



Elements Endpoint Protection

目次

第 章1: WithSecure Elementsソリューションの紹介.....	5
1.1 WithSecure Elementsセキュリティセンターを使用する.....	6
第 章2: Elements Endpoint Protectionの概要.....	41
2.1 製品を使用するには.....	43
第 章3: システム要件.....	44
第 章4: 導入.....	49
4.1 Windowsの展開方法.....	50
4.2 Macデバイスの展開方法.....	74
4.3 Linuxデバイスの展開方法.....	95
4.4 モバイルデバイスの展開方法.....	98
4.5 メールでユーザーを招待する.....	127
第 章5: プロファイルを管理する.....	130
5.1 クライアントに設定を割り当てる.....	131
5.2 プロファイルの管理.....	133
5.3 制御されたアップデート.....	139
5.4 プロファイルの管理 (Windows)	141
5.5 プロファイルの管理 (Mac)	189
5.6 プロファイルの管理 (Linux)	198
5.7 モバイルデバイスプロファイルの管理.....	208
第 章6: セキュリティを監視する.....	215
6.1 デバイスの操作.....	216
6.2 デバイスのセキュリティを監視する.....	217
6.3 セキュリティイベントを表示する.....	221
6.4 Active Directoryをスキャンして保護されていないデバイスを検出します。	222
6.5 デバイスをネットワークから隔離する.....	223
6.6 デバイスを削除する.....	224
6.7 サードパーティ RMM ツールを使用する.....	225
第 章7: 警告と報告.....	238
7.1 通知ハブを使用する.....	239

7.2 セキュリティ概要.....	239
7.3 セキュリティイベントレポート.....	241
7.4 カスタマイズされたメールレポート.....	241
7.5 セキュリティイベント用のカスタムビューを作成する.....	242
7.6 監査ログ.....	242
第 8 章: サードパーティのソフトウェアを最新の状態に保つ.....	244
8.1 利用可能なソフトウェアアップデートを表示する.....	245
8.2 カテゴリ別にアップデートをインストールする.....	246
8.3 ソフトウェアアップデートを自動的にインストールします.....	246
8.4 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.....	249
8.5 デバイスソフトウェアのアップデート.....	250
8.6 ソフトウェアアップデーター用の HTTP プロキシを設定する.....	250
8.7 ソフトウェアアップデーター用コネクタ.....	251
8.8 ソフトウェアアップデーターと WSUS.....	251
第 9 章: WithSecure Luminen の使用.....	253
9.1 セキュリティ意識向上アシスタント.....	254
9.2 調査アシスタント.....	255
9.3 Luminen の概要.....	255
付録 A: 要素エージェントの再インストール.....	257
A.1 重複なしで再インストール.....	258
付録 B: Elements Security Center とソフトウェアをカスタマイズする.....	260
B.1 顧客企業を追加する.....	261
B.2 サブスクリプションキーを割り当てる.....	261
B.3 新規顧客企業向けに製品を注文する.....	262
B.4 カスタマイズ要素セキュリティセンター.....	263
B.5 WithSecure Elements ソフトウェアをカスタマイズする.....	263
付録 C: Windows Management Instrumentation.....	264
C.1 WMI の連携.....	265
C.2 連携用の WMI クラス.....	269
付録 D: 望ましくない Web コンテンツをブロックする.....	276
D.1 Web コンテンツ カテゴリ.....	277
D.2 ブロックするコンテンツを選択してください.....	279
D.3 ブロックされたウェブサイトアクセスする.....	280

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.....	281
E.1 コンピュータを移行する.....	282
E.2 Mac版CSをElementsに移行する.....	282
付録 F: FAQ.....	284
F.1 ポータル言語を変更する.....	285
F.2 ESSメール設定を探す.....	285
F.3 新しいサブスクリプションキーを注文する.....	285
F.4 サブスクリプションキーの更新.....	286
F.5 削除されたコンピューターのリストをクリアする.....	286
F.6 サポートされていないクライアントを確認してください.....	286
F.7 プロフィールを作成するタイミング.....	286
F.8 ソフトウェアを再初期化する.....	287
Glossary.....	289
索引.....	298

第 1 章

WithSecure Elements ソ リューションの紹介

トピック：

- WithSecure Elements セキュリティセンターを使用する

WithSecure Elementsソリューションの紹介

概要 WithSecure Elementsソリューションとその提供内容。

WithSecure Elementsの概要 WithSecure Elements当社の製品は、エンドツーエンドのビジネスおよびクラウド環境をカバーする、包括的なサイバーセキュリティアプリケーション群で構成された、単一の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、エンドポイント検出・対応における、受賞歴のある当社のテクノロジーが含まれています。予測不可能で絶えず変化す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、強靱なビジネスの構築と維持を支援します。

WithSecure Elementsの特長 WithSecure Elementsこれは、外部の脅威環境だけでなく、変化するビジネスニーズにも常に適応する必要がある、現代のアジャイルな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、ビジネスの必要性に応じて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 Security Centerは、以下の言語をサポートしています。

- 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

エンドポイント製品は、以下の言語をサポートしています。

- 英語、チェコ語、デンマーク語、オランダ語、エストニア語、フィンランド語、フランス語、フランス語 (カナダ)、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、ノルウェー語、ポーランド語、ポルトガル語、ポルトガル語 (ブラジル)、ルーマニア語、ロシア語、スロベニア語、スペイン語、スペイン語 (ラテンアメリカ)、スウェーデン語、トルコ語、繁体字中国語 (香港)、繁体字中国語 (台湾)、簡体字中国語 (中国)。

WithSecure Elementsのトレーニング Elementsの入門トレーニングセッションについては、WithSecureパートナーポータル経由でアカデミーにアクセスしてください。

WithSecure Elements Security Centerにアクセスする Elements Security CenterにWithSecure、以下の方法でアクセスできます。

1.1 WithSecure Elementsセキュリティセンターを使用する

WithSecure Elements Security Centerの日常的な使用に必要な基本的なタスク。これには、アクセス権限や管理者アカウントの管理が含まれます。

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
- WithSecure Elements セキュリティセンターに表示される情報の範囲を広げたり狭めたりするには、スコープセレクターを使用します。

注文できます WithSecure Elements 顧客企業のユーザーに製品を提供するとともに、企業のコンピュータやモバイルデバイスにインストールされている製品のサブスクリプションを管理する。

1.1.1 WithSecure Elements Security Center を使い始めましょう

WithSecure Elements Security Center の利用開始は、ログイン、多要素認証の設定、管理者の追加、サブスクリプションの割り当てという 4 つのステップで完了します。

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。アカウントを取得する方法は 2 つあります。

- WithSecure パートナーから製品を購入すると、通常、パートナーが最初の管理者用のアカウントを作成します。その後、一時パスワードとログインリンクが記載されたメールが届きます。



ヒント: メールが届かない場合は、まず迷惑メールフォルダを確認してください。

- サブスクリプションキーはお持ちでもアカウントをお持ちでない場合は、WithSecure Elements Security Center への自己登録リンクを使用して、最初の管理者アカウントを作成してください。

このクイックスタートガイドでは、WithSecure Elements Security Center の使用を開始するための 4 つの主要な手順 (ログイン、多要素認証の設定、管理者アカウントの追加、サブスクリプションの割り当て) について説明します。

1. ログインして Elements Security Center。

- a) WithSecure Elements セキュリティセンターのサインインページに、ビジネスアカウントの認証情報を使用してログインしてください。ログインオプションについては、「ログイン」を参照してください。
- b) 複数の会社を管理している場合は、「管理対象会社間の移動」で説明されているように、スコープセレクターを使用して会社を切り替えます。

2. 多要素認証 (MFA) を設定してください。

- a) 多要素認証の選択の説明に従って、アカウントの MFA を有効にしてください。
- b) ニーズに合った認証方法を選択してください。利用可能な認証方法については、「多要素認証 (MFA) の方法」をご覧ください。

3. 管理者アカウントを追加します。

- a) 追加の管理者を招待し、会社組織にセキュリティ管理者を招待するの説明に従って役割を割り当てます。

4. サブスクリプションを割り当てて、製品をデプロイします。

- a) 顧客企業にサブスクリプションキーを割り当てる方法の説明に従って、企業にサブスクリプションキーを割り当てます。
- b) Elements Security Center からソフトウェアをダウンロードする手順の説明に従って、展開したい製品のインストーラーをダウンロードしてください。

セットアップを完了するには、導入したい製品のクイックスタートガイドに従ってください。

1.1.2 ログイン

ビジネスアカウントを使用して WithSecure Elementsセキュリティセンターにログインするための要件。

あなたには WithSecureElements Security Centerにアクセスするには、ビジネスアカウントが必要です。WithSecureパートナーの場合、パートナーは通常、管理対象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。これがあなたに当てはまる場合、パートナーからメールが届いています。WithSecure一時パスワードと、Elements Security Centerにログインするためのリンクが提供されます。

アカウントがまだ作成されていない場合でも、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、管理対象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。そのためには、お住まいの地域に応じた企業向け自己登録リンクをご利用ください。

フェデレーションされていないドメインにログインする

ユーザー名とパスワードを使用して、フェデレーションされていないドメインにログインします。

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いてください： WithSecure Elementsセキュリティセンターのサインインページ。
[ログイン] ページが開きます。
2. ユーザー名を入力して [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にログインする

Microsoft Entra IDの認証情報を使用して、フェデレーションドメインにログインします。

始める前に、Microsoft Entraアカウントをお持ちであることを確認してください。新規ユーザーの場合は、まずアカウントを作成する必要があります。

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。

1. Webブラウザで次のリンクを開いてください: WithSecure Elements セキュリティ センターのサインイン ページ。
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: 初めてご利用の方で、WithSecureドメインがフェデレーションされる前のビジネスアカウントでは、認証のためにMicrosoftのログインページにリダイレクトされ、Microsoftの認証情報を入力するよう求められます。これにより、アカウントがフェデレーションされたシングルサインオンにリンクされます。以降のログインでは、Microsoft Entra IDアカウントを使用したSSO (シングルサインオン) によって認証が行われます。

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へのアクセスを保護するために、多要素認証 (MFA) のご利用をお勧めします。Elements Security CenterでMFAをすぐに設定してください。



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、複数の多要素認証 (MFA) 方法を採用しています。

方法には次のものがあります。

- 時間ベースワンタイムパスワード (*TOTP*) に対応した認証アプリ (Microsoft Authenticator、Google Authenticator、Auth0 Guardianなど、パソコンやモバイル端末で利用可能な認証アプリ) を使用します。認証アプリに6桁の認証コードが送信されるので、ログインダイアログにそのコードを入力して続行してください。
- *Auth0 Guardian* 認証アプリのプッシュ通知機能を使えば、ボタンをワン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多要素認証アプリは、Google PlayとApp Storeで入手可能です。
- ワンタイムパスワード (*OTP*) 付きショートメッセージサービス (*SMS*) メッセージ用の電話番号 - 設定済みの携帯電話番号に6桁の認証コードがSMSで送信されます。ログインダイアログにそのコードを入力する必要があります。



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があります。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。



ヒント: 短時間に複数のSMS認証コードを要求すると、それ以降のメッセージが一時的にブロックされる場合があります。ブロックはしばらくすると解除されます。日常的なログインには、SMSよりも信頼性の高い認証アプリまたはセキュリティキー (WebAuthn/FIDO2) のご利用をお勧めします。

- Yubico YubiKey、Google Titanなど、FIDO2規格 (FIDO2仕様) をサポートするセキュアUSBキー
- FIDO2規格 (FIDO2仕様) をサポートするスマートフォンまたはその他のデバイス
- デバイスの生体認証、指紋認証、顔認証、またはデバイスからの WebAuthn (Web 認証 (WebAuthn) 仕様) を使用した Windows Hello。



重要: デバイスの生体認証は個々のデバイス固有のものであり、唯一の認証方法として使用することはできません。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。

多要素認証を選択してください

1つ以上の多要素認証方法を選択します。

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、アカウントにアクセスできなくなりますのでご注意ください。



ヒント: 複数の認証方法を登録してください。すべての認証方法にアクセスできなくなった場合、アカウントをリセットすることはできず、再作成する必要があります。

1つ以上の多要素認証方法を選択するには：

1. メールアドレスとパスワードを使用して、WithSecure Elementsセキュリティセンターにログインしてください。
2. 右上隅の



を選択し、次に **[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。

多要素認証を削除する

多要素認証方法を削除します。

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. 右上隅の



を選択し、次に **[マイ設定]** 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。

デバイスの生体認証を使用する

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、事前に別の多要素認証 (MFA) 方法を設定しておく必要があります。

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、右上隅の



を選択し、**[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. 既に設定済みの多要素認証方法を使用して本人確認を行い、**[続行]**を選択してください。
「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]** を選択すると、**ホーム**画面に戻ります。

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。

1.1.3 ユーザ管理

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

このセクションでは、アクセス権限と役割、スコープセクター、管理者アカウントの追加と管理など、WithSecure Elements Security Centerへのアクセス権限を管理する方法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。

新規アカウントを作成する際、または既存のアカウントを編集する際に、アクセス権限を設定できます。

役割ごとのアクセス権限

WithSecure Elementsの各製品領域で利用可能な役割とアクセス権限、および各役割に対応する監査ログエントリ。

曝露管理 - 曝露

完全編集

以下の 露出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)

監査ログエントリ: cspm: admin

リスク管理 - 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)

監査ログエントリ: vm: administrator

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。

監査ログエントリ: vm: team_member

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。

監査ログエントリ: vm: readonly_team_member

Collaboration Protection

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

監査ログエントリ: cpo365:admin

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。

監査ログエントリ: cpo: 読み取り専用

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。

監査ログエントリ: cpo365:quarantine_mgr

コラボレーション保護 - 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)

監査ログエントリ: fusion_admin

エンドポイント保護

アクセス不可 以下のエンドポイント保護機能へのアクセスはできません。

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。

エンドポイント保護 - コンピュータとモバイル機器

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)。

監査ログエントリ: epp: manage_computers_mobiles_only

または epp: manage_all

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。

監査ログエントリ: epp: manage_servers_only

または epp: 読み取り専用

エンドポイント保護 - 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: セキュリティ管理者ロールと「コンピュータとモバイル - 完全編集」ロールは、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ために必要です (IAMロールに置き換えられます)。

監査ログエントリ: epp: manage_servers_only

または epp_manage_all

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。

監査ログエントリ: epp: manage_computers_mobiles_only

epp: 読み取り専用

拡張検出および応答 - オフに切り替える

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
- イベント検索ページ
- 昇格する WithSecure
- サブスクリプションビュー

拡張された検出と対応 - 広範なコンテキスト検出

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
- 昇格する WithSecure該当する場合
- 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。

監査ログエントリ: elements:xdr-incident-full

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
- 昇格する WithSecure 該当する場合
- 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。

監査ログエントリ: elements:xdr-incident-read

拡張型検知・対応システム - 対応

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。

監査ログエントリ: elements:xdr-respons-full

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。

監査ログエントリ: elements:xdr-response-read

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

拡張検出および対応 - 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。

監査ログエントリ: elements:xdr-event-search

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

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。

管理対象企業間を移動する

スコープセクターを使用して、WithSecure Elements セキュリティセンターに表示される情報の範囲を広げたり狭めたりします。

Elements Security Centerには、アクセス権限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および企業グループを管理します。SoPは Elements Security Centerにアクセスして、自社が直接管理する企業、サービスパートナー、およびサービスパートナーの企業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、複数の企業グループを管理します。SePは Elements Security Centerにアクセスして、直接管理する企業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ーに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へのフルアクセス権を取得できます。SoPまたはSeP、あるいは WithSecureによって直接管理されている企業は、Elements Security Centerへの読み取り専用権限を取得します。

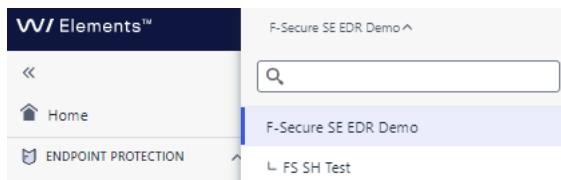
特定の会社にもスコープセクタを重視するには

1. タイトルバーにある



アイコンを選択してください。

アカウントに関連付けられているすべての顧客企業を一覧表示するドロップダウンメニューが表示されます。



2. 目的の会社を選択するか、検索フィールドに会社名を入力して、[Enterキー]を押してください。

選択された企業名は青色の背景色で表示され、ページは選択された企業に関する関連情報を表示するように更新されます。

要素のアイデンティティとアクセス管理 (IAM) ロール

IDおよびアクセス管理 (IAM) ロールは、IAM管理者自身の組織および関連組織内のセキュリティ管理者に対して、すべての Elements 権限を付与および取り消す権限を有します。

概要

IAM の役割は、WithSecure Elements これは、セキュリティ機能とサービスの管理を効率化し、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、以下の方法で Elements Security Center にアクセスします。WithSecure ビジネスアカウント。これらのアカウントへのアクセス権限は、特定の機能、能力、およびサービスに基づいて管理されます。IAM ロールは、以前は複雑だった、さまざまな機能にわたるロールの割り当てプロセスを簡素化します。

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。

- 合理化された役割管理 WithSecure Elements
- 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 ロールに権限昇格が含まれないユーザー (つまり、組織内の従来のユーザーアクセス管理ロールをすべて保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、新しい IAM 管理者ロールを取得でき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、組織は IAM 関連の権限管理方法を慎重に検討する必要があります。そのため、このオプションが利用できなかった場合と比べて、IAM 管理者として行動できるユーザー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。

- セキュリティ機能やサービスへのアクセスを得るために、他の役割を自分に付与する
- によって導入された新しい役割を付与または取り消す WithSecure Elements の機能またはサービスについて
- 作成または削除 WithSecure ビジネスアカウントに対して、役割の付与または取り消しを行う。
- 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
- オンボーディング WithSecure 新規パートナー企業または顧客企業向け

既存の機能またはサービス固有のルールは引き続き有効ですが、最終的にはIAMルールを通じて管理されるようになります。IAMルールは、APIキーの設定など、現在他のル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ルールから、より高い権限を付与する新しいElements IAMル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ルールを要求するように促します。

IAMルールの候補者は、従来の機能固有のIAMルールの所有と、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。

顧客企業向け

以下のレガシールールが特定されている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 セキュリティ管理者は、管理する企業が使用するすべての機能とサービスに関するレガシールールを保有している。



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ル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ルールを割り当てると、IAMル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ルールに関するよくある質問

IAMルールに関するよくある質問への回答。

Q

パートナー(SOP/SEP)は、傘下のすべての企業に対してIAMルールを作成できますか？

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？

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ルールを自動的に取得しますか？

最高レベルの管理者ル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？

A

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。

会社の管理者は、サービスパートナーに問い合わせ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。

はい、最初の管理者にはIAMルールが自動的に付与されます。

ユーザーが誤ってIAMル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ルールを割り当てることができます。

Q

[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？

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？

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？

組織内で誰がIAMロールを登録しているかを確認するにはどうすればよいですか？

A

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。

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。

最初の段階では、組織が契約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 クレームボタンが表示されます。たとえば、企業が Elements Endpoint Protection と Collaboration Protection の両方の契約を結んでいる場合、IAM クレームボタンは両方の製品に対して完全な管理者権限を持つユーザーに表示されます。

IAMロールが表示され、ロールを持つユーザーは以下の表でフィルタリングできます。管理 > [セキュリティ管理者]

新しい管理者を追加する

WithSecure Elements Security Centerでは、管理者と呼ばれる指定された個人に、必要な権限を持つユーザーアカウントを提供できます。

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. 下[管理]選択[組織設定]サイドバーに表示されます。
の組織設定 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. 管理者追加画面で、管理者の詳細を入力します。
 - a) 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。

- b) 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ア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. 管理者の詳細と選択された役割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

WithSecure Elementsで、管理対象組織にサービスパートナーアカウントを追加します。

サービスパートナーアカウントを作成するには

1. 下**[管理]**選択**[組織設定]**サイドバーに表示されます。
の**組織設定**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、**[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」 画面が開きます。
4. 組織アカウントの名前を入力し、**[保存]**を選択してください。

サービスパートナーアカウントが作成されます。

管理者の編集または削除

管理者を変更・削除することができます。

管理者の役割割り当てを編集するか、アクセス権を完全に削除します。すべての役割を削除すると、アカウントは自動的に削除されます。

1. 下**[管理]**選択**[組織設定]**サイドバーに表示されます。
の**組織設定**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。

APIクライアントを作成する

APIクライアントを作成することで、アプリケーションが特定のアクセス権限でElements APIを使用できるようになります。

APIクライアントは、アプリケーションがElements APIを使用できるようにする認証情報を提供します。APIクライアントは、作成時に **[読み取り専用]** オプションを選択するかどうかに応じて、完全なアクセス権を持つか、読み取り専用アクセスに制限されます。利用可能なAPI操作については、Elements APIリファレンスを参照してください。

APIクライアントを作成するには：

1. 下[管理]選択[組織設定]サイドバーに表示されます。
の**組織設定**ページが開きます。
2. [APIクライアント]タブを選択してください。
このタブには、組織の**UUID**と既存の**APIクライアント**の一覧が表示されます。
3. [新規追加]を選択します。
「**新しいAPIクライアントの追加**」ダイアログが開き、「**詳細**」ステップから始まります。
4. APIクライアントの組織を選択し、説明を入力して、[読み取り専用]を選択すると、クライアントのアクセスが読み取り専用で制限されます。
5. [追加]を選択します。
APIクライアントのステップが開き、生成されたクライアント**ID**とシークレットが表示されます。
6. 秘密の内容をコピーして、安全な場所に保管してください。



重要: この手順を終えると、秘密情報に再度アクセスしたり、閲覧したりすることはできません。

7. [秘密情報をコピーして保存しました]を選択し、次に [完了]を選択します。
新しい**APIクライアント**は、クライアント**ID**、アクセス権限、作成日とともにリストに表示されます。

新しいAPIクライアントが作成されます。

APIクライアントを削除する

アプリケーションが不要になったAPIクライアントは削除できます。

APIクライアントを削除すると、その認証情報を使用していたアプリケーションは、その認証情報を使用して Elements APIにアクセスできなくなります。

APIクライアントを削除するには：

1. 下[管理]選択[組織設定]サイドバーに表示されます。
の**組織設定**ページが開きます。
2. [APIクライアント]タブを選択してください。
このタブには、組織の**APIクライアント**の一覧が表示されます。
3. 削除したいAPIクライアントの行で、ゴミ箱アイコンを選択し、削除することを確認します。
APIクライアントが削除されました。

パスワードを復元する

パスワードを忘れた場合は、[パスワードをお忘れですか?]のリンクからパスワードを復元できます。

パスワードを回復するには

1. ログインページで、[パスワードをお忘れですか?]のリンクを選択してください。
[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]を選択してください。

パスワードの変更方法を記載したメールが届きます。

アカウントの詳細を変更する

WithSecure Elementsセキュリティセンターでユーザー名を変更してください。フェデレーションユーザーは、IDプロバイダーでアカウントの詳細を管理します。

WithSecure Elementsセキュリティセンターのアカウント設定からユーザー名を変更できます。



重要：管理対象組織がフェデレーションサインイン (Entra ID) を使用している場合、WithSecure Elementsセキュリティセンターでアカウントの詳細を変更することはできません。代わりに、IDプロバイダーで詳細を管理してください。

ユーザー名を変更するには:

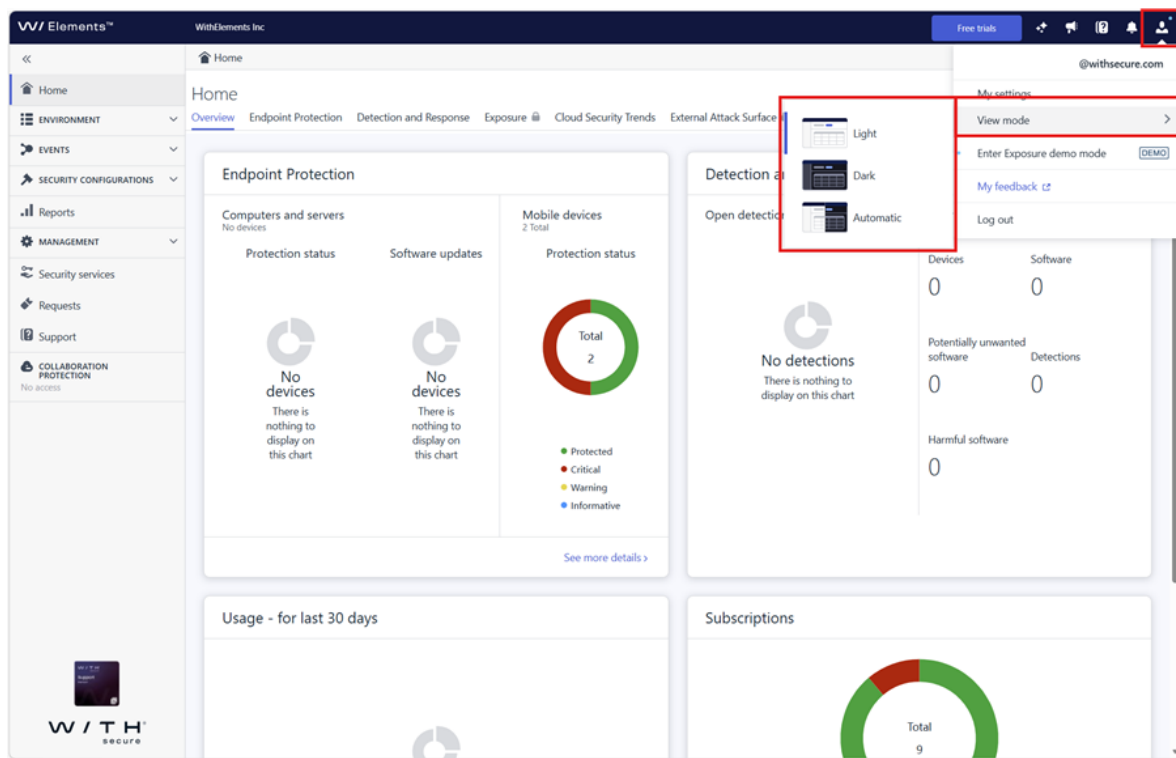
1.  右上隅にある **[マイ設定]** を選択します。
2. **[詳細]** 欄に、新しいユーザー名を入力してください。
3. **[保存]** を選択します。

1.1.4 表示モードを変更する

WithSecure Elements Security Centerの外観をカスタマイズするには、ライト、ダーク、または自動表示モードを選択してください。

Elements Security Centerの外観は、好みに合わせて表示モードを選択することでカスタマイズできます。ダークモードは、管制室などの暗い環境や夜間勤務時に便利です。表示モードを変更するには：

1. ポータルの右上隅にあるユーザープロフィールメニューアイコンを選択してください。
2. **[表示モード]** を選択してください。
3. 以下の選択肢から1つを選んでください。
 - **[Light]** – 明るい環境に適した、明るいインターフェース。
 - **[ダークモード]** – 暗い場所での目の疲れを軽減する、より暗いインターフェース。
 - **[自動設定]** – デバイスのシステム設定に合わせて、ライトモードとダークモードを自動的に切り替えます。



新しい表示モードはすぐに適用されます。これらの手順を繰り返すことで、いつでも変更できます。

1.1.5 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：下管理 > サブスクリプション所有しているすべての製品、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確認できます。

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製品のデプロイ方法については、「一般的なデプロイ方法」をご覧ください。

顧客企業を追加する

WithSecure Elements Security Centerアカウントに新しい顧客企業を追加するには、まずその企業をWithSecure Partner Portalアカウントに新しい顧客として追加し、少なくとも1つの製品を購入する必要があります。WithSecure Elementsそれに対応する製品。



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、Elements Security Centerを通じて 管理者アカウントを作成してください。



注：WithSecureパートナーポータルは、Elements Security Centerと連携するオンラインサービスです。販売とサポートを支援するツール、資料、統合された電子注文システムを提供します。WithSecure解決策。

新規顧客の発注書は、まずパートナーポータルアカウントから正常に追加される必要があります。これが完了すると、顧客は自動的にElements Security Centerアカウントに新規企業として追加されます。

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。

顧客企業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）。パートナーはサブスクリプションキーを次の場所で見つけることができます。**ションサブスクリプション**表示[管理]サイドバーに表示されます。



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. 下[管理]選択[サブスクリプ]サイドバーに表示されます。
2. スコープセクターを使用して、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]を選択してください。
購読割り当てページが開きます。
4. 会社の新しいサブスクリプションキーを入力し、[OK] を選択してください。]

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。

既存顧客企業向けに製品を注文する

既存の顧客企業向けにWithSecure Elements製品を注文するには、WithSecureパートナーポータルをご利用ください。



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。

ご注文はこちら WithSecure Elements WithSecureパートナーポータル経由で既存顧客企業向け製品を提供する：

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へのアクセスには、WithSecure Elementsセキュリティセンターからのログイン認証情報が必要です。ログイン情報をお持ちでない場合は、ページ上の「**認証情報のリクエスト**」フォームに必要事項を入力し、[送信]をクリックしてください。アクセス認証情報の受信には最大24時間かかる場合があります。

電子注文ページが表示されます。

2. 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。
3. [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。
4. [新規注文] の下に、注文の参照番号を入力します。
5. [製品の注文] で、[製品を追加] を選択します。
6. 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。

新規顧客企業向けに製品を注文する

WithSecureパートナーポータルを通じて、新規顧客企業向けにWithSecure Elements製品を注文してください。



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。

ご注文はこちら WithSecure Elements WithSecureパートナーポータル経由で新規顧客企業向け製品を提供する：

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にアクセスするには、WithSecure Elementsセキュリティセンターから別途ログイン認証情報を取得する必要があります。ログイン情報をお持ちでない場合は、ページ上の「**認証情報のリクエスト**」フォームに必要事項を入力し、**[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時間かかる場合があります。

電子注文ページが表示されます。

2. メイン ページで、**[新規注文]** を選択します。
3. 新しい顧客企業の名前を入力し、**[新規追加]** を選択してください。
[新規顧客] ウィンドウが開きます。
4. 顧客情報を入力し、**[保存]** を選択してください。
5. **[新規注文]** の下に、注文の参照番号を入力します。
6. **[製品の注文]** で、**[製品を追加]** を選択します。
7. 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。

利用可能な製品サブスクリプションを見る

利用可能な製品ライセンスを表示するには

サブスクリプションビューには、表示している範囲のすべての製品サブスクリプションが、キー、ステータス、有効期限とともに一覧表示されるため、管理対象組織全体でそれらを検索および管理できます。

1. 下**[管理]**選択**[サブスクリプ]**。

[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: スコープセクター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、デフォルトではすべてのサブスクリプションが表示されます。

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。

オプション	説明
サブスクリプション キー	該当するサブスクリプションキーを入力してください
製品	利用可能な製品リストから選択してください
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] を選択してください。間もなく期限切れになるサブスクリプションを表示するには [14日後] または [60日後] を選択してください。期限切れのサブスクリプションのみを表示するには「期限切れ」を選択してください。
種類	以下の購読タイプから選択できます： [商用] 、 [評価版] 、 [政府機関向け] 、 [教育機関向け] 、または [転売禁止] 。

特定の顧客企業の購読状況を確認するには、スコープセクターを使用して、表示したい企業を選択してください。



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。

購読キーを変更する

WithSecure Elements Security Centerで、1台または複数のデバイスのサブスクリプションキーを変更します。

サブスクリプションキーを変更するには



注：Elements ConnectorまたはEPPサブスクリプションのいずれのバリエーションについても、変更によってEPPを含まないサブスクリプションへのダウングレードが必要となる場合は、サブスクリプションキーを変更することはできません。

1. 下[環境]選択[デバイス]サイドバーに表示されます。
の**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. [購読の変更]を選択してください。
4. 表示されたフィールドに新しい購読キーを入力し、[購読の変更]を選択します。



注：下**管理**>**サブスクリプ**選択した企業のデバイスで利用可能なサブスクリプションキーを見つけることができます。

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

アップグレードのオプション WithSecure Elements購読。

この章では、アップグレードする方法について説明します。WithSecure Elements利用可能なサブスクリプションとアップグレードオプション。

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から WithSecure Elements EPP for Computers Premium へ
- WithSecure Elements EPP for Computersから WithSecure Elements EDR および EPP for Computers へ
- WithSecure Elements EPP for Computersから WithSecure Elements EDR および EPP for Computers Premium まで
- WithSecure Elements EPP for Computers Premiumから WithSecure Elements EDR および EPP for Computers Premiumへ
- WithSecure Elements EDRおよびEPP for Computersから WithSecure Elements EDRおよびEPP for Computers Premiumまで
- WithSecure Elements EPP for Serversから WithSecure Elements EPP for Servers Premium へ
- WithSecure Elements EPP for Servers Premiumから WithSecure Elements EDR および EPP for Servers Premiumへ



注: WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for ServersのStandardバージョンとPremiumバージョンの両方、およびWithSecure Elements EDRとEPP for ComputersまたはWithSecure Elements EDRとEPP for Serversの任意の組み合わせで、同じインストーラー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。

1.1.6 フェデレーションシングルサインオン

フェデレーション型シングルサインオン (FSSO) を使用すると、ユーザーはIDプロバイダーで一度認証するだけで、個別にログインすることなく複数のアプリケーションにアクセスできます。

フェデレーションシングルサインオン (FSSO) を使用すると、ユーザーは一度認証するだけで、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アクセスできます。ユーザーは、それぞれのアプリケーションやサービスに個別にログインする必要はありません。ユーザーがログインする際、ユーザー名やパスワードなどの認証情報をIDプロバイダーに送信します。IDプロバイダーはこれらの認証情報を検証します。認証が成功すると、IDプロバイダーはデジタル署名付きトークンを生成します。このトークンはユーザーの身元を証明するものです。ユーザーが異なるドメインや組織の他のアプリケーションやサービスにアクセスする場合、ブラウザはこのトークンを自動的に使用します。クラウドIDサービスはトークンを検証し、ユーザーが再度ログインすることなくアクセスを許可します。

FSSOは、さまざまなシステム間でのアクセスを簡素化します。ユーザーは一度認証するだけで、異なるアプリケーションやサービス間をスムーズに移動できます。また、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も向上します。ユーザーがIDプロバイダーから削除されると、自動的にログインできなくなります。Elements Security Centerこれにより、ユーザーアクセス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

これらの要件と考慮事項は、シングルサインオン (SSO) を実装する前に適用されます。

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。

FAQ

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 の実装は、フェデレーションされた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またがるアカウントを持っているため、変更はこれらの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、要素レベルにも影響します。メールドメインは組織内で一度しかフェデレーションできませんが、これは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 サインオンを設定する

ユーザーが Microsoft Entra ID の認証情報を使用してサインインできるように、フェデレーション型シングルサインオンを設定します。

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。

ユーザーがMicrosoft Entra IDの認証情報を使用してElementsにサインインできるように、フェデレーション型シングルサインオンを設定します。

1. WithSecure Elementsセキュリティセンターのサインインページにログインしてください。
2. 下管理 > 組織設定 > [セキュリティ管理者は]、[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。
「**フェデレーションシングルサインオンの設定**」ウィンドウが開き、あなたの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、「**検証成功**」と表示されます。



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、[フェデレーションによる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]のフェデレーションシングルサインオンが有効になりました**」に変わります。

ユーザーIDをリンクする

フェデレーションドメインのユーザーIDをElements Security Centerにリンクします。



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
 - ログインに使用するアカウント Elements Security Center以前は本人確認が行われていなかったはず
- ID をリンクするには:

1. WithSecure Elementsセキュリティセンターのサインインページにログインしてください。
2. メールアドレスを入力し、[続行]を選択します。

- 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: ドメイン構成によっては、多要素認証 (MFA) を完了する必要がある場合があります。

- メールアドレスをもう一度入力し、**[続行]**を選択します。
- 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。
- 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
- アカウント Elements Security Center エンドポイント保護による完全な編集権限と、フェデレーションドメイン内のメールアドレスが必要です。



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:

- WithSecure Elements セキュリティセンターのサインインページにログインしてください。
- [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。
- [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。
- [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。

1.1.7 管理対象のデバイスを追加する

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、WithSecure Elements アカウントを使用するには、まずコンピューターまたはモバイルデバイスに エンドポイント保護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。

管理対象デバイスに エンドポイント保護ソフトウェアをインストールする方法はいくつかあります。

- 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には、少なくとも1つの無料インストールが可能な エンドポイント保護ソフトウェアのサブスクリプションが必要です。企業に利用可能な無料インストール数によって、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

WithSecure Elementsエンドポイント保護ソフトウェアをデバイスに配布する方法。

- 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: ソフトウェアをスタンドアロンとしてインストールする場合、既存のエンドポイント保護ソフトウェアの自動アンインストールを無効にするために、コマンドラインパラメータ「--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)
 - WithSecure Elements Exposure Management(Windowsのみ)
- 同じWithSecure Elements Agent for Serversインストールパッケージを使用して、以下のソフトウェアをインストールできます。どのソフトウェアをインストールするかは、サブスクリプションキーによって決まります。
 - WithSecure Elements EPP for Servers (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)
 - WithSecure Elements Exposure Management(Windowsのみ)
- WithSecure Elements Mobile Protectionは、以下の2つの方法でインストールできます。
 - WithSecure Elements EPPポータル の **[新しいデバイスの追加]** を使用してインストールメールを送信します。



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オプションを選択し、招待状を1通送信するか、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することで、デバイスを追加できます]**。

- 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 のインストール方法については、WithSecure Elements Connector のドキュメントを参照してください。

インストールリンクをメールで送信する

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。WithSecure Elementsソフトウェア。



注：インストールリンクは30日間有効です。

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いずれか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、デバイスがあなたのデバイスに表示されます。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. サイドバーの **[環境]** で **[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。スコープセクターがすべての顧客会社を表示するように設定されている場合は、管理する会社を選択してください。

デバイス ページが表示されます。



2. **[デバイス]** を選択します。**[デバイス]** 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]** を選択します。**「新しいデバイスを追加」** ページが開きます。



注：スコープセクターで特定の企業に焦点を絞るように設定すると、ホームページに **「新しいデバイスを追加」** ボタンが表示されます。このボタンをクリックすると、直接 **「新しいデバイスを追加」** フォームに移動できます。

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。
複数の招待状を送信するには、**[CSVファイルからインポート]** の下にある **[ファイルを選択]** を選択し、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]** を選択してください。
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：保留中の招待状を表示するには、まず  を選択します。**[デバイス]** 次に、**[デバイス招待の管理]** を選択します。



注：このソフトウェアは、**[新しいデバイスを追加]** ページで選択したサブスクリプションキーを使用するようにカスタマイズされています。

製品がデバイスにインストールされ、アクティベートされると、**デバイス**ページを開くと、管理対象デバイスの招待ページから招待状が消えます。

Elements Security Centerからソフトウェアをダウンロードしてください。

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. ログインして Elements Security Center。
2. サイドバーから **[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. お使いのデバイスの種類に対応するセクションを探してください。例えば、「**コンピュータ用 WithSecure Elements エージェント**」や「**サーバー用 WithSecure Elements エージェント**」などです。
4. お使いのオペレーティングシステムに対応するダウンロードボタンを選択してください。
使用できるボタンは、オペレーティングシステムによって異なります。
 - Windows: **[.exeファイルをダウンロードする]**か、**[.msiファイルをダウンロードしてください。]**
 - Mac: **[.mpkgをダウンロード]**
 - Linux: **[amd64版をダウンロードする]**か、**[arm64版をダウンロードしてください。]**

ソフトウェアのダウンロードが完了しました。お客様のアカウントに関連付けられたサブスクリプションキーは、インストーラーに組み込まれています。

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専用」のサブスクリプションキーを、WithSecure Elements EDR for Computersがインストールされているデバイスで使用しないでください。また、その逆も同様です。ソフトウェアが破損する可能性があり、その場合は手動でアンインストール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までにオフライン状態である必要がある期間を設定できます。削除されたデバイスがアクティブになった場合、サブスクリプションに空きがあれば、Elements Security Centerに再び表示されます。サブスクリプションが満杯の場合は、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. 下**[環境]**選択**[デバイス]**サイドバーに表示されます。
の**デバイス**ページが開きます。
2.  を選択します**[デバイス]**。
メニューが表示されます。

3. メニューから **[自動削除の管理]** 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...]** をオンにしてください。
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。

招待状を管理する

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. サイドバーの **[環境]** で **[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。スコープセクターがすべての顧客会社を表示するように設定されている場合は、管理する会社を選択してください。

デバイス ページが表示されます。



2. **[デバイス招待の管理]** を選択します。
「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. 有効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。

1.1.8 カスタムラベルによるデバイス管理の強化

ラベルを作成して適用することで、選択した基準に基づいてデバイスをグループ化できます。

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。

デバイスラベルを追加する

デバイス ラベルは 3 つの方法で追加できます。

デバイスラベルは、以下の方法で追加できます。



注: コマンドラインでは、ラベルはタグと呼ばれます。

デバイスラベルを追加するには、以下のいずれかの方法を使用してください。

- **デバイスビュー**で手動で行う場合:**デバイスリストビュー**でデバイスを選択するか、**デバイスの詳細ビュー**で単一のデバイスを開き、**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て、**[追加]**を選択します。
- ラベル割り当てルールを使用する**プロファイルセクション**: 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を設定し]**、**アウトブレイクルール**または**プロファイル割り当てルール**にラベルを追加することで、ルールが一致するたびにラベルが自動的に適用されるようにします。
- Elements エージェントのインストールプロセス中に、エージェントのデプロイ時にインストールタグを割り当ててください。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」の手順2を参照してください。

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

WithSecure Elements Security Centerで選択したデバイスを管理する方法

WithSecure Elements セキュリティセンターでは、以下のいくつかの方法でデバイスを管理できます。

- それらを資産グループに整理する
- デバイスリストの表示とカスタマイズ
- 非アクティブなコンピュータを自動的に削除する
- 診断を依頼する

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 - デバイスを管理グループに割り当てます**デバイスページ**。
- 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

資産グループを使用することで、デバイスの可視性を向上させ、セキュリティイベント管理を効率化し、組織における高度なアクセス制御メカニズムへの準備を整えることができます。

アセットグループを作成する

企業レベルで資産グループを作成します。

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、パートナーとして、まず **スコープセクター**または**[一般]タブ**のリストから会社を選択する必要があります。**管理 > 組織設定**。

1. 下[管理]選択 **組織設定** > [一般的な]。
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. (オプション) [説明]欄に、資産グループの説明を入力します。
5. [保存] を選択します。

次に、**デバイス**デバイスを新しい資産グループに追加するページ。

デバイスを資産グループに追加する

デバイスを1つ以上の資産グループに追加します。

アセットグループはデバイスを整理し、スキャン、スケジュール設定、レポート作成を対象とできるようにします。

1. 下[環境]選択[デバイス]。
2. では**デバイス**ページを開き、1つまたは複数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で管理する

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. サイドバーの [環境]で [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。スコープセクターがすべての顧客会社を表示するように設定されている場合は、管理する会社を選択してください。
デバイス ページが表示されます。
2. 次のいずれかのタブを選択します。
 - [コンピュータ]- WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversを搭載した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 管理] - WithSecure Elements Connectorを搭載したデバイスを表示します
 - [対象外デバイス] - 顧客のActive Directory内のデバイスを表示します (EPP内のデバイスは表示しません)。
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: 操作方法は**デバイスの詳細**ページでも確認できます。一部の操作方法はそ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では、一定期間オフライン状態が続いたデバイスを自動的に削除するように設定できます。



注: この機能はモバイルデバイスには適用されません。



注: デバイスの自動削除は会社レベルでのみ設定できます。

自動削除を管理するには

1. 下[環境]選択[デバイス]サイドバーに表示されます。
の**デバイス**ページが開きます。
2. を選択します。[デバイス]。
メニューが表示されます。
3. [自動削除の管理]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てください。
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。

指定された日数以上オフライン状態が続いたデバイスは、自動的に削除されます。

Active Directory構造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. サイドバーの [環境]で [デバイス]を選択します。
デバイスページが表示されます。
2. 左上隅にある

