バージョンを受信し、サイレントアップグレード用の標準チャネルを通じてリリースされます。

アップグレード プロセスはサイレントのままで、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. [Linux向け]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。
   Linux の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. [クライアント ソフトウェアへの早期アクセス]設定をオンにします。
6. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.6 Linux への EDR センサーの統合

Linux エンドポイントに EDR センサーを統合するための設定を構成します。

WithSecure Elements Connector を使用して EDR センサーを有効にして構成するには、次の手順に従います。

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. [Linux向け]タブを選択します。
3. 編集するプロフィールを選択します。
   Linux の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. [EDR センサーを]オンにして、EDR サブスクリプションを持つデバイスでエンドポイントの検出と応答を有効にします。

   注: この設定はオンのままにすることを強くお勧めします。無効にすると、EDRはエンドポイントへの攻撃を検知または警告しません。

6. EDR で高度な応答モジュールを有効にする場合は、[高度な応答]をオンにします。

   高度なレスポンス機能を使用すると、機密データを含む可能性のある詳細なシステム情報にアクセスできます。この機能を有効にする前に、適用される労働者のプライバシーに関する法律および関連する顧客要件または契約要件に準拠していることを確認してください。

   注: この機能を使用することにより、お客様は法的に許可されており、適用法に基づいて必要なすべての同意を得ていることを確認します。

7. 変更を適用するには、[プロファイルを保存]を選択します。

4.5.7 望ましくない変更から保護する

改ざん防止機能は、エンド ユーザーまたはサードパーティ アプリケーションによる不正な変更から、WithSecure のサービス、プロセス、ファイル、およびレジストリ エントリを保護します。

改ざん防止機能を使用するには:

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. [Linux向け]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。
   Linux の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. [ユーザーがすべてのセキュリティ機能をオフにできるようにする]がオフになっていることを確認します。

   この設定をオンにすると、ユーザーはWithSecureのすべてのセキュリティ機能をオフにすることができます。

   注：ユーザーがいつでも保護を無効にできないように、この設定をオフのままにしておくことを強くお勧めします。

6. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.8 Linuxのリアルタイムスキャンの設定

ユーザーがファイルやフォルダーを開いたり変更したりするたびに、リアルタイムのマルウェアスキャンを実行します。

Linux エンドポイントのリアルタイム スキャンを構成するには、次の手順に従います。

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. [Linux 用]タブを選択し、編集するプロファイルを選択します。
   Linux の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. [リアルタイムスキャン]をオンにすると、アクセスしたファイルに対して継続的なマルウェアスキャンが有効になります。

   リアルタイム スキャンにより、スキャン構成で定義されているすべてのファイルがアクセス時にチェックされます。

   注：この設定を有効にしておくことを強く推奨します。

5. ファイルの評判をオンラインで確認するには、[Use Security Cloud (ORSP)]がオンになっていることを確認してください。

   Security Cloud (ORSP) は、WithSecure Security Cloud に対して未知のファイルを検証し、保護を強化します。

   注：この設定を有効にしておくことを強く推奨します。

6. リアルタイムスキャン中にスキャンするファイルを構成します。
   a) 完全な絶対パスを使用して [、スキャンするファイルとフォルダーを]指定します。
      ディレクトリにはすべてのサブディレクトリが再帰的に含まれます。

      注：デフォルトではこのフィールドは空で、何もスキャンされないことを意味します。

   b) 必要に応じて、[スキャンから除外するファイルとフォルダー]を指定します。
      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ーにのみこれを使用します。

      注意：パスを除外する際は注意してください。例えば、ルートディレクトリ (/) を除外すると、すべての保護が解除されます。

   c) スキャンをバイパスする必要があるプロセスのパスを [信頼できるアプリケーション]に追加します。
      信頼できるアプリケーションによって開かれたファイルはスキャンされません。

      注意：信頼できるアプリケーションのパスを追加する際は注意してください。例えば、ルートディレクトリ (/) を追加すると、すべてのアプリケーションがすべてのセキュリティ対策から除外されます。

d) スキャンを実行可能ファイルのみに制限する場合は、「実行可能ファイル [のみをスキャン]をオンにします。
e) [潜在的に不要なアプリケーションのスキャン」を]オンにすると、潜在的に不要なアプリケーションを検出できます。これらのプログラムは、マルウェアとして分類されないものの、システムのパフォーマンスやセキュリティに悪影響を与える可能性があります。

7. リアルタイム スキャン中にアーカイブを処理する方法を設定します。
   a) 圧縮パッケージ内のファイルをチェックするには、[アーカイブ内のスキャン]をオンにします。
   b) [暗号化されたアーカイブをブロックするには、「暗号化されたアーカイブを安全でないものとして扱う]をオンにします。
   c) スキャンの最大深度を定義するには、[アーカイブのスキャンをネストレベルまで]を設定します。
   d) 深くネストされたアーカイブをブロックするには [、「最大ネスト レベルを超えるアーカイブを安全でないものとして扱う]をオンにします。
8. リアルタイムスキャン検出のアクションを選択します。
   a) マルウェアに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

   b) 望ましくない可能性のあるアプリケーションに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

   c) 疑わしいファイルに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

9. すべての変更を適用するには、[プロファイルの保存]を選択します。

4.5.9 Linuxの手動スキャンの設定

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. [Linux 用]タブを選択し、プロファイルを選択します。
   Linux のプロファイルページが開きます。
3. 左側のメニューから [手動スキャン]を選択します。
4. 手動スキャンから常に除外するファイルを選択します。
   a) 手動スキャンから除外するパスを選択するには、[パスの追加]を選択します。
      除外するファイルまたはフォルダの絶対パスを入力してください。指定したディレクトリ内のすべてのサブフォルダも、すべてのユーザーに対して除外されます。

      注意 : パスを除外する際は注意してください。例えば、ルートディレクトリ (/) を除外すると、すべてのファイルがすべての手動スキャンから除外されます。

   b) [潜在的に不要なアプリケーションのスキャン」を]オンにすると、潜在的に不要なアプリケーションを検出できます。これらのプログラムは、マルウェアとして分類されないものの、システムのパフォーマンスやセキュリティに悪影響を与える可能性があります。
5. 手動スキャン中にアーカイブを処理する方法を構成します。
   a) 圧縮パッケージ内のファイルをチェックするには、[アーカイブ内のスキャン]をオンにします。
   b) [暗号化されたアーカイブをブロックするには、「暗号化されたアーカイブを安全でないものとして扱う]をオンにします。
   c) スキャンの最大深度を定義するには、[アーカイブのスキャンをネストレベルまで]を設定します。
   d) 深くネストされたアーカイブをブロックするには [、「最大ネスト レベルを超えるアーカイブを安全でないものとして扱う]をオンにします。

6. 手動スキャン検出のアクションを選択します。
   a) マルウェアに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

   b) 望ましくない可能性のあるアプリケーションに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

   c) 疑わしいファイルに対するアクションを選択します:[何もしない]、[名前を変更する]、または [削除する]。

      注 : 選択したアクションに関係なくアクセスはブロックされます。

7. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.10 Linuxのスキャンのスケジュール設定

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では、手動スキャンと同じ構成が使用されます。

スキャンをスケジュールするには:

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. [Linux 用]タブを選択し、プロファイルを選択します。
   Linux のプロファイルページが開きます。
3. [手動スキャン]を選択します。
4. [スケジュールされたスキャン]で、スキャンを実行する日を選択します。
5. [時刻]で開始時刻を設定します。

   24時間形式で時刻を入力してください: `HH:mm (00:00 - 23:59)`

6. 変更を適用するには、[プロファイルの保存]を選択します。

4.5.11 Linuxの整合性チェックの設定

整合性チェックは、信頼できるベースラインに対してファイルを検証することで、システムを不正な変更から保護します。

整合性チェックは既知の正常な構成に依存します。システムが信頼できる状態にあると確信できる場合にのみ、整合性チェックを有効にしてください。整合性チェックでは、保護するシステムファイルのベースラインを作成します。このベースライン外にある変更されたファイルは、すべてのユーザーに対してブロックされます。

整合性チェックを構成するには:

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. [Linux 用]タブを選択し、プロファイルを選択します。
   Linux のプロファイルページが開きます。
3. 左側のメニューから、[整合性チェッカー]を選択します。
4. ファイルの整合性の検証を有効にするには、[ファイルの整合性をチェックする]をオンにします。
5. (オプション) [apt パッケージ マネージャーとの統合を]オンにします。

   apt パッケージマネージャーとの統合を有効にすると、apt パッケージのインストール、更新、または削除中の整合性チェックが一時的に無効になります。変更後は、ベースラインが自動的に更新されます。

6. (オプション) [DNF パッケージ マネージャーとの統合]をオンにします。

DNFパッケージマネージャーとの統合を有効にすると、DNFパッケージのインストール、更新、または削除中の整合性チェックが一時的に無効になります。変更後は、ベースラインが自動的に更新されます。

7. 整合性ルールを構成する
   特定のファイルまたはディレクトリのベースラインを作成するためのルールを追加します。
   - 指定されたディレクトリ内のファイルに対してのみ整合性が検証されます。
   - 新しいファイルを追加してもベースラインは壊れず、ベースラインを更新するまで新しいファイルは無視されます。
   - プロファイルを無効にして再度有効にすると、ベースラインが再生成されます。

   a) 整合性チェックに含める [パス]を追加します。
   b) [除外]では、選択したパスの整合性チェックから除外するファイル名パターンを指定します。
   c) [ファイルの書き込み]権限を設定します。[許可]または [拒否を]選択します。

      [拒否」は]ファイルへの書き込みを禁止します。

   d) [ファイルの読み取り]権限を設定します。[許可]または [拒否を]選択します。

      [拒否」は]改ざんされたファイルからの読み取りを防止します。

   e) 整合性ベースラインに含めるファイル属性を構成します。

      [ファイルの読み取り]が [**Deny**]に設定されている場合、次のいずれかの属性が変更されると読み取りがブロックされます。

      - [アクセス モード]: アクセス モードが変更された場合に読み取りを防止します。
      - [所有者]: ファイルの所有者が変更された場合に読み取りを防止します。
      - [グループ]: グループが変更された場合に読み取りを防止します。
      - [サイズ]: ファイル サイズが変更された場合に読み取りを防止します。
      - [変更時刻]: 変更タイムスタンプが変更された場合に読み取りを防止します。

8. 変更を適用するには、[プロファイルの保存]を選択します。

4.6 モバイルデバイスプロファイルの管理

WithSecure Elements Security Centerでモバイルデバイスプロファイルを管理する方法に関する情報。

4.6.1 新しいモバイルデバイスのプロファイルを作成する

特定のモバイルデバイス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 Security Centerにログインします。
2. [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。
3. [モバイル向け] タブを選択します。
4. 既存のプロファイルの横にある ··· を選択し、[プロファイルを複製] を選択します。
   [モバイル用プロファイル] ページが開きます。
5. 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。
6. 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。

4.6.2 ネットワークゲートウェイをオンにする

ネットワーク ゲートウェイは、インターネット トラフィックの脅威をチェックし、悪意のあるリクエストをブロックすることで、モバイル アプリを安全に保ちます。

ネットワーク ゲートウェイをオンにするには:

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. [モバイル用]タブを選択し、編集するプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
3. [ネットワーク保護]で、[ネットワーク ゲートウェイ]をオンにします。