アイコンを選択してください。
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. 次に、[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のみ表示されます。

ドロップダウンメニューに、選択した企業の *Active Directory* 構成が表示されます。

5. 対象の Active Directory グループを選択すると、グループ内のすべてのデバイスが表示されます。



注：Active Directory の構造は、社内コンピュータから報告されたデータに基づいて構築されるため、完全ではない場合があります。新しい Active Directory ドメインは、そのドメイン内のコンピュータで WithSecure Elements EPP for Computers または WithSecure Elements EPP for Servers が有効化されるまで、WithSecure Elements Security Center には表示されません。

デバイスビューをカスタマイズする

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. サイドバーの [環境] で [デバイス] を選択します。
デバイス ページが表示されます。
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. 表の右上隅にある


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. 表の列の順序を変更するには：
 - 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) 表の右上隅にある


を選択してください。
 - 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 ページに表示できるデバイス数よりも多い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、前のページまたは次のページに移動してください。
8. 右上隅の [表示] を選択し、]>[を付けて保存] をクリックすると、カスタマイズした表示を保存できます。



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から、[削除]を選択します。

診断データのリクエスト

診断ファイルをリモートでアップロードするようにリクエストできます WithSecureサポートチーム。

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 の管理者は該当デバイスを選択し、顧客に診断情報 (WSDIAG) ファイルの収集と WithSecure Elements Security Center へのアップロードを許可するよう依頼できます。この診断ファイルは、問題とその根本原因の特定に役立ちます。



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. ログインして Elements Security Center。
2. 複数のアカウントを管理している場合は、該当する顧客アカウントにアクセスしてください。
3. 正しいアカウントにログインしたら、[環境][デバイス]を選択し、該当するデバイス (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。
4. 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 > [デバイスを]選択し、右側の3つの点アイコンを選択して、[操作の管理]を選択します。WSDIAG操作が[デバイスへの配信待ち]ステータスでリストに表示されているかどうかを確認します。

5. ユーザーが診断ファイル (WSDIAGファイル) の収集を許可していることを確認してください。そのためには、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。
6. ユーザーが診断ファイル (WSDIAG) の収集を許可したら、顧客アカウントの「操作の管理」ページに戻ってください。
7. ステータスが [成功、操作が実行されました]に変更されているかどうかを確認してください。
8. 「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ます。
9. サポートチケットに参照番号を含めてください WithSecureサポート。



注: サポートチケットでは、WithSecure参照番号を確認し、詳細な調査のためにファイルをダウンロードできます。

10. 必要に応じて、[アクション]列の3つの点アイコンを選択して診断ファイルをダウンロードしてください。



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。

1.1.10 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復旧措置を実行します。
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、サービスに直接関連するデータのみが含まれます。WithSecure
ご自身の文書やその他のデータのバックアップを取るのは、あなたの責任です。

第 章2

Elements Endpoint Protectionの概要

トピック：

- WithSecure Elements EPP を使い始めましょう

Elements Endpoint Protectionの概要

WithSecure Elementsは、コンピュータやモバイル端末から電子メールやサーバーレベルまで、あらゆるレベルのセキュリティを提供します。

WithSecure Elementsを使用すると、Elements EPP、Elements Endpoint Detection and Response、およびElements Vulnerabilityエージェントをインストールおよび管理できます。

エンドポイント保護は、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およびMacデスクトップコンピュータを保護します。
- **[WithSecure Elements EPP for Servers]**は、WindowsおよびLinuxサーバー向けのセキュリティソリューションです。最新のツールを搭載した新しいWithSecure Elements EPP for Serversは、Windowsサーバーに最も強力な保護機能を提供します。



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、どちらも同じインストーラーを使用します。両製品には、DataGuardによるランサムウェア対策機能の強化と、Application Controlによるアプリケーション固有の制限機能を備えたプレミアムバージョンが含まれています。

- **[WithSecure Linux Security]**は、Linuxサーバー向けのセキュリティソリューションです。
- **[WithSecure Elements Exposure Management]**は、ネットワーク検出とポートスキャン、プラットフォームと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を実行できる脆弱性管理ソリューションです。
- **[WithSecure Elements Mobile Protection]**は、AndroidおよびiOSデバイス向けに、プロアクティブな包括的な保護を提供します。フィッシング詐欺を阻止し、有害なウェブサイトへのアクセスを防止し、マルウェアをブロックし、潜在的な脆弱性を検出し、公共Wi-Fiなどの安全でないネットワークに接続した際にネットワークトラフィックのプライバシーを保護します。

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。
- DeepGuard- 高度な技術を用いて、DeepGuardヒューリスティック分析、行動分析、評判分析に基づいて、非常に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) - USBメモリ、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たシステムへの脅威のアクセスを防止します。また、読み取り専用アクセスを許可するなどして、データ漏洩も防止します。

WithSecure Elements Mobile Protectionは、ネットワークゲートウェイ、危険なコンテンツからの保護など、多くの高度な機能を提供します。独自の「ウルトラライト」テクノロジーにより、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、Microsoft Intuneなどの外部MDMシステムと連携して使用できます。



注：MDMの使用方法に関する詳細については、「Elements Mobile Protection」を参照してください。

2.1 WithSecure Elements EPP を使い始めましょう

デバイスの追加、管理者アカウントの作成、プロファイルの作成を行うことで、WithSecure Elements Security Center の利用を開始できます。

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パートナーから製品を購入すると、通常、パートナーは管理対象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。これがあなたに該当する場合、次のメールが届いています。WithSecure一時パスワードと、Elements Security Centerにログインするためのリンクが提供されます。



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場合でも、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、管理対象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。そのためには、会社のセルフ登録リンクを使用してWithSecure Elements Security Centerにアクセスしてください。

このクイックスタートガイドでは、WithSecure Elementsで Elements Security Center。

1. WithSecure Elements Security Centerのサインインページで、ビジネスアカウントの認証情報を使用して WithSecure Elements Security Centerにログインしてください。
2. 製品のインストールを促すメール招待状を送信するか、自動展開用のインストーラーをダウンロードすることで、管理対象組織にデバイスを追加できます。
3. 管理者アカウントを作成し、管理者情報を入力してください。
4. 管理対象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てください。
5. プロファイルをデバイスに割り当てます。



第 章3

システム要件

システム要件

サポートされているブラウザとOSの一覧。

対応ブラウザ の WithSecure Elementsポータルは、以下のブラウザの最新バージョンをサポートしています。

Microsoft Edge
Mozilla Firefox
Google Chrome
Safari

対応オペレーティングシステム



注: の WithSecureベンダーが現在サポートしているオペレーティングシステムのみをサポートします。詳細については、WithSecureオペレーティングシステムのサポートポリシーについては、「製品のアップデートとサポート対象バージョン」をご覧ください。ベンダーがサポートを終了したプラットフォームの長期サポートをご希望の場合は、営業担当者にお問い合わせください。

Windows ワークステーション

- Microsoft Windows 11 (x86-64またはARM64エディション)



注: クライアントには .NET Framework 4.7.2 が必要で、それが不足している場合は自動的にインストールされます。



注: すべてのオペレーティングシステムでTLS 1.2が構成され、有効になっている必要があります。また、オペレーティングシステムはMicrosoft Azureコード署名証明書をサポートする必要があります。詳細については、Microsoft Azureコード署名のサポート記事を参照してください。

Windows サーバー

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials
- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core
- Microsoft® Windows Server 2025 Standard
- Microsoft® Windows Server 2025 Datacenter
- Microsoft® Windows Server 2025 Core



注: Windows Server 2016 Nano は対応されていません。

以下を除く Microsoft Windows Server editions。

Itanium プロセッサ向け Windows Server
Windows HPC editions (特定のハードウェアを対象)
Windows MultiPoint Server
Windows Home Server

**注:**

- すべてのオペレーティング システムには最新のサービス パックがインストールされ、TLS 1.2 が構成され有効になっている必要があります。また、TLS 接続を確立できるように、Microsoft グループポリシーの[**ルート証明書の自動更新を無効にする**]オプションが無効になっていることを確認してください。オペレーティング システムは、Microsoft Azure コード署名証明書をサポートしている必要があります。詳細については、Microsoft Azure コード署名のサポート記事を参照してください。
- クライアントには .NET Framework 4.7.2 が必要で、それが不足している場合は自動的にインストールされます。
- パフォーマンスとセキュリティの理由で本製品は NTFS パーティションにのみインストールできます。

macOS

注: すべてのオペレーティングシステムで監査と TLS 1.2 が構成され、有効になっている必要があります。

macOS バージョン 27 「ゴールデンゲート」
macOS バージョン 26 「Tahoe」
macOS バージョン 15 「Sequoia」

Linux

注: すべてのオペレーティングシステムで監査と TLS 1.2 が構成され、有効になっている必要があります。

次の 64 ビット (AMD64/EM64T) ディストリビューションがサポートされています。

- アルマ Linux 8、9、10
- Amazon Linux 2、2023 年
- デビアン 11、12、13
- Oracle Linux 8、9、10
- RHEL 8、9、10
- ロッキーマ Linux 8、9、10
- SUSE Linux Enterprise Server 15 (サービスパック 6)
- Ubuntu 20.04、22.04、24.04



注: バージョン 3.16 より前のカーネルを使用しているオペレーティングシステムには、監査パッケージがインストールされている必要があります。より優れた検出機能とパフォーマンス向上のため、カーネルバージョン 5.10 以降を実行することをお勧めします。

以下の 64 ビット (ARMv8/AArch64) ディストリビューションがサポートされています。

- アルマLinux 9、10
- Amazon Linux 2023
- デビアン 11、12、13
- Oracle Linux 9、10
- RHEL 9、10
- ロッキーマシン 9、10
- Ubuntu 22.04、24.04

対応言語 英語、チェコ語、デンマーク語、オランダ語、エストニア語、フィンランド語、フランス語、フランス語 (カナダ)、ドイツ語、ギリシャ語、ハンガリー語、イタリア語、日本語、ノルウェー語、ポーランド語、ポルトガル語、ポルトガル語 (ブラジル)、ルーマニア語、ロシア語、スロベニア語、スペイン語、スペイン語 (ラテンアメリカ)、スウェーデン語、トルコ語、繁体字中国語 (香港)、繁体字中国語 (台湾)、簡体字中国語 (中国)。

ネットワーク要件 表1:ネットワークアドレスとポート

サービスアドレス	プロトコル	ポート	地域	目的
*.fsapi.com	HTTPS	443	すべて	さまざまなサービスに使用
ew1-fsdiag-upload.s3.eu-west-1.amazonaws.com	HTTPS	443	EMEA	リモートwsdiagアップロード サーバー
ac3ujg1ortm4c-ats.iot.eu-west-1.amazonaws.com	HTTPS	443/8883	EMEA	応答サーバー
c3hqxgihnj763.credentials.iot.eu-west-1.amazonaws.com	HTTPS	443	EMEA	応答サーバー
ew1-famp-prd-system-transfer.s3.eu-west-1.amazonaws.com	HTTPS	443	EMEA	応答サーバー
ue1-fsdiag-upload.s3.amazonaws.com	HTTPS	443	AMER	リモートwsdiagアップロード サーバー
ac3ujg1ortm4c-ats.iot.us-east-1.amazonaws.com	HTTPS	443/8883	AMER	応答サーバー
c3hqxgihnj763.credentials.iot.us-east-1.amazonaws.com	HTTPS	443	AMER	応答サーバー
ew1-famp-prd-system-transfer.s3.us-east-1.amazonaws.com	HTTPS	443	AMER	応答サーバー
ane1-fsdiag-upload.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	リモートwsdiagアップロード サーバー

サービスアドレス	プロトコル	ポート	地域	目的
ac3ujg1ortm4c-ats.iot.ap-northeast-1.amazonaws.com	HTTPS	443/8883	APAC	応答サーバー
c3hqxgihnj763.credentials.iot.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	応答サーバー
ew1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	応答サーバー

第 章4

導入

トピック：

- Windowsの展開方法
- Macデバイスの展開方法
- Linuxデバイスの展開方法
- モバイルデバイスの展開方法
- メールでユーザーを招待する

導入

WithSecure Elementsソフトウェアをインストールするための、最も一般的な導入方法とツール。

デバイスにソフトウェアをインストールするための方法やツールはますます増えています。エンドポイントデバイスを保護するには、通常、WithSecure Elements Agentをデバイスにインストールして有効化する必要があります。

WithSecure Computer ProtectionおよびWithSecure Server Protectionソフトウェア用のWithSecure Elements Agentインストーラーは、以下の場所からダウンロードできます。**管理 > ダウンロード** WithSecure Elements セキュリティセンターにて。



注： WithSecure Elements Mobile Protectionのソフトウェアパッケージは、App Store (iOS) またはGoogle Play (Android) を通じて配信されるため、Elements Security Centerからダウンロードすることはできません。必要な WithSecure Elements Endpoint Protectionソフトウェアのインストーラーをダウンロードし、保護対象デバイスに転送したら、インストールを開始できます。

4.1 Windowsの展開方法

Windowsデバイスに WithSecure Elements Endpoint Protectionを配布およびインストールする方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者は、WithSecure Elements Security CenterからEXEインストーラーまたはMSIパッケージをダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な展開や完全自動化された展開の場合、以降のトピックでは、グループポリシー (GPO)、Microsoft Configuration Manager (SCCM)、Microsoft Intune、またはその他のエンタープライズツールを使用して、多数のデバイスに製品をインストールする方法について説明します。

4.1.1 EXEファイルを使用して手動でデプロイする

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。

デバイスに対する管理者権限が必要です。

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。

製品をインストールするには

1. ログインして WithSecure Elements Security Center。



注： または、ログインページの「**ダウンロード**」リンクを選択することで、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。ただし、製品のサブスクリプションキーが必要です。

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. ダウンロードしたい製品の下にある [**EXE**] を選択してください。



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. まず会社を選択し、次にサブスクリプションキー付きの製品を選択し、最後に [**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 (.exe) を見つけてダブルクリックし、インストールを開始してください。
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：(サイドグレードがない場合) サイレントインストールを実行するには、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。これを行うには、インストーラ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. インストールに使用する言語と再起動オプションを選択し、[**次へ**] を選択します。
7. 使用許諾契約書をお読みください。契約内容に同意して続行するには、[**同意する**] をクリックしてください。
8. 画面上の指示に従います。

コマンドラインパラメータ

ご使用の環境の特定の要件に合わせて、.exeインストーラーを設定してください。

.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、以下のコマンドラインパラメータを使用できます。

--profile-id <ID> プロファイルIDの値を指定します。例：--profile-id 18062053。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 (割り当て済みのコンピュータ番号と最終編集日の下) に表示されます。

--language <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。

-l <id>

ID値には次のいずれかを指定できます：en、cs、da、de、el、en、es-MX、es、et、fi、fr-CA、fr、hu、it、ja、ko、nl、no、pl、pt-BR、pt、ro、ru、sl、sv、tr、zh-HK、zh-TW、zh。

例：

```
C:\Users\<username> \Downloads>installer.exe --language en
```

- 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。
- 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 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。
- 競合する名前の前に [skip-reboot] を追加すると、サイドグレードが再起動を必要しないことを示すことができます (サイドグレードは実行されます)。
- `--skip-sidegrade "Sophos Cloud Endpoint|HitmanPro.Alert"`
 - `--skip-sidegrade "HitmanPro.Alert|SG16|SG1"`
 - `--skip-sidegrade "*" - サイドグレードは行いません (以下を含む) WithSecure 製品 )`
 - `--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 Exposure 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。
- 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

インストール時に.NETをインストールしないようにしてください。.NETを自分で管理するには、[プロファイル] > [一般設定] > [自動更新]で、[製品更新時に **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>

マルウェア署名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に、帯域幅の使用量を最小限に抑えるために、製品にコネクタを使用するように指示します。製品のインストール時には、すべてのリクエストが最終的な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://connector.local:80`

--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。

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。

アンインストールコマンド



重要: 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。

表2:アンインストールコマンドの例

実行ファイル	実行パラメータ	説明
<code>fs_uninstall_32.exe</code>	<code>[--silent]</code>	<code>fs_uninstall_32.exe</code> を実行するには、 <code>C:\Program Files\F-Secure\PSB</code> ディレクトリ、または <code>C:\Program Files (x86)\F-Secure\PSB</code> ディレクトリに移動してください。サイレントモードで実行するには、 <code>--silent</code> パラメータを使用できます。
<code>msiexec</code>	<code>/x {PRODUCT_CODE} [/qn]</code>	製品コードを見つけるには、PowerShell コマンドラインに次のコマンドを入力します: <code>get-wmiobject Win32_Product Format-Table IdentifyingNumber, Name.</code> サイレントモードにするには、 <code>/qn</code> パラメータを使用できます。



注: オプションのパラメーターは [角括弧] 内にあります。

4.1.2 MSIファイルを使用して手動でデプロイする

MSIファイルを使用すると、WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversをオフラインでインストールできます。



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、以下を参照してください。MSIプロパティページ55。

製品をインストールするには

1. ログインして WithSecure Elements Security Center。



注: または、ログインページの「**ダウンロード**」リンクを選択することで、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。ただし、製品のサブスクリプションキーが必要です。

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. ダウンロードしたい製品の下にある [**MSI**] を選択してください。

インストールファイルがダウンロードされます。

4. ダウンロードしたインストールファイル (.msi) を見つけてダブルクリックし、インストールを開始してください。

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方法については、以下を参照してください。MSIプロパティ ページ55

。



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。

MSIプロパティ

ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

.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 ページ58。

.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。

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。

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>ダウンロード>msiexec /i installer.msi
```

VOUCHER

購読キーを設定します。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はこのプロキシ経由で送信されます。例：PROXY_SERVER=http://proxy.local: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"

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

サーバー上で Windows Defender を無効化および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。Windows Server 2016 以降のバージョンには Windows Defender は含まれていますが、セキュリティセンターは含まれていないため、別のセキュリティソフトウェアがインストールされても Windows Defender は自動的に無効化されません。通常は、グループポリシーオーダー (GPO) またはその他の標準的な方法で 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使用できます。

CONNECTOR_PROXY

マルウェア署名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に、帯域幅の使用量を最小限に抑えるためにコネクタを使用するように製品に指示します。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を経由して送信されます。例：CONNECTOR_PROXY=http://connector.local:80

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。

WithSecure MSI変換ツールを使用する

WithSecureMSI変換ツールを使用して、パラメータが埋め込まれたカスタマイズされたクライアントインストーラを作成します。

このツールを使用すると、インストーラーにカスタムパラメーター（たとえば、サブスクリプションキー）を埋め込むことができるため、インストール時にそれらを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の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、場合によってはMSIファイルが必須となります。ただし、必要に応じて他の方法を使用することもできます。

のWithSecureMSI変換ツールを使用すると、カスタマイズされたMSIファイルを作成するか、構成情報のみを含むMSTファイルを作成するかを選択できます。どちらを選択するかは、以下の点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、最新バージョンのWithSecure Elements Agentを MSI 形式でダウンロードしてください。



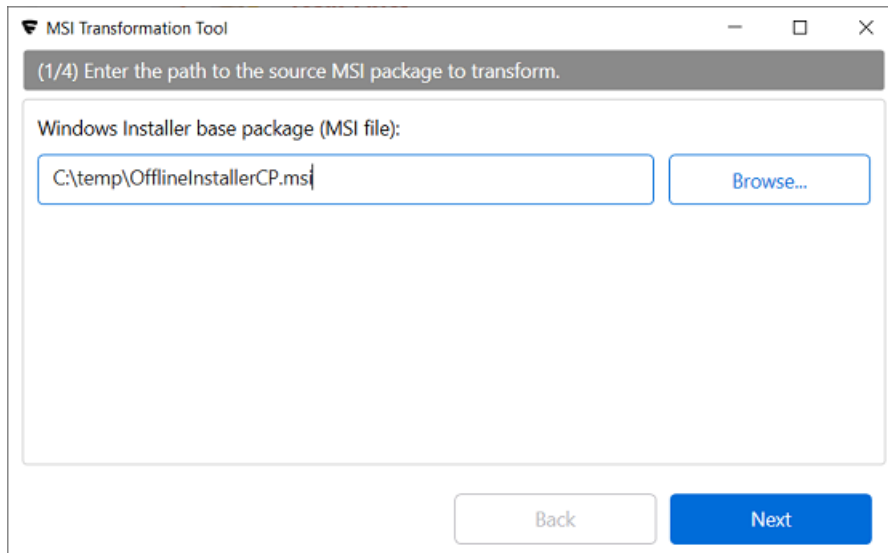
重要: MSIファイルの有効期限は8ヶ月です。8ヶ月以上前にMSIファイルをダウンロードした場合は、新しいMSIファイルをダウンロードする必要があります。

- ダウンロード WithSecureWithSecureダウンロードサイトからMSI変換ツール (FsMsiTool_ui.exe) を入手してください。
- 利用可能なオプションを知る MSIプロパティページ55。

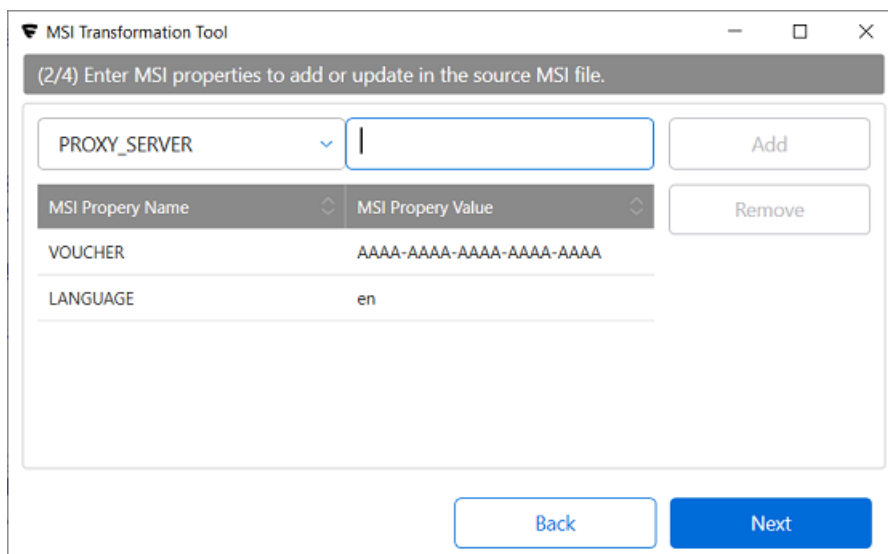
MSI変換ツールを使用するには

1. MSI 変換ツールを起動します。

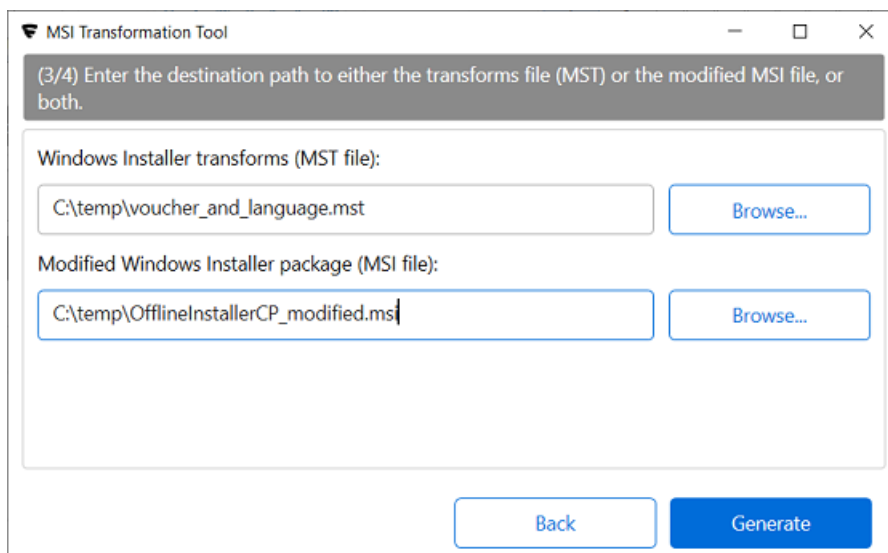
2. 開いたページで、Elements Agentの MSI インストーラーへのパスを指定し、[次へ]を選択します。



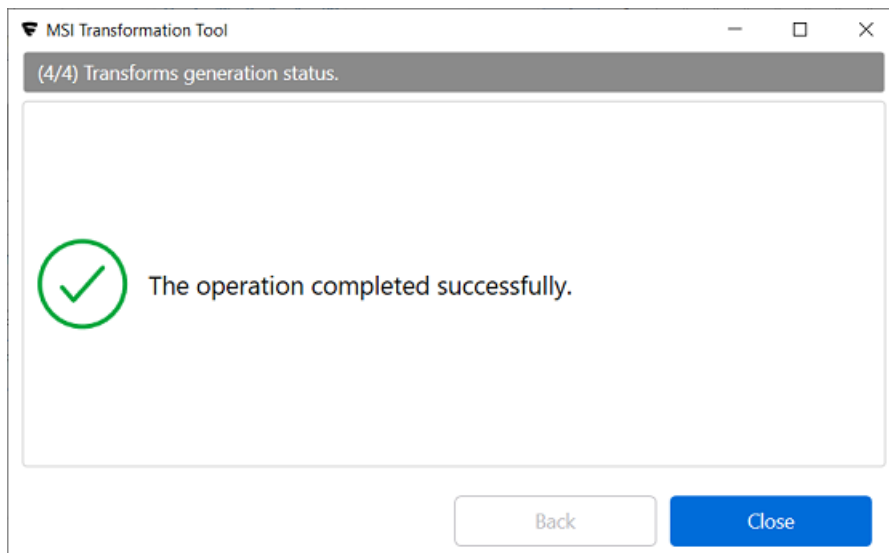
3. 追加する1つ以上のMSIプロパティを指定し、[次へ]を選択します。



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。



関連資料

コマンドラインパラメータページ51

ご使用の環境の特定の要件に合わせて、.exeインストーラーを設定してください。

MSIプロパティページ55

ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

4.1.3 Active Directory GPO を介して展開

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。

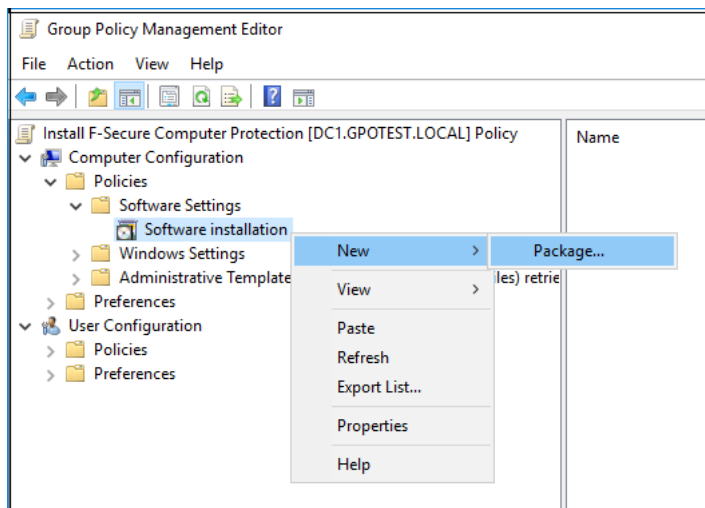
- Active Directory 環境
- ターゲットドメインのすべてのメンバーにユニバーサルCRTがインストールされている必要があります。通常、これはWindowsアップデートに含まれており、定期的に更新されるシステムには存在します。インストール時に検出できない場合は、ターゲットシステムのWindowsイベントログに対応するエラーメッセージが出力されます。手動でインストールまたは修復する必要がある場合は、次のリンクを使用してください: Visual C++ 再頒布可能パッケージ (x86) インストーラー。
- 対象ドメインのすべてのメンバーは、すべての UI 機能が正しく機能するために .NET Framework 4.7.2 をインストールしている必要があります。
- 指示に従って準備されたカスタマイズされた MSI または MST ファイル (推奨) WithSecure MSI変換ツールを使用するページ58サブスクリプションキーを指定するために、VOUCHERパラメータを少なくとも追加していることを確認してください。

WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Servers は、GPO や 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場合は、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、およびその他の設定を準備する必要があります。その後、パッケージを使用してポリシーを定義し、デバイスに適用する必要があります。

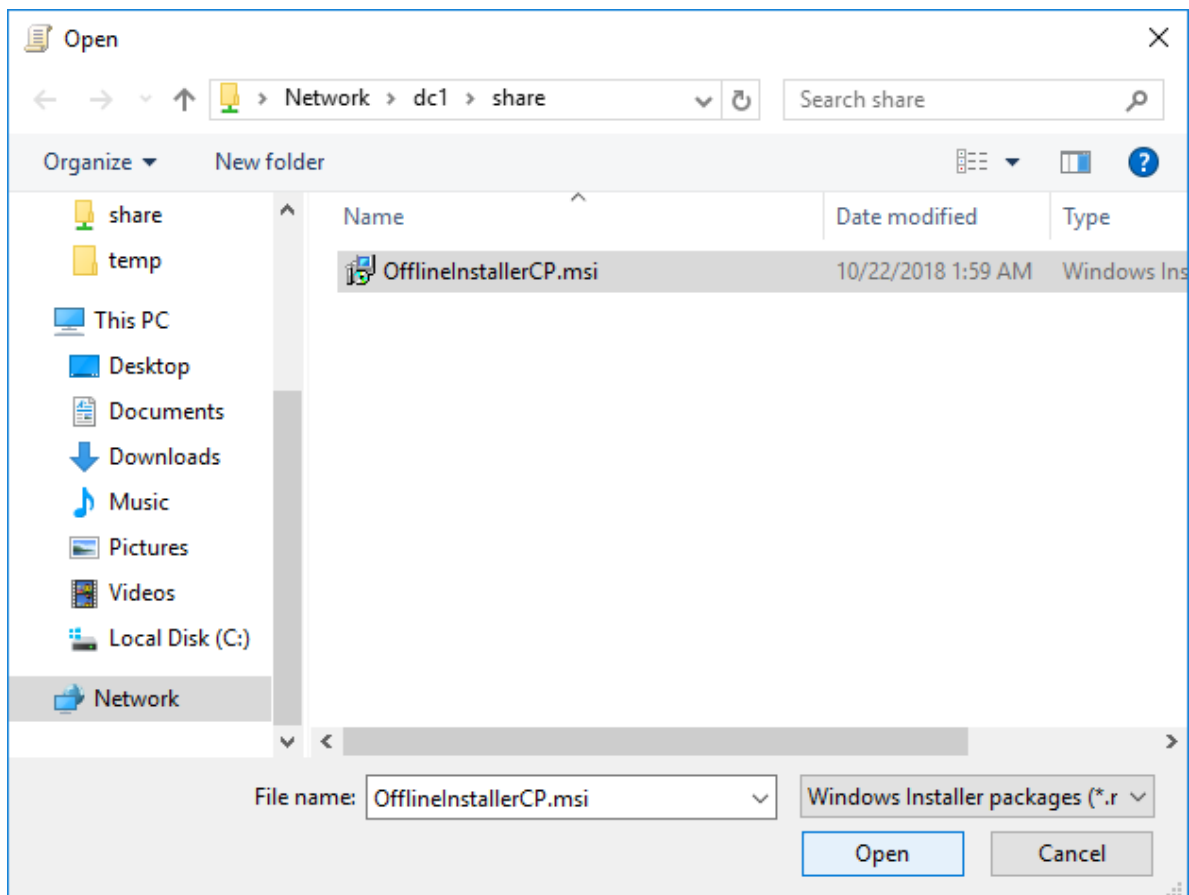
製品をインストールするには

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。

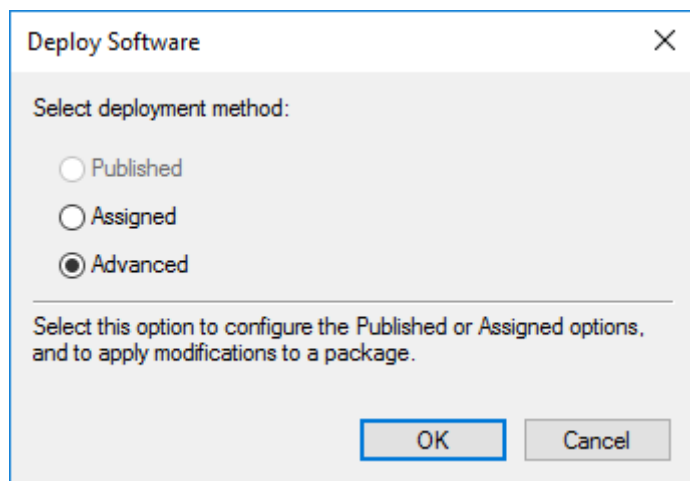
2. グループポリシー 管理コンソールを開き、ドメインに関連付けする新しいグループポリシー オブジェクトを作成します。
3. [コンピューターの構成] > [ポリシー] > [ソフトウェア設定] > [ソフトウェアのインストール]に移動します。
4. 右側のペインを右クリックして、[新規] > [パッケージ...]を選択します。



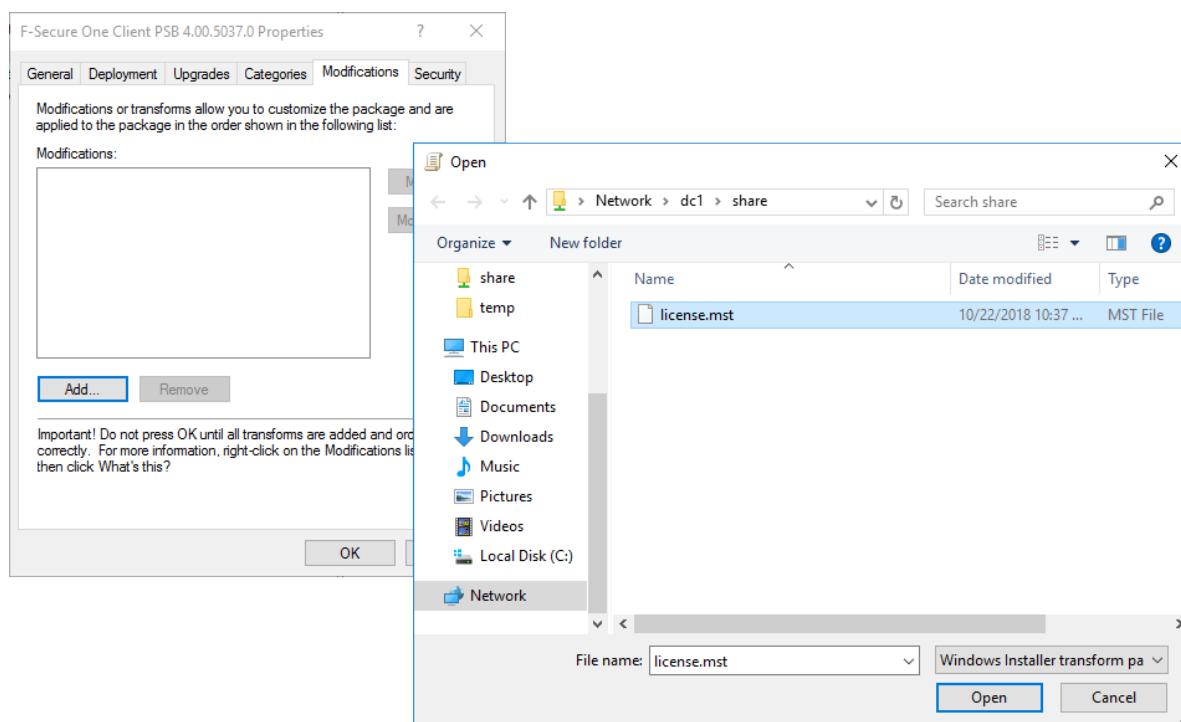
5. 開いているファイルウィンドウで、OfflineInstallerCP.msiを選択し、[開く]を選択します。



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設定し、[OK]を選択します。

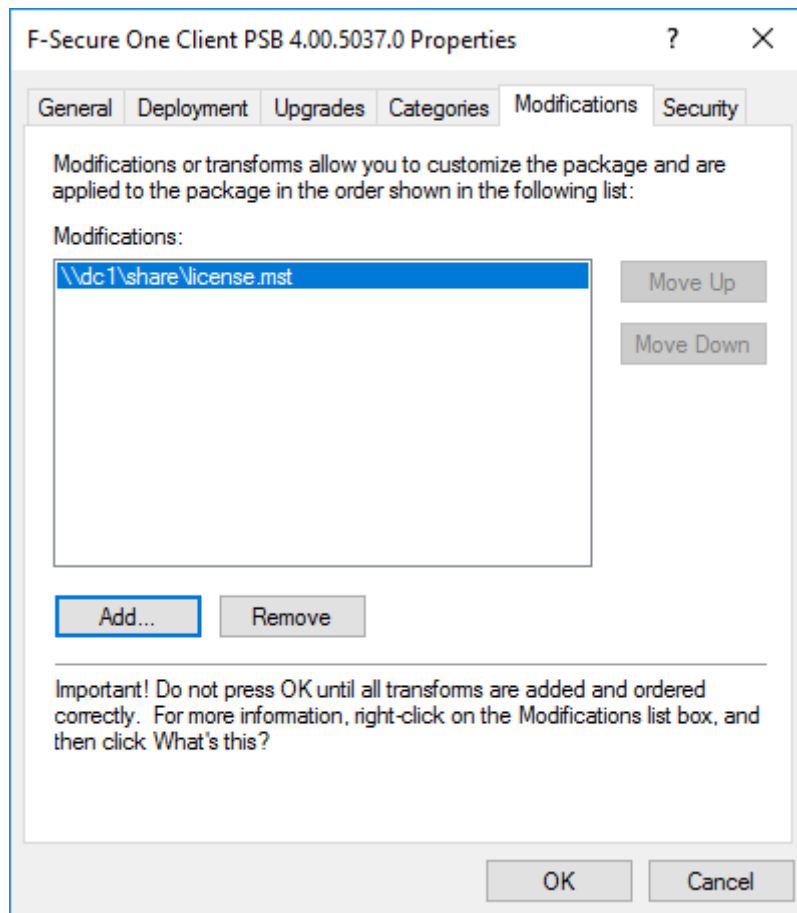


7. [変更]タブに移動し、[追加...]を選択します。
8. ファイルを開くウィンドウで、license.mst (先ほど FsMsiTool.exe で作成した変換ファイル) を選択し、[開く]を選択します。これにより、変換ファイルのパスがGPO設定に追加されます。



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

9. 設定を保存するには [OK] を選択してください。



WithSecure Elements EPP for Computersは、GPO経由での展開準備が整いました。

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。

4.1.4 Microsoft Configuration Manager を使用した Elements Agent の展開

この展開方法は、Microsoft Configuration Manager (SCCM/MECM) を使用している企業で、WithSecure Elements エージェントを管理対象の Windows デバイスに配布したい場合に適しています。

WithSecure Elements Agent MSI は、Configuration Manager アプリケーションとして管理対象の Windows デバイスに展開できます。展開手順では、この製品固有の設定のみを説明します。



注： Configuration Manager でアプリケーションを作成および展開するための一般的なガイドランスについては、Microsoft のドキュメントを参照してください。

Configuration Manager の展開方式では、既存のソフトウェア配布インフラストラクチャを通じて、インストールのタイミングと対象範囲を制御できます。展開後、Configuration Manager はデバイスインベントリ全体のインストール状況をレポートできます。



重要： インストール後、インストーラーパッケージは Configuration Manager クライアントのキャッシュに保持される必要があります。これは、WithSecure Elements エージェントの自動更新と Configuration Manager との適切な統合に必要です。

Microsoft Configuration Managerを使用してElements Agentをデプロイする

Configuration Managerアプリケーションを作成することで、WithSecure Elements Agent MSIを管理対象のWindowsデバイスに展開できます。

- WithSecure Elements Security Centerから Elements Agentインストーラー (.msi) をダウンロードし、Configuration Managerサイトサーバーからアクセス可能なネットワーク共有にコピーしてください。
- インストールコマンドを実行する際に使用するため、購読キーを保存してください。



注: 以下の手順は、この製品に固有の設定のみを扱っています。Configuration Managerでのアプリケーションの作成と展開に関する一般的なガイダンスについては、Microsoftのドキュメントを参照してください。

Configuration Managerでアプリケーションを作成するには：

1. Configuration Manager コンソールで、**アプリケーション作成ウィザード**を起動し、展開タイプとして **[Windows インストーラー (*.msi ファイル)]**を選択します。
2. **[一般]**ページで、以下の設定を行います。
 - a) **[検出方法を]****[インストールファイルからこのアプリケーションに関する情報を自動的に検出する]**に設定します。
 - b) **[場所を]**ネットワーク共有上の ElementsAgentOfflineInstaller.msi のパスに設定してください。

3. **[一般情報]**ページで、以下の設定を行います。

- a) [インストールプログラムを]以下のコマンドに設定してください。

```
msiexec /i "ElementsAgentOfflineInstaller.msi" /qn VOUCHER="<your-key>"
```

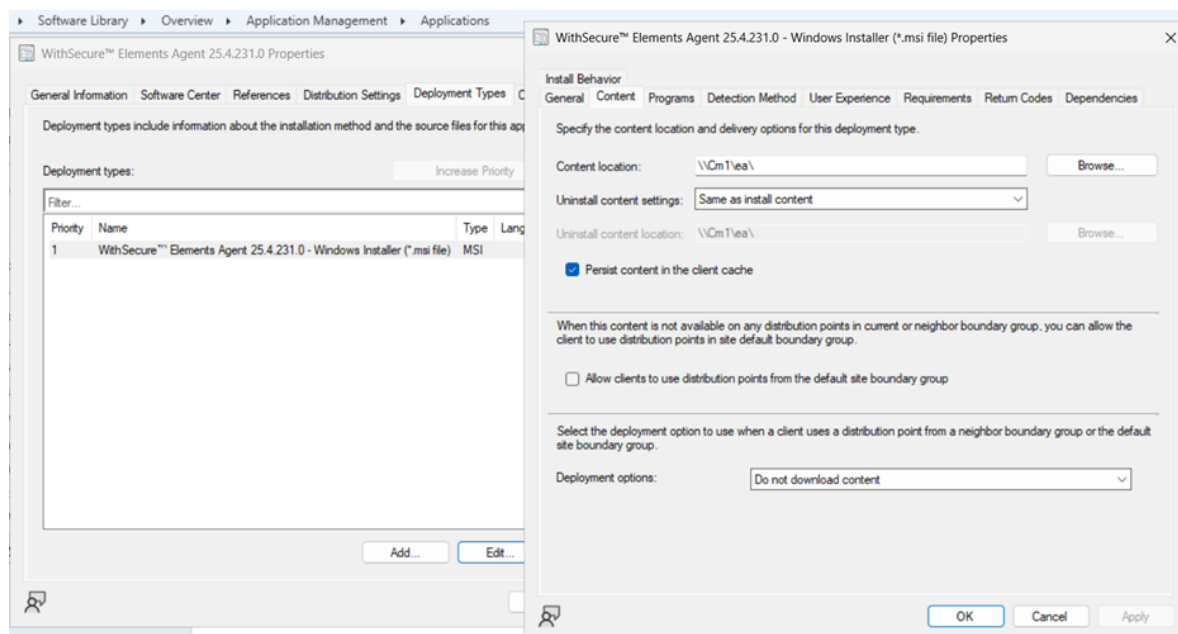


注: <your-key> を Elements Security Center のサブスクリプションキーに置き換えてください。/qn スイッチはインストール中のすべての UI を非表示にします。このコマンドラインでは、その他のサポートされている MSI プロパティを指定できます。

- b) [64 ビット クライアントでインストール プログラムを 32 ビット プロセスとして実行する設定を][いいえ]に設定します。
- c) [インストール動作を][システムに対してインストール]に設定します。

4. ウィザードを完了してアプリケーションを作成してください。

5. [デプロイメントタイプの]設定を開き、[コンテンツ]タブに移動して、[クライアントキャッシュにコンテンツを永続化する]を有効にします。



重要: [クライアントキャッシュにコンテンツを保持する設定]を有効にすると、Configuration Managerがインストール後にインストーラーパッケージをクライアントキャッシュから削除するのを防ぎます。インストーラーがローカルクライアントキャッシュに存在することは、WithSecure Elements Agentのスムーズな自動更新と Configuration Manager との適切な統合に必要です。

4.1.5 Microsoft Intuneを基幹業務 (Windows) ソリューション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場合は、WithSecure Elements Security Centerまたは次のリンク WithSecure Elements Agent オフラインインストーラー)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: Android アプリと iOS アプリを Microsoft Intune MDM を使用して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]。
「**アプリの種類を選択**」 ペインが開きます。
3. [その他の]アプリの種類で [基幹業務アプリ] > [を選択します]。
[アプリを追加する]手順を示すページが開きます。
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、以前ダウンロードしたMSIインストーラーパッケージを選択します。
6. アプリを追加するには、[OK]を選択してください。

7. [アプリ情報]ページで、以下の操作を行ってください。

- a) [アプリのバージョンを無視する]の横にある [はい] を選択すると、Microsoft Intune が自動アップグレードを正しく処理するようになります。
- b) 出版社などの詳細を入力してください (WithSecure) とアプリのコマンドライン引数、例えば VOUCHER=xxxx-xxxx-xxxx-xxxx-xxxx (サブスクリプションキーを挿入) など。



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 プロパティを確認できます。



注: WithSecure Elements EPP エージェントは、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ことがあります。ただし、これにより Microsoft Intune または Windows Autopilot の展開プロセスに支障が生じる可能性があります。この問題を回避するには、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、[課題] ページを開きます。

9. 優先するグループ、ユーザー、またはデバイスを割り当てて、[次へ] を選択します。

10. [レビューと作成] ページで、アプリの値と設定が正しいことを確認してください。

11. [作成] を選択して、アプリを Microsoft Intune に追加します。

関連資料

MSI プロパティ ページ 55

ご使用の環境の特定の要件に合わせて、MSI インストーラーを設定してください。

4.1.6 Intune のインストーラー パッケージを準備します

WithSecure インストーラーをダウンロードし、Microsoft Intune で Windows アプリ (Win32) として展開できるようにパッケージ化します。

WithSecure Elements Security Center または次のリンクから EXE インストーラーをダウンロードしてください: WithSecure Elements Agent インストーラー。



注: Android アプリと iOS アプリを Microsoft Intune MDM を使用して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。

Intune のインストーラー パッケージを準備するには :

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: インストーラーを Windows アプリ (Win32) としてアップロードするのは、標準的な手順です。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。

ElementsAgentInstaller.intunewinパッケージは、Microsoft Intuneにアップロードする準備が整いました。

4.1.7 アプリをMicrosoft Intuneに追加する

WithSecureインストーラーパッケージをMicrosoft Intuneに追加し、Windowsアプリ (Win32) として構成して、デバイスへの自動展開を行います。

Intuneのインストーラーパッケージの準備が完了しました。

アプリをMicrosoft Intuneに追加するには：

1. Microsoft Intuneポータルにログインしてください。
2. [アプリ] > [すべてのアプリ] > [追加]。
「**アプリの種類を選択**」ペインが開きます。
3. [その他の]アプリの種類で [Windows アプリ (Win 32) アプリ] > [を] 選択します。
[アプリを追加する]手順を示すページが開きます。
4. [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インストーラーパッケージを選択します。
5. アプリを追加するには、[OK]を選択してください。
6. [アプリ情報]ページで、以下の詳細を入力してください。
 - ・ 名前: WithSecure Elements エージェント
 - ・ 出版社: WithSecure
7. [次へ]を選択して [プログラム] ページを開きます。
8. [プログラム] ページで、次の操作を行います。
 - a) [インストール] コマンドは次のように入力してください。

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



注： サポートされているコマンドラインオプションはすべてこちらで確認できます。

- b) [アンインストール] コマンドは次のように入力してください。

```
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
```

9. [次へ]を選択して、[要件] ページを開きます。
10. [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べき要件を入力します。



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

11. [次へ]を選択して、[検出ルール] ページを開きます。
12. [検出ルール] ページで、検出ルールのパラメータ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
 - ・ 値の名称：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

13 [次へ]を3回選択して、[課題]ページを開きます。

14 優先するグループ、ユーザー、またはデバイスを割り当てて、[次へ]を選択します。

15 [レビューと作成]ページで、アプリの値と設定が正しいことを確認してください。

16 [作成]を選択して、アプリを Microsoft Intuneに追加します。

このアプリはMicrosoft Intuneに追加されます。

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

ゴールデンイメージを使用して、CitrixおよびVMware Horizonサーバー、その他のVDI環境に製品をインストールします。



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ネットワークインストーラーファイルは、WithSecure Elements Security Centerからダウンロードできます。



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パラメーターを使用できます。詳細については、以下を参照してください。MSIプロパティページ55。

- 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 (SMBIOSGUID) 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SMBIOSGUID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。

関連資料

MSIプロパティページ55

ご使用の環境の特定の要件に合わせて、MSIインストーラーを設定してください。

黄金の像を準備する

ネットワークインストーラとSMBIOS GUIDを使用してゴールデンイメージを準備します。

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、ネットワークインストーラーファイルを実行中のゴールデンイメージテンプレートに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、デバイスを Active Directory コンピューター GUID に関連付けるには、`--use_smbios_guid`の代わりに `--use_ad_guid` を使用できます。また、以下のコマンドライン パラメーターを使用することもできます。EXEファイルを使用して手動でデプロイするページ50そして MSIファイルを使用して手動でデプロイするページ54。

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からサーバーをデプロイする必要があります。手順は以下のとおりです。ゴールデンイメージからサーバーをデプロイするページ70。

黄金のイメージを更新する

最新の製品バージョンとWindowsアップデートを使用して、ゴールデンイメージを更新します。

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にある 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、**[アップデートの確認]**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から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一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を確認するには、**[設定] > [中央管理] > [一意の ID]**に移動します。IDはSMBIOS GUIDではなく、WithSecureイメージを再度復元しても変わらない、入力済みのID。



注：また、Microsoftの以下の手順に従って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。

復元または新規展開したデバイスのプロファイルを設定します。

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。

新しいデバイスに初めてイメージを復元すると、デバイスはWithSecure Elementsセキュリティセンターのプロファイルセクションで定義されたプロファイル割り当てルールに基づいて、会社のデフォルトプロファイルを自動的に取得します。これらの設定を上書きして、プロファイルを手動で指定することもできます。



注：同じSMBIOS GUIDを持つ同じデバイスを再度復元すると、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。デバイスを追加する際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たびにそのプロファイルが使用されます。

1. プロファイルのプロファイルID値をコピーします。
2. 以下のいずれかの方法で、デフォルトのプロファイル割り当てを上書きしてください。
 - コマンドラインに以下のコマンドを入力してください。

```
"%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グループに登録してください。デバイスがシステムに登録されると、Active Directoryグループに割り当てられているデフォルトのプロファイルが使用されます。
- 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。

デバイスは復元時に指定されたプロファイルを使用します。

4.1.9 GPOを通じてブラウザ保護を設定する

Windowsグループポリシーを使用して、Google Chrome、Microsoft Edge、およびMozilla FirefoxにWithSecureブラウジング保護を設定します。



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 Browsing Protectionは、Webブラウザの機能です。インストールされているブラウザで安全な接続 (HTTPS) をサポートします。WithSecureセキュリティ製品。



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 WithSecure不要なウェブコンテンツをブロックし、評価アイコンを表示し、安全な接続が使用されているときに検索エンジンのセーフサーチモードを有効にします。管理者として、WithSecureブラウジング保護機能を有効にし、Windowsグループポリシーを使用してその使用を強制します。

Google ChromeにWithSecureブラウザ保護拡張機能をインストールしてください。

グループポリシーを使用して、Chrome、Edge、またはFirefoxにWithSecureブラウジング保護拡張機能をインストールして有効にします。

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GoogleChrome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てください。
2. 以下の Chrome 管理テンプレートファイルと、システムで使用され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てください。
policy_templates/windows/admx/chrome.admx および google.admx
3. システムで使用されている言語のファイルと言語フォルダを、SYSVOL フォルダ (\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\) にもコピーしてください。

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 (gpmmc.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 ポリシー管理テンプレートの中央ストアを作成および管理する」を参照してください。

5. コンピューターの構成/ポリシー/管理用テンプレート/Google/Google Chrome/拡張機能/強制インストールするアプリと拡張機能のリストを構成するに移動し、ポリシーを次のように編集します。
 - a) ポリシーを有効にするには、[有効]を選択してください。
 - b) 「オプション」で [表示...]を選択し、次の値を入力します。

```
imdndkajeppdomiimjkcblkafeeooghd
```



注：詳細については、Chromeブラウザのポリシー設定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。

Microsoft Edge (Chromium) に WithSecure ブラウザ保護拡張機能をインストールしてください。

グループポリシーを使用して、Chrome、Edge、または Firefox に WithSecure ブラウジング保護拡張機能をインストールして有効にします。



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) 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、およびオペレーティングシステムの下にある **[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]** 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) 抽出したフォルダーから、以下のファイルとフォルダーを C:\Windows\PolicyDefinitions フォルダーと SYSVOL フォルダー (\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\) の両方にコピーします。
 - Microsoft Edge (Chromium) の管理テンプレートファイル: msedge.admx および 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 (gpmmc.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 の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
- コンピューターの構成/ポリシー/管理用テンプレート/Microsoft Edge/拡張機能/サイレントインストールする拡張機能を制御するに移動し、ポリシーを次のように編集します。
 - a. ポリシーを有効にするには、**[有効]** を選択してください。
 - b. 「オプション」で **[表示...]** を選択し、次の値を入力します。

```
aambijcgikmdoehgjhdepcpieghopdl
```

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。

Mozilla FirefoxにWithSecureブラウジング保護拡張機能をインストールしてください。

グループポリシーを使用して、Chrome、Edge、またはFirefoxにWithSecureブラウジング保護拡張機能をインストールして有効にします。



注: Mozilla Firefox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てください。
2. cabファイルを解凍し、以下のMozilla Firefox管理テンプレートファイルと、システムで使用され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 と firefox.admx

3. システムで使用されている言語のファイルと言語フォルダを、SYSVOL フォルダ (\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\) にもコピーしてください。

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 (gpmmc.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. コンピューターの構成/ポリシー/管理用テンプレート/Mozilla/Firefox/拡張機能/拡張機能に移動して、次のようにポリシーをインストールおよび編集します。
 - a) ポリシーを有効にするには、[有効]を選択してください。
 - 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. コンピューターの構成/ポリシー/管理用テンプレート/Mozilla/Firefox/拡張機能/拡張機能の無効化または削除を防止するに移動し、ポリシーを次のように編集します。
 - a) ポリシーを有効にするには、[有効]を選択してください。
 - 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。

4.2 Macデバイスの展開方法

WithSecure Elements Endpoint Protection for Computers (Mac) の配布、インストール、およびアクティベーションの方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者は WithSecure Elements Security Centerからインストーラーをダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な導入や完全自動化された導入の場合、WithSecure Elements Endpoint Protectionソフトウェアは、以下の方法で配布できます。

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



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

4.2.1 SSHを使用して配布する

SSH経由で製品を配布します。

始める前に、.mpkgインストーラーを以下からダウンロードしてください。**管理>ダウンロード**WithSecure Elements Security Centerにあります。.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。

SSHを使用した配布は2つのステップで構成されます。まず製品をインストールし、次にアクティベーターツールを実行してサブスクリプションキーを適用します。

1. scpなどの任意の方法を使用して、.mpkgインストーラーをターゲットマシンにコピーします。
2. SSH経由で対象マシンに接続し、サイレントインストールコマンドを実行します。



注: コマンドとオプションについては、「製品の自動インストール」を参照してください。

3. 同じ sshセッション上で、/Library/ WithSecure /bin/activatorにある アクティベーターツールを、必要な設定パラメータで実行します。



注: アクティベーションコマンドと使用可能なパラメータについては、「サブスクリプションのアクティベーション」を参照してください。

4.2.2 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。

製品を手動で有効化および設定する

MDM (モバイルデバイス管理) を通じて製品を配布し、各デバイス上で手動で有効化および設定を行います。

製品をMDM (モバイルデバイス管理) システムを通じて配布し、その後、各デバイス上で手動で有効化および設定を行ってください。

1. 管理対象組織内のMacコンピュータにソフトウェアをインストールできるように、インストールパッケージをMDMにインポートしてください。

2. ssh を使用して、対象のコンピュータ上で目的の設定パラメータを使用してアクティベータを実行します。
3. コンピュータを起動してください。
4. コンピュータを WithSecure Elements Security Centerに接続します。

カスタムパッケージを使用する

アクティベーションと設定を処理するカスタムパッケージを使用して、MDM経由で製品を配布します。

アクティベーションと設定を処理するカスタムパッケージを使用して、MDM経由で製品を配布します。

1. 管理対象組織内のMacコンピュータに製品をインストールできるようにするには、インストールパッケージをMDMにインポートしてください。
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に付属の 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、macOS のインストール済みパッケージ一覧にパッケージが表示されないことを意味します。これは、システムにファイルがインストールされていないため当然のことです。

3. 必要な数のアクティベーションパッケージを作成してください。
4. ソフトウェア配布ソリューションがサポートする機能に応じて、パッケージを特定のデバイスまたはデバイスグループに割り当ててください。



注: 元のパッケージはそのままの状態、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を使用する

インストールとアクティベーションの両方を単一のパッケージで提供することで、製品を配布します。

インストールとアクティベーションの両方を1つのパッケージでまとめて配布できます。

prepare-installer.shスクリプトを以下のパラメータで実行して、インストールパッケージから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。

4.2.3 MDMプロファイルを使用して製品を設定します

MDMプロファイルを使用すると、管理対象組織内の多数のデバイスに製品をセットアップできます。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 PayloadUUID と PayloadIdentifier の値を、ご自身の値に置き換えてください。例えば、uuidgen コマンドラインツールを使用して UUID を生成できます。

すべて許可する WithSecure システム拡張機能:

```
<?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>

```

コンテンツフィルタリングを許可する WithSecureシステム拡張:



注: macOS 10.15.5以降で必須です。詳細については、Apple Developerドキュメントの WebContentFilterページを参照してください。

```

<?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>
```

フルディスクアクセスを許可する WithSecure プロセス:



注: 必須です。詳細については、Apple Developer ドキュメントの `PrivacyPreferencesPolicyControl.Services` ページを参照してください。

```
<?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>

```

ユーザー通知を許可する WithSecure プロセス:



注: 必須。詳細については、Apple Developer ドキュメントの NotificationSettingsItem ページを参照してください。

```

<?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>
```

- 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。

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

Microsoft Intuneのモバイルデバイス管理プロファイルを使用して、管理対象組織のセキュリティ標準をデバイスに適用します。

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には、デバイスのセキュリティ機能と動作を制御する設定が含まれています。

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プロファイルを作成する

管理対象のmacOSデバイス上で、ユーザーの承認プロンプトなしでネットワークコンテンツフィルタコンポーネントを実行できるようにするMDMプロファイルを作成します。

このプロファイルにより WithSecure管理対象のmacOSデバイス上で、ネットワークコンテンツフィルタコンポーネントがユーザーの承認プロンプトなしで実行される。

- Microsoft Intuneポータルにログインします。
- [デバイス] > [デバイスの管理] > [構成]**
- 新しいポリシーを作成するには、次の手順を実行します。
 - [新規ポリシー][の作成]** を選択します。
 - [macOS]** プラットフォームを選択します。
 - プロファイルタイプとして、**[設定カタログ]** を選択します。
 - [新規作成]** を選択します。
- プロファイルの名前を入力し、**[次へ]** を選択します。
- 構成設定** タブで、**[+ 設定の追加]** を選択します。
- [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]** を選択します。

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プロファイルを作成する

管理対象のmacOSデバイスにアラートを常時表示されるバナーとして表示させ、手動での通知承認を不要にするMDMプロファイルを作成します。

このプロファイルにより WithSecureアラートは、管理対象のmacOSデバイス上に常時表示されるバナーとして表示され、ユーザーが手動で通知を承認する必要はありません。

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) **[新規ポリシー][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]** を選択します。
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でMDMプロファイルを作成する

管理対象のmacOSデバイス上で、ユーザーによる手動承認を必要とせずにエージェントにフルディスクアクセス権限を付与するMDMプロファイルを作成します。

このプロファイルでは、WithSecure管理対象のmacOSデバイスにおいて、エージェントがユーザーによる手動承認なしにフルディスクアクセスを実行できる。

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) **[新規ポリシー][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]** を選択します。
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

管理対象のmacOSデバイス上で、ユーザーによる手動承認を必要とせずにシステム拡張機能が自動的にロードされるようにするMDMプロファイルを作成します。

このプロファイルにより WithSecureシステム拡張機能は、管理対象のmacOSデバイス上で、ユーザーによる手動承認を必要とせずに自動的にロードされます。

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]**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]**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]**を選択します。
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

4.2.5 Jamf管理システム用のMDMプロファイルを作成する

Jamfポータル用のシステム拡張設定を含むMDMプロファイルを作成します。

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してください
2. **[コンピューター]** > **[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**のページで、**[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 **[コンピュータレベル]**を選択します。
 - c) 配布方法のドロップダウンメニューから、**[自動的にインストールする]**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) システム拡張機能の種類ドロップダウンメニューから、**[許可されたシステム拡張機能]**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

Jamfを使用して、macOS Sequoia以降を搭載したデバイス向けに、**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**を作成します。

Jamf で、ユーザーが削除できないようにする構成プロファイルを作成します。WithSecure管理対象デバイス上のシステム拡張機能。

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]**ボタンを選択してください。
8. 次の拡張機能名を入力してください: com.withsecure.wsagent.wssystemextension。
9. テキストフィールドの右側にある **[保存]**を選択します。

10. 「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。
11. プロファイルを保存します。
12. 構成プロファイルをターゲットデバイスに展開します。
13. 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。
の WithSecure システム拡張機能は一覧表示され、無効にしたり削除したりすることはできません。

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用のスマートグループを作成します。



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 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。

4.2.6 製品を自動的にインストールします

コマンドラインインターフェースを使用して、製品のサイレントインストールを実行します。

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は、.mpkg インストーラの名前を .pkg に変更できます。

関連資料

macOS 用インストーラパラメータページ93

インストール時に、これらのインストーラファイル名パターンと アクティベーター コマンドライン オプションを使用して、WithSecure Elements Agent for Computers (Mac) を構成します。

4.2.7 MPKGファイルを使用して製品を手動でインストールします。

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。

デバイスに対する管理者権限が必要です。

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. WithSecure Elements Security Centerの サインインページから、WithSecure Elements Security Centerにログインしてください。



注: または、ログインページの「**ダウンロード**」リンクを選択することで、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。ただし、製品のサブスクリプションキーが必要です。

2. 下[管理]選択[**ダウンロード**]サイドバーに表示されます。
の**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。

関連資料

macOS 用インストーラーパラメータページ93

インストール時に、これらのインストーラファイル名パターンと アクティベーターコマンドラインオプションを使用して、WithSecure Elements Agent for Computers (Mac)を構成します。

4.2.8 フルディスクアクセスを許可する

macOSでディスクへのフルアクセス権限を付与します。

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。

4.2.9 WithSecureシステム拡張機能を許可する

macOSでWithSecureシステム拡張機能を有効にします。

インストール後、macOS は WithSecure許可するまでシステムは拡張します。

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. 許可するために WithSecureシステム拡張機能のポップアップで、[**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。

の WithSecureシステム拡張機能の読み込みが許可されています。

4.2.10 WithSecure Agentの通知を許可する

WithSecureエージェントからの通知を許可します。

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。

WithSecureエージェントは、デバイス上に通知を表示できます。

4.2.11 ネットワークコンテンツをフィルタリングする

ネットワークコンテンツをフィルタリングします。

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。

4.2.12 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](https://unsafe[.]fstestdomain[.]com)。製品ブロックページが表示されるはずですが。

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

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](https://unsafe[.]fstestdomain[.]com)。製品ブロックページが表示されるはずですが。

4.2.13 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有効化した後、**COSMOS**設定でプロファイルIDの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URLに含まれています。例：

<https://emea.psb.f-secure.com/#/c1234567/profiles/computer-protection/edit/1112223/generalSettings>。
 この例では、最初の値 `c1234567` が会社のプロファイルID、2番目の値 `1112223` があなたのプロファイル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. 製品を有効化する前に、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。アクティベーターツールの使用方法と利用可能なオプションの詳細については、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.
```

4.2.14 サブスクリプションを有効にする

製品の定期購入を有効化します。

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 以降に同梱されている アクティベーターツールを使用して、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
- 製品パッケージを手動で変更して、次のようになります:ElementsAgentInstaller[XXXX-XXXX-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付けない場合は、代替手段として二重アンダースコアを使用できます:ElementsAgentInstaller__XXXX-XXXX-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. アクティベーター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てください。

```
/Library/WithSecure/bin/activator --subscription-key "<subscription key>"
```



注: アクティベーターツールは、WithSecure Elements EPP for Computers (Mac)バージョン 17.8.32555 以降に同梱されています。

macOS 用インストーラーパラメータ

インストール時に、これらのインストーラファイル名パターンと アクティベーターコマンドラインオプションを使用して、WithSecure Elements Agent for Computers (Mac)を構成します。

インストーラファイル名にパラメータを埋め込む

インストーラーパッケージのファイル名に、サブスクリプションキー、アクティベーショントークン、プロファイルID、リリースグループを埋め込むことで、インストール時にこれらの値が自動的に適用されます。ファイル名のパターンは、.pkgまたは.mpkgインストーラーパッケージのどちらを使用する場合でも同じです。

表3:インストーラーファイル名のパターン

設定したい内容	ファイル名パターン
サブスクリプションキーまたはアクティベーショントークンがありません	ElementsAgentInstaller.pkg
サブスクリプションキー	ElementsAgentInstaller[<subscription-key>].pkg

設定したい内容	ファイル名パターン
アクティベーショントークン	ElementsAgentInstaller[<アクティベーショントークン>].pkg
購読キー + プロフィール	ElementsAgentInstaller[<subscription-key>][profile=<profile-id>].pkg
アクティベーショントークン + プロフィール	ElementsAgentInstaller[<activation-token>][profile=<profile-id>].pkg
購読キー + リリースグループ	ElementsAgentInstaller[<subscription-key>][cu-group=<group-id>].pkg
アクティベーショントークン + リリースグループ	ElementsAgentInstaller[<activation-token>][cu-group=<group-id>].pkg
購読キー + プロファイル + リリースグループ	ElementsAgentInstaller[<subscription-key>][profile=<profile-id>][cu-group=<group-id>].pkg
アクティベーショントークン + プロファイル + リリースグループ	ElementsAgentInstaller[<activation-token>][profile=<profile-id>][cu-group=<group-id>].pkg



注: ソフトウェア管理ツールが角括弧を受け付けない場合は、代わりにサブスクリプションキーを二重アンダースコア (__) で囲んでください。例：
ElementsAgentInstaller__<subscription-key> __.pkg。



注: プロファイルとリリースグループのパラメータは、括弧内で任意の順序で組み合わせることができます。

アクティベーターのコマンドラインパラメータ

アクティベーターツールを使用すると、インストーラーファイル名の代わりにコマンドラインオプションを使用して同じ値を設定できます。このツールは、WithSecure Elements EPP for Computers (Mac) バージョン 17.8.32555 以降に同梱されています。

表4:アクティベーターのコマンドラインオプション

パラメータ	説明
-p、--profile-id <profile-id>	割り当てるプロファイルのIDを設定します。例： --profile-id 123456。
-t、--tags <タグ>	WithSecure Elements Security Centerに報告するインストール タグを設定します。例: --tags "department=R&D,role=engineer"。
-s、--subscription-key<subscription-key>	有効化するためのサブスクリプションキーを設定します。
-r、--release-group <リリースグループ>	アップデートを確認する際に使用するリリースグループを設定します。
-h、--help	コマンドラインヘルプを表示します。

4.2.15 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。

パッケージに署名および公証を行うには、Appleから配布署名証明書を取得してください。詳細については、Appleのドキュメントを参照してください。

製品パッケージのビルドと署名を行うために設計されたpkgbuild、productbuild、またはproductsignユーティリティを使用して、配布証明書を指定できます。カスタム製品パッケージへの署名が正常に完了したら、それを公証する必要があります。詳細については、「macOSソフトウェアの配布前の公証」を参照してください。



注：インストーラーの `-allowUntrusted` フラグを使用することで、macOS 上でのパッケージインストール時の証明書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。

4.3 Linuxデバイスの展開方法

Linuxデバイスの最も一般的な導入方法。

単一のデバイスまたは小規模な環境の場合は、次のいずれかの方法を選択してください。

- 管理者はインストーラー（下記参照）をダウンロードし、デバイス上で実行します。
- 管理者がユーザーにメールで招待を送ります。ユーザーはエージェントをダウンロードしてインストールするためのリンクを受け取ります。

大規模な展開の場合、これらの方法は、Linux デバイスを使用し、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のディストリビューションに応じて、正しいパッケージ形式を選択してください。

- 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管理モードでインストールすると、WithSecure Elements Security Centerを使用して製品のインストールを一元管理できます。

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。

4.3.1 DEBまたはRPMパッケージを使用して製品をインストールしてください。

DEBまたはRPMパッケージを使用して製品をインストールします。



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ダウンロードページにアクセスし、お使いのオペレーティングシステムとアーキテクチャ (AMD64またはARM64) に合ったDEBまたはRPMインストーラーパッケージをダウンロードしてください。
- b) rootとしてLinuxホストにログインします。
- c) 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。
- d) 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、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。たとえば、--override-distro rhel:8.6を使用します。WithSecureサポート対象外の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: 起動時にHTTPプロキシを使用する場合は、`--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、以下の形式で使用できます。

- `--http-proxy=ホスト:ポート` : 指定されたhostとportを、認証なしでネットワークプロキシとして使用するように本製品を設定します。ポート番号が指定されていない場合、デフォルトでポート番号3128が使用されます。例: `--http-proxy=proxy.example.com:8080`。
- `--http-proxy=username:password@host:port` : これは、指定されたhostとportをネットワークプロキシとして使用し、指定されたusernameとpasswordを認証情報として使用するように製品を設定するものです。ユーザー名またはパスワードに特殊文字が含まれる場合は、URLエンコードを使用します。たとえば、パスワードに「@」文字が含まれる場合は、「%40」と入力します。例: `--http-proxy=abc:x%40y%40z@proxy.example.com:8080`

4.3.2 汎用インストーラーパッケージを使用して製品をインストールします。

汎用インストーラーパッケージを使用して製品をインストールします。



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。

- ログインして WithSecure Elements Security Center。
- 下[管理]選択[ダウンロード]。
- [**WithSecure Elements Agent for Servers** の]項目から、お使いのアーキテクチャ (AMD64 または ARM64) に合ったインストーラーをダウンロードしてください。
- rootとしてLinuxホストにログインします。
- 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。
- AMD64版またはARM64版のどちらを使用しているかに応じて、以下のいずれかのコマンドを実行して、ダウンロードしたインストーラーファイルの実行可能ビットを設定してください。

```
chmod +x ./linuxsecurity-installer.amd64.bin
```

```
chmod +x ./linuxsecurity-installer.arm64.bin
```

2. 使用するバージョンがAMD64かARM64かに応じて、以下のいずれかのコマンドを実行して製品をインストールおよびアクティベートしてください。