   注 : 設定の横にあるロックアイコンを選択して、設定をロックまたはロック解除できます。設定がロックされると、ユーザが設定を変更できなくなります。

4. [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。

4.6.3 ブラウザプラグインのアクティベーションリマインダーの送信

ブラウジング保護プラグインをインストールまたは有効化するためのリマインダーをユーザーに送信することを選択できます。

注 : これはiOSデバイスにのみ適用されます。

この設定がオンの場合、ブラウザ保護プラグインがない場合はインストールするように、また、インストールされているが有効になっていない場合はサポートされているブラウザで有効にするようにユーザーに通知されます。

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
4. 左側のペインから、[ネットワーク保護] を選択します。
5. [ブラウザプラグインを有効にするようユーザーに通知するを]オンにします。
6. [保存して発行] を選択します。
   変更が保存され、選択したプロファイルに公開されます。

4.6.4 評判に基づくブラウジングを有効にする

レピュテーションベースブラウジングは疑わしい、または悪意のあることがわかっているWebサイトをブロックします

評価ベースのブラウジングを有効にするには:

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. [ネットワーク保護]で、[評価ベースのブラウジング]をオンにします。
5. [評判に基づくブラウジング]では、以下をオンにできます。

   - [有害と評価されたウェブサイトへのアクセスをブロックする]
   - [疑わしいと評価されたウェブサイトへのアクセスをブロックする]
   - [禁止されていると評価されたウェブサイトへのアクセスをブロックする]
   - [ウェブサイトで見つかったトラッカーをブロックする]
   - [最近作成されたドメインへのアクセスをブロックする]

   注: 設定の横にあるロックアイコンを選択して、設定をロックまたはロック解除します。設定がロックされると、ユーザが設定を変更できなくなります。

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。

4.6.5 ブロックするWebコンテンツを選択する

ブロックするWebコンテンツの種類を選択できます。

Webコンテンツ コントロールは、コンテンツに基づいてWebサイトをブロックします。

注 : [不明] カテゴリをオンにすると、評判が不明なWebサイトへのアクセスがブロックされます。

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. 左側のメニューから [ネットワーク保護] を選択し、[Webコンテンツコントロール] まで下にスクロールします。
5. [Webコンテンツ制御] を有効にします。
6. [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覧が開きます。
7. [許可されていない] 列で、モバイルデバイスに対してブロックするカテゴリをオンにします。
8. [アラート] 列で、セキュリティイベントを送信するカテゴリをオンにします。

   注 : [許可されたサイト以外のすべてをブロックする] をオンにすると、[Webコンテンツコントロール] テーブルの選択が上書きされます。

9. [保存して発行] を選択します。

4.6.6 ウェブサイトの許可とブロック

許可された Web サイトと拒否された Web サイトのリストに Web サイトを追加できます。

ウェブサイトを許可またはブロックするには:

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. [モバイル向け] タブを選択します。
3. 目的のプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. 左側のメニューから [ネットワーク保護] を選択し、[Webサイトの例外] まで下にスクロールします。
5. [Web サイトの例外]で、次の操作を行います。
   a) ウェブサイトを許可するには、[許可されたサイト]で[サイトの追加]を選択し、[アドレス]フィールドにウェブサイトの URL を入力します。
   b) ウェブサイトをブロックするには、[拒否されたサイト]で [サイトの追加]を選択し、[アドレス] フィールドにウェブサイトの URL を入力します。

   注 : 「メモ」フィールドに説明を入力できます。

4.6.7 セキュリティイベントでブロックされたウェブサイトのURLを表示する

セキュリティ イベントにブロックされた URL に関する詳細情報を含める場合は、この設定をオンにできます。

注 : この設定をオフにすると、セキュリティ イベントには悪意のある URL のみが表示されます。

重要 : ユーザーの Web アクティビティの監視を規定する現地の法律により、この機能を有効にすることが制限される場合があります。この機能と現地の法律の関係を完全に理解し、それに従うことはお客様の責任となります。

ブロックされた URL に関する情報を含めるには:

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
4. [ネットワーク保護]の下で、下にスクロールして[ブロックされたURLをすべてのセキュリティイベントに含める]をオンにします。

ブロックされたURLに関する詳細情報は、セキュリティ イベントに含まれます。

4.6.8 セキュリティイベントでブロックされた悪意のあるウェブサイトのURLを表示する

ブロックされた悪意のあるURLに関する詳細情報をセキュリティ イベントに含める場合は、この設定をオンにできます。

注: この設定をオフにすると、セキュリティ イベントにはブロックされたURLのみが表示されます。

重要: ユーザーのWebアクティビティの監視を規定する現地の法律により、この機能を有効にすることが制限される場合があります。この機能と現地の法律の関係を完全に理解し、それに従うことはお客様の責任となります。

ブロックされた悪意のあるURLに関する情報を含めるには:

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
4. [ネットワーク保護]の下で、下にスクロールして[ブロックされた悪意のあるURLをすべてのセキュリティ イベントに含める]をオンにします。

ブロックされた悪意のあるURLに関する詳細情報は、セキュリティ イベントに含まれます。

4.6.9 アプリの例外を追加する

ネットワークゲートウェイの保護をバイパスして、インターネットに直接接続する信頼できるアプリケーションとしてアプリを追加できます。

注: これはAndroidデバイスにのみ適用されます。

アプリの例外を追加するには

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. [モバイル向け] タブを選択します。
3. 目的のプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. 左側のメニューから、[ネットワーク保護] を選択します。
5. [アプリの例外] で、[アプリケーションの追加] 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) [説明] 列にアプリ名を入力します。
   c) [アプリ名（ID）] 列に、Google Playストアに表示されるアプリケーションIDを入力します。
6. [保存して発行] を選択します。

4.6.10 マルウェア対策を有効にする

オンにすると、マルウェア対策によってファイルとアプリケーションがスキャンされます。

注: これはAndroidデバイスにのみ適用されます。

マルウェア対策を有効にするには:

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. [モバイル向け] タブを選択します。

3. 編集するプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. 左側のペインから、[マルウェア保護] を選択します。
5. [マルウェア対策を]オンにします。