```
./linuxsecurity-installer.amd64.bin --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

```
./linuxsecurity-installer.arm64.bin --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：インストール時にサブスクリプションキーとプロファイルIDを指定するには、プログラムを実行する前に、linuxsecurity-installerプログラムの名前を以下のいずれかのパターンに一致するように変更します。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は必ず角括弧[]で囲んでください。名前を変更したインストーラープログラムは、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。たとえば、--override-distro rhel:8.6のように指定します。WithSecureサポート対象外の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：起動時にHTTPプロキシを使用する場合は、--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、以下の形式で使用できます。

- --http-proxy=ホスト:ポート：指定されたhostとportを、認証なしでネットワークプロキシとして使用するように本製品を設定します。ポート番号が指定されていない場合、デフォルトでポート番号3128が使用されます。例：--http-proxy=proxy.example.com:8080。
- --http-proxy=username:password@host:port：これは、指定されたhostとportをネットワークプロキシとして使用し、指定されたusernameとpasswordを認証情報として使用するように製品を設定するものです。ユーザー名またはパスワードに特殊文字が含まれる場合は、URLエンコードを使用します。たとえば、パスワードに「@」文字が含まれる場合は、「%40」と入力します。例：--http-proxy=abc:x%40y%40z@proxy.example.com:8080

4.4 モバイルデバイスの展開方法

モバイルデバイスの最も一般的な展開方法。

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使い捨てのインストールトークンが埋め込まれているため、サブスクリプションキーは非表示になります。これにより、ユーザーはソフトウェアを1台のデバイスにインストールするだけで、そのデバイスがWithSecure Elementsセキュリティセンターに表示されるようになります。

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。情報が何も無い場合は、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るため、端末に個人用プロファイルと仕事用プロファイルの両方がある場合は、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：まずは1台のデバイスで登録テストを行うことをお勧めします。



注：変数は通常、MDMプラットフォーム上で WithSecure Elements Mobile Protectionを構成する際に定義されます。これらの変数は、アプリがメールアドレス、ユーザー名、またはUUIDのいずれで登録されているかを定義します。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」

4.4.1 Google Chrome 用のブラウザ拡張機能をインストールする

Chrome ブラウザを安全に使用するには、Google Chrome 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。

4.4.2 Google Workspace MDM を使用した導入

WithSecure Elements Mobile Protection を Google Workspace MDM と連携させて Android デバイスに展開する。

WithSecure Elements Mobile Protection アプリを Google Workspace に展開するには、管理対象の Android デバイスにアプリを追加して設定し、Chromebook を登録して保護します。

Android アプリを Google Workspace エンドポイント管理に追加する

Android デバイス向け Google Workspace MDM において、WithSecure Elements Mobile Protection を許可されたアプリとして追加します。

WithSecure Elements Mobile Protection を MDM に統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPN とファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elements モバイル保護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 提供するサブスクリプションキーを使用して設定します。

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] > [Webアプリとモバイルアプリ]を選択します。
3. ウェブおよびモバイルアプリのページで、[アプリを追加] > [プライベート Android アプリを追加]を選択します。
4. 管理対象のAndroidアプリのページで、[Playストアを検索] を]選択し、検索ボックスに「モバイル保護要素」と入力します。
5. アプリを選択し、次に [承認] > []を選択します。
6. [ユーザーアクセス]で、希望するオプションを選択し、[続行]を選択してください。
7. [アクセス方法の]項目で、希望するオプションを選択し、[完了]を選択してください。

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

Google WorkspaceでAndroidアプリを設定する

サブスクリプションキーと登録キーを使用して、Google WorkspaceでAndroidアプリを設定します。



注: Google Workspace は変数をサポートしていません。ただし、登録キーのフィールドでは、標準形式のサブスクリプションキーを変数として受け入れます。そのため、サブスクリプションキーはそのまま入力し、メールアドレスは入力しないでください。メールアドレスを入力すると、WithSecure Elements セキュリティセンターですべてのデバイスに同じメールアドレスが表示されます。メールアドレスを空欄にすると、WithSecure Elements Mobile Protectionがインストールされているデバイスにデバイス UUID が表示されます。

1. 管理コンソールページの [管理構成] で、[管理構成の追加] 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セキュリティセンターの以下の場所にあります。**管理 > サブスクリプ > サブスクリプ**。
 - 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。
管理対象構成が作成されました。

4.4.3 VMware Workspace ONE MDM を使用した展開

AndroidおよびiOS上で、VMware Workspace ONE (旧AirWatch) MDMと連携した WithSecure Elements モバイル保護機能の導入。



注: この展開には、ユーザーとデバイスの作成および構成は含まれていません。

VMware Workspace ONEに WithSecure Elements Mobile Protectionアプリをデプロイするには、Workspace ONE が管理する iOS デバイスと Android デバイスにアプリを追加して構成します。

iOSアプリをVMware Workspace ONE MDMに追加する

VMware Workspace ONE MDMに WithSecure Elements Mobile Protection iOSアプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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
- アプリを割り当てて、サブスクリプションキーで構成します。WithSecure提供する、または

Workspace ONEにアプリを追加すると、MDMに登録されているiOSデバイスにアプリを展開および管理できるようになります。

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. **[公開]**タブを選択してください。
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) プラットフォームのドロップダウンメニューから **[Apple iOS]**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。たとえば、**[WithSecure Mobile Protection]**などです。
 - 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]**をクリックしてください。
「アプリケーションの追加 - WithSecure Mobile Protection」ビューが開きます。
 - f) 開いた画面で、**[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、**[保存して割り当てる]**を選択します。

次に、iOSアプリを構成する必要があります。

VMware Workspace ONEでiOSアプリを設定する

VMware Workspace ONE MDMで WithSecure Elements Mobile Protection iOSアプリを設定します。

VMware Workspace ONEにWithSecure Elements Mobile Protectionアプリを既に追加している必要があります。

デバイスに公開する前に、割り当て、制限、および自動有効化の設定を構成してください。

1. **[割り当て] > [配分]**に以下を入力してください。

オプション	説明
名前	アプリ名 (WithSecure Mobile Protection)
説明	課題の説明 (任意)
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てください。たとえば、 [すべてのデバイス] など]です。
アプリ配信方法	アプリの配信方法を選択してください： [自動] 配信または [オンデマンド配信] 。

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]**タブを選択してください。

5. 「**設定の送信**」オプションをオンにして、以下の手順を実行してください。

- a) 次に、**[追加]**を選択して、設定キーとデバイス識別情報を追加し、アプリの自動アクティベーションを可能にします。
- b) **[構成キー]**の下に、以下の構成項目の値を入力してください。
 - *fate_registration_key* - 購読キー
 - *first_name* (オプション) - WithSecure Elements Security Centerでデバイスを識別しやすくなるための名前
 - *last_name* (オプション) - WithSecure Elements Security Centerでデバイスを識別しやすくなるための名前
 - *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) オプションキーを入力するには、**[検索値の挿入]**の横にあるアイコンを選択し、該当する変数を選択してください。アプリケーションがユーザーデバイスに展開されると、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. 開いた画面で、**[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. メイン画面で、**[デバイス][一覧表示]**を選択します。

お使いのデバイスがリストに表示されています。

VMware Workspace ONE MDMにAndroidアプリを追加する

VMware Workspace ONE MDMに WithSecure Elements Mobile Protection Androidアプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elements モバイル保護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提供するサブスクリプションキーを使用して設定します。

Workspace ONEにアプリを追加すると、MDMに登録されているAndroidデバイスにアプリを展開および管理できるようになります。

1. VMware Workspace ONE管理ポータルで、**[アプリと書籍]**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) **[プラットフォームの]**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**[アプリストアを検索]**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] > []を選択します。
6. アプリケーションの編集画面で、「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を表示する

VMware Workspace ONE MDMで管理されているアプリケーションの一覧を表示します。

リストビューページには、Workspace ONEに追加されたアプリが表示されるので、アプリが正常に追加されたことを確認できます。

1. VMware Workspace ONEコンソールウィンドウで、[アプリと書籍]を選択し、[アプリケーション]の下にある [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. [公開]タブを選択してください。

WithSecure Elements Mobile Protectionアプリは、VMware Workspace ONE管理ポータルアプリの一覧に表示されます。

VMware WorkspaceONEを使用したAndroid Enterpriseの導入

VMware Workspace ONEを使用した Android Enterprise環境における WithSecure Elements Mobile Protectionの展開。

VMware Workspace ONEを使用して Android Enterprise環境にアプリをデプロイするには、Android Enterpriseをセットアップし、アプリプロファイルを追加し、WithSecure Elements Mobile Protectionアプリを追加して構成します。

VMware Workspace ONE MDMでAndroid Enterpriseをセットアップする

Android Enterprise環境に WithSecure Elements Mobile Protection Android アプリをセットアップします。

Android Enterprise環境でアプリをデプロイするには、企業はGoogle管理者アカウントを保有する必要があります。また、すべてのユーザーは、事前に定義されたアカウント、または登録時に生成されたアカウントをGoogle管理者アカウントに保有する必要があります。

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てください。
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. 設定画面で、[デバイスとユーザー]の下にある [Android]を選択します。
4. [Android の]項目で、[Android EMM 登録]を選択します。
5. 右上隅のアカウントアイコンを選択し、[Google アカウントを管理]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. Android を職場に導入するページで、[開始する]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の設定が完了したら、[登録設定] タブと [登録制限] タブの設定を承認してください。
9. [保存] を選択します。
Android EMMの登録設定が保存されました。

VMware Workspace ONEにプロファイルを追加する

VMware Workspace ONE を介して展開された Android デバイス上でのアプリの動作を制御する SDK プロファイルを追加します。

SDKプロファイルは、Workspace ONEを通じてAndroidデバイスにアプリがデプロイされた後のアプリの動作を制御します。

1. VMware Workspace ONE管理ポータルで、**[アプリと書籍]** > **[すべてのアプリと書籍]** > **[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]** > **[SDKプロファイル]** > **[(Android)]**
[新しいAndroidプロファイルの追加] ページが開きます。
4. **[一般]**を選択してください。
5. 新しいプロフィール名と説明を入力してください。
6. **[保存]**を選択します。

Androidアプリを追加する

Android Enterprise 環境において、WithSecure Elements Mobile Protection Android アプリを VMware Workspace ONE MDM に追加します。

VMware Workspace ONEに WithSecure Elements Mobile Protectionアプリを追加して、管理対象の Android Enterpriseデバイスに展開できるようにします。

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]**に移動します。
[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) **[プラットフォームの]**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てください：モバイル保護要素。
 - c) **[次へ]**を選択します。
アプリのページが開きます。
4. WithSecure Elementsモバイル保護を選択してください。
5. WithSecure Elements Mobile Protectionビューで、**[承認]** > **[]**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の]**ドロップダウンメニューから **[MP strings @ 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、以下の手順を実行してください。
 - a) 「名前」フィールドに、配布物の名前を入力します。たとえば、「alldevices」などです。
 - 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、**[アプリケーション構成]**を選択し、以下の手順を実行します。
 - a) **[登録キー]**欄に、製品のサブスクリプションキーを入力してください。



注: WithSecure Elements Mobile Protectionのサブスクリプションキーは、WithSecure Elements Security Centerの[エンドポイント保護] > [サブスクリプション] セクションで確認できます。

- b) 「名 (任意)」欄に [{FirstName}]と入力してください。
- c) 「姓 (任意)」欄に [{LastName}]と入力してください。
- 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) 「メールアドレス (任意)」欄に [{EmailAddress}]と入力してください。
- 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。

VMware Workspace ONEでAndroidアプリを設定する

VMware Workspace ONE MDMのAndroid Enterprise環境において、WithSecure Elements Mobile Protection Androidアプリを設定します。

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]の下に、以下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。

オプション	説明
運命登録キー	ライセンスキー
名 (任意)	WithSecure Elementsセキュリティセンターでユーザーを識別しやすくする名前
姓 (任意)	WithSecure Elementsセキュリティセンターでユーザーを識別しやすくする名前

オプションキーについては、[ルックアップ値の挿入]を選択し、該当する変数を選択してください。アプリケーションがユーザーデバイスに展開されると、これらのフィールドは自動的に入力されます。

5. [詳細]と「割り当て」の下にあるアプリ設定の残りの項目を入力し、[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。
アプリがリストビューで利用可能になります。

証明書を使用してデバイスを登録します

証明書を使用してデバイスを登録します。

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. 管理対象組織の管理者アカウントを使用して、WithSecure Elementsセキュリティセンターにログインしてください。

2. [サブスクリプション]の下にある



を選択し、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を追加]**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. **[認証情報]** 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. **[保存して公開]** を選択してください。
7. プロファイルをデバイスに割り当てます。

4.4.4 Microsoft Intune MDM を使用した展開

Microsoft Intune MDMと連携した WithSecure Elementsモバイル保護機能の導入 (AndroidおよびiOSデバイスに対応)。

Microsoft Intuneを使用して WithSecure Elements モバイル保護アプリを展開するには、Intune が管理する iOS デバイスと Android デバイスにアプリを追加して構成します。

Microsoft Intune MDMを使用したiOSアプリの導入

Microsoft Intune MDM を使用した WithSecure Elements Mobile Protection iOS アプリの展開。

Microsoft Intuneを使用して iOS アプリを展開するには、WithSecure Elements Mobile Protectionアプリを追加し、管理対象の iOS デバイス向けに管理設定を構成します。

iOSアプリをMicrosoft Intune MDMに追加する

Microsoft Intune MDMに WithSecure Elements Mobile Protection iOSアプリを追加します。

WithSecureElementsMobileProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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
- アプリを割り当てて、サブスクリプション キーで構成します。WithSecure提供する、または

アプリをIntuneに追加すると、MDMに登録されているiOSデバイスにアプリを割り当てて公開できるようになります。

1. Microsoft Intuneポータルにログインしてください。

2. [iOS/iPadOS] > [アプリ] > [追加します]。
「**アプリの種類を選択**」ペインが開きます。
3. [アプリの種類]ドロップダウンメニューから [iOSストアアプリ]を選択し、[選択]を選択します。
4. アプリの追加画面で、[App Storeを検索]を選択します。
「**App Storeを検索**」画面が開きます。
5. 検索フィールドに WithSecure Mobile Protection」と入力してください。
6. [WithSecure Elements Mobile Protection] > [を]選択してください。
[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を会社ポータルの注目アプリとして表示し、[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に追加されました。

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を追加する

管理対象のiOSデバイス向けに、WithSecure Elements Mobile Protectionアプリの構成ポリシーを追加します。

アプリ構成ポリシーを作成するには

1. [アプリ]を選択してください。
「**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. [管理対象デバイス] > [の追加]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、次の操作を行います。
 - a) 「名前」欄に WithSecure Mobile Protection」と入力します。
 - b) **プラットフォーム**のドロップダウンメニューから、[iOS/iPadOS]を選択します。
 - c) [対象アプリ]の横にある [アプリを選択]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) **構成設定フォーマットの**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、以下を参照してください。構成デザイナーを使用するページ109
 - 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わらず、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、以下のキーと値が必須です。

表5: 必須設定キー

キー	種類	説明	値	参考
<i>fate_registration_key</i>	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 モバイル保護アプリから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事項については、「VPNを自動的にオンにする」をご覧ください。

以下のオプションキーは、WithSecure Elements セキュリティセンターで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 の動的変数を使用してください。

表6: オプションのデバイス識別キー

キー	種類	説明
<i>email</i>	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
<i>env</i>	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。
<i>data_usage_permission</i>	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。
<i>diagnostic_usage_permission</i>	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。
<i>create_vpn_profile</i>	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 を使用した WithSecure Elements モバイル保護の展開。

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

Microsoft Intune MDMに WithSecure Elementsモバイル保護Androidアプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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提供するサブスクリプションキーを使用して設定します。

アプリをIntuneに追加すると、マネージドGoogle Playでアプリを承認し、MDMに登録されているAndroidデバイスに割り当てることができます。

1. Microsoft Intuneポータルにログインしてください。
2. **[Android] > [アプリ] > [追加します]**。
「**アプリの種類を選択**」 ペインが開きます。
3. **[アプリの種類]** ドロップダウンメニューから **[管理対象の Google Play アプリ]** を選択し、次に **[選択]** を選択します。
4. **管理対象の Google Play** ビューの検索フィールドに **WithSecure Elements** と入力します。
アプリ 画面が開きます。
5. **[WithSecure Elementsモバイル保護]** を選択してください。
6. 開いた画面で、**[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要求したときに承認済みのままにする]** を選択し、**[完了]** を選択します。
管理対象のGoogle Play 画面が開きます。
8. 左上隅の **[同期]** を選択してください。
Androidアプリの 画面が開きます。
9. **[更新]** を選択し、次に **[WithSecure Elements Mobile Protection]** を選択します。
WithSecure Elementsモバイル保護 ビューが開きます。
10. **[管理]** の下にある **[プロパティ]** を選択します。
WithSecure Elementsモバイル保護プロパティ 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**」 画面が開きます。
12. 「**課題**」 タブで、以下の操作を行います。

- a) [必須]で[すべてのユーザーを追加]を選択します。
- b) [レビュー]を選択して保存します。
- 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に追加されました。

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を追加する

管理対象のAndroidデバイス向けに、WithSecure Elementsモバイル保護構成ポリシーを追加します。

アプリ構成ポリシーは、サブスクリプションキーやその他のアクティベーション値をアプリに送信し、割り当てられたAndroidデバイス上でアプリが自動的にアクティベートされるようにします。

1. [アプリ]を選択してください。
[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. [管理対象デバイス] > [の追加]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、次の操作を行います。
 - a) 「名前」欄に WithSecure Mobile Protection」と入力します。
 - b) プラットフォームの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のドロップダウンメニューから、[個人所有のワークプロファイルのみ]または[完全管理、専用、および企業所有のワークプロファイル]のいずれかを選択します。
 - d) [対象アプリ]の横にある[アプリを選択]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]の下にある「構成設定形式」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:[String]; 設定値: [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以下の場所にあります。**管理 > サブスクリプ**。

- エイリアス: 値の型:[文字列]; 設定値: {{username}}
- メールアドレス: 値の型:[文字列]; 設定値: {{mail}}
- env: 値の型:[整数]; 設定値: 2



注: env設定キーとその値は、VPNエンドポイントが接続する場所を定義します。

- 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。

アプリに権限を付与する

アプリにサイレント起動の権限を付与します。

管理対象のAndroidデバイスでアプリがサイレント起動できるように、必要な権限を付与してください。

1. Microsoft Endpoint Manager管理者センターにログインしてください。
2. [アプリ] > [アプリ構成ポリシー] > [管理対象デバイス] > [を追加します]。



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. 基本情報ページで、以下の詳細を入力してください。

オプション	説明
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. [対象アプリ] の横にある [アプリを選択] を選択します。
[関連アプリの] ペインが開きます。
6. [関連付けられたアプリの] 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] を選択してください。
「アクセス許可の追加」 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。

オプション	説明
プロンプト	ユーザーに承認または拒否を求める
自動付与	ユーザーに通知せずに自動的に承認する
自動拒否	ユーザーに通知せずに自動的に拒否する

10. [レビュー] を選択して保存します。

アプリの設定ポリシーが保存されました。

4.4.5 IBM MaaS360 MDMを使用した展開

IBM MaaS360 MDMと連携したWithSecure Elementsモバイル保護機能の導入 (AndroidおよびiOSデバイスに対応)。

IBM MaaS360にWithSecure Elements モバイル保護アプリをデプロイするには、MaaS360 が管理するiOS デバイスとAndroid デバイスにアプリを追加して構成します。

IBM MaaS360 MDMを使用したiOSアプリの導入

IBM MaaS360 MDMに WithSecure Elementsモバイル保護iOSアプリを追加および展開する。

IBM MaaS360でiOSアプリを展開するには、WithSecure Elementsモバイル保護アプリを追加し、ユーザーに配布してください。

iOSアプリをIBM MaaS360 MDMに追加する

IBM MaaS360 MDMに WithSecure Elementsモバイル保護iOSアプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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
 - アプリを割り当てて、サブスクリプションキーで構成します。WithSecure提供する、または
 1. IBM MaaS360管理者ポータルに管理者としてログインしてください。
 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]**を選択し、次に **[iTunes App Storeアプリ]** を選択します。
 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. **設定**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 **アプリ一覧**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のユーザーに配信されます。

WithSecure Elements Mobile Protection iOS アプリは、IBM MaaS360で定義した配布グループを通じてユーザーに配信されます。アプリを受け取るユーザーをそのグループに割り当ててください。

IBM MaaS360 MDMを使用したAndroid Enterpriseの導入

IBM MaaS360 MDM を使用した Android Enterprise環境における WithSecure Elements モバイル保護の展開。

IBM MaaS360を使用して Android Enterprise環境にアプリをデプロイするには、まず Android Enterprise を構成し、次に WithSecure Elements Mobile Protectionアプリを追加、構成、配布します。

Android Enterprise の構成

IBM MaaS360で Android Enterpriseを設定します。



注： デバイスを登録する前に、Android Enterpriseを設定してください。

1. IBM MaaS360管理ポータルで、[サービスの] > [設定]を選択します。
2. [モバイルデバイス管理]で、管理対象のGoogle Play アカウント経由で[Android Enterprise ソリューションセットを有効にする]([G Suite for Business は使用しない])を選択し、[ここをクリック]します。
「Android管理のGoogle Playアカウントの有効化を確認する」ウィンドウが開きます。
3. [有効にする]を選択してください。
4. セキュリティチェック画面で、パスワードを入力し、[確認]を選択してください。
GooglePlayが開きます。
5. Androidを職場に導入するページで、[開始する]を選択し、以下の手順を実行してください。
 - a) 会社名を入力し、[次へ]を選択してください。
 - b) 連絡先の詳細ページで、名前、メールアドレス、電話番号 (任意) を入力し、[マネージド Google Play 契約を読み、同意します]オプションを選択してから、[確認]を選択します。
6. [登録を完了する]を選択してください。

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

IBM MaaS360にWithSecure Elementsモバイル保護アプリを追加する

IBM MaaS360 MDMに WithSecure Elementsモバイル保護アプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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提供するサブスクリプションキーを使用して設定します。

アプリをアプリカタログに追加すると、登録済みのAndroid端末に配布できるようになります。

1. IBM MaaS360管理ポータルで、**[アプリ]** > **[カタログ]**を選択します。
2. アプリカタログのページで、**[Android]** > **[Google Play アプリ]** > **[を追加]**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。

アプリを設定する

IBM MaaS360 で WithSecure Elements モバイル保護アプリを設定します。

アプリを設定することで、サブスクリプションキーやその他のアクティベーション値が提供され、デバイスにインストールされた後、自動的にアクティベートされるようになります。

1. 「Google Play アプリを追加」ウィンドウの「**構成**」タブで、**[アプリ設定の構成]**を選択し、以下の手順を実行します。
 - 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セキュリティセンターの**[エンドポイント保護]** > **[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て **[確認]**を選択してください。
アプリが追加されます。

アプリを配布する

選択した対象にアプリを配布します。

アプリの設定が完了したら、保護したいデバイス、グループ、または対象に配布してください。

1. アプリカタログページで、**[WithSecure Elements Mobile Protection]**の下にある **[表示]**を選択します。
2. 開いたページの右上隅で、**[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。

4.4.6 Ivanti Endpoint Managementを使用した展開

Ivanti Endpoint Management (旧 MobileIron Cloud MDM) と連携した WithSecure Elements Mobile Protectionの導入。AndroidおよびiOSデバイスに対応。

Ivanti Endpoint Management (旧 MobileIron) に WithSecure Elements Mobile Protection アプリをデプロイするには、管理対象のiOSおよびAndroidデバイスにアプリを追加して構成します。

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

Ivanti Endpoint Managementを使用した iOS アプリの展開。

Ivanti Endpoint Managementを使用して iOS アプリをデプロイするには、WithSecure Elements Mobile Protectionアプリを追加し、アプリ管理を構成し、追加の構成キーを設定します。

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

Ivanti Endpoint Managementに WithSecure Elements Mobile Protection iOSアプリを追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elements モバイル保護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
- アプリを割り当てて、サブスクリプションキーで構成します。WithSecure提供する、または

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

1. Ivanti Endpoint Management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]**を選択してください。
3. WithSecure Elements Mobile Protectionを検索してください。
4. アプリを選択し、次に**[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]**を選択してください。
6. アプリケーションの配布設定を行います。
7. **[次へ]**を選択します。

iOSアプリ管理の設定

iOSアプリの管理を設定します。



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 管理アプリ構成]**を選択し、次に**[+]**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てください。たとえば、WithSecure Elements Mobile Protection ライセンス構成」などです。
 - b) `[fate_registration_key]` フィールドに、WithSecure Elements Endpoint Protection のライセンス キーを入力してください。
3. この設定を関連するデバイスまたはデバイスグループに配布してください。
4. その他必要な設定を行ってください。
5. **[完了]** を選択します。
アプリの設定が作成されました。

追加の構成キー

以下の Ivanti Endpoint Management 変数を使用すると、WithSecure Elements Security Center 上で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。

表7:追加の構成キー

キー	値
<code>fate_registration_key</code>	ABCD-EFGH-IJKL-MNOP
<code>email</code>	<code>\$(userEmailAddress)</code>
<code>first_name</code>	<code>\$(userFirstName)</code>
<code>last_name</code>	<code>\$(userLastName)</code>
<code>alias</code>	<code>\$(userDisplayName)</code>

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

Ivanti Endpoint Management を使用した Android アプリの展開。これには、サブスクリプションキーを使用した WithSecure Elements Mobile Protection の手動設定が含まれます。

Ivanti Endpoint Management を使用して Android アプリをデプロイするには、WithSecure Elements Mobile Protection アプリを追加し、アプリ管理を設定します。

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

Ivanti Endpoint Management MDM に WithSecure Elements Mobile Protection Android アプリを追加します。

WithSecure Elements Mobile Protection を MDM に統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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提供するサブスクリプションキーを使用して設定します。

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

1. Ivanti Endpoint Management MDM 管理ポータルで、**[アプリ]**に移動して **[追加]**を選択します。
2. メニューから **[Google Play]**を選択してください。
3. WithSecure Elements Mobile Protectionを検索してください。
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てください。
6. 必要に応じて、説明欄にアプリ情報を追加してください。
7. **[次へ]**を選択します。
8. 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。
9. 希望する配布グループを選択し、**[次へ]**を押してください。

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設定する

Androidアプリの管理を手動で設定します。

アプリ管理を手動で設定すると、管理対象のAndroidデバイス上でアプリが必要とするアクティベーション、権限、およびインストールオプションを設定できます。

1. **[アプリ構成]** > **[Android の管理構成]**で、プラスアイコンを選択します。
構成設定画面が開きます。
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) **[値が定義されているプッシュ設定のみ]**が選択されていることを確認してください。
 - d) **[登録キー]**の横に、購読キーを入力してください。



注: 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。

- e) メールアドレス欄に、`${userEmailAddress}`と入力してください。
 - f) **[権限の管理]**を選択します。
「**アクセス許可の選択**」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]**をクリックしてください。
 - h) **[ランタイム権限]**の下にあるすべてのドロップダウンメニューから **[自動許可]**を選択し、**[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、以下の手順を実行します。
 - 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]有効にします。
 - 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。
- [アプリ設定]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、以下の手順を実行してください。

- a) 構成設定の名前を入力します。
- b) [おすすめリスト]を選択してください。
- c) [次へ]を選択します。

5. [委任されたデバイスのアクセス許可]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

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アプリを設定する

証明書を使用してAndroidアプリを設定します。

証明書は、管理対象のAndroidデバイスでアプリを有効化するための登録キーに代わる手段となります。

1. [Ivanti Endpoint Management]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]を選択してください。
3. 証明書の名前を入力します。
4. WithSecure Elements Mobile Protection用の WithSecure Elements証明書をアップロードしてください。



注：証明書は WithSecure Elementsセキュリティセンターで確認できます。

5. [次へ]を選択します。
6. 次のページで、証明書の展開に使用するオプションを選択し、[完了]を選択してください。



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

証明書の設定が作成されました。

Ivanti Endpoint Management を使用した Android Enterprise の導入

Ivanti Endpoint Managementを使用した Android Enterprise環境における WithSecure Elements モバイル保護の展開。

Ivanti Endpoint Management のAndroid Enterprise環境に WithSecure Elements Mobile Protectionアプリをデプロイするには、管理対象の Android デバイスにアプリを追加して構成します。

Ivanti (Android Enterprise版) にWithSecure Elementsモバイル保護アプリを追加する

Android Enterprise環境において、WithSecure Elements Mobile Protectionアプリを Ivanti Endpoint Managementに追加します。

アプリをIvanti (Android Enterprise) に追加すると、Google Playとの連携が設定され、管理対象デバイスに配布された際に自動的に起動するようにアプリが構成されます。

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を承認する]を選択します。
 3. [登録を完了する]を選択してください。
 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」画面で、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、次に [承認] > []を選択します。
 8. [完了] > [次へ] > [を選択します]。
 9. 「説明」ビューで [次へ]を選択します。
 10. 委任ビューで、[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]をクリックします。
 12. 設定画面で、[Android の管理構成] 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、[管理構成]の下で、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セキュリティセンターの以下の場所にあります。管理 > サブスクリプ。
- 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. [このアプリ構成を配布する]で [アプリを使用するすべての人]を選択し、[次へ]を選択します。
 15. アプリ構成ページで、[完了]を選択します。
WithSecure Elements Mobile Protectionは、**アプリカタログ**ページに表示されます。

4.4.7 Miradore MDMを使用した展開

WithSecure Elements Mobile Protectionを Miradore MDMと連携させて導入し、AndroidおよびiOSデバイスに対応させる。



注: この展開には、ユーザーとデバイスの作成および構成は含まれていません。

Miradoreで WithSecure Elementsモバイル保護アプリを展開するには、Miradoreが管理するiOSおよびAndroidデバイスにアプリを追加して構成します。

iOSアプリをMiradore MDMに追加する

WithSecure Elements Mobile Protection iOSアプリを Miradore MDMに追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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
 - アプリを割り当てて、サブスクリプションキーで構成します。WithSecure提供する、または
1. Miradore管理ポータルで、左側のメニューから **[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、**[iOSアプリケーション]** > **[を追加]** 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) ステップ1で、**[App Store]** を選択し、次に **[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 モバイル保護
 - 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。
 - **[デバイスの登録が解除されたら、「アプリケーションを削除する」]** を選択してください。
 - c) **[新規作成]** を選択します。
 - d) ステップ3では、情報が正しいことを確認し、**[閉じる]** を選択してください。

MiradoreでiOSアプリを設定する

Miradore MDMで WithSecure Elements Mobile Protection iOSアプリを設定します。



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、アプリケーション一覧から「WithSecure Elements Mobile Protection」をダブルクリックします。
2. **[設定]** 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
 - データ型: 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。
こ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。
5. ユーザーの詳細を追加するには、**[新規追加]** を選択し、以下の値を使用してください。



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。

表8:設定キー

キー	種類	説明
<code>email</code>	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
<code>env</code>	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。
<code>data_usage_permission</code>	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。
<code>diagnostic_usage_permission</code>	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。
<code>create_vpn_profile</code>	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にAndroidアプリを追加する

WithSecure Elements Mobile Protection Androidアプリを Miradore MDMに追加します。

Miradore MDMは、XMLファイルまたはGoogle Playストアのインストールリファラーサービスのいずれかを使用して、アプリにライセンス情報を提供できます。アプリをMDMに追加する前に、使用方法を選択してください。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elements モバイル保護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提供するサブスクリプションキーを使用して設定します。
1. Miradore管理ポータルで、左側のメニューから **[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、**[Android アプリケーション] > [を追加]** 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) ステップ1で、**[Google Playストア]** を選択し、次に **[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) **[インストール参照元]**フィールドに以下の情報を追加してください。

- ライセンス情報を配信するためにインストールリファラーサービスを使用する場合は、WithSecure Elementsサービスのインストールリファラー文字列を使用します。WithSecure WithSecureモバイル保護のアクティベーション文字列を含む **[Google PlayのダウンロードURLを]**探します。文字列の後半部分 (utm-mediumから始まる部分) 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要素を追加できます。

4. **[新規作成]** を選択します。

5. ステップ4で、情報が正しいことを確認し、**[閉じる]**を選択します。

4.4.8 Jamf Pro MDMを使用した展開

Jamf Pro MDMを使用して、iOSおよびiPadOSデバイスに WithSecure Elementsモバイル保護機能を展開する。

Jamf Proで WithSecure Elements モバイル保護アプリを展開するには、アプリのライセンスを購入し、管理対象の iOS および iPadOS デバイス向けにアプリ、通知、および Safari ブラウジング保護拡張機能を設定します。

お使いのデバイスのライセンスを購入してください。

お使いのデバイス用のライセンスを購入します。

WithSecure Mobile Protectionアプリは App Storeから無料で入手できます。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ごとにボリューム購入プログラム (VPP) ライセンスを購入する必要があります。この金額は、購入した WithSecure Mobile Protectionライセンスの金額と同額でなければなりません。WithSecure。

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、購入した WithSecure Mobile Protectionライセンスの数を入力してください。WithSecure、そして **[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デバイス向けにアプリを設定する

Jamf Pro MDMで、iOSおよびiPadOSデバイス向けのセキュアモバイル保護アプリを設定します。



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。

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 WithSecure Protectionのサブスクリプションキーに置き換えてください。WithSecure Mobile Protectionのサブスクリプションキーは、以下の場所に記載されています。WithSecure Elements Security Center。



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。

アプリの通知を設定する

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

アラート設定を管理対象組織の好みに合わせて構成し、ポリシーの範囲をそれに合わせて調整します。

4.4.9 Samsung Knoxを使用した展開

Samsung Knoxと連携したWithSecure Elementsモバイル保護アプリのAndroidデバイスへの展開。



注: この展開には、ユーザーとデバイスの作成および構成は含まれていません。

WithSecure Elements Mobile Protectionアプリを Samsung Knoxと連携させるには、管理対象のAndroid デバイスにアプリを追加して設定します。

Samsung Knox を使用した Android アプリの展開

Samsung Knoxを使用したAndroidアプリの展開。

Samsung Knoxと連携して Android アプリを展開するには、管理対象の Android デバイスに WithSecure Elements Mobile Protectionアプリを追加して設定します。

AndroidアプリをSamsung Knoxに追加する

WithSecure Elements Mobile Protection AndroidアプリをSamsung Knoxに追加します。

WithSecure Elements Mobile ProtectionをMDMに統合する前に、以下の前提条件を満たし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、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するサポートや説明を提供しません。

- VPNとファイルのパーミッションを設定するためのインターネット接続環境
- 有効な WithSecure Elementsモバイル保護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提供するサブスクリプションキーを使用して設定します。

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てください。
2. **[アプリケーション]**を選択してください。
[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. 「アプリケーションの種類を選択」画面で、**[Androidプラットフォーム]** > **[パブリック マネージド Google Play]**を選択し、**[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」と入力して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から、国を選択してください。

6. 検索結果から **[WithSecure Elements Mobile Protection]** を選択し、**[選択]** を選択します。

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。

オプション	説明
名前	アプリケーション名を入力してください
カテゴリ	アプリケーションのカテゴリを選択してください。 [カテゴリの管理] を選択すると、アプリケーションの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てください

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。

- 情報を保存するには **[保存して割り当てる]** を選択し、**[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]** を選択すると、情報が保存され、アプリケーション一覧に戻ります。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設定

Androidアプリを割り当て、設定します。



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]** を選択してください。

[アプリケーション] ページが開きます。

2. **[WithSecure Elements Mobile Protection]** を選択し、**[割り当て]** 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。

- 対象デバイス - 次のいずれかのオプションを選択できます: **[Android Enterprise]**、**[Android Legacy]**、または **[Android Enterprise + Legacy]**。
- 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。
 - **[手動インストール]** - デバイスユーザーがアプリケーションを手動でインストールできるようにします
 - **[自動 (削除可能)]** - アプリケーションを自動的にインストールするように設定します。デバイスユーザーは、アプリケーションを手動で削除することもできます。
 - **[自動 (取り外し不可、Android管理APIのみ)]**
- インストール後に自動実行 (非 Android 管理 API) - インストール後すぐにアプリケーションを起動するように設定できます。
- 自動更新モデル - 利用可能なオプションは、**[デフォルト更新]**、**[高優先度]**、および **[延期 (90日 間)]** です。

4. 「管理構成」の横にある **[構成の設定]** を選択し、以下の手順を実行します。

- 管理構成フィールドに、説明的な名前を入力します。たとえば、「作業」などです。
- 「登録キー」欄に、WithSecure Elements Mobile Protectionのサブスクリプションキーを入力してください。
- エイリアスフィールドに、\$username\$と入力します。

- メールアドレス欄に「\$emailaddress\$」と入力してください。
- 環境フィールドに「2」と入力します。



注：登録済みデバイス WithSecure Elements値 \$ emailaddress\$を設定すると、メールアドレスとともに表示されます。

5. 変更を保存するには、[保存]を選択してください。
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。

4.5 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セキュリティセンターを通じてユーザーを招待するには、WithSecure Elements Agentをダウンロードするためのリンクを含むメールを送信します。

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. サイドバーの [環境]で [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。スコープセクターがすべての顧客会社を表示するように設定されている場合は、管理する会社を選択してください。

デバイスページが表示されます。

2. 「デバイス」タイトルの横にある「 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]を選択します。
「新しいデバイスの追加」フォームが表示されます。



注：スコープセクターで特定の企業に焦点を絞るように設定すると、ホームページに「新しいデバイスを追加」ボタンが表示されます。このボタンをクリックすると、直接「新しいデバイスを追加」フォームに移動できます。

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。
複数の招待状を送信するには、[CSVファイルからインポート]の下にある[ファイルを選択] を選択し、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]を選択してください。
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できます。



注：このソフトウェアは、[新しいデバイスの追加]ダイアログで選択したサブスクリプションキーを使用するようにカスタマイズされています。

製品がデバイスにインストールされ、アクティベートされると、**デバイスページ**を開くと、管理対象デバイスの招待ページから招待状が消えます。

4.5.1 Android端末にアプリをインストールして有効化してください。

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*ストアにリダイレクトされますので、そこで *WithSecure* モバイル保護アプリをダウンロードしてインストールしてください。
3. アプリをデバイスにインストールしたら、インストールメールに戻り、**[Android版を有効化]**を選択してサブスクリプションを有効化してください。



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. 求められたら、**[許可]**を選択してアプリに必要な権限を付与してください。



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。

アプリはAndroid端末にインストールされ、有効化されています。

4.5.2 iOSデバイスにアプリをインストールして有効化してください。

iOSデバイスに *WithSecure Elements Mobile Protection* をインストールするには、以下の手順に従ってください。



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。
*App Store*にリダイレクトされますので、そこで *WithSecure Mobile Protection* アプリをダウンロードしてインストールしてください。
3. アプリをデバイスにインストールしたら、インストールメールに戻り、**[iOSで有効化]**を選択してサブスクリプションを有効化してください。



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. 求められたら、[許可]を選択してアプリに必要な権限を付与してください。



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。

アプリはiOSデバイスにインストールされ、有効化されています。

第 5 章

プロファイルを管理する

トピック：

- クライアントに設定を割り当てる
- プロファイルの管理
- 制御されたアップデート
- Elements EPP for Computers および Elements EPP for Servers (Windows) でのプロファイルの管理
- Elements EPP for Computers (Mac) でプロファイルを管理する
- WithSecure Elements EPP for Linux でのプロファイルの管理
- モバイルデバイスプロファイルの管理

プロファイルを管理する

プロファイルとは、アカウント内のワークステーション、サーバー、モバイルデバイスに適用するセキュリティ設定の集合体です。

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を使用して、ユーザーが実行できる操作を制御できます。プロファイルは、デバイスに適用できる設定の集合です。プロファイルは、次のような特定のユーザーグループ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。

5.1 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。

クライアント設定は、デバイスにプロファイルを割り当てることで適用します。このセクションでは、プロファイルを手動で割り当てる方法と、割り当てルールを使用してプロファイルを自動的に割り当てる方法について説明します。

5.1.1 プロファイル割り当てルールを追加する

一致する条件に基づいて、新しいデバイスにプロファイルを自動的に適用するプロファイル割り当てルールを追加します。

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: [変更追跡] トグルをオンにすることができます。オンにすると、システムはルールを継続的に評価します。システムは、以下のいずれかに変更が検出されると、各デバイスのプロファイルとラベルの割り当てを更新します。

- Active Directory 組織単位
- IP
- リバースDNS
- WINS名

- 資産グループ



注: デフォルトのプロファイルでは、ユーザーがウイルス対策機能を無効にしたりアンインストールしたり、ほとんどの機能を制御できてしまうため、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. 下[セキュリティ構成]選択[プロファイル]サイドバーに表示されます。
の**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. [カスタムルールを追加]を選択します。
「カスタムルールの追加」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てください：Windowsワークステーション、Windowsサーバー、Linux、Macコンピュータ、モバイルデバイス、コネクタ。
 - 割り当てるプロファイルを選択します。
 - ルールにラベルを追加します (オプション)。
 - ルールの説明を追加します。
5. [カスタムルールを追加]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. 作成したルールの順序は、以下のいずれかの方法で変更できます。
 - ルールを目的の位置にドラッグ & ドロップします。
 - 移動したいルールの行で、[アクション] 列から **[一番上に移動]** または **[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。

5.1.2 Elements Agentのインストール時にプロファイルIDを指定してください。

使用状況に合ったルールを作成できない場合でも、Elements Agentのインストール時にプロファイルを指定することで、どのプロファイルが割り当てられるかを制御できます。

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]**そして、プロフィールを選択してください。
 - 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. Elements Agentをコマンドラインまたはスクリプトからインストールする場合、例の数値を自分のプロファイルに表示されている数値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: インストールパラメータとしてプロファイルIDを渡すと、プロファイル割り当てルールは評価されません。

5.1.3 プロファイルを手動で割り当てる

1つまたは複数のデバイスにプロファイルを手動で割り当てます。

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. 下**[環境]**選択**[デバイス]**次に、1つまたは複数のデバイスを選択します。
ページの下にメニューが表示されます。
3. **[プロファイルの割り当て]**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. **[プロファイルの割り当て]**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。

5.2 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。

5.2.1 Active Directory でグループの既定の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。

WithSecure Elements EPPに新しいデバイスを追加すると、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: 既定の Active Directory プロファイルは、WithSecure Elements セキュリティ センター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 グループを変更したときに、その AD グループのプロファイルをそのデバイスに自動的に割り当てる**」設定をオフにして、AD 階層内のデバイスの場所が変更された場合、デバイス プロファイルは変更されません。この設定をオンにしてデバイスの場所が変更された場合、デバイス プロファイルは 10 分以内に新しい AD 既定のプロファイルで更新されます。この設定がオフで、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 プロファイルは変更されません。

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. 行く[**プロファイル**]そして[**デフォルトプロファイル**]を選択します。
2. **Active Directory**で、既定のプロファイルを変更したい Active Directory グループに移動します。
3. メニュー列で[**変更**]を選択します。
「**既定の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 と WithSecure Elements EPP for Servers では、それぞれ個別にプロファイルを選択できます。

選択したプロファイルが、*Active Directory*グループの既定のプロファイルになります。

5.2.2 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てください。
3. 編集したいプロフィールを選択してください。
4. 変更内容を現在のプロファイルに保存するには、[**保存して公開**]を選択してください。



注: 編集した設定を複数のプロファイルで使用する場合は、[**保存して複数のプロファイルに公開**]を選択してください。ただし、変更内容を複数のプロファイルに公開した場合、オン/オフ切り替え可能な設定のみが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。

5.2.3 プロファイルのエクスポート

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できません。

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. 右上隅の  を選択し、次に[**プロファイルのエクスポート**]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。

5.2.4 プロファイルのインポート

WithSecure Elementsセキュリティセンターでは、プロファイルを別のプロファイルにインポートできます。



注: Elements Endpoint Protectionのエクスポート済みプロファイルだけでなく、その他のエクスポート済みファイルもインポートできます。たとえば、WithSecure Policy Manager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. 既にエクスポートしたプロファイルをインポートしたいプロファイルを開きます。
3.  を選択し、**[プロファイルのインポート]** 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。
 - 変更を保存するには、**[保存して公開]** を選択してください。
 - 変更をキャンセルする場合は、**[キャンセル]** を選択してください。

5.2.5 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. 削除したいプロファイルの横にある  を選択してください。
3. **[プロファイルの削除]** を選択し、**[OK]** を選択します。



注意: プロファイルを削除すると、元に戻すことはできません。正しいプロファイルを選択したことを確認してください。

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

5.2.6 プロファイルを割り当てる

管理対象のデバイスにセキュリティプロファイルを割り当ててください。

プロファイルを指定するには

1. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
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。

5.2.7 プロファイルを比較する

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] タブを選択してください。
3. 比較したいプロファイルの横にある  を選択し、[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を選択」 ページで、比較するプロファイルを1つ以上選択し、[次へ] 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。

5.2.8 ユーザーがコンピュータのプロファイル設定を変更できないようにする

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



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

プロファイルの設定をロックするには:

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

表9: ロックとロック解除のオプション

[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]

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。

5.2.9 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は、類似のテーブルにのみインポートできます。1つのプロファイルでアプリケーションコントロール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、同じプロファイルまたは別のプロファイルのアプリケーションコントロール除外ルールテーブルにのみデータをインポートできます。たとえば、別のプロファイルにインポートすることはできません。DeepGuard保護ルール表。

テーブルからデータをエクスポートする

テーブルからデータを JSONファイルにエクスポートします。

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. 編集する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. テーブルの右上隅にある  を選択し、**[ファイルにエクスポート (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 ファイルを保存してください。



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。

テーブルにデータをインポートする

選択したプロファイル内のテーブルにデータをインポートします。

[ファイル (JSON) からインポート] オプションを使用すると、テーブルに既に存在する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は、類似のテーブルにのみインポートできます。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、同じプロファイルまたは別のプロファイルの別の **アプリケーション制御除外ルール** テーブルにのみデータをインポートできます。たとえば、次のテーブルにはインポートできません。DeepGuard保護ルール表。

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. 編集する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. テーブルの右上隅にある  を選択し、[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. エクスポートした .json ファイルに移動し、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場合、重複する値が含まれていない、または部分的にしかインポートされない場合があります。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ることを示します。このような場合は、[ファイル (JSON) から置換] オプションを使用することをお勧めします。

6. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

テーブル内のデータを置換する

テーブル内のデータを、.json ファイルの値で置き換えます。

[ファイル (JSON) から置換] を選択すると、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. 編集するプロファイルを選択します。
3. プロフィールページで、該当する設定を選択してください。
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. 設定がオンになっていることを確認してください。
5. テーブルの右上隅にある  を選択し、[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。

6. エクスポートした .json ファイルに移動し、テーブル内のデータを置き換えてください。
テーブル内のすべての値は削除され、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。
7. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

5.3 制御されたアップデート

コントロールされたアップデートを使用すると、デバイスが新しいWithSecure Elementsエージェントバージョンにアップデートされるタイミングを制御できます。リリース後すぐにアップデートする必要はありません。

デフォルトでは、デバイスは新しいものに更新されます WithSecure Elementsエージェントのバージョンを自動的に更新します WithSecureアップデートは自動的にリリースされます。コントロールアップデートを使用すると、デバイスがこれらのアップデートをいつ、どのように受信するかを自分で決定できます。次のことが可能です。

- ご自身の都合の良い時間に、手動でアップデートしてください。
- 自動的に更新されますが、更新は指定した時間帯のみに行われます。
- アップデートを全端末に適用する前に、少数の端末でテストしてください。

コントロールアップデートは、Windows、macOS、Linuxデバイスでサポートされています。どちらのモードを選択しても、アップグレード自体はサイレントで実行され、通常のアップデートと同じように動作します。

更新モード

プロファイルエディタの **[クライアントソフトウェアへのアクセス]** 設定は、デバイスがアップデートを受信する方法を決定します。この設定には3つのモードがあります。

[自動更新]

デバイスは新しいバージョンがリリースされると自動的にアップデートされます。これがデフォルトモードです。このモードには2つのサブモードがあります。

[一般的に入手可能]

デバイスはアップデートを受け取ります WithSecure一般公開されます。これがデフォルトのサブモードです。

[早い]

デバイスは一般リリース前にアップデートを受け取ります。エージェントとエンジンのアップデートは約1週間早く、セキュリティ定義のアップデートは約2時間早く配信されます。



重要: 問題が全端末に及ぶ前に発見できるよう、少数の代表的な端末を早期対策対象として割り当てることをお勧めします。

[制御されたアップデート - 手動]

デバイスは、プロファイルを変更して別のバージョンを指定するまで、選択したリリースグループのバージョンに留まります。

[制御されたアップデート - スケジュール設定]

デバイスは、ユーザーが定義したスケジュールに従って、最新のリリースグループに自動的に移行します。



注: 各デバイスプロファイルには **[クライアントソフトウェアへのアクセス]** 設定がそれぞれあります。たとえば、パイロットグループには **[早期]**、本番グループには **[制御された更新 - スケジュール済み]** を使用するなど、デバイスグループごとに個別のプロファイルを作成できます。



注: 制御されたアップデートは、エージェントソフトウェアとエンジンコンポーネントに適用されます。セキュリティ定義のアップデートは、独自のスケジュールで引き続き更新され、アップデートモードの影響を受けません。ただし、**[早期]** サブモードでは、一般リリースに先駆けて定義が提供されます。

適切なモードを選択する

表10:目標による更新モード

ゴール	推奨モード
最小限の手間で自動的に最新情報を入手できます	[自動アップデート]-[一般提供開始]
アップデートが全車両に適用される前に検証してください。	[自動アップデート]- 試験運用中のデバイスグループで [早期に実施]
デバイスは既知の安定したバージョンに保ち、自分のペースでアップデートしてください。	[制御されたアップデート - 手動]
各新リリースに自動的に移行するが、移行は予測可能なタイミングでのみ行う。	[制御されたアップデート - スケジュール設定]

5.3.1 リリースグループ

リリースグループとは、WithSecure Elementsエージェントコンポーネントの検証済みバンドルであり、四半期ごとに公開されます。

WithSecure各四半期 (2月、5月、8月、11月) の第2火曜日に、新刊情報をまとめて公開します。

各リリースグループには、連番のバージョン番号が割り当てられています。この番号は、リリースグループの公開月ではなく、リリースグループの順番を示すものです。[クライアントソフトウェアへのアクセス]設定を[制御されたアップデート - 手動]に設定すると、そのプロファイル内のデバイスが使用するリリースグループのバージョンを選択できます。プロファイルを別のリリースグループに変更するまで、デバイスはそのバージョンのままになります。



注: デバイスに現在インストールされているリリースグループバージョンを確認するには、Elements Security Centerのデバイス インベントリを確認してください。

退職者グループの退職

WithSecure設定されたサポート期間が経過すると、古いリリースグループはサポート対象外となります。リリースグループのサポート終了日を迎えると、プロファイル設定に関係なく、そのバージョンのデバイスはアップグレードする必要があります。



重要: リリースグループのサポート終了日の1か月前、WithSecure[エンドポイント保護]ダッシュボードでホストの問題に関する警告が表示されます。

5.3.2 スケジュールの更新

更新スケジュールは、制御された更新 - スケジュールされた更新に設定されているデバイスが、最新のリリースグループを確認してインストールするタイミングを定義します。

更新スケジュールはタイミングのみを制御します。どのバージョンがデバイスにインストールされるかは制御しません。チェック実行時に利用可能な最新のリリースグループが、デバイスにインストールされます。

スケジュールを設定する際には、例えば毎週または毎月といった繰り返し頻度と、チェックを実行する1時間の時間帯を設定します。



注: デバイスがスケジュールされたチェック時刻にオフライン状態だった場合、次のスケジュールされた間隔を待つのではなく、次にオンラインになったときにチェックを行います。

小切手の仕組み

1. デバイスがチェックしますWithSecure最新のリリースグループ向けの配布インフラストラクチャ。
2. そのリリースグループが現在インストールされているものよりも新しい場合、デバイスは新しいリリースグループにアップグレードされます。
3. より新しいリリースグループが利用できない場合、デバイスは次の定期点検まで現在のバージョンのままになります。

例

スケジュールは毎月1日に設定します。WithSecureリリースグループバージョン2は、5月の第2火曜日に公開されます。6月1日、デバイスはバージョン2を確認し、バージョン2が見つかったらアップグレードします。6月1日までにバージョン2が公開されていない場合は、デバイスはバージョン1のままとなり、7月1日に再度確認します。

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

WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversソフトウェアにおけるプロファイル管理。

プロファイルとは、Windows上のWithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversクライアントに割り当てる設定の集合です。このセクションでは、プロファイルの作成方法と、スキャン、ブラウジング保護、ファイアウォール、デバイス制御、自動タスクなどの設定構成方法について説明します。

5.4.1 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. ログインして WithSecure Elements Security Center。
2. 下[セキュリティ構成]選択[プロファイル]。
の[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。



注: または、を選択し、[プロファイルの複製]を選択して、デフォルトのセキュリティプロファイルのいずれかをベースに使用することもできます。

「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」ページが開きます。

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。



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。

新しいプロファイルが作成されます。

5.4.2 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。

一般設定には、管理対象デバイス上でエンドポイント保護クライアントがどのように動作するか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、以下の項目を制御できます。

- 機能の利用可能性
- ユーザーとクライアントアプリケーションのインタラクション
- 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

これらのオプションは通常、ポリシー作成時に設定されます。これらは、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用クライアントソフトウェアへのアクセスを設定する

Windows デバイスが新しいWithSecure Elements エージェント バージョンを受信する方法を設定します。

[クライアントソフトウェアへのアクセス]設定は、Windows デバイスが新しいソフトウェアを受信する方法を制御します。WithSecure Elements エージェントのバージョン。更新のタイミングをどの程度制御したいかに応じて、[自動更新]、[手動による]更新」、または[スケジュールによる更新]を選択してください。

クライアントソフトウェアへのアクセスを設定するには：

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。
3. 編集するプロファイルを選択します。
4. 左側のメニューから [一般設定]を選択してください。
5. [クライアントソフトウェアへのアクセスを定義する] ドロップダウンメニューで、モードを選択します。
 - [自動アップデート機能は]、新しいバージョンがリリースされると、デバイスを自動的にアップデートします。
 - [制御されたアップデート-手動アップデートでは]、デバイスをユーザーが選択したリリースグループのバージョンに維持します。
 - [制御されたアップデート-スケジュールされた]アップデートは、デバイスを自動的にアップデートしますが、設定したスケジュールに従ってのみ実行されます。
6. [自動更新]を選択した場合は、サブモード [一般公開]または [早期公開]を選択してください。

[初期]デバイスは一般リリースに先駆けてアップデートを受け取ります。エージェントとエンジンのアップデートは約1週間早く、セキュリティ定義のアップデートは約2時間早く提供されます。



重要：問題が全端末に及ぶ前に発見できるよう、少数の代表的な端末を [早期]検出グループに割り当てることをお勧めします。

7. [制御された更新-手動]を選択した場合は、このプロファイルに割り当てるリリースグループのバージョンを選択してください。
8. [制御された更新-スケジュール済み]を選択した場合は、更新チェックの繰り返し頻度、曜日、および1時間ごとの時間帯を設定してください。
9. 変更を適用するには、[プロファイルを保存]を選択してください。

変更内容は保存され、現在のプロファイルに適用されます。

WindowsにEDRセンサーを統合する

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 センサーを有効化および構成するには、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. **[Windows用]** タブを選択してください。
3. 編集するプロファイルを選択します。
Windows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 **[一般設定]** を選択してください。
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: この設定は有効にしておくことをお勧めします。無効にすると、EDRはエンドポイントへの攻撃を検知したり、警告を発したりしなくなります。

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. 外部ツールやスクリプトから Windows Management Instrumentation (WMI) 経由で WithSecure Elements エージェントの状態を照会する場合は、**[WMIプロバイダーを]** 有効にしてください。
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]** を選択してください。

WindowsでBitLockerを管理する

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]** タブを選択してください。
3. 編集するプロファイルを選択します。
Windows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 **[一般設定]** を選択してください。
5. **[BitLocker回復キーの収集]** をオンにすると、デバイスで使用可能なすべての BitLocker 回復キーが収集されます。



注：デバイスが管理ポータルで復旧キーを報告していることを確認してください。

6. [BitLocker 保護]で、BitLocker 保護が適用されるディスクを選択します。

オプション

説明

[変更なし]

デバイス上のBitLocker設定には変更は加えられません。

[システムのみ]

BitLockerはシステムディスクのみを保護します。

[すべて修正済み]

システム内のすべての固定ディスクでBitLockerが有効になっています。

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。

BitLockerの設定は、このプロファイルを使用するデバイスに適用されます。

ライセンス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]タブを選択してください。
の [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]に進みます。
5. [通知を表示]で、通知をオンにしてください。
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. [ライセンス有効期限までの日数] に、ライセンス有効期限の何日前に通知を表示するかを入力してください。



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. 「ライセンス有効期限に関するカスタムメッセージ」欄には、ライセンスの有効期限が切れる前にユーザーに表示したい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を管理する

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]タブを選択してください。

3. 編集するプロファイルを選択します。

Windows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 [一般設定] を選択してください。

5. [ユーザーが製品をアンインストールすることを許可する] を選択すると、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できます。

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. [ユーザーがセキュリティ機能をオフにできるかどうかを制御するには、[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] を選択します。WithSecureセキュリティ機能。

この設定をオンにすると、ユーザーは WithSecure デバイスに搭載されている保護機能。



重要: セキュリティ機能を有効にするため、この設定はオフのままにしておくことをお勧めします。

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。

アンインストールおよびセキュリティ機能の設定は、このプロファイルを使用する Windows デバイスに適用されます。

5.4.3 Windowsの通信設定

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し、アップデートを取得し、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送信する方法を制御します。

管理対象の Windows エンドポイントクライアントは、クラウドサービスに接続します。接続方法は、直接接続するか、構成済みのプロキシサーバーまたは WithSecure Elements コネクタを介して接続します。

これらのオプションを使用して、ネットワークポリシーに従ってください。たとえば、インターネットへの送信アクセスを制御したり、特定のゲートウェイ経由でトラフィックを送信したりできます。

プロキシ設定を構成する

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は、以下のように構成してください。

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. [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コンピューター用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]** を選択してください。
4. **[通信設定]** に移動します。
5. 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。

6. 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。
7. 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。
8. 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。

このプロキシ設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

ソフトウェアアップデーターの通信設定を構成する

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アップデートサービスに接続する方法を決定します。コンポーネントを、専用のHTTPプロキシを使用するように構成するか、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構成できます。

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コンピューター用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]** を選択してください。

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ーは設定された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ーは自動的に直接接続にフォールバックします。

5. **[WithSecure要素コネクタを使用する]**を選択すると、ソフトウェアアップデーターのトラフィックが要素コネクタ経由でルーティングされます。

ソフトウェアアップデーターの通信設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

コンピュータプロファイルでWithSecure Elementsコネクタを使用する

WithSecure Elements Connectorは、WithSecureが提供するサービスで、WithSecure Elements EPP for Computersクライアントへのアップデートダウンロード時の帯域幅使用量を最小限に抑えることを目的としています。

このプロキシは、マルウェア署名データベースであるGUTS2のアップデート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なります。

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、以下の手順に従ってください。

1. WithSecure Elements Connectorの最新バージョンをダウンロードしてください。
2. お使いのプラットフォームに対応した WithSecure Elements Connectorをインストールしてください。
 - Windowsの場合：WindowsにElements Connectorをインストールする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手順に従ってください。
3. WithSecure Elements Connectorを使用するようにプロファイルを設定します。
 - a) **[セキュリティ構成]**で、**[プロファイル]**。
 - 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 をプロキシとして構成する」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。

- 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 Connector]**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てください。また、**[Use WithSecure Elements Connector]**設定にも適切な値を選択してください。



注：WithSecure Elements Connector は、デフォルトでは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 をプロキシとして構成する」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ーがインターネットに直接接続されておらず、Elements Connectorを最終的なプロキシとして使用する場合は、**[一般]**タブを開き、**[手動で定義したプロキシ アドレ**

ス](Windows プロファイル)]または[リモートで管理するプロキシアドレス](Mac プロファイル)]の下に、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。

4. 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」のアドレス値が指定されていることを確認してください。
 - c) [今すぐ確認]を選択してください。

チェックはエラーなしで実行されるはずです。

5.4.4 Windowsのスキャン設定の構成

スキャン設定は、Windowsエンドポイントクライアントがマルウェアを検出および処理する方法、リムーバブルメディアをスキャンする方法、および除外設定を適用する方法を制御します。

スキャン設定は、Windowsエンドポイントクライアントがファイルやシステムアクティビティを監視して悪意のあるコンテンツを検出する方法を制御します。また、脅威の検出、リムーバブルメディアのスキャン、および通知も制御します。

Windowsで一般的なスキャン設定を構成する

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コンピューター用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]を選択してください。
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: [ブロックモード]以外のモードでは、Windows Elements Agent はオペレーティングシステムを積極的に保護せず、検出された脅威のみを報告します。

- 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]モードのままにしておくことをお勧めします。

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。

オプション	説明
[何もしない]	USBストレージデバイスが接続された場合、クライアントはスキャンを実行しません。
[ユーザーにUSBをスキャンするように依頼する]	ユーザーは、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促されます。
[USBをサイレントスキャン]	USBストレージデバイスは、ユーザーに通知することなく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する]	USBストレージデバイスは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を強制的にスキャンし、結果をユーザーに表示する]	USBストレージデバイスは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回避することはできません。

6. [通知を表示]で、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的に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。

このプロファイルを使用するWindowsコンピューターには、共通のスキャン設定が適用されます。

スキャン除外設定

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されるファイル、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保護されないため、必要な場合にのみ除外を使用してください。WithSecure保護。



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 コンピューター用のプロファイルが開きます。
3. [スキャン設定] を選択してください。
4. [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、[クライアントからの除外を非表示] にするを選択すると、ユーザーが Elements Agent または スキャンレポートで除外項目を確認できなくなります。

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)。

スキャン除外設定は、このプロファイルを使用する Windows コンピューターに適用されます。

Windows で隔離設定を構成する

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コンピューター用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]** を選択してください。

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 **[自動的に削除するには、「古い隔離アイテムを自動的に削除する」]** を選択してください。

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。

この隔離設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

改ざん防止機能を設定する

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。

改ざん防止機能により、不正なアプリケーションやユーザーによる変更を防止します。WithSecure管理対象デバイス上のサービス、プロセス、ファイル、およびレジストリエントリ。

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用コンピュータ保護]** または **[サーバー保護]** タブを選択してください。
の **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]** で、**[改ざん防止]** までスクロールしてください。
5. **[改ざん防止をオンにする]** を選択します。

選択すると、改ざん防止機能が外部アプリケーションやユーザーによる制御を防止します。WithSecure サービス、プロセス、ファイル、またはレジストリエントリ。

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。

改ざん防止設定は、このプロファイルを使用するデバイスに適用されます。

スキャンアーカイブファイル

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

アーカイブスキャンでは、ZIP、7Z、JAR、ARJ、LZH、TAR、TGZ、GZ、CAB、RAR、BZ2、R??、および 0??形式の圧縮アーカイブ内のファイルをスキャンできます。



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



注: アーカイブスキャンでは、他のスキャン操作と同じ最大一時ファイルサイズ設定が使用されます。

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. **[Windows コンピューター用]**または**[Windows サーバー用]**タブを選択してください。
3. 編集するプロファイルの名前を選択します。
4. **[手動スキャンの]**設定で、**[圧縮ファイル (ZIP、RARなど) の内部をスキャンする]**がオンになっていることを確認してください。
5. アーカイブのスキャン設定は、「含まれる拡張機能」の下にリストされます。設定を変更するには、次の手順を実行します。
 - a) **[スキャンするファイル]**の下にあるドロップダウンメニューから、**[次の拡張子のファイル]**を選択します。
 - b) **[含まれる拡張機能]**で、拡張機能リストを編集します。
 - c) **[保存して公開]**を選択してください。
変更が保存され、現在のプロファイルに公開されます。

5.4.5 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有効になっている場合、エンドポイント保護クライアントは、ファイルがアクセス、実行、または転送される際に分析を行います。サポートされているチャンネルには、Webトラフィックとネットワークドライブが含まれます。

設定可能な項目：

- 脅威の検出方法
- 不審な行動への対処方法
- 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どのように連携するか

マルウェア対策スキャンインターフェースを使用する

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。

アンチマルウェアスキャンインターフェイス (AMSI) 統合により、オペレーティングシステムは WithSecure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する前に分析する保護エンジン。

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コンピューター用のプロファイルが開きます。
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. **[AMSI を有効にする]**を選択します。

設定が選択されると、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、スクリプトやその他のコンテンツを WithSecure実行前にセキュリティ分析を行うための保護エンジン。

ファイルスキャン設定を構成する

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コンピューター用のプロファイルが開きます。
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. **[感染時に実行されるアクション]**を選択して、クライアントが感染していると検出されたオブジェクトをどのように処理するかを決定します。
 - **[感染時の対応を自動的に決定すると]**、]ユーザーに確認することなく、自動的に対応が選択されます。
 - **[名前変更機能は]**、感染したオブジェクトを削除せずに、実行できないように名前を変更します。
 - **[Deleteは]**感染したオブジェクトを削除します。
 - **[Disinfectは]**、感染したオブジェクトから悪意のあるコードを削除し、クリーンアップされたファイルを保持します。
 - **[隔離とは]**、]感染した物体を隔離場所に移動させることです。
 - **[スキャン後に確認する機能は]**、]スキャンが完了するまで待機し、検出された各項目に対してアクションを選択するように求めます。
 - **[ブロック]機能は**、感染したオブジェクトを削除せずに、そのアクセスを遮断します。
5. **[リスクウェアに対するアクション]**を選択して、クライアントがリスクウェアとして分類されたオブジェクトをどのように処理するかを決定します。

- **[削除すると]**、リスクウェアオブジェクトが削除されます。
 - **[隔離機能は]**、リスクウェアオブジェクトを隔離場所に移動します。
 - **[スキャン後に確認する機能は]**、スキャンが完了するまで待機し、検出された各項目に対してアクションを選択するように求めます。
 - **[ブロック機能]**は、リスクウェアオブジェクトを削除せずに、そのアクセスをブロックします。
6. **[スパイウェアに対するアクション]**を選択して、クライアントがスパイウェアとして分類されたオブジェクトをどのように処理するかを決定します。
- **[削除]**はスパイウェアオブジェクトを削除します。
 - **[隔離機能は]**、スパイウェアオブジェクトを隔離場所に移動します。
 - **[スキャン後に確認する機能は]**、スキャンが完了するまで待機し、検出された各項目に対してアクションを選択するように求めます。
 - **[ブロック]**機能は、スパイウェアオブジェクトを削除せずに、そのアクセスを遮断します。
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。

選択された場合、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は、WithSecureSecurity Cloud さらなる分析のため。

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: この設定は、ゼロデイマルウェアの検出に役立ち、誤検出を減らすため、オンにしておくことをお勧めします。

10. **[ホストファイルを保護する]**を選択します。

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。

ファイルスキャン設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

除外設定

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コンピューター用のプロファイルが開きます。

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. 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。

リアルタイムスキャンの除外設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

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コンピューター用のプロファイルが開きます。
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. **[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. ウェブトラフィックのスキャン方法と、検出されたマルウェアを自動的に削除するかどうかを選択してください。

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]**、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。

ウェブトラフィックのスキャン設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

DeepGuardをセットアップする

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: 保つ DeepGuard 常時有効。ランサムウェアなどの高度な脅威に対する重要な保護機能を提供します。

いつ DeepGuard が有効な場合、以下の保護機能が有効になります。

- エクスプロイト保護
- ランサムウェア保護
- ヒューリスティック分析
- 動作監視

設定するには DeepGuard:

1. オンにする DeepGuard:

- 下**[セキュリティ構成]**選択**[プロファイル]**。
の**プロファイル**ページが開きます。
- 使用するプロファイルを選択します。
- [リアルタイムスキャン]**を開く。



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。

- [DeepGuardを]**オンにしてください。

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 行動分析と評判情報に基づいて、稀なファイルや疑わしいファイルをブロックする。

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独自開発の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出が発生する場合があります。しかし、有効にしておくことをお勧めします。

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除外できます DeepGuard スキャンするか、明示的にブロックしてください。この機能は必要な場合にのみ使用してください。DeepGuard 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。



ヒント: もし DeepGuard 信頼できるアプリケーションがブロックされた場合は、[保護ルール] でそのアプリケーションを信頼できるアプリケーションとして追加し、サンプル検証にファイルを送信して検出結果を修正してください。

- [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 アプリケーションを処理します。

アプリケーションが信頼されている場合、DeepGuard 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 常にアプリケーションの実行を妨げます。

4. 除外するアプリケーションに関するルールを追加します DeepGuard 必要に応じてスキャンする。



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。

DeepGuard の設定は、このプロファイルを使用する Windows コンピューターに適用されます。

5.4.6 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。

定期スキャンを設定する

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コンピューター用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]** を選択してください。
 4. **[定期スキャン]** で、**[スキャン頻度]** と定期スキャンを実行する曜日を選択します。
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。
このオプションを選択すると、スキャンはマルウェアが一般的に使用する実行ファイルやスクリプトなどのファイルタイプだけに焦点を絞ります。

 **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ー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. **[ユーザーに通知を表示する]** を選択します。
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。
- スケジュールされたスキャン設定は、このプロファイルを使用する Windows コンピューターに適用されます。

手動スキャンを設定する

- 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コンピューター用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]**を選択してください。

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、手動スキャンで利用できるシステム 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. 手動スキャン中に感染が検出されたオブジェクトを製品がどのように処理するかを定義するには、**[感染時のアクション]**を選択します。

- **[Cleanは、]**感染したオブジェクトから悪意のあるコードを削除し、クリーンアップされたファイルを保持します。
- **[Deleteは]**感染したオブジェクトを削除します。
- **[名前変更機能は、]**感染したオブジェクトを削除せずに、実行できないように名前を変更します。
- **[スキャン後に確認する機能は、]**スキャンが完了するまで待機し、検出された各項目に対してアクションを選択するように求めます。
- **[隔離とは、]**感染した物体を隔離場所に移動させることです。
- **[この報告書は検出結果を報告するだけで]**、何らの措置も講じません。

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。

このオプションを選択すると、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脅威が検出された場合の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、**[レポートのみ]**となります。

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、すべてのファイルをスキャンするか、特定のファイル拡張子のみをスキャンするかを選択します。

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\)。

手動スキャン設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

5.4.7 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。

ブラウジング保護機能は、ウェブ上の脅威からユーザーを保護するのに役立ちます。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します。

閲覧保護の設定は以下から行えます。

- 危険なウェブサイトをブロックする
- 安全な検索行動を強制する
- 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する

閲覧保護を設定する

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 コンピューター用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にアクセスできるようにする]を選択してください。

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]を選択します。

選択すると、ブロックされたウェブサイトの 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: ユーザーのウェブ活動の監視に関する地域的な法令によっては、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、該当する地域の法令および組織の方針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]を選択します。

選択すると、ブロックされたウェブ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まれます。



注: ユーザーのウェブ活動の監視に関する地域的な法令によっては、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、該当する地域の法令および組織の方針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>)。

ブラウジング保護の設定は、このプロファイルを使用する Windows コンピューターに適用されます。

Windowsで評判に基づくブラウジングを使用する

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

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] タブを選択してください。
3. 編集するプロファイルを選択します。
Windows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、[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]
 - [不審と判断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。

ウェブコンテンツを管理する

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 コンピューター用のプロファイル 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。これらは通常、あまり人気のないウェブサイトや、開設されたばかりでアクセス数が少ないウェブサイトです。

コンテンツの種類をフィルタリングする

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コンピューター用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]** でルールを追加または編集します。

このリストは、ブロックするコンテンツの種類を定義します。推奨フィルターのオン/オフを切り替えたり、**[コンテンツタイプフィルターを追加]** 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する機能] が無効になっている場合、フィルタリングは、Security Cloud。

- **[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は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は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ー ルールの説明が保存されます。

ウェブサイトの例外を設定する

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コンピューター用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]** を選択してください。

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、参照元に基づいてページへのアクセスが許可されなくなります。通常、承認された参照元から読み込まれたページは許可され、許可されたウェブサイトにも埋め込まれたコンテンツが正しく機能するようにします。



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. [アクセスが拒否されたサイトに関するセキュリティイベントを送信する]を選択します。

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。

ウェブサイトの例外規定は、このプロファイルを使用するWindowsコンピューターに適用されます。

接続制御を使用する

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コンピューター用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]**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]**を選択してください。

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。

接続制御を有効にすると、保護されたセッション中にコマンドラインツールや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がブロックされます。

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。

5.4.8 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ー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製ファイアウォールを使用している場合、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を適用する]** 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製ファイアウォール用に構成されたケース固有の設定と一致させる必要があります。



重要: **[その他のルールを許可する]** をオンにして、ファイアウォールルールを許可します。WithSecure作成されませんでした。このオプションをオフにすると、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が適用されます。このオプションはオンにしておくことをお勧めします。

異なるサイトで異なるファイアウォールプロファイルを使用できます。オフィスネットワークと外部ネットワーク間でプロファイルを切り替えるには、自動選択ルールを作成します。WithSecure **[ファイアウォールWithSecure]** に移動し、**[自動選択]** を選択してルールを追加します。このルールは、設定に基づいてファイアウォールプロファイルを選択します。

ルールを追加する

ファイアウォールプロファイルにルールを追加して、ネットワークトラフィックを許可またはブロックします。

ルールの追加するには

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、表の上部にある **[ルールを追加]** を選択してください。
- 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。

新しいルールは、選択した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テーブルに表示されます。

ファイアウォールルールのアラートを設定する

トラフィックをブロックするファイアウォールルールのアラートを設定します。



注: アラート機能は、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. ログインして WithSecure Elements Security Center。
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 コンピューター用] タブを選択し、編集したいプロファイルを選択します。
4. [ファイアウォール] を選択してください。
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. アラートを以下のように定義します。
 - a) 「アクティブ」列のスイッチがオンになっていることを確認してください。
 - 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。

更新されたアラート設定が、選択したファイアウォールルールに適用されます。

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 プロセスが停止します。選択したデバイスに対して、他のすべてのファイアウォールルールが無効になります。また、許可されていないアドレスのDNS解決もブロックするため、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はインターネットに接続されていないため、外部からアクセスしたり、インターネット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。

「許可されたドメイン」フィールドでは、隔離されたデバイスが接続できるドメインを指定できます。



注: DNSによって解決されるのは、「許可されたドメイン」フィールドに指定されたドメインのみです。

ネットワーク分離機能は、WithSecure Elements Endpoint Protection プロファイル設定でファイアウォールが無効になっている場合でも機能します。ネットワーク分離モードでは、ファイアウォールとネットワーク分離プロファイルが強制的に有効になります。ただし、デバイスの GPO 設定でファイアウォールが無効になっている場合は、ネットワーク分離モードでも有効になりません。

不明な接続を許可する

ファイアウォールプロファイルで、未知の受信接続と送信接続を許可します。

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]の設定はオフになっています。これらの設定がオフの場合、ファイアウォールは不明なトラフィックをブロックします。自動的に選択されたプロファイルを使用したり、定義済みのWithSecureファイアウォール プロファイルを選択したり、ニーズに合わせてプロファイルのカスタマイズしたりできます。この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は、デフォルトのルールが使用されます。つまり、最初にWithSecureファイアウォールの一般設定が適用され、次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。他のルールも一致しない場合は、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。

例えば、[不明な接続を許可する]をオンにしてファイアウォールルールをすべて削除すると、すべての接続が許可されます。[不明な接続を許可する]をオフにすると、すべての接続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は不明とみなされ、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で、それ以外のトラフィックをブロックできます。あるいは、**[不明な接続を許可する]**をオンにしてすべてのトラフィックを許可し、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てそれ以外のすべてのトラフィックを許可することもできます。

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。

オプション

説明

[不明な受信接続を許可する]

この設定がオンになっている場合、コンピュータへの未知の着信接続が許可されます。この設定はオフにしておくことをお勧めします。

[不明な発信接続を許可する]

この設定がオンになっていると、コンピュータからの未知の外部接続が許可されます。この設定はオフにしておくことをお勧めします。

6. 変更内容を保存して公開する：

- ・ 変更内容を現在のプロファイルに保存するには、**[保存して公開]**を選択します。
- ・ 変更内容を複数のプロファイルに保存するには、**[保存して複数のプロファイルに公開]** を選択します。

5.4.9 デバイス制御を使用する

デバイス制御機能は、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。これにより、USB ストレージデバイスやDVD/CD-ROMドライブなどの外部デバイスからマルウェアがネットワークに拡散するのを防ぎます。ブロックされたデバイスがクライアントコンピュータに接続されると、デバイス制御機能はそのデバイスをオフにしてアクセスを防止します。

このセクションでは、デバイス制御の設定方法、デバイスのブロック方法、デバイスマスクを使用したデバイスの除外方法、およびデバイスIDの検索方法について説明します。

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. 左側のメニューから **[デバイス制御]** を選択します。

4. **[デバイス制御を]**オンにしてください。



注: デバイス制御がオンになっている場合、コンピュータ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 **[接続されているデバイス]**の下に表示されます。

5. 「リムーバブル大容量記憶装置」では、以下のいずれかのオプションを有効にできます。

オプション	説明
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、ユーザーはリムーバブルストレージデバイスにファイルをコピーできません。リムーバブル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、リムーバブル大容量記憶装置からのファイルの実行は防止されます。

デバイス制御設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

マスクを使用している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を見つけるには、[環境]選択[デバイス]。の**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]フィールドにマスクを入力します。たとえば、「USB*」と入力します。
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. リストに除外したいデバイスがすべて含まれていることを確認してください。
6. 下[プロファイル]目的のプロファイルを選択し、次に**[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]**の下にあるルールテーブルで、**[ルールの追加]**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. **[保存して公開]**を選択してください。

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。

ブロックハードウェアデバイス

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. 左側のメニューから**[デバイス制御]**を選択します。
4. デバイスアクセスルールを追加するには、次の手順を実行します。
「**デバイスアクセスルール**」では、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するためのルールを追加または削除できます。
 - 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]については、[許可] または [ブロック] を選択してください。
ルールが有効になっている場合、**デバイスへのアクセス**が [ブロック] に設定されているデバイスにはアクセスできません。
- d) 新しいルールを公開するには、[公開] を選択してください。

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ーを使用して、以下の手順でハードウェアIDを見つけてください。

1. クライアントコンピュータでWindows **デバイスマネージャー**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] タブに移動してください。
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。

5.4.10 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: 自動タスク表の[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かった場合でも、タスクは可能な限り早く実行されます。そうでない場合は、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。

Windowsでスキャンをスケジュールする

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. 編集するプロファイルを選択します。
3. [自動化タスク]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. [タスクの追加]を選択します。
6. 「種類」列で、[マルウェアの定期スキャン]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. (任意) 説明欄に、選択したスキャンの説明を入力します。
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. [保存して公開]を選択してください。
変更が保存され、現在のプロファイルに公開されます。

特定の時間に製品を更新するタスクを設定する

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てください。
4. 自動化タスク表の上にある **[タスクの追加]** を選択し、以下の手順を実行してください。
 - a) 「タイプ」ドロップダウンメニューから **[WithSecureElementsエージェントの更新を許可する]** 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、この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。

不足している重要なセキュリティ更新プログラムやその他のセキュリティ更新プログラムをインストールするタスクを設定します。

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てください。
4. 重要なセキュリティ更新プログラムを毎日インストールするタスクを作成するには、自動化タスク表の上にある **[タスクの追加]** を選択し、次の手順を実行します。
 - a) 「種類」ドロップダウンメニューから **[重要なセキュリティ更新プログラムをインストールする]** を選択します。
 - b) スケジュールの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. 週に一度、その他のセキュリティ更新プログラムを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、以下の手順を実行します。
 - a) 「種類」ドロップダウンメニューから[すべてのセキュリティ更新プログラムをインストールする]を選択します。
 - b) スケジュールの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。

セキュリティ更新プログラムの不足をスキャンするタスクを設定します。

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: 不足している更新プログラムをスキャンするタスクを作成した場合、ソフトウェア更新ページで[不足している更新プログラムを自動的にスキャンする]をオフにすることができます。



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てください。
4. 自動化タスク表の上にある [タスクの追加]を選択し、以下の手順を実行してください。
 - a) 「タイプ」ドロップダウンメニューから[不足しているアップデートをスキャンする]を選択します。
 - b) スケジュールの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を設定する

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てください。
4. 自動化タスク表の上にある [タスクの追加]を選択し、以下の手順を実行してください。

- a) 「タイプ」ドロップダウンメニューから **[マルウェアのスキャン]** を選択します。
- b) スケジュールの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。

5.4.11 ネットワーク拠点の設定

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. **[ネットワークの位置情報設定]** を選択し、オンになっていることを確認してください。
4. **[場所とルール]** で **[場所を追加]** を選択し、以下の手順を実行します。
 - a) 「名前」列には、場所を表す説明的な名前を入力します。たとえば、**[自宅]** などです。
 - 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を入力します。たとえば、「10.0.0.0/24」と入力します。



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. 別の場所を追加するには、**[場所を追加]** を選択し、以下の手順を実行してください。
 - a) 「名前」列には、場所を説明する名前を入力します。たとえば、**[オフィス]** などです。
 - b) 「トリガー」列の「タイプ」ドロップダウンメニューから **[デフォルトゲートウェイ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、ルール表の上にある **[ルールの追加]** を選択し、以下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、ルールを適用する場所を選択します。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のいずれかを選択します。この例では、**[ソフトウェアアップデーター]** を選択します。
 - c) 「値」列で、スイッチがオン **[に]** になっていることを確認してください。

7. 別のルールを作成するには、[ルールの追加]を選択し、以下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]を選択します。
 - b) 「設定」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]になっていることを確認してください。
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) 最初のルールについては、[設定]列で[ソフトウェアアップデーター]を選択し、[値]列でスイッチを[オフ]にします。
 - b) 2番目のルールについては、[設定]列で[ファイアウォール]を選択し、[値]列でスイッチを[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。

新しい場所とルールは、選択したプロファイルの「場所とルール」テーブルに表示されます。

5.4.12 ランサムウェアからファイルを保護します

ランサムウェア攻撃が疑われる際に、製品が自動的に復元したファイルとシステム設定を復元します。

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。

ローカルで除外されたパスを削除します

WithSecure Elements Security Centerを使用すると、管理対象組織にとってリスクが高いと考えられる除外項目を、ローカルの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. サイドバーの[環境]で[デバイス]を選択します。
デバイスページが表示されます。

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。

5.4.13 プレミアム製品でプロファイルを管理する

WithSecure Elements EPP for Computersと WithSecure Elements EPP for Serversには、それぞれ WithSecure Elements EPP for Computers Premiumと WithSecure Elements EPP for Servers Premiumというバージョンも用意されています。

これらには高度なセキュリティ機能が含まれています。最初の高度なセキュリティ機能は DataGuard で、ランサムウェアなどの脅威に対する追加の保護層を提供します。

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には、特定の場所を保護し、予期しないアプリケーションによるデータの変更を防止する WithSecure DataGuard 機能が追加されます。



注： DataGuard は、 WithSecure Elements EPP for Computers および WithSecure Elements EPP for Servers ソフトウェアのプレミアムバージョンでのみ利用可能です。プレミアムサブスクリプションをお持ちでない場合、DataGuard 機能はグレー表示され、使用できません。

DataGuard は、DeepGuard また、ユーザーコンテンツフォルダを監視します。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。DataGuard は、WithSecure Elements EPP for Computers および WithSecure Elements EPP for Servers が提供するすべてのセキュリティレイヤーを回避する新しいランサムウェアが発生した場合に特に役立ちます。



重要： DeepGuard DataGuard を機能させるには、これを有効にする必要があります。

DataGuard をセットアップします

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 **[の高度な動作ブロック]** を有効にしてください。
4. DataGuard が文書、画像、その他のエンドユーザーコンテンツを含むフォルダを自動的にチェックするようにするには、**「監視対象ユーザーデータフォルダを自動的に検出する」** を有効にしてください。
5. **[手動で含めたフォルダー]** と **[手動で除外したフォルダー]** では、エンドユーザーのコンピューター上の DataGuard 保護対象にフォルダーを追加または除外することができます。手順は次のとおりです。

- [手動で追加したフォルダー] で、[パスを追加]を選択します。



注: パスを追加すると、指定したパスとそのすべてのサブフォルダーが追加されます。たとえば、C:\Documentsを追加すると、DataGuardはC:\Documents配下のすべてのファイルとフォルダーを監視します。

- [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、指定したパスとそのすべてのサブフォルダーが除外されます。たとえば、C:\Documentsを除外すると、DataGuardはC:\Documents配下のすべてのファイルとフォルダーの監視を停止します。

6. [アクセス制御]を有効にして、DataGuardが保護するファイルやフォルダを変更できる信頼できるアプリケーションを定義します。

- DataGuardに信頼できるアプリケーションを自動的に検出させたい場合は、[信頼できるアプリケーションを自動的に検出する]を有効にしてください。
- 信頼できるアプリケーションを手動で追加する場合は、[手動で追加した信頼できるアプリケーションとフォルダー]の下にある [パスの追加] を選択します。



注: パスを追加すると、指定したパスとそのすべてのサブフォルダーが追加されます。たとえば、C:\Documentsを追加すると、DataGuardはC:\Documents配下のすべてのファイルとフォルダーを監視します。

DataGuardの設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

金庫を追加する

DataGuardに、特定のアプリケーションがフォルダに書き込める範囲を制限するボルトを追加します。

ボルトとは、そのボ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ーの書き込み、作成、名前変更を行えるフォルダーのことです。ボルトを使用すると、特定の場所へのアクセスを制限するため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ルト内にサブフォルダーを作成する場合は、%windir%\explorer.exeを信頼済みアプリケーションのリストに追加する必要があります。また、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SQL Server実行可能ファイルのみが変更できるようにしたい場合は、それを許可するボルトを作成します。

各ボルトには監視機能があります。アプリケーションがボ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。

ボルトを追加するには:

1. [セキュリティ構成] で、サイドバーの [プロファイル] を選択します。
[プロファイル] ページが開きます。
2. 編集するプロファイルを選択します。
[プロファイル] ページが開きます。
3. 左側のメニューから、[プレミアム]の下にある [データガード]を選択してください。
4. 下にスクロールして [保管庫]を選択し、[保管庫を追加]を選択します。
5. [保管庫へのパス] 欄にパスを入力してください。
6. [信頼できるアプリケーションを追加する]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、保管庫へのアクセスを許可したいアプリケーションへのパスを入力します。



注：信頼できるアプリケーションを追加するには、[信頼できるアプリケーションを追加]を選択します。

8. [保存して公開]を選択してください。

データガードの使用に関するヒント

これらのヒントは、Windows上で DataGuardで保護されたフォルダーと許可された場所を設定するのに役立ちます。

プログラムがProgramFilesフォルダから実行される場合、ブロックされません。しかし、同じプログラムが例えば AppData\Local フォルダから実行される場合、DataGuardによってブロックされます。そのため、WindowsではソフトウェアプログラムをProgram Files フォルダにインストールすることをお勧めします。Windowsには、マルウェア配布者がその場所に侵入しにくくするセキュリティ対策が組み込まれています。

ユーザーから安全でない場所へのアクセスを許可してほしいというリクエストがあり、それを許可した場合、DataGuardはその場所にあるすべてのファイルを許可します。これは特定のファイル名にも適用されます。たとえば、ある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。

DataGuardを有効にすると、ドキュメントなどのユーザーコンテンツを含むフォルダーが自動的にチェックされます。DataGuardがチェックするフォルダーを手動で追加することもできます。個々のユーザーの要求に基づいてパスを追加することもできますが、Windowsの場合は環境変数を使用することをお勧めします。たとえば、c:\user\JohnSmithを追加する代わりに、環境変数 %HOME% を使用してください。

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および 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: 事前設定されたセキュリティルールは WithSecure 侵入テスト担当者は、企業環境への侵入に使用される攻撃経路を網羅的に調査します。
- ポリシーの適用: ルールエディタを使用すると、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

アプリケーションコントロールを使用する

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. 開いた 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、以下のオプションから1つを選択してください。

オプション	説明
すべてのアプリケーションを許可する	除外ルールのいずれもアプリケーション、インストーラー、またはスクリプトをブロックしない場合、それは許可されます。
信頼できないアプリケーションをすべてブロックする	除外ルールのいずれにも該当しないアプリケーション、インストーラー、またはスクリプトはブロックされます。
すべてのアプリケーションを許可および監視します	除外ルールのいずれにも該当しないアプリケーション、インストーラー、またはスクリプトは許可されますが、その動作は監視され、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. 変更内容を保存して、現在のプロファイルまたは複数のプロファイルに公開します。



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。

変更内容は選択したプロファイルに適用されます。

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は決定は、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. 左側のメニューから [アプリケーション制御] を選択します。
4. 追加したいルールの種類に応じて、[新しいトップルールを追加] または [新しいルールを追加] を選択してください。
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。
7. アクションの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。

表11:除外ルール属性

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 filename (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。

表12:除外規則の条件

選択した条件	説明
に等しい	値は選択した属性と完全に一致する必要があります。たとえば、iexplore.exe です。
に等しくない	値が選択した属性と違う値である必要があります。
未満	数値は、選択した属性よりも小さいものである必要があります。
より大きい	数値は、選択した属性よりも大きいものである必要があります。
以下	数値は、選択した属性よりも小さい、またはまったく同じものである必要があります。
以上	数値は、選択した属性よりも大きい、またはまったく同じものである必要があります。
を含む	選択した属性が値を含めている必要があります (例: explore)。
開始値	選択した属性が指定した値で始まる必要があります (例: ie)。
終了値	選択した属性が指定した値で終わる必要があります (例: explore.exe)。



注: 各パラメータの内容に関する情報については、以下をご覧ください。**プロファイル** > **[アプリケーション制御を開き]**、**[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ます。各条件タイプごとの条件値の説明が表示されます。たとえば、ターゲットファイルのサイズは、起動され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単位で表示されます。

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:

- ルール条件で属性「ターゲットSHA1」または「親SHA1」を使用する場合は、イベントタイプとして**[アプリケーション開始]**を使用する必要があります。
- 動的リンクライブラリ (.dll) がブロックされている場合、それをアプリケーション制御で許可リストに追加するには、ルールで**[モジュールロード]**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、ルールで属性「ターゲットSHA1」や「親SHA1」を使用することはできません。
- **[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が実行されないようにする

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。

- 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
- [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。
- [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。

- [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。

- [条件]** ドロップダウンメニューから**[含む]**を選択します。
- [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: ターゲットファイルの説明に「Internet Explorer」が含まれているため、ファイル名や場所に関係なく、プログラムはブロックされます。

3. 除外ルールに2つ目の条件を追加します。

- [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。
- [条件]** ドロップダウンメニューから**[以下]**を選択します。
- [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。

アプリケーション制御イベントの種類

アプリケーション制御ルールで選択できるイベントの種類と、それぞれのイベントがトリガーされるタイミング。

表13:アプリケーション制御イベントの種類

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時に発生されます。
インストーラの開始	msiexec.exe が MSI パッケージをコマンドラインパラメータとして使用して起動されたときに発生されます。
ファイル アクセス	ファイルにアクセスするとトリガーされます。
アプリケーションの起動とモジュールの読み込み	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とモジュールの読み込みの際、および DLL がプロセスにロードされる時に発生します。

カスタム侵害指標の提出

カスタム侵害指標 (IOC) を送信することで、ファイルハッシュ、IPアドレス、ホスト名に基づいて検出ルールを作成し、これらの指標が検出された場合にシステムがどのように応答すべきかを定義できます。

IOC (侵害指標) は、管理対象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。特定の環境に合わせて、カスタム検出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、自社の内部調査など、信頼できる情報源からの脅威データを利用することで、より積極的な防御アプローチを取ることも可能です。

IOC検出ルールを作成する

独自の侵害指標 (IOC) ルールを作成することで、プラットフォームが脅威として指定したファイルハッシュ、IPアドレス、またはDNSホスト名を自動的に検出またはブロックできるようになります。

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、DNSoverHTTPS (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. 下[**セキュリティ構成**]選択[**プロファイル**]サイドバーに表示されます。
の**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、後でルールを識別および追跡するのに役立つ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広範囲コンテキスト検出 (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情報入力、インシデントタイムラインへの表示などを行い、イベントの全体像を把握できます。

IOCルールを設定したら、保存して公開することで、管理対象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の一貫した適用が保証されます。

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のサブスクリプションに含まれ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特定するのは難しい場合があります。システムイベント検出機能を使用すると、セキュリティ関連のWindowsイベントログエントリをWithSecure Elementsセキュリティセンターで直接特定できます。これらのイベントは、不審なアクティビティを示している可能性があります。調査して、正当な説明があるかどうかを確認してください。

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」)**] - 認証が失敗すること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 デバイスを標的とした認証試行が突然複数回発生した場合は、攻撃者がエンドポイントデバイスへのアクセス権を取得するために、ユーザー アカウントに対して複数の認証情報を送信している可能性があります。
- [**イベント ID: ユーザーロック (「ユーザーアカウントがロックされました」)**] - これは、認証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い兆候です。



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」)] - 攻撃者がデバイスへのアクセス権を取得すると、監査ログをクリアすることで痕跡を隠蔽しようとする可能性があります。このような場合、監査ログのクリアが正当な操作によるものではないことを確認する必要があります。



注：デフォルトでオフになっているイベントがいくつかあります。通常、これらは、SIEM または SOAR ソリューションに関連データを収集したいプロのセキュリティ運用管理チームにとって興味深いイベントです。このようなイベントはアクティビティの間接的な指標であるため、デフォルトではオフになっています。

システムイベント検出の設定

WithSecure Elements Agentが監視し、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サーバー用] または [Windowsコンピューター用] タブを選択し、編集するプロファイルを選択します。
[プロファイル] ページが開きます。
3. 左側のメニューから [システムイベント検出] を選択してください。
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. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

デバイスドライブの暗号化

Elements Endpoint暗号化機能を使用すると、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を確認できます。

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暗号化を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。また、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、デバイス詳細ページの左側メニューで確認できます。

リカバリキーは、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や、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にはリカバリキーが必要です。これらのキーを収集するためのツールは多数ありますが、いずれかを使用することが重要です。WithSecure Elements Endpoint Protection WithSecure、必要に応じてリカバリキーを収集できます。設定は、[一般] タブにあります。[プロファイル]。



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。

デバイスドライブを暗号化する

ドライブ暗号化のオン/オフ切り替えは、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に含まれ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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
2. ドライブを暗号化するデバイスを選択します。
3. ページ下部のアクションメニューから、**[システムドライブの暗号化]** > **[ドライブの暗号化]** を選択し、以下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]** を選択してください。

5.4.14 Server Protection

サーバー共有保護は、WithSecure Elements EPP for Serversのサブスクリプションに含まれ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。

許可および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。

検出可能な項目とその詳細は以下で確認できます。 **イベント** > **[セキュリティイベント]**。

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、編集するプロファイルを選択します。
Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護] を選択してください。
4. [許可および報告モード] の設定をオンにしてください。
5. [保存して公開] を選択してください。

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することを防止する

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、編集するプロファイルを選択します。
Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護] を選択してください。
4. [ユーザーアクセスをブロックする時間 (分)] 欄に時間を入力します。



注: デフォルトの時間は 30 分です。

5. [保存して公開] を選択してください。

共有フォルダを除外する

サーバー共有保護の監視対象から共有フォルダを除外します。

Server Share Protection は共有フォルダを監視し、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がある場合は、除外フォルダに追加できます。



注: 共有フォルダ全体を除外することはできますが、個々のサブフォルダ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、編集するプロファイルを選択します。
Windows サーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護] を選択してください。
4. [除外フォルダ] を選択し、次に [除外フォルダを追加] を選択します。
5. 除外する共有フォルダへのパスを入力します。
6. [保存して公開] を選択してください。

ユーザーを除外する

サーバー共有保護の監視およびファイル編集ブロックからユーザーを除外します。

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。

ユーザー名は、完全修飾形式（ドメイン名\ユーザー名）で入力するか、ユーザーSID（セキュリティ識別子）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、編集するプロファイルを選択します。
Windowsサーバーのプロファイルが開きます。
3. 左側のメニューから [サーバー共有保護] を選択してください。
4. [除外ユーザー] を選択し、次に [ユーザーを追加] 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. [保存して公開] を選択してください。

5.4.15 Elements Security CenterからElements Agentを再起動してください。

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. サイドバーの [環境] で [デバイス] を選択します。
デバイスページが表示されます。
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。

5.5 Elements EPP for Computers (Mac) でプロファイルを管理する

WithSecure Elements EPP for Computers (Mac) ソフトウェアにおけるプロファイル管理。

プロファイルとは、Mac 上の WithSecure Elements EPP for Computers クライアントに割り当てる設定の集合です。このセクションでは、プロファイルの作成方法と、アップデート、リアルタイムスキャン、スケジュールスキャン、スキャン除外、ブラウジング保護、ファイアウォールなどの設定構成方法について説明します。

5.5.1 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. [セキュリティ設定] > プロファイル > [Mac の場合は]、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。

Mac版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。

5.5.2 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] タブを選択してください。
3. 編集するプロファイルを選択します。
Mac版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 [一般設定] を選択してください。
5. [ユーザーが製品をアンインストールできるようにする設定] をオンにしてください。

5.5.3 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と、デバイスは一般提供開始前に最新の製品バージョンを受信できるようになります。

[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ン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: 新機能や今後追加される機能をテストするために、この設定をオンにすることをお勧めします。

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] タブを選択してください。
3. 編集するプロファイルを選択します。
Mac版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 [一般設定] を選択してください。
5. [クライアントソフトウェアへの早期アクセス] 設定をオンにしてください。
6. [保存して公開] を選択してください。

5.5.4 自動更新の設定

WithSecure Elements 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した場合は、[リモート管理プロキシアドレス] 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。

製品がアップデートを取得するために使用する社内 GUTS2 サーバーのアドレスを設定できます。製品は、設定済みで利用可能な場合は、まず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。そうでない場合は、グローバルサーバーからアップデートをダウンロードします。WithSecure サーバー、[グローバル WithSecure アップデート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は、**セキュリティ構成 > プロファイル > [一般設定]**。各サーバーについて、製品は許可されている HTTP プロキシ オプションを次の順序で確認します: [リモート管理 HTTP プロキシを使用する]; [システム環境設定からの 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)。

5.5.5 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] タブを選択し、次にプロファイルを選択します。
Mac 版のプロファイル 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. 以下のリアルタイムスキャンオプションを設定してください。
 - a) リアルタイム スキャンを有効にします。



注： この設定はオンにしておくことをお勧めします。

- b) [セキュリティクラウド (ORSP)] が有効になっていることを確認してください。



注： Security Cloud は、未知の悪意のあるアプリケーションやウェブサイトの脆弱性に関するセキュリティデータを収集します。この設定は有効にしておくことをお勧めします。

- c) [XFence] がオフになっていることを確認してください。



注： XFence は高度な機能であり、一般的な設置環境では無効にしておくことを推奨します。

5.5.6 Macでスキャンをスケジュールする

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] > [またはスケジュールスキャン] を選択してください。
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。

オプション	説明
毎日	毎日スキャンする
毎週	週のうち特定の日にスキャンを実施
月刊	毎月スキャン

6. 「スキャン開始」 で、以下のいずれかのオプションを選択してください。

オプション	説明
時間	スキャンを開始する時間を選択してください。コンピューターを使用していない時間帯を選択することをお勧めします。
分	スキャンを開始する分を選択してください。

5.5.7 スキャン除外設定

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**を選択し、プロファイルを選択します。
Mac 用のプロファイルが開きます。
3. [一般設定]を選択してください。
4. [すべてのセキュリティスキャンからフォルダーとファイルを除外する]の下にある「除外を追加」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ーとファイルは、すべてのセキュリティスキャンと対策から除外され、保護されません。WithSecure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、すべてのユーザーに対して「`folder-to-exclude`」に含まれるすべてのファイルを除外します。



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。

5.5.8 Macで隔離設定を構成する

ユーザーが隔離されたファイルを復元できるかどうか、およびファイルが隔離状態に置かれる期間を設定します。

本製品は、感染したファイルを見つけて隔離します。隔離設定では、ユーザーが隔離されたファイルを復元できるかどうか、および製品が古い隔離ファイルを自動的に削除するかどうかを制御できます。

隔離設定を構成するには：

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. **Mac 用** 選択し、プロファイルを選択します。
Mac 用のプロファイル が開きます。
3. 左側のメニューから **[スキャン設定]** を選択してください。
4. **[隔離]** 設定で、「ユーザーが隔離されたファイルを復元できる場合、**[ブロックおよび隔離されたアイテムをユーザーが解放できるようにする]**」をオンにします。
5. 隔離されたファイルを **[自動的に削除するには、「古い隔離アイテムを」自動的に削除する**」をオンにしてください。
6. **[隔離期間]** に、製品が隔離されたファイルを削除するまでの日数を入力します。

この隔離設定は、このプロファイルを使用するMacコンピュータに適用されます。

5.5.9 閲覧保護を設定する

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]** タブを選択し、次にプロファイルを選択します。
Mac版のプロファイル ページが開きます。
3. 左側のメニューから **[ブラウジング保護]** を選択してください。
4. 以下の閲覧保護オプションを設定してください。
 - a) **[閲覧保護機能]** をオンにしてください。



注： この設定を有効にしておくことを推奨します。

- b) **[ウェブコンテンツ制御]** を有効にすることができます。



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]** がオンになっていることを確認してください。



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。

5.5.10 Macのファイアウォールを有効にする

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] タブを選択し、次にプロファイルを選択します。
Mac版のプロファイル ページが開きます。
3. 左側のメニューから [ファイアウォール] を選択してください。
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。

オプション

説明

の上

Appleファイアウォールをオンにする

オフ

Appleファイアウォールをオフにする

外部委託管理

ファイアウォール設定が外部管理されている場合、変更は行われません。



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コンピュータでは、コマンドラインからファイアウォール設定を変更することはできません。」というメッセージが表示されます。このメッセージが表示された場合は、Appleファイアウォールのオプションで「外部管理」を選択してください。

5.5.11 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、ここでは次のように呼ばれます。WithSecureアプリケーション層ファイアウォール。

プロファイルエディタでは、[WithSecure Firewallの] オン/オフを切り替えたり、ファイアウォールプロファイルを編集したり、ファイアウォールルールを作成、エクスポート、インポートしたりできます。



注: 現在、設定できます WithSecureアプリ層ファイアウォールプロファイルは、WithSecure Elements Security Centerでのみ利用可能です。

WithSecureアプリ層ファイアウォールとは何ですか？

の WithSecure アプリ層ファイアウォールは、クライアントデバイスの送受信ネットワーク接続を制御します。設定は、アプリケーションカテゴリまたは個々のアプリケーションに適用できます。ファイアウォールプロファイルには、一連のアプリケーションのネットワーク接続を許可またはブロックする既製のルールが含まれています。また、個々のアプリケーションのトラフィックを許可またはブロックするルールを定義することもできます。

macOS のファイアウォールでは、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からの着信接続を許可またはブロックできます。WithSecure ファイアウォール WithSecure は、より幅広い設定が可能で、例えば、着信接続と発信接続の両方を許可またはブロックできます。単一のアプリケーション、あるいは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群に対して設定できます。

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]** タブを選択してください。
3. 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]** を選択してください。
5. 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。
6. **WithSecure プロファイルのファイアウォールルール** で、**[ルールの追加]** を選択し、以下の手順を実行します。
 - a) 「**アクティブ**」列のスイッチがオンになっていることを確認してください。
 - 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。

表14: ファイアウォールルールの指示

方向	説明
[入出庫]	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ージャー。
[で]	定義されたり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
[外]	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」欄に、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。通常はバンドル識別子と一致します。たとえば、com.apple.Safari などです。



注: 複数の識別子を入力する場合は、カンマで区切ってください。または、最後の文字としてワイルドカード (*) を使用することもできます。例: 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、macOS 用アプリケーションを提供するベンダーに Apple が割り当てる一意の識別子です。たとえば、APPLE や EQHXZ8M8AV などです。複数の識別子を入力する場合は、カンマで区切ることができます。例: APPLE, EQHXZ8M8AV

WithSecureによって信頼された」設定を使用する

WithSecureによる信頼済み」設定を使用して、信頼できるベンダーまたは開発者によって署名されたアプリケーションのネットワーク接続を許可またはブロックします。

この設定は、Mac コンピュータ用の WithSecure アプリ層 ファイアウォール プロファイルで使用してください。

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. [Mac用] タブを選択してください。

3. 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] を選択してください。

5. 編集したい WithSecure ファイアウォール プロファイルを選択してください。

6. WithSecure 設定を使用して、ベンダーまたは開発者によって署名された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します。WithSecure。

選択されたファイアウォール プロファイルは、信頼できるベンダーまたは開発者によって署名されたアプリケーションに対して、選択された接続動作を適用します。

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、編集したいプロファイルを選択してください。
3. **[ファイアウォール]**を選択してください。
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、ルールをインポートする.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。

署名とチーム識別情報を取得する

Applecodesign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** をを押します:
codesign -dv "<アプリケーションへのパス>"
4. 出力結果から、IdentifierフィールドとTeamIdentifierフィールドを探してください。