   注: 設定の横にあるロックアイコンを選択して、設定をロックまたはロック解除します。設定がロックされると、ユーザが設定を変更できなくなります。

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。

4.6.11 従量制スキャンをオンにする

従量制ネットワーク接続では、使用できるデータ量に制限があります。

従量制接続でのスキャンを許可できます。制限を超えると追加料金が発生する可能性があります。

注 : これはAndroidデバイスにのみ適用されます。

従量制スキャンをオンにするには:

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
4. 左側のペインから、[マルウェア保護] を選択します。
5. [従量制スキャンを]オンにします。
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。

4.6.12 感染症に対する行動の選択

感染したオブジェクトに対するアクションを選択できます。

注 : これはAndroidデバイスにのみ適用されます。

アクションを選択するには:

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。
   [モバイル用プロファイル] ページが開きます。
4. 左側のメニューから、[マルウェア保護] を選択します。
5. [感染時のアクション]ドロップダウンメニューから、感染したオブジェクトに対して必要なアクションを選択します。
   - 削除 - このオプションは、感染したオブジェクトをデバイスから自動的に削除します
   - スキャン後に確認する - 感染したオブジェクトをデバイスから手動で削除する必要があります

4.6.13 スケジュール スキャン

デバイスの安全を確保するために、マルウェアやその他の有害なアプリケーションを定期的に自動的にスキャンして削除するようにデバイスを設定します。

注 : これはAndroidデバイスにのみ適用されます。

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. [モバイル向け] タブを選択します。
3. 編集するプロファイルを選択します。

[モバイル用プロファイル] ページが開きます。

4. 左側のメニューから[マルウェア対策]を選択し、[スケジュールされたスキャン]まで下にスクロールします。
5. [スケジュール スキャン] を有効にします。
6. [スケジュールされたスキャン]の横にある矢印を選択します。
スキャン頻度のドロップダウン メニューが表示されます。
7. ドロップダウン メニューから、デバイスを自動的にスキャンする頻度を選択します。

オプション	説明
日単位	毎日デバイスをスキャンしてください。
[毎週]	選択した曜日にデバイスをスキャンします。リストから曜日を選択します。
4週間ごとに	選択した平日に4週間間隔でデバイスをスキャンします。リストから曜日を選択します。スキャンは、選択した曜日の次の発生時に開始されます。
[月次]	毎月、選択した平日にデバイスをスキャンします。リストから曜日を選択します。スキャンは、選択した曜日の次の発生時に開始されます。

8. [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。

第
5
章

セキュリティを監視する

トピック：

WithSecure Elements Security Centerを通じて保護しているコンピューター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サブスクリプションキーと有効期限
- 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、Elements Security Center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：Elements Security Centerを通じてデバイスを隔離することもできます。

- 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 Security Centerを使用して、保護しているコンピューター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Elements Security Center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 Security Center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 Security Center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
- UPN
- IPアドレス
- サブスクリプションキー

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. [モバイル デバイス]タブを選択します。

   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]フィールドに検索文字列を入力します。
   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ー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、[コンピューター]、[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。
   コンピューターの場合、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 イベントページを使用して、システムで検出されたすべてのセキュリティ イベントを確認し、適切なアクションを実行します。

セキュリティ イベントを表示するには:

1. スコープ セレクターを使用して、セキュリティ イベントを表示する会社を選択します。
2. セキュリティ イベントページを開きます。

   サイドバーの [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」ページには、次の情報が表示されます。

   - [時間]- セキュリティ イベントが検出されたタイムスタンプ。
   - [重大度]- イベントの重大度 (低、中、高) を示します。
   - [ソース]- イベントの発生源。
   - [デバイス]- イベントが検出されたデバイスの名前または識別子。
   - [説明]- イベントの概要。
   - [確認済み]- イベントがレビューされたかどうかを示します。

3. イベントの詳細を表示:

   選択してください イベントの横にあるアイコンをクリックすると 詳細ビューが開き、次の内容が表示されます。

   - [インシデント ID] - セキュリティ イベントの一意の識別子。
   - [リスク]- 評価された脅威レベル。
   - [解決]- イベントを解決するために実行されたアクション。
   - [フィンガープリント]- 検出されたファイルまたは脅威の一意のハッシュ。
   - [初期検出タイムスタンプ]- 検出時刻。
   - [ユーザー名]- イベントが発生したユーザー アカウント。
   - [クライアントタイムスタンプ]- クライアントデバイスによって記録された時刻。
   - [トランザクション ID] - イベント処理の識別子。
   - [デバイス UUID] - デバイスの一意の識別子。

4. イベントに対してアクションを実行します。

   イベントの横にある [メニュー]を開いて、次のいずれかのアクションを選択します。

   - [確認]– イベントを確認済みとしてマークします。
   - [すべてのターゲット イベントを表示]- 同じターゲットに関連するすべてのイベントを表示します。
   - [類似イベントを表示]- 類似した特性を持つイベントを表示します。

- [隔離から削除]- 隔離されたファイルを完全に削除します。
- [元の場所に復元]- 隔離されたファイルを元の場所に戻します。
- [誤検知の可能性を報告する]-将来の脅威検出の精度を向上させるために、誤っている可能性がある検出について WithSecure に通知します。
- [フルパスでファイルを除外する]-フルパスに基づいてファイルが今後検出されるのを防ぎます。
- [ハッシュによってファイルを除外する]-固有のハッシュ値に基づいて、ファイルが今後検出されるのを防ぎます。

5.2.1 セキュリティイベントをフィルタする

セキュリティ イベントページに表示されるセキュリティ イベントをフィルターできます。

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、[デバイス タイプを]選択します。
3. 値の選択ドロップダウンメニューから、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
   - URL
4. [値の選択]ドロップダウン メニューから、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. [適用]を選択します。
   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、まだ WithSecureによって管理されていない、会社の Active Directory 内のコンピューターまたはサーバーです。保護されていないデバイスは、新しいデバイスか、WithSecure Elements Security Centerから完全に削除されたデバイスです。