```
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: "/Applications/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: この共同署名出力では、署名識別子は「com.google.Chrome」、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: このコード署名出力では、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、Appleの組み込みアプリケーションであるため（つまり、識別子に「com.apple.」という接頭辞が付いているため）、「APPLE」を使用できます。

5.6 WithSecure Elements EPP for Linux でのプロファイルの管理

WithSecure Elements EPP for Linuxソフトウェアにおけるプロファイル管理。

プロファイルとは、WithSecure Elements EPP for Linuxクライアントに割り当てる設定の集合です。このセクションでは、プロファイルの作成方法と、接続設定、自動更新、リアルタイムおよびスケジュールスキャン、改ざん防止、整合性チェックなどの設定構成方法について説明します。

5.6.1 Linux 用の新しいコンピュータ プロファイルを作成します

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. **[セキュリティ設定] > プロファイル > [Linux の場合は]**、既存のプロファイルの横にある



を選択し、**[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たら、**[プロファイルを保存]**を選択してください。
新しいプロファイルが作成されます。

5.6.2 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、次に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 **[一般]** を選択してください。

4. アップデートのプロキシ設定を指定し、Security Cloud接続性:

Linux Protection アップデート (製品およびマルウェア定義) のプロキシ設定を構成し、Security Cloud (ORSP)

a) **[HTTPプロキシを使用する]** ようにオンにして、更新にプロキシを使用し、Security Cloud接続性。

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、**[プロファイルを保存]**を選択してください。

変更内容は保存され、現在のプロファイルに適用されます。

5.6.3 WithSecure Elementsコネクタを使用する

Linuxプロファイルで WithSecure Elementsコネクタの設定を構成します。

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用]** タブを選択してください。

3. 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。

4. 左側のメニューから **[一般設定]** を選択してください。

5. [WithSecure Elements Connector]内。

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

複数のコネクタを指定する場合は、セミコロンで区切ってください。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、[プロファイルを保存]を選択してください。

5.6.4 自動更新を設定する

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どのように処理するかを制御します。WithSecure製品およびマルウェア定義ファイルの更新。Linuxシステムで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 [一般] を選択してください。

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。

オプション	説明
[到着時]	アップデートはダウンロード後すぐにインストールしてください。
[一度]	特定の日時を指定して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時を両方設定してください。
[予定通り]	アップデートを定期的に特定の曜日と時間にインストールします。インストールする曜日と時間を指定してください。

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、[プロファイルを保存]を選択してください。

変更内容は保存され、現在のプロファイルに適用されます。

5.6.5 Linux 用クライアントソフトウェアへのアクセスを設定する

Linux デバイスが新しいWithSecure Elements エージェントバージョンを受信する方法を設定します。

[クライアントソフトウェアへのアクセス]設定は、Linuxデバイスが新しいソフトウェアを受信する方法を制御します。WithSecure Elementsエージェントのバージョン。更新のタイミングをどの程度制御し

たいかに応じて、[自動更新]、[手動による]更新」、または[スケジュールによる更新]を選択してください。

クライアントソフトウェアへのアクセスを設定するには：

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] タブを選択してください。
 3. 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。
 4. 左側のメニューから [一般設定] を選択してください。
 5. [クライアントソフトウェアへのアクセスを定義する] ドロップダウンメニューで、モードを選択します。
 - [自動アップデート機能]により、新しいバージョンがリリースされるとデバイスが自動的にアップデートされます。
 - [制御されたアップデート-手動アップデートでは、]デバイスをユーザーが選択したリリースグループのバージョンに維持します。
 - [制御されたアップデート-スケジュールされた]アップデートは、デバイスを自動的にアップデートしますが、設定したスケジュールに従ってのみ実行されます。
 6. [自動更新]を選択した場合は、サブモード [一般公開]または [早期公開]を選択してください。
[初期]デバイスは一般リリースに先駆けてアップデートを受け取ります。エージェントとエンジンのアップデートは約1週間早く、セキュリティ定義のアップデートは約2時間早く提供されます。
-  **重要：**問題が全端末に及ぶ前に発見できるよう、少数の代表的な端末を [早期]検出グループに割り当てることをお勧めします。
7. [制御された更新-手動]を選択した場合は、このプロファイルに割り当てるリリースグループのバージョンを選択してください。
 8. [制御された更新-スケジュール済み]を選択した場合は、更新チェックの繰り返し頻度、曜日、および1時間ごとの時間帯を設定してください。
 9. 変更を適用するには、[プロファイルを保存]を選択してください。
変更内容は保存され、現在のプロファイルに適用されます。

5.6.6 LinuxにEDRセンサーを統合する

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センサーを有効化および構成するには、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] タブを選択してください。
3. 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。
4. 左側のメニューから [一般設定] を選択してください。
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: この設定は有効にしておくことをお勧めします。無効にすると、EDRはエンドポイントへの攻撃を検知したり、警告を発したりしなくなります。

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. 変更を適用するには、**[プロファイルを保存]**を選択してください。

5.6.7 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用]** タブを選択してください。
3. 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。
4. 左側のメニューから **[一般設定]** を選択してください。
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、ユーザーはすべてをオフにすることができます WithSecure セキュリティ機能。



注: ユーザーが保護機能を無効にしてしまうことを防ぐため、この設定はオフにしておくことをお勧めします。

6. 変更を適用するには、**[プロファイルを保存]**を選択してください。

5.6.8 Linux のリアルタイムスキャンを設定する

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: この設定はオンにしておくことをお勧めします。

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)は未知のファイルをチェックします WithSecureSecurity Cloudさらなる保護のために。



注: この設定はオンにしておくことをお勧めします。

6. リアルタイムスキャン時にスキャンするファイルを指定します。

- 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す (何もスキャンされません)。

- 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どのように処理するかを指定します。

- 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。
変更内容は保存され、現在のプロファイルに適用されます。

5.6.9 Linux 用の手動スキャンを設定する

Linuxエンドポイント向けに、オンデマンド (手動) マルウェアスキャンを設定します。

手動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、次に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**] を選択してください。
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、[**プロファイルを保存**]を選択してください。
変更内容は保存され、現在のプロファイルに適用されます。

5.6.10 Linux のスキャンをスケジュールする

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、次に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] を選択してください。
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、[プロファイルを保存] を選択してください。

スケジュールされたスキャン設定は、このプロファイルを使用するLinuxデバイスに適用されます。

5.6.11 Linuxのスキャン除外設定を行う

Linux上でリアルタイムスキャンから除外するファイル、フォルダ、プロセスを定義します。

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. [Linux用] タブを選択し、次に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** を有効にします。

この設定により、エンド ユーザーがアクセスする、スキャンするファイルとフォルダーの設定で定義されたすべてのオブジェクトに対して、リアルタイムのマルウェア スキャンが有効になります。



注: この設定はオンにしておくことをお勧めします。

5. [Security Cloud (ORSP) の使用] がオンになっていることを確認します。

この設定では、未知のファイルの評判をチェックします。WithSecureSecurity Cloud。



注：この設定はオンにしておくことをお勧めします。

6. リアルタイムスキャン中にスキャンするファイルを選択します。

- a) スキャン対象 **[のファイルとフォルダを、]** 完全な絶対パスで指定してください。

ここで指定されているフォルダーとファイルはリアルタイムスキャンに含まれるため、WithSecure保護のため、個々のファイルまたはディレクトリの完全な絶対パス名を使用してください。リストされたディレクトリには、サブディレクトリも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す (何もスキャンされません)。

- b) **[スキャン対象から除外するファイルとフォルダ]** を指定します。

ここで指定されたフォルダーとファイルはリアルタイムスキャンから除外されるため、いかなる保護も適用されません。WithSecure保護。これには、すべてのユーザーに対して指定されたフォルダー内のサブフォルダも含まれます。



重要： 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、このオプションを使用してください。例えば、/ をスキャンから除外すると、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、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。

- c) **[信頼済みアプリケーション]** にパスを追加します。

信頼できるアプリケーションとプロセスへのパスのリスト。これらのアプリケーションとプロセスによって開かれるファイルは、その場所に関係なくスキャンされません。



重要： 絶対に信頼する必要があるアプリケーションとプロセスにのみ使用してください。例えば、ここに / を追加すると、すべてのアプリケーションとすべての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。

- d) **[実行可能ファイルのみ]** をスキャンするには、「実行可能ファイルのみをスキャン」をオンにしてください。

この設定では、実行可能ファイルのみをスキャンできます。

- e) **[潜在的に不要なアプリケーションのスキャン]** を有効にしてください。

この設定により、望ましくない可能性のあるアプリケーションのスキャンが有効になります。

7. リアルタイムスキャンでアーカイブを処理する方法を選択する

- a) **[アーカイブ内のファイルをスキャンするには、「アーカイブ内をスキャン」]** をオンにしてください。

アーカイブ内のファイルのスキャンを有効にします。

- b) **[暗号化されたアーカイブを安全でないものとして扱う]** を有効にすると、暗号化されたアーカイブをマルウェアとして扱うことができます。

暗号化されたアーカイブはマルウェアとして処理されます。

- c) **[スキャンアーカイブをネストレベルまで]** 設定して、スキャンする最大ネストレベルを指定します。

スキャン アーカイブの最大ネスト レベルを設定します。

- d) **[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設定]** をオンにします。

最大ネストレベルを超えるアーカイブはマルウェアとして処理されます。

8. リアルタイムスキャンのアクションを選択する

- a) **[マルウェアに対するアクション]**を選択してください：[何もしない]、[名前を変更する]、または[削除]。

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]、[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) **[不要な可能性のあるアプリケーションに対するアクション]**を選択してください：[何もしない]、[名前を変更する]、または[削除]。

PUA (潜在的に望ましくないアプリケーション) に対するアクションを選択してください。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]**を選択してください：[何もしない]、[名前を変更する]、または[削除]。

疑わしいファイルに対するアクションを選択します。



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. 変更を適用するには、[プロファイルを保存]を選択してください。

変更内容は保存され、現在のプロファイルに適用されます。

5.6.12 Linuxの整合性チェックを設定する

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、次に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]** を選択してください。

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]** を有効にする。

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選択してください。
[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、**[プロファイルを保存]**を選択してください。
 変更内容は保存され、現在のプロファイルに適用されます。

5.7 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。
 プロファイルとは、WithSecure Elements Mobile Protectionデバイスに割り当てる設定の集合です。このセクションでは、プロファイルの作成方法と、VPN、ブラウジング保護、マルウェア対策、スケジュールスキャン、Webサイトおよびアプリの例外設定など、プロファイルの設定方法について説明します。

5.7.1 新しいモバイルデバイス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. ログインして WithSecure Elements Security Center。
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]**タブを選択してください。
4. 既存のプロファイルの横にある

 を選択し、**[プロファイルの複製]**を選択します。
モバイル版プロフィー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。

5.7.2 ネットワークゲートウェイを有効にする

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。
モバイル版プロフィールページが開きます。
3. [ネットワーク保護の] 設定で、[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せん。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. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

5.7.3 ブラウザプラグインの有効化リマインダーを送信する

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. 下[セキュリティ構成] 選択[プロファイル] サイドバーに表示されます。
の [プロファイル] ページが開きます。
2. [モバイル向け] タブを選択してください。
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の有効化をユーザーに促す機能を] オンにします。
6. [保存して公開] を選択してください。
変更が保存され、選択したプロファイルに公開されます。

5.7.4 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] タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィー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]
- [不審と判断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. [保存して公開]を選択してください。

変更が保存され、現在のプロファイルに公開されます。

5.7.5 ブロックするウェブコンテンツを選択してください

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] タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィー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. [ウェブコンテンツ制御を] 有効にする。
6. 「Webコンテンツコントロール」の横にある ▼ を選択します。
Webコンテンツカテゴリ一覧が開きます。
7. 「許可しない」列で、モバイル端末でブロックしたいカテゴリをオンにしてください。
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. [保存して公開]を選択してください。

5.7.6 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] タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィー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. [ウェブサイトの例外設定]で、以下の手順を実行してください。

- 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。

5.7.7 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. 下[セキュリティ構成]選択[プロファイル]サイドバーに表示されます。
の**プロファイル**ページが開きます。
2. [モバイル向け]タブを選択してください。
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]の下にある[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]までスクロールダウンし、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。

5.7.8 セキュリティイベントにブロックされた悪意のあるWeb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. 下[セキュリティ構成]選択[プロファイル]サイドバーに表示されます。
の**プロファイル**ページが開きます。
2. [モバイル向け]タブを選択してください。

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]の下にある[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]までスクロールダウンし、これをオンにします。
- 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。

5.7.9 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] タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィー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、以下の手順を実行します。
 - 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) [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. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

5.7.10 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] タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィールページが開きます。
4. 左側のペインから [マルウェア対策] を選択します。
5. [マルウェア対策] を有効にしてください。



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. [保存して公開] を選択してください。
変更が保存され、現在のプロファイルに公開されます。

5.7.11 計測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. 下[セキュリティ構成]選択[プロファイル]サイドバーに表示されます。
の**プロファイル**ページが開きます。
2. [モバイル向け]タブを選択してください。
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 [マルウェア対策]を選択します。
5. [従量制スキャン]をオンにする。
6. [保存して公開]を選択してください。

変更が保存され、現在のプロファイルに公開されます。

5.7.12 感染症に対する対策を選択してください

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]タブを選択してください。
3. 編集するプロファイルを選択します。
モバイル版プロフィー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

5.7.13 モバイルデバイスでスキャンをスケジュールする

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]タブを選択してください。
3. 編集するプロファイルを選択します。

モバイル版プロフィー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]をオンにする。
- 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
[毎日]	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]	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。
[月刊]	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. [保存して公開]を選択してください。
変更が保存され、現在のプロファイルに公開されます。

第 章6

セキュリティを監視する

トピック：

- デバイスの操作
- デバイスのセキュリティを監視する
- セキュリティイベントを表示する
- Active Directoryをスキャンして保護されていないデバイスを検出します。
- デバイスをネットワークから隔離する
- デバイスを削除する
- サードパーティ RMM ツールを使用する

セキュリティを監視する

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

6.1 デバイスの操作

WithSecure Elements Security Centerから選択したデバイスに対して実行できる操作には、スキャン、プロファイルの割り当て、隔離、アンインストールなどがあります。

利用可能なデバイスアクション

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 - 「診断ファイルのリクエスト」を選択して、診断データのアップロードを許可するようユーザーにリクエストを送信します。WithSecureプライバシー保護のため、ユーザーには同意を求められます。また、デバッグログを有効にし、自動的に無効になるまでの時間を指定することもできます。

- 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を選択します (ファイアウォール、DeepGuard (リアルタイムスキャン、リソース保護など) を無効にするか、すべてのセキュリティ機能をオフにする)
- 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。

6.2 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: Elements Security Centerでは、スコープセクターを使用して表示する情報の詳細レベルを選択できます。これを使用して、次の項目を切り替えることができます。

顧客企業の概要または
特定の企業に関する詳細情報

6.2.1 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。

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. 選択[**ホーム**]サイドバーに表示されます。

の**ホーム**ページが表示されます。

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。
 - エンドポイント保護
 - 検出と対応
 - Collaboration Protection
 - 過去30日間の使用状況
 - サブスクリプション
- **[エンドポイント保護]**以下のように表示されます。
 - 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
 - 問題点 - 対処すべき問題点の一覧 (項目タイプ、深刻度、影響を受けるデバイスの数)
- **[検出とレスポンス]**以下のように表示されます。
 - 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
 - カテゴリー別の検出結果

- デバイス数別のOS
- **[露出]** (露出管理サブスクリプションが必要です) 以下を表示します。
 - カバレッジ
 - 組織の露出リスク
 - 最も影響力のある推奨事項
 - カテゴリー別の曝露リスク
 - 最も高いエクスポージャーリスクを持つ資産
- **[クラウドセキュリティトレンド]** (エクスポージャー管理サブスクリプションが必要です) には、以下の情報が表示されます。
 - 発見件数
 - スキャンされたリソースの数
 - タグで検索
 - 所見の重症度
- **[外部攻撃対象領域]** (エクスポージャー管理サブスクリプションが必要です) には、以下の情報が表示されます。
 - 総資産数
 - 最近発見された資産
 - 時間の経過に伴う資産



注: エクスポージャー管理のサブスクリプションがない場合、**[露出]****[クラウドセキュリティのトレンド]**および**[外部攻撃対象領域]**タブには、ウィジェットの代わりに「**トライアルをリクエスト**」ボタンとリンクが表示されます。

2. 選択した会社のより詳細な **会社ステータス** 情報を表示するには、**ホームページ**を開き、**スコープセクター**で会社を選択します。

6.2.2 フィルター装置

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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
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. 「値」ドロップダウンメニューから、選択したカテゴリに希望する値を選択してください。



注: 例えば、カテゴリとして **[接続状態]** 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. **[適用]** を選択してください。
5. 選択したフィルターカテゴリと値をリセットするには、**[フィルターをクリア]** 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。

6.2.3 モバイルデバイスを検索

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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
2. 選択してください **[モバイル デバイス]** タブ。



ヒント: フィルタ機能はデバイスの検索にも活用できます。

3. **[検索]** 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。

6.2.4 デバイスの保護ステータスを表示する

WithSecure Elements Endpoint Protection アカウントに追加された各デバイスに関する詳細情報 (保護ステータス、サブスクリプションの詳細、デバイス情報、インストールされているソフトウェア、統計情報など) を確認できます。

WithSecure Elements Endpoint Protection に追加された各デバイスには、保護ステータス、サブスクリプションの詳細、デバイス情報、インストールされているソフトウェア、および統計情報を表示する詳細ビューがあります。

デバイスの保護状態の詳細を表示する

[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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
2. デバイスページで、**[コンピュータ]**、**[モバイル デバイス]**、**[コネクタ 管理]**、または **[対象外デバイス]** タブ。
選択したタイプに一致するデバイスの詳細を含む表が表示されます。デフォルトでは、**[全体ステータス]** 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

コネクタの場合、次のビューを使用できます。

- コネクタすべて

選択した情報が表に反映されます。

6.2.5 デバイスのセキュリティ状態を確認する

デバイスがセキュリティに関する推奨事項に準拠しているかどうかは、「**デバイスのセキュリティ状態**」ページで確認できます。

お使いのデバイスのセキュリティに関する推奨事項を表示するには：

1. WithSecure Elements Security Centerで、**[デバイスのセキュリティ状態]**を選択します。**[環境]**サイドバーに表示されます。
デバイスのセキュリティ状態ページが表示されます。**[セキュリティ推奨事項]**パネルには、デバイスが**[準拠している]**推奨事項と**[準拠していない]**推奨事項の数が表示され、その後に個々の推奨事項の一覧表が表示されます。
2. 表の各列を確認して、デバイスのセキュリティ状況を評価してください。
この表には以下の列が表示されます。
 - **[セキュリティ推奨事項]**- 推奨されるセキュリティ設定の名前。
 - **[ステータス]**- デバイスが推奨事項に準拠しているか、準拠していないかを示します。
 - **[デバイス数]**- 推奨事項の影響を受けるデバイスの数。
 - **[プロファイル数]**- 推奨事項の影響を受けるプロファイルの数。
 - **[対応プラットフォーム]**- この推奨事項がサポートされているプラットフォーム。**[セキュリティ推奨事項]**または**[サポート対象OS]**で表をフィルタリングできます。
3. 詳細情報をご覧になるには、おすすめ商品を選択してください。
設定の説明、解決されない場合の潜在的なリスク、および関連するベンダーのドキュメントへのリンクを示すパネルが開きます。
4. 推奨事項を解決するには、推奨事項に記載されている設定を更新してください。
[プロファイルでパスワードなしでクライアントをアンインストールできる]などの推奨事項は、プロファイル内の該当する設定を更新することで解決できます。**[最小パスワード長が定義されていないか、8文字未満である]**などのその他の推奨事項は、グループポリシー設定などのオペレーティングシステムレベルの設定を変更することで解決できます。

6.3 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、適切な措置を講じてください。

セキュリティ イベントを表示するには:

1. スコープセクターを使用して、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するには、イベント名の横にある



アイコンを選択してください。

詳細ビューが開きます。内容は以下のとおりです。

- **[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。
- **[誤検出の可能性を報告する]**- 通知 WithSecure将来の脅威検出精度を向上させるため、誤っている可能性のある検出結果について報告する。
- **[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。

6.3.1 セキュリティイベントをフィルタリングする

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は、フィルタリングすることができます。

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 [デバイスの種類] 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てください。



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]を選択してください。

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。

6.4 Active Directoryをスキャンして保護されていないデバイスを検出します。

WithSecureによってまだ管理されていないデバイスを、管理対象組織のActive Directoryからスキャンします。

保護されていないデバイスとは、管理対象組織のActive Directoryに登録されているコンピューターまたはサーバーのうち、WithSecureによってまだ管理されていないデバイスのことです。保護されていないデバイスは、新規デバイスであるか、WithSecure Elements Security Centerから完全に削除されたデバイスのいずれかです。

スキャンが開始されると、Elements Security Center は各 Active Directory ノードでスキャン操作を実行する1つ以上のデバイスを自動的に選択します。これらのデバイスは WithSecure-管理対象デバイス ページ。スキャン操作を行う際、Elements Security Centerは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. サイドバーの [環境] で [デバイス] を選択します。

デバイス ページが表示されます。

2. 選択してください [対象外デバイス] タブ。

3. [スキャン開始] を選択してください。

システムは、管理対象組織の *Active Directory* をスキャンして、保護されていないデバイスを検出します。スキャンが完了すると、ページ上部にノード名とスキャンに使用されたデバイスが表示されます。保護されていないデバイスは、以下の表に一覧表示され、それぞれの情報が表示されます。

- 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



•

アイコンの列には、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、スキャン完了後24時間で削除されます。



注: 保護されていないデバイスを Elements Security Center に追加するには、そのデバイスに WithSecure Elements Agent を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あっても、そのデバイスを信頼できると判断した場合は、信頼済みとしてマークすることができます。これを行うには、デバイスの行にある



を選択します。

5. [信頼済みとしてマーク] を選択してください。

6. 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) デバイスの行にある



を選択し、次に [コメント] を選択します。

- b) コメントを入力し、[保存] を選択してください。

6.5 デバイスをネットワークから隔離する

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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
2. ネットワークから隔離するホストを選択します。
3. ページ下部のアクションメニューから、**[ネットワーク分離]** > **[ネットワークから分離]** を選択します。
選択したデバイス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再接続するには、**[ネットワーク隔離から]** > **[ネットワーク隔離]** を選択します。

デバイスの隔離状態を解除すると、ネットワークとの通信が再び可能になります。

6.6 デバイスを削除する

WithSecure Elements Security Centerからデバイスを削除し、サブスクリプションのライセンスを解放します。

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は、そのデバイスが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は、デバイスはElements Security Centerに表示されず、保護されません。

[デバイスからの返却をブロックする] オプションをオンにすると、そのデバイスはブロックリストに移動されます。



注: デバイスを再度追加するには、横にある

アイコンを選択します。**[デバイス]** 次に、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**」オプションを選択します。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れば、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. サイドバーの **[環境]** で **[デバイス]** を選択します。
デバイス ページが表示されます。
2. Elements Security Centerから削除したいデバイスを1つ以上選択してください。



注: デバイスを削除する前に、正しいデバイスを選択したことを確認してください。

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、**[デバイスの削除]** 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、**[デバイスの返却をブロック]** を選択し、**[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: [ブロックリストからデバイスを復元する]管理>サブスクリプションブロックリストに移動したデバイスを再度追加することができます。その場合、デバイスが再接続した際に、サブスクリプションに空きライセンスがあれば、デバイスリストに再び表示されます。

6.7 サードパーティ RMM ツールを使用する

WithSecure Elements EPPは、サードパーティ製のリモート監視・管理 (RMM) ツールの統合をサポートしています。



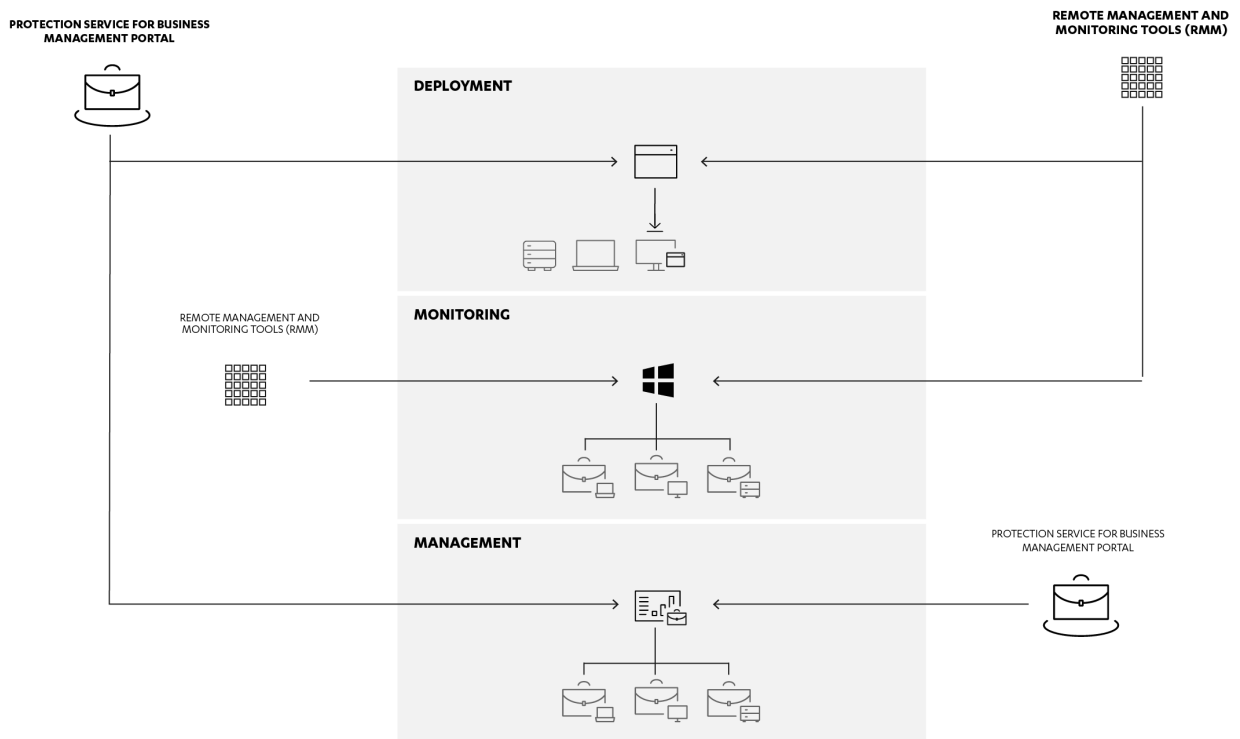
注: WithSecure Elements EPPの現行バージョンは、Datto、Kaseya、およびSolarWindsのRMMツールをサポートしています。その他のRMMツールと連携する場合は、Windows Management Instrumentation (WMI) APIを使用してください。

WithSecure Elements Security Centerを使用すると、システムの展開、監視、管理を行うことができます。ただし、RMM ツールを使用したい場合は、以下の手順を実行してください。

- MSIパッケージを展開し、RMMツールを使用してシステムを監視し、Elements Security Centerを使用してシステムを管理します。
- Elements Security Centerを通じてシステムを導入・管理し、RMM ツールを使用してシステムを監視できます。



注: システムの管理は、Elements Security Centerを通じてのみ可能です。



6.7.1 Kaseya RMM との連携 (Windows)

Kaseyaポータルは、既製のエージェント手順を使用して、WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversを監視および管理します。

Kaseyaポータルにある既製のエージェント手順を使用して、WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversを監視および管理します。

WithSecureダウンロードサイトから、既製のエージェント手順をダウンロードしてください。

手順をインポートすると、以下のエージェント手順が利用可能になります。必要に応じて、Kaseyaの標準機能を使用して、これらの手順の一部またはすべてをスケジュールできます。

CheckProductInstalled WithSecure Elements EPP for ComputersまたはWithSecure Elements EPP for Serversソフトウェアがインストールされているかどうかを検出します。製品がインストールされていない場合は、警告が表示されます。このプロシージャは、他のすべてのプロシージャから呼び出されます。これは、他のプロシージャが動作するために製品のインストールが必要だからです。

CheckWmiProviderEnabled WMIプロバイダモジュールが有効になっているか検出します。モジュールが無効の場合、警告が発行されます。WMIプロバイダモジュールが機能するために必要であるため、このプロシージャは他のすべてのプロシージャ(CheckProductInstalledを除く)によって呼び出されます。



注: プロファイル設定のWithSecure Elements Security CenterでWMIプロバイダーをオンにすることができます。

CheckLicenseStatus 製品のサブスクリプションステータスを確認します。サブスクリプションが失効しているか、インストールされていない場合、警告が発行されます。

CheckDefinitionsAreUpToDate ウイルス対策定義が更新されているか確認します。7日以上経過している場合、警告が発行されます。インターネット接続または他の障害に関する問題が発生している可能性があります。

CheckConnectivityToManagementPortal Elements Security Centerへの接続を確認します。接続が成功してから24時間以上経過している場合は、アラートが発行されます。これは、インターネット接続の問題やその他の障害を示している可能性があります。

RunFullComputerScan フルコンピュートースキャンを実行します。感染したオブジェクトが検出されると、警告が発行されます。

CheckRealTimeScanning リアルタイムスキャンが有効になっているか確認します。無効の場合、警告が発行されます。

CheckDeepGuard チェックします DeepGuardモジュールがオンになっている場合。オフになっている場合は、アラートが発行されます。

CheckFirewall ファイアウォールモジュールが有効になっているか確認します。無効の場合、警告が発行されます。

CheckBrowsingProtection ブラウザ保護モジュールが有効になっているか確認します。無効の場合、警告が発行されます。

CheckSoftwareUpdater ソフトウェアアップデーターモジュールが有効になっているか確認します。無効の場合、警告が発行されます。

輸入代理店の手続き

WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversのインストールおよび監視手順をKaseyaポータルにインポートします。

エージェント手順をインポートするには

1. Kaseyaポータルにログインします。
2. [エージェント手順]モジュールを開きます。
3. [手順の管理]で[スケジュール/作成]を選択します。
4. 右側のペインで、[共有]を右クリックします。
5. 開いたメニューから[フォルダ/手順のインポート]を選択し、アップロードするXMLファイル (Kaseya_F-Secure.xml) を指定します。

6.7.2 リモートのMacコンピュータにKaseyaエージェントをインストールする

リモートのMacコンピュータにKaseyaエージェントをインストールします。

Kaseya エージェントをリモート コンピューターに手動でインストールするには

1. Kaseya ポータルにログインします。
2. エージェントパッケージをダウンロードするには、[エージェント] > [パッケージ] > [パッケージの管理]を選択してください。



注: Macintosh エージェントのインストールパッケージの完全なファイル名はKcsSetup.appです。このパッケージはKcsSetup.zipファイルとしてダウンロードされ、その中にAgentというフォルダがあり、その中にKcsSetup.appが含まれています。

3. KcsSetup.zipファイルを選択して展開してください。
4. エージェントフォルダを選択してください。
5. 実行するには、KcsSetup.appファイルを選択してください。
6. WithSecure Elements EPP for Computers (Mac) のインストール」で説明されているように、Kaseya エージェントの手順を使用して WithSecure Elements EPP for Computers (Mac) ソフトウェアをインストールします。

WithSecure Elements EPPをコンピュータ (Mac) にインストールする

Kaseyaエージェントの手順を使用して、コンピュータ (Mac) 用のWithSecure Elements EPPをインストールします。

Kaseyaエージェントの手順を使用して、WithSecure Elements EPP for Computers (Mac) をインストールするには :

1. エージェント手順モジュールにナビゲートして、PKG ファイルをアップロードします。
2. [スケジュール/ ファイルの作成 /] > [ファイルの管理]を選択します。
3. サーバー上のファイルをアップロードします。



注: サーバーに保存されているファイルはスクリプトを介してエージェントに送信できません。

4. 新しいエージェント手順を作成するには、[エージェント手順] > [スケジュール] /] > [新しい手順]を選択します。



注: Kaseya が提供する OS X 用のエージェント手順モジュールは限られています。



注: writeFileモジュールを使用すると、PKGファイルをリモートマシンの指定した場所に書き込むことができます。パッケージをインストールするには、installPKGモジュールを使用します。例 :

```
writeFile("F-Secure_PSB_Mac_Installer[License key].pkg", "/tmp/ F-Secure_PSB_Mac_Installer[License key].pkg", "Mac OS X", "Halt on Fail")
installPKG ("/tmp/ F-Secure_PSB_Mac_Installer[License key].pkg", "Mac OS X", "Halt on Fail")
```

5. エージェント手順を実行またはスケジュールするには、エージェント手順の一覧から新しく作成したエージェント手順を選択します。

6. 対象デバイスを選択してください。
7. 「エージェント手順のスケジュール設定」または「今すぐ実行」を選択してください。

6.7.3 Kaseya RMM との連携 (Linux)

Kaseyaポータルは、既製のエージェント手順を使用して WithSecure Linux Protectionをインストールおよび監視します。

Kaseyaを使用すると、管理対象のLinuxコンピュータに WithSecure Linux Protectionをインストールして監視できます。このセクションでは、エージェント手順のインポート方法、ソフトウェアのインストール方法、およびKaseyaポータルを介したリモートインストール方法について説明します。

WithSecureダウンロードサイトから、既製のエージェント手順をダウンロードしてください。

輸入代理店の手続き

Kaseyaポータルを使用して、WithSecure Linux Protectionのインストールおよび監視手順をインポートします。

エージェント手順をインポートするには

1. Kaseya ポータルにログインします。
2. [エージェント手順]モジュールを開きます。
3. [手順の管理]で[スケジュール/作成]を選択します。
4. 右側のペインで、[共有]を右クリックします。
5. 開いたメニューから[フォルダ/手順のインポート]を選択し、アップロードするXMLファイル (Kaseya_F-Secure_Linux_Procedures.xml) を指定します。

エージェント手順

WithSecureリモートクライアントのステータスを確認し、KaseyaRMMポータルに報告するために、次のエージェント手順を使用できます。

- *CheckProductInstalledForLinux* - WithSecure Linux Protectionソフトウェアがインストールされているか検出します。製品がインストールされていない場合、警告が発行されます。この手順は、機能させるために製品のインストールが必要なため、他のすべての手順によって呼び出されます。
- *CheckLicenseValidForLinux*は、製品のサブスクリプションの状態を確認します。製品がオフになっている場合は、警告が表示されます。サブスクリプションの有効期限が切れている場合、または製品がインストールされていない場合も、警告が表示されます。機能チェックを実行するには製品がアクティブである必要があるため、このプロシージャは他のすべてのプロシージャ (*CheckProductInstalledForLinux*を除く) から呼び出されます。
- *CheckRealTimeScanningForLinux* - リアルタイム スキャンが有効になっているか確認します。無効の場合、警告が発行されます。
- *CheckIntegrityCheckingForLinux* - 完全性検査がオンになっているかどうかをチェックします。オフの場合、アラートが発行されます。
- *CheckDatabaseUpToDateForLinux* - ウイルス対策定義が更新されているか確認します。7日以上経過している場合、警告が発行されます。インターネット接続または他の障害に関する問題が発生している可能性があります。



注: 必要に応じて、Kaseya の標準的な方法を使用して、Procedure (手順) の一部または全部をスケジュールすることができます。

リモートコンピュータにKaseyaエージェントをインストールする

リモートコンピュータにKaseyaエージェントをインストールします。

Kaseyaエージェントをインストールするには

1. Kaseyaポータルで、**[エージェント]>[パッケージ]>[パッケージの管理]**を選択して、エージェントパッケージ (KcsSetup.sh) をダウンロードします。
2. ダウンロードしたファイルを実行します。

WithSecure Linux保護をインストール

Kaseyaポータルを使用して、WithSecure Linux Protectionソフトウェアをインストールします。

WithSecure Linux Protectionをインストールするには：

1. WithSecure Elements Security Centerで、**ダウンロード**ページ。
2. Linux環境では、**[Generic]**を選択して linuxsecurity-installer.tarアーカイブをダウンロードしてください。
3. tarアーカイブから linuxsecurity-installerファイルを抽出します。
4. リモートデバイスにソフトウェアをインストールするためのエージェント手順を作成するには



注：Kaseyaが提供するLinux用のエージェント手順モジュールは限られています。

- a) **[エージェント手順]**モジュールを開き、抽出したインストーラーファイルをKaseyaポータルにアップロードします。
- b) **[スケジュール] → 「ファイルの作成」>[ファイルの管理]**を選択します。
- c) サーバー上のファイルをアップロードします。



注：サーバーに保存されているファイルはスクリプトを介してエージェントに送信できます。

- d) ソフトウェアのインストール手順に、サンプルエージェントの手順を参考にします。

[LinuxProtectionのインストール(使用前に編集してください)] の手順を編集して、WithSecure Linux Protectionのサブスクリプションキーを含め、アップロードされたインストーラーへのパスを修正してください。



注：製品をインストールする前に、リモート デバイスに WithSecure Linux Protection の依存関係 (ディストリビューション固有のもの) がインストールされていることを確認してください。サンプル プロシージャに必要なパッケージのインストールを追加するには、executeShellCommandまたはexecuteShellCommandToVariableステートメントを使用できます。詳細については、LinuxProtection のドキュメントを参照してください。

- e) エージェントプロシージャの実行をスケジュールするには、利用可能なプロシージャのリストからエージェントプロシージャを選択します。
- f) 対象デバイスを選択してください。
- g) **[エージェント手順のスケジュール]**または**[今すぐ実行]** のいずれかを選択してください。

6.7.4 SolarWinds MSP RMM との連携 (Windows)

SolarWinds MSPを使用すると、WithSecure Elements EPP for ComputersおよびWithSecure Elements EPP for Serversソフトウェアを管理できます。

詳細については、N-ableユーザーガイドを参照してください。

6.7.5 Macコンピュータ向けSolarWinds MSP RMMとの統合

SolarWinds MSPを使用して、WithSecure Elements EPP for Computers (Mac) ソフトウェアを管理します。

デバイスが「**すべてのデバイス**」ビューに表示され、選択したリモートデバイスに対して「**リモートコントロール**」オプションが有効になっていることを確認してください。また、以下のものも必要です。

- 製品のサブスクリプションキー
- ローカルまたはネットワーク共有にある、コンピュータ用WithSecure Elements Agent (Mac) のパッケージ

MSP N-Centralを使用してリモートデバイスに製品をインストールする

1. MSP N-Central にログインします。
2. macOS エージェントをリモート macOS デバイスにダウンロードします。
3. [リモートコントロール]を使用して、WithSecure Elements Agent for Computers (Mac) パッケージをリモートデバイスにコピーします。
4. リモートデバイスでinstall_mac_client.shスクリプトを実行するために、Macスクリプトタスクを実行します。



注: スクリプトを実行するには管理者権限が必要です。このスクリプトは、リモートデバイスのパッケージパス、パッケージ名、および製品のサブスクリプションキーの各コマンドライン引数を受け入れます。

```
sh install_mac_client.sh -p /Users/Shared/F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg -n F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg -k 4T16-E2VW-U2U9-J5V8-9Z0F
```

レポート用のカスタムサービスをインポートする

WithSecureリモートクライアントがSolarWindsRMMポータルにステータスを報告する方法についての説明。

カスタム サービスをインポートするには

1. リモートコンピュータに WithSecure Elements EPP for Computers (Mac)ソフトウェアがインストールされていることを確認してください。
2. [管理] > [サービス管理] > [カスタムサービス] > [インポート]を選択します。
3. レポート用のカスタム サービスを含むすべての XML ファイルを参照してインポートします。



注: XMLファイルは以下のリンクから入手できます: SolarWindsカスタムサービスファイル (Mac用)

4. モニタリング用のカスタム サービスを追加するには
 - a) これらのカスタムサービスを監視するデバイスを選択するには、[表示] > [すべてのデバイス]に移動してください。
 - b) 次に、[デバイスの詳細] > [監視の] > [追加]を選択します。
インポートしたすべてのカスタム サービスを表示できます。

- c) 以下のカスタムサービスをそれぞれ追加してください。
- d) 変更を適用してください。

サービスが更新され、個々の設定のレポートを見ることができます。WithSecureリモートマシン上のクライアント。各設定の状態に基づいて、レポートには、期待される動作と一致しない場合に、失敗または警告が表示されます。

Mac コンピューターで利用できるカスタム サービス

要件に応じて、関連するカスタム サービスをインポートできます。

- WithSecure アンチウイルス データベース ステータス (Mac用) - データベースのステータスを表示します。データベースが最新でない場合、警告が表示されます。
- WithSecure アンチウイルス ファイアウォール管理 (Mac用) - システム ファイアウォールのステータスを表示します。ファイアウォールがオフの場合、警告が表示されます。
- WithSecure アンチウイルス保護 (Mac用) ステータス - リアルタイム スキャンのステータスを表示します。リアルタイム スキャンがオフの場合、エラーが表示されます。
- WithSecure アンチウイルス Safari 拡張機能 (Mac用) - Safari 拡張機能がオンになっている場合に表示されます。オフにすると、警告が表示されます。
- WithSecure アンチウイルス ウイルス保護 (Mac用) - ウイルス保護のステータスを表示します (「ライセンスの有効期限が切れました」、「OASが無効」、「OASエラー」、「古いアップデート」など)。
- WithSecure ブラウザ保護 (Mac用) ステータス - ブラウザ保護のステータスを表示します。オフにすると、警告が表示されます。

6.7.6 SolarWinds MSP RMM との連携 (Linux)

WithSecure Linux Protectionを導入した管理対象の Linux デバイスは、SolarWinds MSP N-Central を通じて監視できます。

Linux デバイスとそのデバイスにインストールされている WithSecure Linux Protectionソフトウェアの状態を監視するには、SolarWinds独自のLinuxエージェントがデバイス上で実行されている必要があります。インストール手順については、N-Central ユーザーガイドの「Linux エージェントのインストール」セクションを参照してください。



注: MSP N-CentralではLinuxデバイスのサポートが限られているため、リモートデバイスへの WithSecure Linux Protectionソフトウェアの自動インストールはできません。WithSecure Linux WithSecureソフトウェアのインストール手順は、Linux Protectionインストールガイドに記載されています。

レポート用のカスタムサービスをインポートする

WithSecureリモートクライアントの状態をSolarWinds RMMポータルに報告します。

リモートコンピュータに WithSecure Linux Protectionソフトウェアがインストールされ、rmmドサービスが有効になっていることを確認してください。

カスタムサービスをインポートするには

1. [管理] > [サービス管理] > [カスタムサービス] > [インポート]を選択します。
2. レポート用のカスタム サービスを含むすべてのXML ファイルを参照してインポートします。



注: XML ファイルは、次のリンクから入手できます: SolarWinds カスタム サービス ファイル (Linux用)。

3. モニタリング用のカスタム サービスを追加するには

- a) **[表示] > [すべてのデバイス]**に移動し、これらのカスタムサービスを監視するデバイスを選択します。
- b) **[デバイスの詳細] > [監視の] > [追加を]**選択します。
インポートしたすべてのカスタム サービスを表示できます。
- c) 以下のカスタムサービスをそれぞれ追加してください。
- d) 変更を適用してください。

サービスが更新され、個々の設定のレポートを見ることができます。WithSecureリモートマシン上のクライアント。各設定の状態に基づいて、期待される動作と一致しない場合は、レポートにエラーまたは警告が表示されます。