スキャンが開始されると、Elements Security Center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、デバイスページにリストされている WithSecure管理デバイスです。スキャン操作では、Elements Security Center常に最近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. [保護されていないデバイス]タブを選択します。

3. [スキャンの開始を]選択します。
   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 Elements Security Centerに追加するには、WithSecure Elements Agent手動でインストールする必要があります。
4. WithSecure Elements Agentで保護されていないデバイスでも信頼できる場合は、信頼できるデバイスとしてマークすることができます。これを行うには、 ··· デバイスの行で、[信頼済みとしてマーク]を選択します。
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 ··· デバイスの行で、[コメント]を選択します。
   b) コメントを入力し、[保存]を選択します。

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 : ネットワークの隔離は、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、ネットワーク隔離 > ネットワークから隔離を選択します。
   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。WithSecure Elements Security Center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WithSecure Elements Security Center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Elements Security Center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. Elements Security Centerから削除する1つまたは複数のデバイスを選択します。
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Elements Security Center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。

第
6
章

警告と報告

トピック：

レポートセクションでは 、WithSecure Elements Security Centerアカウントに登録されているコンピューターとモバイル デバイスのセキュリティ状態を評価するのに役立つメトリックを追跡します。

[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。

- [マイレポート] タブでは、ウィジェットを追加して、EDR Broad Context Detectionレポートなどの独自のレポートを作成できます。
- 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 Responseレポートを構成する
- 事前設定されたシステムビューのダッシュボードには、デバイス、ソフトウェアの更新、セキュリティイベントに関する情報が表示されます。
- 脆弱性レポートを表示する
- 脆弱性通知を表示する

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。

- [コンピューターの保護ステータス] - 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ー、重要でない問題があるコンピューター、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ーの数を示します。
- 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 - コンピューター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ーと構成されていないコンピューターの数

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 CSVレポートのエクスポート

コンピューター、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ー 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ー 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。
   - コンピューター 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 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ー] - 感染をブロックした上位1コンピューターの名前、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ーの名前。
- [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 カスタマイズされたセキュリティ警告レポートの作成

電子メール通知およびレポート機能を使用すると、カスタマイズされたセキュリティ イベント アラート レポートを作成し、選択した受信者に電子メールで送信できます。

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 レポートを作成するには:

1. まず、「セキュリティイベント」ページでカスタムビューを作成する必要があります。ここで、メールレポートに追加するセキュリティイベントを選択します。カスタムビューを作成するには、以下の手順に従います。
   a) [イベント] で [セキュリティイベント] を選択します。
   b) フィルターを適用して、電子メール レポートを作成するセキュリティ イベントを指定します。
   c) 右上隅にある [表示] ドロップダウン メニューを開きます。
   d) [名前を付けて保存]を選択し、カスタム ビューの名前を入力します。
   e) [保存]を選択します。カスタム ビューが [マイ ビュー]の下に表示されます。
2. 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します。
   a) サイドバーから [レポート] を選択します。

b) [レポート]ページで、[電子メール通知とレポート]タブを選択します。
c) [電子メールレポートの追加]を選択します。
新しい電子メールレポートの追加ペインが開きます。
d) レポートの名前を入力します。
e) データ ソースドロップダウン メニューから、[セキュリティ イベント]を選択します。
f) [テンプレート]ドロップダウン メニューから、[セキュリティ イベント]ページで以前に作成したテンプレートを選択します。
g) レポートに使用する言語を選択します。
h) [スケジュール]では、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 分ごとに送信されることを意味します。

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。

i) [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。このオプションをオフにすると、イベントがない場合でもレポートを受信します。
j) [受信者]ボックスに、選択した受信者の電子メール 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。

k) [保存] を選択します。

6.4 監査ログ

[監査ログ] ページでは、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、ターゲット、およびトランザクションIDが表示されます。

次の基準でイベントをフィルタリングできます。

- アクション
- 管理者
- デバイスUUID
- 組織
- プロファイル名
- タイムスタンプ
- トランザクションID

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
7
章

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ー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ー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。

注：WithSecure Software Updaterに含まれているベンダーのリストは、こちらで確認できます。

WithSecure Elements Security Center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ー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ー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 Security Center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 : ソフトウェアのアップデートは、*重要度が高い*、*中程度*、*低い*、*分類されていない*、*セキュリティ関連ではない*、の *カテゴリ*に分類されます。

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ー (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

WithSecure Elements Security Centerを設定することで、ネットワーク上のコンピュータにソフトウェアのセキュリティ更新プログラムを自動的にインストールできます。

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。

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します。
   - 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

WithSecure Elements Security Centerを使用すると、選択したデバイスをスキャンして、適用されていないソフトウェアアップデートを検出できます。

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Elements Security Center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

Software Updater を設定して、WithSecure Elements Connectorを通じて更新を受け取ることができます。

[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. [Use WithSecure Elements Connector] 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。
   - 常に - 常に WithSecure Elements Connector使用する
   - 可能であれば、WithSecure Elements Connector使用してください。
   - 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。

第 8 章

WithSecure Luminenの使用

トピック：

WithSecure Luminenは、サイバーセキュリティタスクをより管理しやすく、効率的にするように設計されています。高度なAIテクノロジーを活用することで、サイバー脅威から組織をより効果的に保護し、より安全なデジタル環境を確保します。

Luminenは、前処理された構造化データを利用してAIとLLMテクノロジーを活用し、不正確な推奨事項のリスクを大幅に最小限に抑えます。レポートは理解しやすく、WithSecure Elements Cloudにシームレスに統合されています。Luminenは、サイバーセキュリティの管理をより簡単かつ効果的にします。