利用可能なカスタムサービス

要件に応じて、監視用の関連するカスタムサービスを追加できます。

Linuxコンピューターで利用可能なカスタムサービスは次のとおりです。

- WithSecureアンチウイルスデータベースのステータス(Mac用)-データベースのステータスを表示します。データベースが最新でない場合、警告が表示されます。
- WithSecureアンチウイルス (Linux用) 完全性チェックの保護ステータス-完全性チェックのステータスを表示します。完全性チェックがオフの場合、エラーが表示されます。



注: 整合性チェック用にファイルパスが追加されていない場合も、この機能はオフになっていると見なされます。

- WithSecureアンチウイルス (Linux用) のライセンスステータス-製品ライセンスのステータスを表示します。ライセンスが無効な場合は、エラーが表示されます。
- WithSecureAV製品 (Linux用) のステータス-製品のマスタースイッチのステータスを表示します。製品の電源が切れている場合は、エラーが表示されます。
- WithSecureリアルタイムアンチウイルス保護 (Linux用) のステータス-リアルタイムスキャンのステータスを表示します。リアルタイムスキャンがオフの場合、エラーが表示されます。



注: スキャン用のディレクトリが含まれていない場合も、この機能はオフになっていると見なされます。

RMMの上流レポート機能を有効にする

WithSecureLinuxProtectionをインストールした後、RMMアップストリームレポートサービスを有効にして、デバイスがSolarWinds MSPにステータスを報告するようにします。

WithSecureLinuxProtectionをインストールしたら、RMMアップストリームレポートサービスを有効にしてください。

ルートユーザーとして、以下のコマンドを実行してください。

```
/opt/f-secure/linuxsecurity/bin/setup-rmmd.sh install
```



ヒント: サービスが不要になったら、アンインストールオプションを指定してコマンドを実行し、サービスを削除してください。

6.7.7 Datto RMM との連携 (Windows)

Dattoプラットフォームを使用して WithSecure Elements EPP for Computersをインストールおよび管理するために使用できるコンポーネントに関する情報。

Dattoのオンラインコンポーネントリポジトリ (ComStore) には、以下のものが含まれています。

WithSecure構成要素:

WithSecure Elementsエージェントの展開 [WIN]	このスクリプトコンポーネントを使用して、対象コンピュータに WithSecure Elements EPP for Computersをインストールします。実行時には、有効なライセンスキーコードを入力し、リストから適切な地域を選択する必要があります。
WithSecure Elements エージェントタスク [WIN]	このスクリプトコンポーネントを使用すると、WithSecure Elements EPP for Computersがインストールされているエンドポイントでタスクを実行できます。利用可能なタスクには、コンピュータ全体のスキャンやセキュリティ更新プログラムのインストール (重大、重要、またはすべての更新プログラム) などがあります。
WithSecure Elements Agent Monitor [WIN]	この監視コンポーネントを使用して、現在の状態を確認できます。WithSecure WithSecure EPP for Computersがインストールされているかどうか、現在のライセンスの状態、各種保護コンポーネントの状態、ウイルス対策定義ファイルの有効期限、および不足している重要な更新プログラムなどを確認できます。各チェック項目は、オンまたはオフに切り替えることができます。

すべてのコンポーネントの詳細については、Datto RMM 管理ポータルの説明を参照してください。すべての構成変数にはヘルプ テキストが含まれています。

これらのコンポーネントの最新バージョンは、以下のリンクからも入手できます : DattoRMMコンポーネントパッケージ

6.7.8 Datto RMM との連携 (Mac)

WithSecure Computer Protection for Macは、Datto RMMプラットフォームを介して管理対象のMacコンピュータにインストールおよび監視できます。

Datto RMMを使用すると、管理対象のMacコンピュータに WithSecure Computer Protection for Macをインストールして監視できます。このセクションでは、DattoRMMを介してソフトウェアをインストールする方法と、そのステータスを監視する方法について説明します。

WithSecure Elements EPPをコンピュータ (Mac) にインストールする

Dattoプラットフォームを使用する コンピュータ (Mac) 向けに、WithSecure Elements EPPをインストールします。

製品をインストールするには

1. Dattoポータルで、[コンポーネント]メニューの[アクション]の下にある[新しいコンポーネント]を選択します。
2. [カテゴリ]のドロップダウンメニューから [アプリケーション]を選択します。
3. 「名前」フィールドに「[WithSecure Elements EPP for Computers (Mac)]と入力します。
4. [説明]欄にアプリケーションの説明を入力し (任意)、[保存]を選択します。
コンポーネント申請ページが開きます。
5. [インストールコマンド]のドロップダウンメニューから [Unix (Linux、Mac OSX)]を選択し、次のコマンドを入力します。

```
InstallerBaseName=$(ls -d ElementsAgent*.mpkg)
installer -pkg "$InstallerBaseName" -target /
if [ $? -ne 0 ]; then
  echo "$InstallerBaseName installation failed"
```

```
else
  echo "$InstallerBaseName installation was successful"
fi
```



注：このスクリプトは次のケースをカバーします。

- ファイル名に埋め込まれたライセンス キーを使用して製品をインストールします。
- ファイル名に埋め込まれたライセンス キーを使用せずに製品をインストールします。
「サブスクリプションのアクティビ化」で説明されているように、アクティベータツールを使用して製品をアクティビ化します。

6. [ファイルを追加...]を選択し、パッケージ名にキーが埋め込まれている [WithSecure Elements EPP for Computers (Mac)] インストーラーを選択します。
7. [保存] を選択します。
インストーラ ファイルが新しいコンポーネントにアップロードされます。
8. [サイト] メニューから [サイト] を選択し、「管理対象」または「オンデマンド」のいずれかの下にある [デバイス] を選択します。
9. [アクション] で [ジョブをスケジュールする] を選択します。
10. スケジュール ジョブの名前を入力します。
11. [スケジュールの] セクションで、[すぐに] を選択します。



注：別のオプションを選択するには、[クリックして変更...] を選択してください。

- 12 次に、[コンポーネント名] の下で [コンポーネントを追加] を選択します。
開いたページには、あなたが作成したコンポーネントが表示されます。
- 13 コンポーネントを選択し、[保存] を選択します。

製品を監視する

Datto プラットフォームを使用する コンピュータ (Mac) 向け WithSecure モニター。

製品を監視するには

1. [コンポーネント] メニューの「アクション」 から [新しいコンポーネント] を選択します。
2. [コンポーネント] メニューの [カテゴリ] から、[デバイスモニター] を選択します。
3. 「名前」 フィールドに「[WithSecure Elements EPP for Computers (Mac)] と入力します。
4. [説明] 欄に説明を入力し (任意)、[保存] を選択します。
コンポーネントモニター ページが開きます。
5. [インストールコマンドの] ドロップダウンメニューから [Unix (Linux、Mac OSX)] を選択し、次のコマンドを入力します。

```
InstallerBaseName=$(ls -d ElementsAgent*.mpkg)
installer -pkg "$InstallerBaseName" -target /
if [ $? -ne 0 ]; then
  echo "$InstallerBaseName installation failed"
else
  echo "$InstallerBaseName installation was successful"
fi
```



注：このスクリプトは次のケースをカバーします。

- ファイル名に埋め込まれたライセンス キーを使用して製品をインストールします。

- ファイル名に埋め込まれたライセンス キーを使用せずに製品をインストールします。
「サブスクリプションのアクティブ化」で説明されているように、アクティベータツールを使用して製品をアクティブ化します。

6. [ファイルを追加...]を選択し、パッケージ名にキーが埋め込まれている [WithSecure Elements EPP for Computers (Mac)] インストーラーを選択します。
7. [保存] を選択します。
インストーラ ファイルが新しいコンポーネントにアップロードされます。
8. [サイト] メニューから、[管理対象] または [オンデマンド] のいずれかの下にある [サイト] を選択します。
9. 開いたページで、監視するデバイスを選択します。
10.  を選択し、次に [モニター] を選択します。
11. ページの右側にある 「モニター」 オプションを選択してください。
[デバイス] ページが開きます。
12. [モニターを追加...] を選択してください。
13. 「モニターの追加」 ページで、ドロップダウンメニューから [コンポーネントモニター] を選択し、[次へ] を選択します。
14. [コンポーネントモニターを実行する] ドロップダウンメニューから、作成したコンポーネントを選択し、[次] > [へ] をクリックします。
警告は、リアルタイムスキャン、ファイアウォール、ブラウザ保護など、コンポーネントの1つがデバイスでオフになったときに生成されます。

6.7.9 Datto RMM との連携 (Linux)

WithSecure Linux Protectionは、 Datto RMMプラットフォームを介して、管理対象のLinuxコンピュータにインストールおよび監視できます。

Datto RMMを使用すると、管理対象のLinuxコンピュータに WithSecure Linux Protectionをインストールして監視できます。このセクションでは、Datto RMMを介してソフトウェアをインストールする方法と、そのステータスを監視する方法について説明します。

WithSecure Linux保護をインストール

Dattoプラットフォームを使用して WithSecure Linux Protectionをインストールします。

WithSecure Linux Protectionをインストールするには：

1. WithSecure Elements Security Centerから、最新の汎用 WithSecure Linux Protectionソフトウェアインストーラーをダウンロードしてください。
2. Dattoポータルで、[コンポーネント] メニューの[アクション]の下にある[新しいコンポーネント]を選択します。
3. [カテゴリ]のドロップダウンメニューから [アプリケーション] を選択します。
4. 「名前」 フィールドに [Deploy WithSecure Linux Protection [LIN]] と入力します。
5. [説明] 欄にアプリケーションの説明を入力し (任意)、[保存] を選択します。
コンポーネント申請ページが開きます。
6. [インストールコマンド]のドロップダウンメニューから [Unix (Linux、MacOSX)] を選択し、テキストフィールドに次のファイルからスクリプトを入力します： `deploy_f-secure_linux_protection.sh`。



注： WithSecure Linux Protectionのデプロイメントスクリプトは、こちらからダウンロードできます。

7. 必要に応じて、実際のインストール手順の前に依存関係のインストールを含めるようにスクリプトを編集してください。
8. Linux Protectionの依存関係ガイドで必要な依存関係を確認してください。
9. スクリプトの有効なサブスクリプションキーを編集します。
10. **[ファイルの追加...]**を選択し、次に「**[WithSecureLinuxProtection]**」インストーラーを選択します。
11. **[保存]**を選択します。
インストーラファイルが新しいコンポーネントにアップロードされます。
12. **[サイト]**メニューから、**[管理対象]**の下にある**[デバイス]**を選択します。
13. インストールするデバイスを確認してください。
14. ジョブをスケジュールするには、
 **[ジョブのスケジュール]**を選択してください。
 - a) スケジュール ジョブの名前を入力します。
 - b) **[スケジュールの]**セクションで、**[すぐに]**を選択します。



注： 別のオプションを選択するには、**[クリックして変更...]**を選択してください。

- c) **[コンポーネント名]**で**[コンポーネントを追加]**を選択します。
開いたページには、あなたが作成したコンポーネントが表示されます。
- d) コンポーネントを選択し、**[保存]**を選択します。
- e) ジョブを開始するには、**[保存]**を選択してください。

WithSecure Linux保護で監視する

Dattoプラットフォームを使用した、WithSecure Linux保護機能を備えたモニター。

WithSecure Linux Protectionを監視するには：

1. 以下のリンクから、既製のLinux監視コンポーネントをダウンロードしてください：WithSecure Linux Protection Monitorコンポーネント

これには、F-Secure Linux Protection Monitor [LIN]というコンポーネントが含まれています。この監視コンポーネントを使用して、現在の状態、およびWithSecure Linux Protectionがインストールされ有効になっているかどうかを確認できます。また、現在のライセンスの状態、さまざまな保護コンポーネントの状態、およびウイルス定義ファイルの有効期限も確認できます。個々のチェック項目は、オンまたはオフに切り替えることができます。



注： コンポーネントの詳細については、DattoRMM管理ポータルの説明を参照してください。

すべての構成変数には、ヘルプテキストが含まれています。

2. Dattoポータル「**コンポーネント**」ページで、コンポーネントファイル (.cpt) をインポートしてください。
3. インポートしたコンポーネントを使用して、次のようにコンポーネントモニターを作成します。
 - a) サイトメニューから、**[管理対象]**の下にある**[デバイス]**を選択します。
 - b) 開いたページで、監視するデバイスを選択します。
 - c) アイコンを選択し、次に**[モニター]**を選択します。

- d) ページの右側にある「**モニター**」オプションを選択してください。デバイスページが開きます。
 - e) [**モニターを追加...**]を選択してください。
 - f) 「**モニターの追加**」ページで、ドロップダウンメニューから[**コンポーネントモニター**]を選択し、[**次へ**]を選択します。
 - g) 「コンポーネントモニターを実行する」ドロップダウンメニューから、インポートしたコンポーネントを選択します。
 - h) コンポーネント構成変数を確認し、監視したい保護コンポーネントごとに個別のチェックをオンまたはオフにします。その後、各ページで [**次へ**]を選択してモニターを作成します。
- アラートは、デバイスでコンポーネントの1つがオフになっている場合に生成されます。たとえば、リアルタイムスキャンや整合性チェックなどです。最初に失敗したチェックはアラートを生成します。1つのモニターから同じデバイスに対して新しいアラートが生成される前に、アラートを解決する必要があります。

第7章

警告と報告

トピック：

- 通知ハブを使用する
- セキュリティ概要
- セキュリティイベントレポート
- セキュリティイベントに関するカスタマイズされたメールレポートを作成する
- セキュリティイベント用のカスタムビューを作成する
- 監査ログ

警告と報告

のレポートこのセクションでは、WithSecure Elements Security Centerアカウントに登録されているコンピューターやモバイルデバイスのセキュリティ状態を把握するのに役立つ指標を追跡します。

オンレポートこのセクションでは、以下の操作や表示が可能です。

- [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
- 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。
- 脆弱性通知を表示する

7.1 通知ハブを使用する

通知ハブは、WithSecure Elementsセキュリティセンターの中心的な場所であり、重要な製品メッセージを表示および管理できます。

通知ハブは、ほとんどのバナー形式のお知らせに代わり、重大な問題や障害、警告や運用状況の更新、一般的な情報などを表示します。右上隅のベルアイコンは、新しい未読の通知があることを示します。

通知を表示および管理するには：

1. Elements Security Centerの右上隅にある



を選択します。

通知パネルが開き、「未読」タブにすべての新しい通知が表示されます。

2. パネル内の通知を確認してください。
3. 新しいメッセージと過去のメッセージを区別するために、通知を既読としてマークしてください。



注: 既読通知は、今後の参照のために「既読」タブに残ります。ただし、定期メンテナンス通知など、一部の通知はイベント終了後まもなく削除され、「既読」タブには表示されなくなります。

7.2 セキュリティ概要

デバイスタブのチャートレポート登録済みコンピュータの感染状況と保護状況の概要を提供します。

チャートには次の情報が表示されます。

- **[コンピュータ保護ステータス]**- セキュリティに影響する問題のない保護対象のコンピュータの数、[軽微な]問題を抱えているコンピュータの数、[重大な問題]を抱えているデバイスの数、および2週間以上サーバーに接続していないコンピュータの数を表示します。
- **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。

7.2.1 CSVレポートをエクスポートする

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。

スコープセクターを使用すると、顧客企業を表示し、選択した企業のデバイスおよびソフトウェア アップデートのインストールに関するレポートをエクスポートすることもできます。

1. 選択[デバイス]サイドバーに表示されます。

2. 

を選択してください。

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：例えば、プロファイルフィルタのドロップダウンメニューからプロファイルフィルタオプションを選択し、選択したプロファイルが割り当てられているデバイスを表示するように設定できます。デバイスページでは、フィルタ（または検索）結果に基づいて検出されたデバイスのみ[をエクスポートするために、「検出されたコンピューターレポートを]エクスポート」オプションを選択できます。

- 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。

7.3 セキュリティイベントレポート

[レポート] ページの [セキュリティイベント] タブのグラフには、セキュリティイベントの概要が示されています。

チャートには次の情報が表示されます。

- **[感染阻止数上位のコンピューター]**- 過去30日間に感染を阻止した上位コンピューターの名前と、阻止した感染の総数。
- **[上位の感染事例]**- 過去30日間の上位10件の感染事例名と件数。感染事例名を選択すると、WithSecure Labsの脅威記述データベースから感染の詳細を表示するWebブラウザページが開きます。バーを選択すると、セキュリティイベントページが開きます。
- **[リアルタイムスキャンで処理された感染症]**- 1日あたりのリアルタイムスキャンで処理された感染症の数、および過去30日間に処理された感染症の総数。
- **[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- アクセスがブロックされた上位アプリケーション]**- 過去30日間に DataGuardがアクセスをブロックした上位アプリケーション。
- **[デバイス制御-上位ルール-デバイスをブロック]**- 過去30日間にデバイスをブロックした上位のデバイス制御ルールと、そのルールに基づいてデバイスがブロックされた回数。
- **[改ざん防止-主なアラートの種類]**- 最も一般的な改ざん防止アラートの種類と、過去30日間に各アラートの種類がトリガーされた回数。
- **[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。

7.4 セキュリティイベントに関するカスタマイズされたメールレポートを作成する

「レポート」メニューの「メール通知とレポート」機能を使用すると、カスタマイズしたメールレポートを作成し、自動的に送信できます。

メールレポートを作成する際にテンプレートとして使用するには、**セキュリティイベント**ページにカスタムビューが必要です。

カスタムビューを作成したら、セキュリティ イベントに関する電子メール レポートを作成できるようになります。

1. 選択**[レポート]**サイドバーに表示されます。

2. オンレポートページを開き、[メール通知とレポート]タブを選択します。
3. [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。
4. レポートの名前を入力します。
5. 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。
6. テンプレートの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既に作成済みのテンプレートを選択します。
7. レポートに使用する言語を選択します。
8. [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。

9. [レポートにコンテンツがある場合のみ送信する]をオンにすると、イベントが発生した場合にのみレポートを受信できます。オフにすると、イベントがない場合でもレポートを受信できます。
10. [受信者]ボックスに、レポートを配信する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。

11. [保存]を選択します。

7.5 セキュリティイベント用のカスタムビューを作成する

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ことで、イベントのセットをフィルタリングして保存できます。たとえば、メールレポートを作成する際のテンプレートとして使用できます。

1. 下[イベント][セキュリティイベント]を選択します。
2. フィルターを適用して、ビューに含めるセキュリティイベントを指定します。
3. 右上隅にある [表示] ドロップダウンメニューを開きます。
4. [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。
5. [保存]を選択します。

カスタムビューは[マイビュー]の下に表示されます。

7.6 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。

監査ログページには、以下の列が表示されます。

- [タイムスタンプ]- イベントが発生した日時。
- [説明]- イベントを説明する自由形式のテキスト。たとえば、IPアドレス、ユーザーエージェント、認証済みユーザーを含む管理者ログインなど。
- [ターゲット]- イベントの影響を受けたオブジェクト。プロファイルやデバイスなど。
- [トランザクションID]- イベントの一意の識別子。

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

デフォルトでは、**監査ログ**ページには過去14日間のイベントが表示されます。イベントは期間で絞り込むこともできます。指定した日付より前または後に発生したイベントを表示するように選択できます。

例えば、管理者ログインエントリには、「IP 203.0.113.5 から Mozilla/5.0 を使用して管理者がログインしました。認証名は jane.doe@example.com です。」といった説明があります。

監査ログのエントリは、管理対象組織のデータ保持設定で許可されている期間保持されます。

第 8 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：

- 利用可能なソフトウェアアップデートを表示する
- ソフトウェアアップデートを個別に、またはカテゴリ別にインストールする
- ソフトウェアアップデートを自動的にインストールします
- 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
- 特定のデバイス上のソフトウェアアップデートを表示およびインストールする
- ソフトウェアアップデーター用のHTTPプロキシを設定する
- ソフトウェアアップデーター用のWithSecure Elementsコネクタを構成する
- 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

サードパーティのソフトウェアを最新の状態に保つ

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。そのため、**[実行中のアプリケーションを強制終了] オプション**を]オンにすることをお勧めします ([更新] を選択すると開くアクションメニュー内)。[パッチ管理]すべてのソフトウェアアップデートがインストールできることを確認するため。



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。

8.1 利用可能なソフトウェアアップデートを表示する

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。

アップデートが欠落していることに加えて、**パッチ**この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。

8.2 ソフトウェアアップデートを個別に、またはカテゴリ別にインストールする

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、中程度のセキュリティ、低、未分類、およびセキュリティ関連以外、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。

- 利用可能なすべてのアップデートをインストールするには、**パッチページ**を開き、表のヘッダーの横にあるチェックボックスを選択してください。最初の50社のベンダーの更新情報が表示されます。
- 個々のソフトウェアアップデートをインストールするには、**パッチページ**を開き、インストールしたいアップデートを選択してください。

2. ページ下部のメニューで、**[更新するデバイスを選択]**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. **[更新]**を選択してください。

アップデートのインストール要求が、選択されたデバイスに送信されます。インストールが完了すると、各デバイスにアップデート状況が表示されます。

8.3 ソフトウェアアップデートを自動的にインストールします

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. **[自動化タスク]**を選択します。
4. **[自動タスクを]**オンにしてください。
5. **自動化タスクの一覧**から **[タスクの追加]**を選択し、以下の手順を実行します。

- 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) **[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、更新プログラムをインストールする間隔（例：1時間ごと、毎日、平日）を選択してください。または、CRON式を使用し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、更新プログラム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、利用可能になり次第インストールされます。スイッチがオフの場合、更新プログラム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： 下 **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が見つからない場合の通知]** オプションをオンにすると、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アラシが表示されます。

- 6. ポリシーを配布するには、**[保存して公開]** を選択してください。
変更が保存され、現在のプロファイルに公開されます。

8.3.1 ソフトウェアアップデートを含めるか除外するか

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。

更新プログラムの包含と除外は、管理対象ホストから報告される更新プログラムのインストール状況に基づいて決定されます。包含の場合、更新プログラムは重要度に基づいてチェックされ、**[セキュリティ更新プログラムを自動的にインストールする]** で選択された内容に応じて判断されます。その後、除外された更新プログラムを除くすべての更新プログラムがインストールされます。

ホストが不足している更新プログラムのインストールを開始すると、除外されている更新プログラムがないか確認し、管理者による除外のためインストールされなかったことを報告します。これは、ホストが不足している更新プログラムのインストールを試みた後にのみインストール状況を報告するため、除外された更新プログラムが「**ソフトウェア更新プログラム**」タブのリストからすぐに消えるわけではないことを意味します。

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ター]** を選択してください。
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。

- ・ 「自動インストール対象ソフトウェアを含める」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する」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. ポリシーを配布するには、[保存して公開]を選択してください。

8.3.2 スキャン結果に更新情報を含める

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. 選択[プロファイル]サイドバーに表示されます。

[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、[スキャン結果に更新プログラムを含める]を選択します。

[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. 変更内容を現在のプロファイルに保存するには、[保存して公開]を選択してください。

8.3.3 セキュリティ関連以外の更新プログラムをスキャン対象から除外する

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. 選択[プロファイル]サイドバーに表示されます。
[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、[更新プログラムのスキャンを除外する]を選択します。
4. [セキュリティ以外の更新プログラム]を有効にしてください。
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。

8.3.4 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. 選択[プロファイル]サイドバーに表示されます。
[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、[更新プログラムのスキャンを除外する]を選択します。
[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. 変更内容を現在のプロファイルに保存するには、[保存して公開]を選択してください。

8.4 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. 選択[デバイス]サイドバーに表示されます。
デバイス ページが表示されます。
スコープセレクト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は、管理したい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 **[不足しているソフトウェアアップデートをスキャンする]** を選択してください。

インストールされている *Elements Endpoint Protection* ソフトウェアにコマンドが送信され、デバイスをスキャンして不足しているソフトウェアアップデートを特定します。

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。

8.5 特定のデバイス上のソフトウェアアップデートを表示およびインストールする

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: 不足しているソフトウェアアップデートもリストされています **ホーム** 問題一覧表のページ (重要、重大、参考情報に分類されています) で、該当するカテゴリのアップデートがインストール待ちとなっているデバイスを表示します。 **[表示]** ボタンをクリックすると、該当するカテゴリのアップデートがインストールされているデバイスが表示されます。

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. クリック **[デバイス]** サイドバーに表示されます。

の **デバイス** ページが表示されます。

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. 保護ステータス表で、「ソフトウェア更新プログラム」の横に



アイコンをクリックします。

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する**」ボタンをクリックしてください。

「**ソフトウェア更新プログラムのインストール**」ページには、特定のソフトウェアで利用可能な最新の更新プログラムが一覧表示されます。更新プログラムには、カテゴリ、CVE ID、セキュリティ情報ID、および更新プログラムの詳細情報が記載された外部Webページへのリンクが含まれています。また、表内の項目は、「すべての更新プログラム」、「すべてのセキュリティ更新プログラム」、「重大なセキュリティ更新プログラム」、「重要なセキュリティ更新プログラム」、「セキュリティ以外の更新プログラム」、「サービスパック」のいずれかを選択して並べ替えることで、見やすくすることができます。

「**ソフトウェアアップデートのインストール**」ページが表示され、このデバイスにまだインストールされていないすべてのアップデートが一覧表示されます。

5. インストールするには、必要なアップデートを選択し、「**インストール**」ボタンをクリックしてください。

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。

8.6 ソフトウェアアップデーター用の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. 下 **プロファイル** > **[ソフトウェアアップデーターで]**、**[通信]** を選択します。

2. 「HTTPプロキシを使用する」ドロップダウンメニューから、以下のいずれかのオプションを選択してください。

オプション	説明
いいえ	インターネットに直接接続する
製品構成から	製品のプロキシ設定を使用する
リモート管理	代替プロキシURLを指定する (ユーザー定義)

3. 前の手順で [リモート管理] を選択した場合は、「リモート管理プロキシ アドレス」フィールドに次の形式で HTTP プロキシ アドレスを入力します: `http://[user[:password]@]host:port`。

HTTPプロキシ設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

8.7 ソフトウェアアップデーター用のWithSecure Elementsコネクタを構成する

WithSecure Elements Connectorを介してソフトウェアアップデーターのアップデートを受信するように設定できます。

[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. 下 **プロファイル** > [ソフトウェアアップデーターで]、[通信] を選択します。
2. **WithSecure Elements Connectorを使用する**」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。

オプション	説明
いつも	常に WithSecure Elements Connectorを使用してください
もし可能なら	可能な限り WithSecure Elements Connectorを使用してください。
一度もない	インターネットに直接接続する

Elements Connectorのプロキシ設定は、このプロファイルを使用するWindowsコンピューターに適用されます。

8.8 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では、ソフトウェアアップデーター (SWUP) が常にWindowsアップデートをインストールします。

Windows Update のインストールを無効にする方法はありません。「[WSUS が使用されている場合、ソフトウェア アップデーターと WSUS の両方で Microsoft 更新プログラムをインストールする]設定は、ソフトウェアアップデーター (SWUP) と Windows Server Update Services (WSUS) の両方で Windows Update が同時にインストールされるのを防ぐために存在します。



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WSUS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。WSUS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 章9

WithSecure Luminenの使用

トピック：

- 毎週のセキュリティ意識向上サマリーをご覧ください
- 調査アシスタントを使用して検出結果を分析する
- Luminenの月次セキュリティレポートの概要

WithSecure Luminenの使用

WithSecure Luminenは、サイバーセキュリティ業務をより管理しやすく、効率的にします。高度なAI技術を活用することで、管理対象組織をサイバー脅威からより効果的に保護します。

Luminenは、AIと大規模言語モデル (LLM) 技術を前処理済みの構造化データと組み合わせることで、不正な推奨事項のリスクを大幅に低減します。レポートは分かりやすく、WithSecure Elements Cloudに統合されています。

Luminenは膨大なデータを分析し、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を減らし、最も重要な問題への対応に集中できます。例えば、未処理のインシデントを特定し、それらを軽減するための具体的な対策を提案できます。

Luminenは、セキュリティイベントの調査を支援し、脅威を理解して対応できるようにします。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が可能になり、対応時間と有効性が向上します。

使い方

WithSecure LuminenはElementsのユーザーエクスペリエンスレイヤーです。生成AIとLLM (言語学習モデル) を用いて、自然言語によるローカライズされた支援を提供します。

欧州を代表するサイバーセキュリティ企業として、WithSecure Luminenは厳格なプライバシー基準を遵守しています。実績のあるAIモデルを継続的に改良し、各AIモデルは単一の組織専用となることで、組織間でのデータ漏洩を防止しています。

LuminenはAmazon AWS BedrockのLLMを使用しており、分析データは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、将来の基盤モデルのトレーニングには使用されません。WithSecure匿名化されたデータのみを使用します。

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、LuminenはRAG (Retrieval-Augmented Generation) と呼ばれる手法を採用しています。この手法では、セキュリティイベント、拡張検出・対応 (XDR)、広域コンテキスト検出 (BCD) インシデント、関連する脅威インテリジェンスなど、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。これらのデータには、ユーザー名、ホスト名、メールアドレスなど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やXDR/BCDインシデントに既に含まれているデータ以外にはアクセスできません。

9.1 毎週のセキュリティ意識向上サマリーをご覧ください

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。

セキュリティ意識向上アシスタントは、過去1週間のセキュリティ活動を簡潔にまとめたサマリーを作成し、組織のセキュリティ体制の概要を提供します。Luminenはこれらのサマリーを平易な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、必要となる可能性のある即時対応策を容易に理解できます。レポートは、検出結果を重要度に基づいて優先順位付けするため、最も緊急性の高い問題に優先的に対処できます。

右上隅の



を選択してください。

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。

9.2 調査アシスタントを使用して検出結果を分析する

Investigation AssistantはWithSecure Luminenの一部です。広範なコンテキスト検出の概要を迅速かつ明確に提供することで、複雑なセキュリティイベントの理解にかかる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. 選択 イベント > 広範なコンテキスト検出

「**広範なコンテキスト検出**」ビューには、検出されたすべての広範なコンテキスト検出結果が表示されます。

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は検出結果を分析し、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。

9.3 Luminenの月次セキュリティレポートの概要

Luminenが生成する、企業のセキュリティ体制に関する月次概要レポート。Elements Security Centerで企業レベルで利用可能です。

エグゼクティブサマリーは、Luminenの生成型AIを使用してセキュリティ関連データを分析し、組織の現在のセキュリティ状況を説明する簡潔で平易な言葉による要約を作成します。この要約は、経営幹部に現在のセキュリティ状況を伝え、脆弱性を強調し、セキュリティ改善のための情報に基づいた意思決定を支援します。要約には、次のような重要な詳細情報が含まれています。

- 暗号化ステータス
- パスワードの強度
- アップデートとパッチの準拠
- 悪用される可能性
- オペレーティングシステムのライフサイクルステータス



注: 具体的な内容は、利用している Elementsのサブスクリプションによって異なります。

この要約には以下の特徴があります。

- 箇条書き形式で、素早く読めるようにしています。
- Elements Security Centerで設定された言語に基づいて自動的にローカライズされます。
- 迅速な状況認識を必要とする経営幹部、ITマネージャー、セキュリティコンサルタント向け。
- 情報に基づいた意思決定と是正措置の優先順位付けを支援する。

この概要は、経営幹部やセキュリティチームが組織のセキュリティ体制を理解するのに役立ちます。また、リスクや脆弱性を特定し、対策の優先順位を決定し、情報に基づいたセキュリティ上の意思決定を行う上でも役立ちます。

9.3.1 エグゼクティブサマリーレポートを作成する

管理対象組織のセキュリティレポートの月次エグゼクティブサマリーを生成するカスタムウィジェットを作成します。

1. 開ける Elements Security Center。
2. 認証情報を使用してログインしてください。
3. 選択[レポート]メインナビゲーションメニューから。
4. 利用可能なレポートオプションの一覧から [マイレポート]を選択してください。
5. 新しいカスタムレポートビューを作成するには、[新しいビューテンプレート]を選択してください。
このテンプレートは、エグゼクティブサマリーの表示方法を決定します。
6. テンプレートに分かりやすい名前を入力してください (例：エグゼクティブレポート)。
7. 新しいビューテンプレートを保存するには、[保存]を選択してください。
8. 新しく作成したレポートビューから [ウィジェットを追加]を選択します。
ウィジェットを使用すると、関連する指標や概要をダッシュボードに直接配置できます。
9. ウィジェットに「エグゼクティブレポート」などの名前を付けます。
10. [データソース]として、[AI生成サマリー]を選択してください。
11. [データ]の下にある [エグゼクティブサマリーレポート] > [の作成]を選択します。

このウィジェットはレポートに追加され、選択した企業の *Luminen* 月次セキュリティサマリーを自動的に読み込みます。

管理対象組織のセキュリティ体制の月次状況を示す、カスタマイズされたサマリーレポートを作成しました。

9.3.2 パートナーとしてセキュリティに関するエグゼクティブサマリーレポートをご覧ください

パートナーレベルの認証情報を使用して、組織階層内の企業向けセキュリティレポートの月次エグゼクティブサマリーにアクセスし、生成します。

パートナーレベルでセキュリティレポートの月次エグゼクティブサマリーを設定すると、そのレポートとウィジェットはパートナー階層内のすべての企業で再利用できます。レポートの設定は一度行うだけで済みます。

1. エグゼクティブサマリーレポートウィジェットを含むレポートビューを開きます。
2. スコープセクターを使用して、顧客企業を選択してください。
エグゼクティブサマリーは企業レベルで作成されるため、どのレポートが表示されるかは選択された企業によって決まります。
3. 選択した顧客に関するエグゼクティブサマリーレポートを作成します。
4. エグゼクティブサマリーレポートをご覧ください。
5. 別の企業の概要を表示するには、スコープセクターで別の顧客を選択してください。
エグゼクティブサマリーは、レポートを再設定することなく即座に更新されます。

単一の再利用可能なレポートビューを通じて、すべての顧客企業のエグゼクティブサマリーレポートを確認できます。

付録 A

要素エージェントの再インストール

トピック：

- デバイスを複製せずにElements Agentを再インストールする

要素エージェントの再インストール

WithSecure Elements WithSecureセンターに重複エントリを作成せずに、デバイスに WithSecure Elements エージェントを再インストールします。

この章では、デバイスに WithSecure Elements Agentを再インストールする方法について説明します。また WithSecure Elements Security Centerに重複エントリを作成せずに再インストールする方法についても解説します。

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、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)

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: SMBIOS GUIDが機能しない場合、例えばイメージの起動時にSMBIOSが変更される非永続的なVDI展開の場合などに、この方法をお勧めします。

この識別子は、Elements Agent のインストール前に Active Directory に登録されているコンピューターに対してのみ有効です。

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に同じ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せん。



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は、**「既存のコンピューター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、システムが重複するデバイスを生成しないようにしてください。Active Directoryアカウントを作成すると、クローン操作後も変更されません。そのため、Elements Security Centerは、たとえ同じ名前であっても、それらを別々のデバイスとして認識しません。

.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
```

Elements Agentを.msiファイルでインストールする場合は、以下のパラメータを使用してください。

- 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
```

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：

- 顧客企業を追加する
- 顧客企業にサブスクリプションキーを割り当てる
- 新規顧客企業向けに製品を注文する
- カスタマイズ要素セキュリティセンター
- WithSecure Elementsソフトウェアをカスタマイズする

Elements Security Centerとソフトウェアをカスタマイズする

スコープセクターを使用して表示情報の範囲を変更したり、パートナー向けにElements Security CenterおよびElements Endpoint Protectionソフトウェアをカスタマイズしたりします。



注: 下 **プロファイル** > **[一般設定]**、パイロットクライアント設定をオンにできます。このオプションをオンにすると、このプロファイルに割り当てられたデバイスで新機能を事前にテストできます。パイロットコンピュータは、他のユーザーよりも数日早くソフトウェアアップデートを受け取ります。新機能のプレビューを入手し、お客様に情報を提供するために、この機能を使用することをお勧めします。

B.1 顧客企業を追加する

WithSecure Elements Security Centerアカウントに新しい顧客企業を追加するには、まずその企業をWithSecure Partner Portalアカウントに新しい顧客として追加し、少なくとも1つの製品を購入する必要があります。WithSecure Elementsそれに対応する製品。



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、Elements Security Centerを通じて 管理者アカウントを作成してください。



注: WithSecureパートナーポータルは、Elements Security Centerと連携するオンラインサービスです。販売とサポートを支援するツール、資料、統合された電子注文システムを提供します。WithSecure解決策。

新規顧客の発注書は、まずパートナーポータルアカウントから正常に追加される必要があります。これが完了すると、顧客は自動的にElements Security Centerアカウントに新規企業として追加されます。

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 顧客企業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)。パートナーはサブスクリプションキーを次の場所で見つけることができます。 **サブスクリプション**表示[管理]サイドバーに表示されます。



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. 下[管理]選択[サブスクリプ]サイドバーに表示されます。
2. スコープセクターを使用して、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]を選択してください。
購読割り当てページが開きます。
4. 会社の新しいサブスクリプションキーを入力し、[OK] を選択してください。]

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 新規顧客企業向けに製品を注文する

WithSecureパートナーポータルを通じて、新規顧客企業向けにWithSecure Elements製品を注文してください。



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。

ご注文はこちら WithSecure Elements WithSecureパートナーポータル経由で新規顧客企業向け製品を提供する:

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にアクセスするには、WithSecure Elementsセキュリティセンターから別途ログイン認証情報を取得する必要があります。ログイン情報をお持ちでない場合は、ページ上の「**認証情報のリクエスト**」フォームに必要事項を入力し、[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時間かかる場合があります。

電子注文ページが表示されます。

2. メインページで、[新規注文] を選択します。
3. 新しい顧客企業の名前を入力し、[新規追加]を選択してください。
[新規顧客] ウィンドウが開きます。
4. 顧客情報を入力し、[保存]を選択してください。
5. [新規注文] の下に、注文の参照番号を入力します。
6. [製品の注文] で、[製品を追加] を選択します。
7. 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 カスタマイズ要素セキュリティセンター

WithSecure Elementsセキュリティセンターは、ロゴやサポートリンクを追加して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」タブを選択してください。
3. 「 アイコンを選択し、[ポータルのカスタマイズ]を選択します。
組織のロゴページが開きます。
4. 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。
あなたが提供するリンクはデフォルトの WithSecure サポートリンク。
6. 変更を保存します。

カスタマイズが完了すると、Elements Security Centerの画面左下隅にあなたのロゴが表示されます。

B.5 WithSecure Elementsソフトウェアをカスタマイズする

WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversソフトウェアには、お客様のロゴとサポートリンクを追加してカスタマイズできます。



注：ソフトウェアにロゴや URL、またはその両方を表示させるには、カスタム プロファイル を割り当てて使用する必要があります (WithSecure デフォルト プロファイル)。

ソフトウェア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。
オプションのリンクはロゴに適用されます。たとえば、サポートサイトへのリンクはデフォルトのリンクを置き換えます。WithSecure サポートリンク。

アップロードしたロゴは、WithSecure Elements EPP for Computersおよび WithSecure Elements EPP for Serversソフトウェアに表示されます。

付録 C

Windows Management Instrumentation

トピック：

- WMI の連携
- 連携用の WMI クラス

Windows Management Instrumentation

WithSecure Elementsは、Windows Management Instrumentation (WMI) との統合機能を提供しており、例えば、リモート監視および管理 (RMM) ツールとの統合に利用できます。

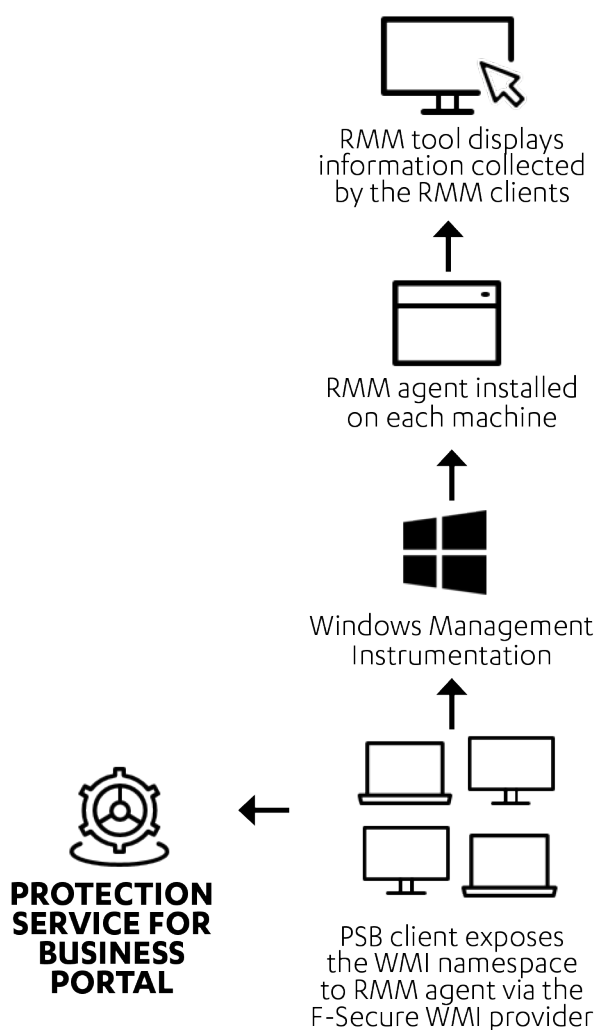
サービスプロバイダの多くはアセット(資産)ディスカバリー、管理、設定、プロセス・サービスの自動化、セキュリティ サービス、バックアップなどの管理機能を強化するために WMI の連携を使用します。

C.1 WMI の連携

WithSecure Elementsは、Windows Management Instrumentation (WMI) インターフェイスを使用して、読み取り専用のステータス情報を収集します。WithSecureクライアントアプリケーション。

WMI インターフェイ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 インターフェイスを通して通知されることはありません。

管理者は WMI インターフェイ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 インターフェイスを通じて 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セキュリティセンターへの最終接続時刻
- WithSecure Elements Security Centerからの最終ポリシー更新時刻
- 使用中の WithSecure Elementsエンドポイント保護プロファイルの名前
- DeepGuard状態
- 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 を介してプロパティを取得します

PowerShellを使用してWMIインターフェイス経由でステータスプロパティを取得します。

WithSecureWindows Management Instrumentation (WMI) インターフェイスを介して、読み取り専用のステータス情報を公開します。

1. WMI プロバイダの設定を有効にするには

- WithSecure Elements Security Centerにログインします。
- [**セキュリティ構成**] で、[**プロファイル**] を選択します。
 - [**一般設定**]を選択してください。
 - [**統合**] で [**WMIプロバイダー**]をオンにします。
 - [**保存して公開**]を選択してください。
 - 下[**環境**]選択[**デバイス**]次に、お使いのデバイスを選択してください。
 - [**プロファイルの割り当て**]を選択します。
 - 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へのポリシーの最終接続時刻

```
$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
```