Luminenは膨大な量のデータを分析して、正確で実用的な推奨事項を提供します。これにより、データの精査に費やす時間が短縮され、最も重要な問題への対応に多くの時間を費やすことができます。たとえば、未処理のインシデントを特定し、それを軽減するための具体的なアクションを提案できます。

Luminenはセキュリティ イベントの調査を支援し、脅威の理解と対応を容易にします。Luminenは、セキュリティ イベントのより広範な影響を理解するのに役立つ豊富なコンテキスト情報を提供します。このコンテキストにより、情報に基づいた意思決定を迅速に行うことができ、全体的な対応時間と有効性が向上します。

Luminenは、正確で実用的な推奨事項を提供し、セキュリティ インシデントの詳細な分析を提供します。Luminenを使用すると、サイバー脅威に対する組織の防御をより効果的に強化できます。

使い方

WithSecure Luminenは、生成AIと大規模言語モデル(LLM)を使用して自然言語でローカライズされた支援を提供するElementsのユーザー エクスペリエンス レイヤーです。

ヨーロッパの大手サイバーセキュリティ企業であるWithSecureは、厳格なプライバシー基準に従っています。Luminenは、継続的に改善されている実績のあるAIモデルを使用しています。各AIモデルは単一の組織専用であるため、組織間でデータが漏洩するリスクはありません。

LuminenはAmazon AWS Bedrockが提供するLLMを使用しており、分析されたデータはAWS内に留まります。すべてのデータはヨーロッパで処理され、将来の基礎モデルのトレーニングには使用されません。WithSecureによる非基礎モデルのトレーニングでは、匿名化されたデータのみが使用されます。

データ漏洩やAIエラーなどのリスクを最小限に抑えるために、Luminenは Retrieval-Augmented Generation (RAG) と呼ばれる手法を使用しています。この手法では、セキュリティイベント、XDR/BCDインシデント、関連する脅威インテリジェンスなどの特定のプロンプトとコンテキスト データをAIに提供します。このデータには、ユーザー名、ホスト名、電子メール アドレスが含まれる場合があり

ます。ただし、Luminenは、セキュリティイベントまたはXDR/BCDインシデントにすでに存在するデータ以外の追加データにはアクセスできません。

8.1 セキュリティ意識向上アシスタント

Security Awareness Assistant は WithSecure Luminen の一部です。過去 7 日間の組織からの調査結果の概要を提供します。

Security Awareness Assistant は、過去 1 週間のセキュリティ活動の簡潔な概要を作成し、組織全体のセキュリティ状況を迅速に把握します。Luminenはこれらの概要をわかりやすい言葉で記述するため、検出されたセキュリティ イベントの種類や必要な即時のアクションを理解しやすくなります。レポートでは、重要度に基づいて検出結果に優先順位が付けられるため、最も緊急の問題に最初に集中することができます。

選択  右上隅にあります。
セキュリティ イベントの概要が開きます。

注 : このレポートは生成 AI を使用して生成されるため、慎重に扱う必要があります。すべての脅威に完全に対処するには、さらに調査と専門家の相談が必要になる場合があります。

8.2 調査アシスタント

Investigation Assistant は WithSecure Luminen の一部です。幅広いコンテキスト検出の概要をすばやく明確に提供し、複雑なセキュリティ イベントを理解するための時間と労力を節約します。

Investigation Assistant は、Broad Context Detection (BCD) の簡単な概要と要約を提供します。この要約では、インシデント中に発生した重要な詳細と重要なイベントが強調表示されるため、この要約をさらなる調査の出発点として使用できます。また、脅威をより深く理解するのに役立つ追加のコンテキストも含まれています。

1. イベント > **Broad Context Detections** を選択します。
   [**Broad Context Detections**] ビューには、検出されたすべての Broad Context Detection が含まれます。
2. リストから調査したい Broad Context Detection を選択します。
3. [**Luminen**で分析」を]選択します。

   各検出にはリスクレベルのスコアがあり、お客様の環境における検出の推定影響を示します。

   Luminen は検出を分析し、概要を表示します。

注 : 調査アシスタントの概要は AI によって生成されるため、注意して扱う必要があります。すべての脅威に完全に対処するには、さらに調査と専門家の相談が必要になる場合があります。

付録

A

要素エージェントの再インストール

トピック：

この章では、WithSecure Elements Security Centerでデバイスを複製せずに Elements Agent を再インストールする方法について説明します。

A.1 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。

WithSecure Elements Security Centerでは、デバイス名が主な識別子としてデバイスがリストされます。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、より微調整された方法が必要です。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、使用している WithSecure Elements管理ソフトウェアで WithSecure Elements Agentアンインストールして再インストールすると、新しいUUIDが生成され、Elements Security Centerに同じ名前の2番目のデバイスが表示されます。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ことがあり、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。

- コンピュータの 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
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、Elements Security Center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

    - 登録中に、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、両方が保存されます。
    - Elements Security Centerに新しいデバイスが追加されました
- 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
    - 登録中に、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 Elements Security Centerに追加されませんが、既存のデバイスは更新されます。

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。

注 : Horizon デスクトップ プールで、[既存のコンピュータ アカウントの再利用を許可する]オプションをオンにして、システムが重複したデバイスを生成しないようにします。Active Directory アカウントを作成すると、クローン操作後もアカウントは変更されません。そのため、Elements Security Center同じ名前を共有していても、それらを個別のデバイスとは見なしません。

.exe ファイルを使用して Elements Agent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、EXEファイルを使用した手動展開（41ページ）そしてMSIファイルを使用した手動展開（46ページ）。

付録
B

Elements Security Centerとソフトウェアをカスタマイズする

トピック：

この章では、スコープ セレクタを使用してWithSecure Elements Security Centerに表示される情報の範囲を変更する方法、およびElements Security CenterとElements Endpoint Protectionソフトウェアをカスタマイズする方法について説明します。

注：顧客企業の追加、サブスクリプションキーの追加、および顧客企業の製品の注文方法については、Elements製品を使用する（23ページ）を参照してください。

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 コンピューターは、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。

B.1 顧客企業を追加する

WithSecure Elements セキュリティ センターアカウントに新しい *顧客会社*を追加するには、まずその会社を ***WithSecure*** *パートナー ポータル*アカウントに *新しい顧客*として追加し、その会社に対して少なくとも１つの WithSecure Elements製品を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。

新しい顧客企業でサブスクリプションとデバイスを管理する管理者が必要な場合は、Element Security Centerを通じて 管理者アカウントを作成する必要があります。

注：WithSecureパートナー ポータルは、Element Security Centerと連携して機能し、WithSecureソリューションの販売とサポートを促進するツール、資料、統合された電子注文システムを提供するオンライン サービスです。

新規顧客の注文書がパートナーポータルアカウントから正常に追加されると、Element Security Centerアカウントに新規顧客会社として自動的に追加されます。

その後、顧客企業のユーザーに WithSecure Elements製品を提供したり、購入した製品のサブスクリプションを管理したりできるようになります。

B.2 企業アカウントにサブスクリプションキーを割り当てる

企業アカウントにサブスクリプションキーを追加すると、WithSecure Elements Security Centerにコンピューターを割り当てることができます。

以下の点を考慮する必要があります。

- ソリューションプロバイダおよびサービスパートナーは企業アカウントにサブスクリプションキーを割り当てることができます。
- 企業ユーザーは、パートナーから提供された未使用のサブスクリプション キーを自社の組織に割り当てることができます。
- ユーザーには、Endpoint Protectionソフトウェアでの完全な編集ロールが付与されている必要があります（コンピューターとサーバーの両方に適用されます）。
- サブスクリプションはパートナーレベルで割り当てる必要があります（サブスクリプションキーが存在する必要があります）。パートナーは、サイドバーの[管理]の下の[サブスクリプション]ビューでサブスクリプションキーを見つけることができます。

  注：企業ユーザーはパートナーにサブスクリプションキーを要求する必要があります。

サブスクリプションキーを割り当てるには

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。
2. スコープ セレクターで、サブスクリプションキーを割り当てる会社を選択します。
   選択した会社の現在のサブスクリプションの一覧表が開きます。
3. フィルターの上にある [サブスクリプションを割り当てる] を選択します。
   [サブスクリプションを割り当てる] ページが開きます。
4. 企業アカウントの新しいサブスクリプションキーを入力して [**OK**] を選択します。

新しいサブスクリプションキーが企業アカウントに追加されます。

B.3 顧客企業に製品を注文する

WithSecureパートナーポータルを通じて、顧客企業向けの WithSecure Elements製品を注文できます。

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 パートナー ポータルから WithSecure Elements製品を注文するには:

1. ウェブ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では、WithSecure Elementsセキュリティセンターとは別のログイン認証情報が必要です。ログイン情報がまだお手元にない場合は、ページ上の「認証情報のリク

エスト」フォームにご記入の上、[送信」を]クリックしてください。アクセス認証情報が届くまで最大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。

   購入注文が完了すると、製品情報の変更が WithSecure パートナー ポータルと Elements Security Center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。

   注文が完了すると、新しい顧客企業が、購入した製品とともにパートナー ポータルアカウントに表示されます。

   注 : 新しい顧客会社が Elements Security Centerアカウントに表示されるまでには、しばらく時間がかかる場合があります。

B.4 Elements Security Centerをカスタマイズする

WithSecure Elements Security Centerは、お客様の口ゴやサポートリンクでカスタマイズできます。

Elements Security Center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. [カスタマイズ]タブを選択します。
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。
   組織の口ゴページが開きます。
4. 口ゴを口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 : 口ゴは .png 形式である必要があります。口ゴに必要な寸法は 64 x 64 ピクセルです。
5. [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。
6. 変更を保存します。

カスタマイズすると、Elements Security Centerの左下隅に口ゴが表示されます。

B.5 WithSecure Elementsソフトウェをカスタマイズする

口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 : 口ゴまたは 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. [クライアントのカスタマイズ]タブを選択します。
   クライアントカスタマイズ ロゴページが開きます。
3. ロゴを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 : ロゴは .png 形式である必要があります。ロゴに必要なサイズは 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を検討してください。

4. [パートナー **URL**]フィールドにリンクを入力します。
   指定するリンクは、ロゴのオプション リンクです。たとえば、サポート サイトへのリンクであれば、デフォルトの WithSecureサポート リンクが置き換えられます。

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。

付録
C

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。

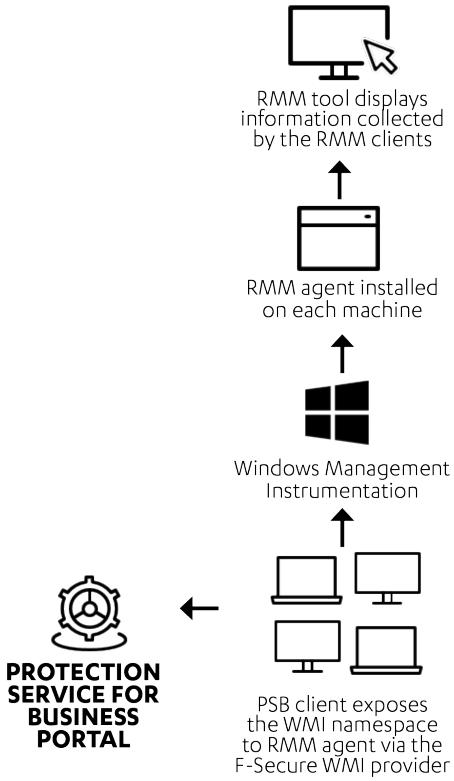
サービス プロバイダの多くはアセット (資産) ディスカバリー、管理、設定、プロセス・サービスの自動化、セキュリティ サービス、バックアップなどの管理機能を強化するためにWMIの連携を使用します。

C.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 サーバーに転送します。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 コンピューターに対してフル 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ー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 Security Centerへの最終接続時刻
- WithSecure Elements Security Centerからの最終ポリシー更新時刻
- 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

C.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 セキュリティ センターにログインします。
   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 Security Centerへの最後のポリシー接続の時刻

```
$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 Security Centerからの最終ポリシー更新時刻

```
$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
```

C.2 連携用の WMI クラス

この付録では、WithSecure ElementsでのWindows Management Instrumentation (WMI) 統合に使用されるクラスについて詳しく説明します。

C.2.1 WMI クラス

ここでは、WithSecure Elements Security Center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（200ページ）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、コンピューターの完全スキャンを実行できます。

プロパティ名	説明	種類
RealTimeScanning	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	***AvDefinition***

メソッド名	説明	戻り型
ScanComputer	フル コンピューター 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
Version	APIの実バージョン	***string***

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	***string***
EngineVersion	該当するエンジンのバージョン	***string***
UpdateSerialNumber	インストールしたアップデートの一意識別子	***string***

プロパティ名	説明	種類
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	***string***

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***
Profile	インストールされているプロファイル。	***Profile***

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、MNS、MAC、またはホスト IDが定義されていない場合は空）。	***string***
HostIdentity	ホストID	***string***

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	***string***
ApplicationControl	アプリケーション制御の現在のステータス	***component***
Version	WithSecureファイアウォールのバージョン	***string***
Build	WithSecureファイアウォールのビルド	***string***

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***

プロパティ名	説明	種類
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（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	***string***

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口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	***string***

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	***string***

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
Name	製品の名前	***string***
Version	製品のバージョン	***string***
Build	製品のビルド	***string***

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	***string***
ProfileVersion	プロファイルパッケージのバージョン	***string***
SeriesName	プロファイルパッケージの名前	***string***
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***	***string***

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***

C.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 Security CenterでWMIプロバイダ設定を有効にする必要があります。

付録

D

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。

重要：Webコンテンツコントロールが正しく機能するには、Browsing Protection拡張機能が必要です。

Webコンテンツコントロールは、WithSecureの評価分析データを使用して Web サイトを分類し、ポリシーで選択されたコンテンツを含むサイトへのアクセスをブロックします。

D.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。
人工知能	人工知能 (AI) または機械学習 (ML) を使用または提供するウェブサイト。これには、AIツールの使用、AIソフトウェアのダウンロード、AIに関する学習、AIを活用したサービス (チャットボット、画像ジェネレーター、スマートアシスタントなど) の利用ができるサイトが含まれます。
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、他のコンピューター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ーを攻撃し、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。

D.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。

重要: Webコンテンツコントロールが正しく機能するには、BrowsingProtection拡張機能が必要です。

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. [コンピュータープロファイル] 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。

D.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、[このコンピューターで**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

E

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ーを移行します。

E.1 コンピューターを移行する

コンピューターを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。

コンピューターを移行するには

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ー 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ーにポリシーを配布します。
   選択したコンピューターが移行され、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ーを再起動する必要があるかもしれません。

E.2 Client Security for Mac から Elements Agent for Computers (Mac) への移行

次の手順に従って、Client Security for MacElements Agent for Computers (Mac)に移行します。

注：これらの手順は Elements Agent for Computers (Mac)バージョン 25.1 以降にのみ適用されます。

製品をインストールする前に、次の手順を実行します。

1. WithSecure Elements Security Centerで、Client Security for Macポリシーに一致するカスタム プロファイルを作成します。詳細な手順については、「新しいコンピューター プロファイルの作成」および「ポリシーの管理」を参照してください。
2. Elements Agent for Computersインストーラー パッケージの名前を変更して、前の手順のサブスクリプション キーとプロファイル ID を含めます。次の形式を使用します。

   ```
   ElementsAgentInstaller__<subscription-key>__<profile-id>__.pkg
   ```

   注：区切り文字として必ず二重アンダースコア (__) を使用してください。プロファイル ID は常にサブスクリプション キーと組み合わせて使用する必要があります。例:
   `ElementsAgentInstaller__XXXX-XXXX-XXXX-XXXX-XXXX__0000001__.pkg`
3. Elements Agent for Computers で利用可能な展開方法を確認し、手動展開または自動展開のいずれかを選択します。前の手順のインストーラー名を自動化スクリプトに組み込みます。

Elements Agent for Computers インストーラーは、Client Security for Mac自動的にアンインストールし、新しい製品をアクティブ化し、インストーラー名で指定されたプロファイルを適用します。

付録
F

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、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。

F.1 Elements Security Centerで言語を変更するにはどうすればよいですか？

言語を変更するには、まずWithSecure Elements Security Center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、Elements Security Centerで使用する言語を選択し、[保存] を選択します。

F.2 WithSecure Email and Server Securityのメール設定はElements Security Centerルのどこにありますか？

WithSecure Elements Security Center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。

F.3 Elements Security Center 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?

WithSecure Elements Security Center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、こちらをご覧ください。

F.4 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。

F.5 Elements Security Centerから削除されたコンピューターのリストを消去するにはどうすればよいですか？

WithSecure Elements Security Centerからコンピューターを削除すると、対象のコンピューターはブロックリストに追加され、コンピューターはElements Security Center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ーを同じコンピューター（該当するサブスクリプションキーで）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ー上で動作するため、このコンピューター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、Elements Security Centerへの接続がブロックされます。

F.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ー上にある場合、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。

F.7 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。

ws_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WithSecure Elements Security Center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Elements Security Centerに自動的に登録するには、次のコマンドを入力します。

```
.\ws_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。
--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\ws_oneclient_logout.exe" --keycode <subscription-key> --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ws_oneclient_logout.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。

パラメータ	説明
--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。`ws_oneclient_logout.exe`ツールをこのオプション（`ws_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Elements Security Center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。