- DeepGuard状態 :

```
$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\fssecure" -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\fssecure" -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\fssecure" -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\fssecure" -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\fssecure" -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における Windows Management Instrumentation (WMI) 統合に使用されるクラスの詳細について説明します。

この付録では、Windows Management Instrumentation (WMI) クラスについて説明します。WithSecure Elements RMM統合のために、WMI名前空間やWindowsレジストリで利用可能なデータなどを公開します。

C.2.1 WMI クラス

WithSecure Elements Security Centerで WMI 統合に使用されるクラス。

WMIクラス入門

一部のクラスはシングルトンインスタンスとして利用可能であり、一部は補助型としてのみ使用されます。詳細については、例を参照してください。WMI を介してプロパティを取得しますページ266。

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。

表15:抗ウイルス特性

プロパティ名	説明	種類
<i>RealTimeScanning</i>	リアルタイムスキャンのステータス情報	<i>component</i>
<i>DeepGuard</i>	ディープガードのステータス情報	<i>component</i>
<i>AvDefinitionsUpdateTime</i>	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	<i>datetime</i>
<i>AvDefinitions</i>	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	<i>AvDefinition</i>

表16:ウイルス対策方法

メソッド名	説明	戻り型
<i>ScanComputer</i>	フル コンピューター スキャンの 開始と完了までの待機	<i>AvScanResult</i>

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。

表17:AntiVirus2の特性

プロパティ名	説明	種類
<i>RealTimeScanningEnabled</i>	リアルタイムスキャンのステータス情報	<i>boolean</i>

プロパティ名	説明	種類
<i>DeepGuardEnabled</i>	ディープガードのステータス情報	<i>boolean</i>
<i>AvDefinitionsAgeInHours</i>	アンチウイルス定義が発行されてからの経過時間	<i>uint32</i>

API

基本的な情報を提供します WithSecureWMI名前空間API。

表18:APIプロパティ

プロパティ名	説明	種類
<i>Version</i>	APIの実バージョン	<i>string</i>

AvDefinition

アンチウイルス エンジンの情報。

表19:AvDefinition プロパティ

プロパティ名	説明	種類
<i>EngineId</i>	該当するエンジンの一意識別子	<i>uint32</i>
<i>EngineName</i>	対応するエンジンの説明的な名称	<i>string</i>
<i>EngineVersion</i>	該当するエンジンのバージョン	<i>string</i>
<i>UpdateSerialNumber</i>	インストールしたアップデートの一意識別子	<i>string</i>
<i>UpdateTime</i>	アップデートがインストールされた時間	<i>datetime</i>

AvScanResult

ウイルス スキャンの結果。

表20:AvScanResult のプロパティ

プロパティ名	説明	種類
<i>StartTime</i>	スキャンが開始された時間	<i>datetime</i>
<i>EndTime</i>	スキャンが終了した時間	<i>datetime</i>
<i>InfectedFilesCount</i>	スキャン中に検出した感染ファイルの数	<i>uint32</i>
<i>InfectedSectorsCount</i>	スキャン中に検出した感染セクターの数	<i>uint32</i>
<i>ScanningReportFilePath</i>	スキャンレポートのパス	<i>string</i>

CentralManagement

プロテクション サービスの相互作用に関する情報。

表21:中央管理プロパティ

プロパティ名	説明	種類
<i>LastConnectionTime</i>	プロテクション サービスの前の接続時間。	<i>datetime</i>
<i>PolicyUpdateTime</i>	前のポリシー アップデート時間。	<i>datetime</i>
<i>Profile</i>	インストールされているプロファイル。	<i>Profile</i>

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。

表22:CentralManagement2 プロパティ

プロパティ名	説明	種類
<i>LastConnectionTimeInHoursAgo</i>	プロテクションサービスの前の接続時間	<i>uint32</i>

CentralManagement3

ホストIDとそのタイプに関する情報を提供します。

表23:CentralManagement3 プロパティ

プロパティ名	説明	種類
<i>HostIdentityType</i>	ホスト ID タイプ (<i>SMBCSGUDRANDOMGUDWNSMAC</i> 、またはホスト IDが定義されていない場合は空)。	<i>string</i>
<i>HostIdentity</i>	ホストID	<i>string</i>

Component

製品コンポーネントの概要情報。

表24:コンポーネントのプロパティ

プロパティ名	説明	種類
<i>Enabled</i>	コンポーネントのステータス	<i>boolean</i>

Firewall : Component

情報を提供します WithSecureファイアウォール。

表25:ファイアウォールのプロパティ

プロパティ名	説明	種類
<i>Enabled</i>	現在の状態 WithSecureファイアウォール	<i>boolean</i>

プロパティ名	説明	種類
<i>SecurityLevel</i>	現在のセキュリティレベル WithSecureファイアウォール	<i>string</i>
<i>ApplicationControl</i>	アプリケーション制御の現在のステータス	<i>component</i>
<i>Version</i>	バージョン WithSecureファイアウォール	<i>string</i>
<i>Build</i>	構築 WithSecureファイアウォール	<i>string</i>

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。

表26:インターネットプロパティ

プロパティ名	説明	種類
<i>BrowsingProtection</i>	ブラウザ保護のステータス	<i>component</i>
<i>EmailFiltering</i>	メールフィルタのステータス	<i>component</i>

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。

表27:Internet2のプロパティ

プロパティ名	説明	種類
<i>BrowsingProtectionEnabled</i>	ブラウザ保護のステータス	<i>boolean</i>

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。

表28:LastManualScanReport のプロパティ

プロパティ名	説明	種類
<i>Valid</i>	レポートが正常に検出およびロードされたか示します	<i>boolean</i>
<i>StartTime</i>	スキャンが開始された時間	<i>datetime</i>
<i>EndTime</i>	スキャンが終了した時間	<i>datetime</i>
<i>StartTimeInHoursAgo</i>	スキャンが開始された時刻 (何時間前)	<i>uint32</i>
<i>EndTimeInHoursAgo</i>	スキャンが終了した時刻 (何時間前)	<i>uint32</i>
<i>InfectedFilesCount</i>	スキャン中に検出した感染ファイルの数	<i>uint32</i>

プロパティ名	説明	種類
<i>TotalScannedFilesCount</i>	スキャンされたファイルの総数	<i>uint32</i>
<i>HarmfulItemsFound</i>	有害なアイテムが見つかったかどうかを示します	<i>boolean</i>
<i>ScanningReportFilePath</i>	スキャンレポートのパス	<i>string</i>

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。

表29:LastScheduledScanReport プロパティ

プロパティ名	説明	種類
<i>Valid</i>	レポートが正常に検出およびロードされたか示します。	<i>boolean</i>
<i>StartTime</i>	スキャンが開始された時間	<i>datetime</i>
<i>EndTime</i>	スキャンが終了した時間	<i>datetime</i>
<i>StartTimeInHoursAgo</i>	スキャンが開始された時刻 (何時間前)	<i>uint32</i>
<i>EndTimeInHoursAgo</i>	スキャンが終了した時刻 (時間単位)	<i>uint32</i>
<i>InfectedFilesCount</i>	スキャン中に検出した感染ファイルの数	<i>uint32</i>
<i>TotalScannedFilesCount</i>	スキャンされたファイルの総数	<i>uint32</i>
<i>HarmfulItemsFound</i>	有害なアイテムが見つかったかどうかを示します	<i>boolean</i>
<i>ScanningReportFilePath</i>	スキャンレポートのパス	<i>string</i>

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。

表30:LicenseStatus プロパティ

プロパティ名	説明	種類
<i>Valid</i>	ライセンスの有効性ステータス	<i>boolean</i>
<i>EndDate</i>	サブスクリプションの終了日	<i>datetime</i>
<i>DaysTillEndDate</i>	サブスクリプションの終了日までの日数	<i>uint32</i>
<i>SubscriptionName</i>	製品のサブスクリプション名	<i>string</i>

Product

インストールされているセキュリティ製品の情報。

表31:製品特性

プロパティ名	説明	種類
<i>Name</i>	製品の名前	<i>string</i>
<i>Version</i>	製品のバージョン	<i>string</i>
<i>Build</i>	製品のビルド	<i>string</i>

Profile

インストールされているプロファイルの情報。

表32:プロファイルプロパティ

プロパティ名	説明	種類
<i>ProfileName</i>	プロファイルの説明的な名前	<i>string</i>
<i>ProfileVersion</i>	プロファイルパッケージのバージョン	<i>string</i>
<i>SeriesName</i>	プロファイルパッケージの名前	<i>string</i>
<i>InstallationTime</i>	プロファイルがインストールされた時間	<i>datetime</i>

RebootStatus

再起動ステータスに関する情報を提供します。

表33:RebootStatus プロパティ

プロパティ名	説明	種類
<i>Pending</i>	再起動が保留中かどうかを示します	<i>boolean</i>
<i>Reason</i>	再起動が保留されている理由。可能な値: <ul style="list-style-type: none"> <i>swup</i> (ソフトウェアアップデーター) <i>update</i> (自己更新) <i>virus</i> <i>spyware</i> <i>critical</i> (自己更新に失敗した) <i>malfunction</i> 	<i>string</i>

SimpleComponent : Component

ベース クラスのデフォルト導入。

表34:SimpleComponentのプロパティ

プロパティ名	説明	種類
Enabled		boolean

SoftwareUpdater : Component

情報を提供します WithSecureソフトウェアアップデーター。

表35:ソフトウェアアップデーターのプロパティ

プロパティ名	説明	種類
Enabled	州 WithSecureソフトウェアアップデーター	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 <ul style="list-style-type: none"> 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、WithSecureElementsセキュリティセンターでWMIプロバイダーの設定を有効にする必要があります。

関連資料

WMI クラスページ269

WithSecure Elements Security Centerで WMI 統合に使用されるクラス。

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 カテゴリ
- ブロックするコンテンツを選択してください
- ブロックされたウェブサイトアクセスする

望ましくない Web コンテンツをブロックする

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。

ウェブコンテンツ制御は WithSecure の評判分析データを使用してウェブサイト进行分类し、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 Web 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	人々があらゆる商品やサービスを購入できるウェブサイト。これには、オンラインでの注文や購入を支援する商品カタログを掲載しているサイトや、オンラインでの商品の注文や購入に関する情報を提供するサイトなどが含まれる。
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ィー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してください

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、Browsing Protection拡張機能が必要です。

ウェブコンテンツ制御は、ブラウジング保護が有効になると、管理対象デバイスに対して選択したウェブサイトカテゴリをブロックします。

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. [コンピュータープロファイル] タブを選択し、編集したいプロファイルを選択します。
3. [閲覧保護] を選択してください。
4. [ウェブコンテンツ制御を] 有効にする。
5. 「Webコンテンツコントロール」の横にある ▼ を選択します。
Webコンテンツカテゴリ一覧が開きます。
6. 「許可しない」の下で、管理対象ホストに対してブロックしたいカテゴリを有効にします。
7. [保存して公開] をクリックしてください。

関連資料

Web コンテンツ カテゴリページ277

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。

D.3 ブロックされたウェブサイトアクセスする

「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. それでもウェブサイトアクセスしたい場合は、**[このコンピューターでウェブサイトを許可する]**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、管理者アカウント情報を入力してください。
3. Windowsのユーザーアカウント制御ダイアログで、**[はい]**を選択して、このコンピューターでWebサイトの使用を許可します。

これでウェブサイトアクセスできるようになりました。

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：

- コンピュータを移行する
- Client Security for Mac から Elements Agent for Computers (Mac) への移行

ポリシーマネージャコンソールを使用して移行する

.jarファイルを使用して、ポリシーマネージャーからコンピュータを移行します。

コンピュータを管理する場合 Policy Managerそれらを移行できます WithSecure Elements.jarファイルを使用します。このセクションでは、Windowsコンピュータの移行方法とMacコンピュータの移行方法について説明します。

E.1 コンピュータを移行する

コンピュータを WithSecure Client Securityから WithSecure Elements EPP for Computersへ、および Server Securityから WithSecure Elements EPP for Serversへ移行します。

.jarファイルを適用して移行するには、ポリシー マネージャー 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: bs2elements.jar。

コンピュータを移行するには

1. ポリシー マネージャ コンソールを開き、移行するコンピュータ グループを選択します。
2. 「インストール」タブを選択してください。
インストールページが開きます。
3. ポリシーベースのインストールで、[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. インストールパッケージをインポートするには、[インポート...]を選択してください。
利用可能な .jarファイルが表示されます。
5. .jarファイルを選択し、次に[インポート]を選択します。
ポリシーマネージャーは .jarファイルをインポートし、パッケージの詳細を表示します。
6. [OK]を選択して、.jarファイルを適用します。
7. 開いた **インストールオプション**ウィンドウで、以下の操作を行います。
 - a) サブスクリプションキーを入力します。
 - b) インストール言語を選択し、[完了]を選択してください。
8. インストールウィンドウで、左上隅にある



アイコンを選択して、選択したコンピュータにポリシーを配布します。

選択したコンピュータが移行され、ポリシーも配布されます。

必要に応じて、選択したコンピュータを再起動してインストールを完了してください。

E.2 Client Security for Mac から Elements Agent for Computers (Mac) への移行

Client Security for Mac をElements 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 セキュリティセンターで、クライアントセキュリティ 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: 区切り文字として二重アンダースコア (__) を使用することを忘れないでください。プロファイルIDは必ずサブスクリプションキーと一緒に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 の利用可能な展開方法を確認してください。
4. 手動デプロイまたは自動デプロイのいずれかを選択してください。
5. 以前作成したインストーラー名を自動化スクリプトに組み込んでください。

Elements Agent for Computersのインストーラーは、Client Security for Macを自動的にアンインストールし、新しい製品をアクティベートし、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。

関連資料

macOS 用インストーラーパラメータページ93

インストール時に、これらのインストーラファイル名パターンと アクティベーターコマンドラインオプションを使用して、WithSecure Elements Agent for Computers (Mac)を構成します。

付録 F

FAQ

トピック：

- Elements Security Centerで言語を変更するにはどうすればよいですか？
- WithSecure Email and Server Securityのメール設定はElements Security Centerのどこにありますか？
- 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？
- 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？
- 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？
- サポートされていないElementsクライアントを確認してください
- 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？
- インストールされているソフトウェアを再初期化する

FAQ

WithSecure Elements Endpoint Protectionおよび Elements Security Centerに関するよくある質問への回答。

このセクションでは、WithSecure Elements Endpoint Protectionおよび Elements Security Centerに関するよくある質問にお答えします。ポータル、サブスクリプション、デバイス管理に関する一般的なタスクについて説明します。

ご質問に対する回答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： 議論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確認ください。

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？

WithSecure Elements Security Centerのインターフェース言語は、個人設定で変更できます。

1. ログインして WithSecure Elements Security Center。
2. 右上隅にある



を選択してください。

3. **[マイ設定]**を選択してください。
4. **[言語]**ドロップダウンメニューから、使用したい言語を選択してください。
5. **[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のどこにありますか？

WithSecure Elementsセキュリティセンターでは、WithSecure EmailおよびServer Securityのメール設定は利用できません。

WithSecure Elements Security Centerでは、WithSecure EmailおよびServer Securityのメール設定は確認できません。代わりに、ローカルの Elements Endpoint Protection管理コンソールからこれらの設定を表示および変更してください。

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のサブスクリプションは、パートナーポータルからご注文いただけます。

WithSecure Elements Security Centerのサブスクリプションは、パートナーポータルを通じて注文します。

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？

パートナー企業は、パートナーポータルを通じてWithSecure Elements Endpoint Protectionのサブスクリプションキーを更新または拡張できます。



注：これはパートナーにのみ適用されます。

WithSecure Elements Endpoint Protectionの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からコンピュータを削除すると、そのコンピュータはブロックリストに追加されます。ブロックリストに登録されたコンピュータは、Elements Security Centerに再接続できなくなります。

その結果、WithSecure Email and Server Security (ESS) のインストールでは、同じサブスクリプションキーを使用して同じコンピュータを新規インストールすることはできません。ただし、新しいサブスクリプションキーまたは別のサブスクリプションキーを使用すれば、このコンピュータでも動作します。つまり、このコンピュータは、特定のサブスクリプションキーに紐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るということです。

F.6 サポートされていないElementsクライアントを確認してください

WithSecure Elementsセキュリティセンターの「**問題**」ページには、古いバージョンまたはサポート対象外のElementsクライアントを実行しているデバイスが一覧表示されます。

古いバージョンのElementsクライアントは、エンジンおよび定義ファイルのアップデートを受け取れなくなりました。デバイスのセキュリティを維持するため、サポート対象外のクライアントを特定し、最新の WithSecure Elementsバージョンにアップグレードしてください。

1. ログインして WithSecure Elements Security Center。
2. 選択 **ホーム > エンドポイント保護 > [問題]**。
3. リストされているデバイスを確認し、それぞれを最新の WithSecure Elementsクライアントにアップグレードしてください。

アップグレードされたデバイスは、最新のエンジンと定義ファイルのアップデートを受け取り、セキュリティが維持されます。**問題**ページでは、これらのデバイスが古いバージョンとして表示されなくなります。

F.7 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事前定義済みプロファイルがエンドユーザーのニーズに合致しない場合、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。

例えば、リアルタイムスキャン処理によってコンピュータの動作が著しく遅くなるプログラムがインストールされている場合があります。その場合は、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クライアントなどの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もあります。その場合は、そのソフトウェア専用のファイアウォールルールを設定した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.8 インストールされているソフトウェアを再初期化する

ws_oneclient_logoutを使用してWithSecure Elements EPP for Computersからログアウトし、新しいサブスクリプションキーを入力して、WithSecure Elements Security Centerでデバイスを正しい会社に接続します。

このツールを使用すると、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まだ入力されていない初期状態に戻すことができます。



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. 以下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。

--psb1, --psb2, 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。
--psb3, --psb4,
--psbsmieu



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) は動作を停止し、アプリケーションのメイン画面を開いた際に、新しいサブスクリプションキーを手動で入力するよう求められます。

--profile-id
<profileid> プロファイルの割り当てを強制的に行うことができます。デバイスを再登録すると、デフォルトのプロファイルが割り当てられます。このパラメータを使用すると、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は製品に保存されます。
ws_oneclient_logout.exeツールを再度実行する際に、コマンドラ

インパラメータ「`--profile-id`」を追加しない場合、同じプロファイルが再度割り当てられます。

--proxy

ログイン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

クローンされた仮想マシンで、クローン作成後すぐに SMBIOS UUID が変更されない場合に使用できます。このオプション (`ws_oneclient_logout.exe -wait_uuid_changed`) を使用して `ws_oneclient_logout.exe` ツールを使用すると、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 に正しい一意の ID で登録されるようにします。

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、結果として `0` が返されます。それ以外の場合、たとえばネットワークが利用できない場合や、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「期限切れ」状態のままになり、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。

Glossary

アクセス制御

アクセス制御とは、定義された権限とポリシーに基づいて、システム内のリソースを閲覧、使用、または変更できる人物やものを制限および規制する手法のことです。

アクティベーターツール

アクティベーターツールは、製品のインストールをアクティブ化し、展開時にプロファイルやサブスクリプション設定などの構成パラメーターを適用するために使用されるコマンドラインユーティリティです。

Active Directory (AD)

Active Directory (AD) は、ユーザー、コンピューター、ポリシーなどのネットワークリソースの管理を集中化し、Windows ドメインネットワーク内で認証と承認を提供する Microsoft ディレクトリ サービスです。

エージェント

エージェントとは、管理対象デバイスにインストールされるクライアントソフトウェアであり、保護機能の実装、デバイスの状態報告、管理サービスとの通信を行うものです。より広義には、ユーザーまたは他のシステムに代わって動作するプログラムを指します。

アンチウイルス

ウイルスなどのマルウェアを予防・検出・駆除するソフトウェア。

アプリ構成

アプリケーション構成とは、デプロイ時または管理時にアプリケーションの動作、権限、または機能を事前に構成するために使用される設定または値の集合のことです。

アプリケーション制御

アプリケーション制御は、選択したアプリケーションの実行やインストールを防止し、スクリプトの実行を停止するルールベースのエンドポイントセキュリティ機能です。

自動タスク

自動化タスクとは、設定されたスケジュール、トリガー、または条件に基づいて、デバイスやシステム上で自動的に実行される、あらかじめ定義されたタスクのことです。

自動化

自動化とは、人間の介入を最小限に抑えてタスクやプロセスを実行し、効率、精度、およびスケーラビリティを向上させるテクノロジーの使用です。

バンキング保護

オンラインバンクへのアクセスやオンライン取引の際に、有害な行為からユーザーを保護します。

行動分析

行動分析とは、既知の特徴だけに頼るのではなく、通常の活動パターンからの逸脱を観察することによって脅威を特定する検出手法である。

ブロックリスト

ブロックリストとは、アプリケーション、ウェブサイト、送信者、ファイルハッシュなど、アクセスや実行が明示的に拒否されるエンティティのリストであり、許可リストの反対です。

侵害

侵害とは、機密データまたは保護されたデータが、権限のない第三者によってアクセス、開示、または盗まれるセキュリティインシデントのことです。

広範なコンテキスト検出 (BCD)

広範囲コンテキスト検出とは、WithSecure Elements EDRが関連する検出結果をまとめて単一のインシデントとして関連付け、重要度順にランク付けすることで、攻撃の全体像を示すものです。

ブラウザ保護

アクセスしたWebサイトの安全性を評価し、ユーザーが意図せず有害なWebサイトにアクセスすることを防ぐ機能。

ブラウザ保護拡張機能

ブラウジング保護拡張機能は、評判に基づくサイト分析やポリシーに基づくウェブコンテンツ制御といったウェブ保護機能を実現するブラウザコンポーネントです。

証明書

証明書は、安全な通信と認証を可能にするために証明機関(CA)によって発行される、公開キーの所有権を証明するために使用されるデジタル文書です。

クラウドセキュリティ

クラウドセキュリティとは、クラウド環境でホストされているデータ、アプリケーション、インフラストラクチャを保護するためのポリシー、制御、およびテクノロジーの集合体です。

クラウドサービス

クラウドサービスとは、保護、監視、または管理のためにプラットフォームに接続されたオンラインサービスまたはワークロードのことです。

会社

パートナーによって管理されているか、または独立して運営されている顧客組織で、組織階層の最下位レベルに位置し、子組織を持たないもの。

構成キー

構成キーとは、アプリケーションの動作や機能値を、展開時またはデバイス管理時に事前に構成するために使用される、名前付きの設定のことです。

接続制御

オンラインバンキングのWebサイトアクセスを自動的に検出し、他の接続をブロックする機能。

Connector

コネクタは、2つ以上のシステム、アプリケーション、またはデバイス間の通信とデータ交換を可能にするソフトウェアまたはハードウェアコンポーネントです。

封じ込め

攻撃者が拡散するのを阻止し、情報の盗難、改ざん、破壊を防ぐために、影響を受けたホストまたはアカウントを隔離する対応措置。

コンテンツフィルタ

コンテンツフィルタリングとは、カテゴリ、ポリシー、またはルールに基づいてオンラインコンテンツやネットワークコンテンツへのアクセスを制限することです。例えば、macOSのネットワークコンテンツフィルタリングなどが挙げられます。

重要度

検出の影響度は、重大度と影響を受けるホストの重要性に基づいて、顧客環境に与える可能性のある影響。

カスタムラベル

デバイスの整理と管理のために使用される、WithSecure Elementsセキュリティセンターのタグ付け機能。

顧客企業

顧客企業とは、パートナーが管理するプラットフォームまたはサービス構造内で設立、管理、またはサービス提供を受ける顧客組織のことです。

DataGuard

機密ファイルを不正アクセス、ランサムウェアによる暗号化、または流出から保護するセキュリティ機能。

ディープガード

プログラムの動作をリアルタイムで監視し、危険な動作を停止させることで、未知の脅威からコンピュータを保護する機能。

検出

検出とは、セキュリティ制御システムまたは分析システムによって認識された、疑わしい、悪意のある、またはポリシーに関連するイベント、活動、または発見事項を指します。

デバイス制御

USB ドライブ、Bluetooth 周辺機器、その他のリムーバブルメディアなどの外部デバイスの使用を制限し、データの漏洩やマルウェアの感染を防ぐセキュリティ機能。

ディスクバリアスキャン

ディスクバリアスキャンとは、ネットワークまたは環境内に存在する資産、システム、またはターゲットを特定するスキャンのことです。

駆除

ファイル全体を削除せずに、感染したファイルからウイルスを除去しようとするウイルス対策プログラムの機能。

暗号化

暗号化とは、暗号化アルゴリズムを使用してデータを安全な形式に変換し、機密性を確保し、不正アクセスから保護するプロセスです。

Endpoint Detection and Response (EDR)

エンドポイント検出・対応 (EDR) は、エンドポイントを継続的に監視し、不審な活動や高度な脅威を検出、調査、対応するセキュリティ技術です。

Endpoint Protection

エンドポイント保護とは、ワークステーション、サーバー、モバイルデバイスなどのエンドポイントデバイス上の脅威を防止、検出、および対処するために使用される一連のセキュリティ機能のことです。

Entra ID

Microsoft のクラウドベースの ID およびアクセス管理サービス (旧称 Azure AD)。

イベント

センサーが検知し、検知の定義に合致する、デバイス上で監視されている事象。

除外ルール

除外ルールとは、特定のファイル、パス、プロセス、またはその他の項目をスキャン、監視、または適用対象から除外するルールのことです。

エクスプロイト

プログラムの欠陥を利用して予期しない動作を引き起こすオブジェクトや手法。これにより、攻撃者が他の有害な操作を実行するための条件ができあがります。

Exposure Management

エクスポージャー管理とは、資産、サービス、環境全体にわたる脆弱性やリスクを特定し、優先順位を付け、修復を支援するセキュリティ機能です。

外部攻撃対象領域 (EAS)

攻撃者が悪用できる、インターネットに接続された資産、サービス、および脆弱性の集合。

誤検知

誤検知とは、正当なファイル、メッセージ、URL、またはアクティビティであるにもかかわらず、セキュリティシステムが誤って「悪意がある」、「疑わしい」、または「有害である」と判定してしまったもののことです。

フェデレーションシングルサインオン (FSSO)

ユーザーが一度認証すれば、再度ログインすることなく、異なるドメインの複数のアプリケーションにアクセスできるメカニズム。

ファイアウォール構成

受信および送信ネットワークトラフィックを制御し、ネットワークのセキュリティとコンプライアンスを確保するためのルールとポリシーを設定するプロセス。

ファイアウォールプロファイル

ファイアウォールプロファイルとは、デバイスまたはネットワーク環境に適用される、定義済みのファイアウォールルールと設定のセットのことです。

ファイアウォールルール

ファイアウォールルールとは、ファイアウォールのトラフィックの処理方法を定義する、個別の許可、ブロック、またはフィルタリング指示のことです。

ゴールデンイメージ

ゴールデンイメージとは、同一のデバイスや仮想マシンを複製または展開するための標準ソースとして使用される、事前設定済みのシステムイメージです。

グループポリシー (GPO)

グループポリシー (GPO) は、管理者がドメイン内の複数のコンピューターにわたってセキュリティポリシー、ユーザー設定、およびシステム構成を定義できるようにする Microsoft Windows の機能です。

最もインパクトのある推奨事項

サイバーリスクを軽減するためにすぐに対処する必要があるセキュリティ検出結果の優先順位リスト。

ホスト

センサーを動作させ、そのセンサーのプラットフォームが監視するデバイス。

IAM ロール

IAMロールとは、ユーザー、サービス、またはワークロードが引き受けることができる一連の権限を定義する、IDおよびアクセス管理の役割です。

ID およびアクセス管理 (IAM)

アイデンティティおよびアクセス管理 (IAM) とは、適切なユーザーが適切なリソースへのアクセス権を持つことを保証するためのポリシーとテクノロジーのフレームワークであり、認証、認可、およびユーザーIDのライフサイクルを網羅しています。

アイデンティティ管理

アイデンティティ管理とは、ユーザーやデバイスがシステム間で確実に識別されるように、デジタルアイデンティティとその属性を作成、維持、削除する分野のことである。

ID プロバイダー (IdP)

アイデンティティ プロバイダー (IdP) は、デジタルIDを作成、保存、管理し、ユーザーが複数のアプリケーションを安全に認証してアクセスできるようにするサービスです。

インシデント

インシデントとは、セキュリティ侵害、ポリシー違反、またはその他の脅威を示すセキュリティイベント、あるいは関連する一連のイベントであり、調査、封じ込め、または修復が必要となるものです。

感染

感染とは、ファイル、オブジェクト、システム、またはワークロードが、悪意のあるコードやその他の有害なコンテンツを含んでいる、または影響を受けている状態を指します。

横方向の動き

初期侵入の後、追加のシステムにアクセスするためにネットワーク内を移動するプロセス。

ライセンスキー

ライセンスキーとは、ソフトウェア製品またはサブスクリプションを有効化し、その使用が許可されていることを確認するための固有のコードです。

ライセンスステータス

セキュリティ製品のサブスクリプションの現在の状態。その有効性と有効期限を決定します。

Lightweight Directory Access Protocol (LDAP)

軽量ディレクトリアクセスプロトコル (LDAP) は、ネットワーク経由でユーザー、グループ、デバイスなどのディレクトリ情報にアクセスし、管理するためのオープンなプロトコルです。

Linux 認証スキャン

Linux認証スキャンとは、提供された認証情報またはキーを使用してLinuxシステムに接続し、スキャン結果やシステム情報を収集するスキャン方法です。

マルウェア

害を及ぼすことを目的として開発されたプログラムまたはファイル。コンピュータウイルス、ワーム、トロイの木馬などが含まれます。

マルウェア定義

マルウェア定義とは、ウイルス対策ソフトウェアが既知の悪意のあるファイルを識別するために使用する、署名またはパターンのことです。

マルウェア保護

マルウェア対策とは、デバイス上のウイルスや潜在的に不要なアプリケーションを検出し、ブロックし、削除する機能です。

マルウェアスキャン

マルウェアスキャンとは、デバイス、ファイルセット、またはワークロードに対して、悪意のあるソフトウェアやその他の有害なコンテンツがないかを確認するスキャンのことです。

手動スキャン

手動スキャンとは、ユーザーが開始するセキュリティスキャンであり、スケジュールに基づいて自動的に実行されたり、リアルタイムで実行されたりするのではなく、必要に応じて実行されます。

メンバー

組織または他のセキュリティグループに所属するセキュリティ管理者またはセキュリティグループ。

メンバーシップ

メンバーシップとは、グループ、組織、ディレクトリ、またはその他の管理されたコレクションに属している状態であり、可視性、アクセス、または継承された権限に影響を与えます。

モバイルデバイス管理 (MDM)

IT管理者がモバイルデバイスのセキュリティポリシーをリモートで管理、監視、適用できるようにするセキュリティソリューションです。

MSIプロパティ

Microsoft インストーラー (MSI) 経由のソフトウェアパッケージのコマンドラインインストールで使用するパラメーター。

多要素認証 (MFA)

アカウントへのアクセスを許可する前に複数の認証方法を必要とするサインイン方法。そのた

め、パスワードが漏洩しただけではアクセスすることはできません。

ネットワークゲートウェイ

ネットワークゲートウェイは、モバイル端末の通信をルーティングおよび検査する（例えば、リモートプロキシ経由で）ことで、安全でない宛先やコンテンツをブロックするモバイル保護コンポーネントです。

ネットワーク隔離

ネットワーク隔離とは、悪意のある活動や拡散を阻止するために、デバイスのネットワーク通信を制限または遮断する封じ込め措置のことです。

ネットワーク保護

ネットワーク保護とは、ネットワークトラフィックを監視または制御することで、ユーザーやデバイスを安全でない接続やコンテンツから保護するセキュリティ機能です。

組織

ElementsRBACにおけるセキュリティ管理者、セキュリティグループ、および役割割り当てを格納するコンテナ。組織の種類は、ソリューションプロバイダー、サービスパートナー、および会社の3種類です。

パートナー

ソリューションプロバイダーまたはサービスパートナーとして、1社以上の顧客企業を管理する組織。

パッチ管理

オペレーティングシステムおよびサードパーティ製ソフトウェアのパッチ適用状況を監視し、既知の脆弱性を解消するためのアップデートを適用する。

フィッシング

フィッシング攻撃とは、攻撃者が信頼できる送信者を装って偽のメッセージを送信し、受信者を騙して認証情報や金融情報などの機密データを漏洩させる攻撃のことです。

不要な可能性があるアプリケーション (PUA)

悪意はないかもしれませんが、セキュリティ上のリスク、侵入的な動作、または不要な広告をもたらす可能性のあるソフトウェアプログラム。

プライバシー

プライバシーとは、個人または組織の情報を、不正な収集、アクセス、使用、または開示から保護することである。

プロファイル割り当て

プロファイル割り当てとは、手動選択または割り当てルールに従って、選択したプロファイルをデバイス、グループ、またはターゲットに適用するプロセスです。

隔離

隔離とは、潜在的に有害なファイル、メッセージ、その他のアイテムを隔離された保管場所または状態のことで、それらがシステムやユーザーに影響を与えるのを防ぎつつ、後で確認、解放、または削除できるようにするものです。

ランサムウェア

ユーザーが自分のデータやデバイスにアクセスできないようにし、「通常のアクセスを回復する」ために身代金を要求する悪意のあるプログラム。このプログラムは、身代金を支払っても、実際には正常なアクセスを回復しないことがあります。

ランサムウェア保護

ランサムウェアやそれに類する有害なソフトウェアによって、有害な変更が行われていないかフォルダを監視する機能。

リアルタイム保護

リアルタイム保護機能は、ファイルへのアクセス時に継続的にスキャンを行い、マルウェアを含むファイルをブロックすることで、リアルタイムスキャンによる常時保護を提供します。

リアルタイムスキャン

リアルタイムスキャンとは、コンテンツやアクティビティがアクセス、保存、処理される際に、継続的にスキャンしてチェックする機能です。

RMM(遠隔監視・管理)連携 (RMM)

リモート監視・管理 (RMM) 統合とは、製品と RMM プラットフォームを接続し、ステータス、データ、または管理アクションを交換できるようにすることです。

レピュテーションサービス

経過時間、頻度、場所に基づいてファイルをコンテンツストに配置し、他の方法では見逃される可能性のある脅威を明らかにするサービス。

リソース

RBACの主体・役割・リソースモデルにおいて、役割割り当てが適用される組織。

リスクウェア

特にコンピュータに害を与えるようには設計されていないが、誤用すると問題を引き起こす可能性があるソフトウェア。

ロール割り当て

役割の割り当てとは、ユーザー、グループ、またはその他の主体に役割を付与し、その役割に関連付けられた権限を受け取らせることです。

ロールベースアクセス制御 (RBAC)

最小権限の原則を適用するために、ユーザーの役割と権限に基づいてシステムアクセスを制限するセキュリティ モデル。

サンプル提出

サンプル送信とは、分析およびフォローアップ処理のために、疑わしいファイル、URL、または電子メールを送信するリクエストのことです。

サンプル検証

サンプル検証とは、疑わしいファイル、URL、またはメールを専門家による分析のために送信し、そのリクエストの結果を追跡するサービスです。

スキャン

スキャンとは、デバイス、システム、アプリケーション、アカウント、またはその他の対象物を検査し、脅威、脆弱性、不審な活動、またはポリシーに関連する発見事項を検出するセキュリティチェックのことです。

スキャンノード

スキャンノードとは、スキャンを実行し、その進行状況と結果を管理サービスに報告するホストまたはサービスコンポーネントのことです。

スキャンテンプレート

スキャンテンプレートとは、保存済みで再利用可能なスキャンオプションのセットであり、複数のスキャンに適用できます。

スケジュールスキャン

スケジュールスキャンとは、ユーザーが手動で開始する必要なく、定義された時間、間隔、またはシステム条件に基づいて自動的に実行されるように設定されたスキャンのことです。

SCIM

クロスドメインID管理システム (System for Cross-domain Identity Management) は、Entra IDがセキュリティ管理者とセキュリティグループをElementsにプロビジョニングするために使用するプロトコルです。

スコープセクター

WithSecure Elementsのポータルサイトに表示される情報の範囲を広げたり狭めたりするためのユーザーインターフェイスコンポーネント。

Secure Shell (SSH)

セキュアシェル(SSH)は、セキュリティ保護されていないネットワーク経由でリモートデバイスに安全にアクセスして管理するために使用される暗号化プロトコルです。

セキュリティ管理者

セキュリティ管理者とは、割り当てられた役割に基づいて、セキュリティ設定、アクセス、または運用タスクを管理するユーザーアカウントのことです。

セキュリティ管理者ロール

WithSecure Elementsセキュリティセンターで、セキュリティ構成の管理アクセス権を付与するロール。

Security Cloud

Security Cloudは、WithSecureが提供するクラウドベースの脅威分析およびレピュテーションサービスであり、ファイル、ウェブサイト、その他のセキュリティ関連の観測データを分類し、新たな脅威に対する最新の保護を提供します。

セキュリティイベント

セキュリティイベントとは、セキュリティに関連する出来事、検出、またはアクションを記録したもので、レビュー、監視、または対応のために表示されます。

セキュリティグループ

セキュリティグループとは、共有された役割割り当てを受けるユーザーの集合体であり、そのメンバーは同じアクセス権限を継承します。

セキュリティ情報イベント管理 (SIEM)

セキュリティ情報およびイベント管理 (SIEM) は、環境全体からログデータとイベントデータを収集、関連付け、分析することで、脅威を検出し、インシデント対応を支援する技術です。

セキュリティ監視

セキュリティ監視とは、潜在的なセキュリティ脅威を検知、警告、調査するために、システムおよびネットワークの活動を継続的に収集・分析することです。

セキュリティポリシー

製品の設定がどのように管理、保護、配布されるかを定義する一連のルール。主にPolicy Managerで使用されますが、他の管理者レベルの企業向け製品にも表示されます。

センサー

監視対象のデバイス (ホスト) 上で動作するソフトウェア。センサーはデバイスの状態を監視し、Elements Endpoint Detection and Responseのバックエンドと通信します。

サーバー共有保護

サーバー共有保護とは、共有ファイルへのアクセスを監視し、共有データに影響を与えるランサムウェアの活動を検知または制限する機能です。

サービスアカウント

サービスアカウントは、多くの場合、事前定義された権限を使用して、システムやサービスと対話するためにアプリケーション、スクリプト、または自動プロセスによって使用される特別な種類のアカウントです。

サービスパートナー

サービスパートナーとは、他者に代わってサービス、顧客組織、または委任された運用責任を管理する組織またはパートナー階層のことです。

重大度

サイバー攻撃がネットワーク環境に与える可能性のある影響は、攻撃が与える可能性のある損害の程度に基づいています。

ソフトウェアアップデート

サードパーティソフトウェアのアップデートの有無をスキャンし、セキュリティアップデートを展開する機能。

ソリューションプロバイダー

ソリューションプロバイダーは、WithSecure Elementsの管理階層における最上位のパートナー組織であり、顧客企業を管理し、パートナー企業の従業員にアクセス権限を委任します。

スパム

スパムメールは、通常、多数の受信者リストに一括して送信される未承諾のメールです。

スパイウェア

個人または組織に関する情報を、知らない間に収集することを目的とし、ユーザーの同意なしにその情報を他の団体に送信する可能性があるソフトウェア、またはユーザーの知らないうちにコンピュータを制御することを主張するソフトウェア。

主題

RBACの主体-役割-リソースモデルでは、役割の割り当てを受けるセキュリティ管理者またはセキュリティグループを指します。

サブスクリプションキー

サブスクリプションキーとは、サブスクリプションを識別および検証するための固有のコードであり、組織向けにWithSecure製品を有効化するために使用されます。

改ざん防止

権限のないユーザーやマルウェアによるセキュリティソリューションの無効化や変更を防ぐセキュリティ制御。

テナント

テナントとは、Microsoft Entra IDディレクトリなどのマルチテナント型クラウドサービスの独立したインスタンスであり、単一の組織に属し、データ、構成、およびユーザーを他のテナントとは分離して保持します。

脅威検出

脅威検出とは、環境内における悪意のある活動、異常、または侵害の兆候を特定し、調査および阻止できるようにするプロセスです。

脅威インテリジェンス

脅威インテリジェンスとは、攻撃者の戦術、インジケーター、動機など、既存または新たに出現した脅威に関する、根拠に基づいた知見のことであり、防御における意思決定を行うために活用されます。

トランスポート層セキュリティ (TLS)

トランスポート層セキュリティ (TLS) は、データ転送を暗号化し、IDを検証することで、ネットワーク上で安全な通信を提供する暗号化プロトコルです。

不要なアプリケーション

プライバシーを侵害する可能性のあるアプリケーション、またはデバイスのセキュリティに深刻な影響を与える可能性のあるアプリケーション。

仮想デスクトップインフラストラクチャの保護 (VDI)

仮想デスクトップインフラストラクチャ保護とは、非永続イメージやクローンイメージを含む、仮想デスクトップ (VDI) 環境に対応したエンドポイント保護のことです。

ウイルス

ウイルスは通常、ファイルに感染して繰り返し複製することができるプログラムであり、他のファイルの内容を変更したり置き換えたりすることで、コンピュータに損害を与えることができます。

ウイルス保護

ウイルス、ワーム、トロイの木馬の侵入を防ぐとともに、すでに感染している悪意のあるソフトウェアコードを削除します。

クーポン

製品またはサービスの試用期間の延長など、サブスクリプションの認証または特別オファーの利用に使用されるコード。

脆弱性

攻撃者が影響を受けるシステム/デバイスで不正なアクションを実行するために悪用できる、プログラムまたはOSの欠陥、抜け穴、または予期しない動作。

Vulnerability Management

脆弱性管理とは、システムやソフトウェアにおけるセキュリティ上の弱点を特定、評価、優先順位付け、および修復する継続的なプロセスである。

Web コンテンツ制御

事前に定義されたカテゴリとセキュリティポリシーに基づいてWebコンテンツへのアクセスをブロックする機能。

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) は、システム管理者がスクリプトまたはリモートコマンドを使用して Windows ベースのデバイスを管理および監視できるようにする Microsoft フレームワークです。

ゼロデイ

ゼロデイとは、ベンダーに知られておらず利用可能な修正プログラムがない脆弱性またはエクスプロイトのことで、パッチがリリースされるまで影響を受けるシステムが露出したままになります。

索引

記号

悪意のあるウェブサイト 161, 163, 209
圧縮ファイル 152
以下 181
以上 181
移住 282
一般設定 142, 144, 192, 199, 202
閲覧保護 100, 161, 163–165, 211
黄金の像 69–71
画像更新 70
回復キー 143
改ざん防止 151
改ざん防止機能 202
開始値 181
隔離されたファイル 193
隔離施設 150, 193
隔離対象品目 150
感染した物体 213
感染を阻止する 241
感染症対策 213
監査ログ 242
監視 188–189
監視コンポーネント 234, 236
管理コンソール 285
管理者アカウント 7, 43
管理対象Androidアプリ 100
管理対象構成 118
企業レベル 35, 37
許可および報告モード 187
許可されたウェブサイト 210
許可されたドメイン 164
共有ファイル 187–188
共有フォルダ 188
脅威インテリジェンス 184
脅威のカテゴリ 155
脅威のブロック 209
脅威への対処 159
業務分野別アプリ 66
計測スキャン 213
警告 168
検疫 177
検出ルール 184
言語 55
言語設定 285
公証 95
更新が不足しています 175
更新スケジュール 139–140
更新除外 247, 249
更新情報を含める 248
更新内容 247–248
構成プロファイル 87, 124
購読を更新する 286
再インストール 258
再発 140
削除されたコンピュータ 286
参考情報 250
指紋 11
私の設定 10, 21, 285
資産グループ 35–36
自動インストール 88
自動化されたタスク 172, 174–175
自動更新 191

自動削除 33, 37
取り外し不可能なシステム拡張機能 87
手順のインポート 226, 228
手動インストール 88
手動スキャン 152, 158–159
手動割り当て 133
手動起動 75
手動展開 54
週間概要 254
従量制接続 213
重大 250
重複デバイス 258
重要 246, 250
除外されたパス 177
除外されたファイル 192
除外ルール 137–138
招待待ち 34
証明書 106, 119
信頼できるアプリケーション 155, 212
申請除外 151, 156
世界的な除外事項 149
制御されたアップデート 139, 142, 200
制御されたアップデート - スケジュール設定 140
制御されたアップデート - 手動 140
生体認証 11
製品アクティベーション 75–76, 92
製品アップデート 172, 174
製品コード 54
製品バージョン 190
製品メッセージ 239
製品構成 75, 77
静音インストール 51, 88
脆弱性ロール 11
脆弱性管理 6
接続制御 165
設定キー 111, 123
設定を更新する 191
設定割り当て 131
組織設定 20–21, 35
早期アクセス 190
多要素認証 7, 9–11
妥協の兆候 184
対象 181
大量購入プログラム 123
中程度のセキュリティ 246
調査アシスタント 255
通知 124, 144, 239
通知ハブ 239
通知ハブは 239
通知権限 90
通知設定 84
低 246
定期レポート 241
定期購入の注文 285
適用規則 179
展開方法 50, 74, 95
電子メールアドレス 27
電子注文 23, 261
登録キー 101
特別商品パッケージ 76
二段階認証 9
認証アプリ 9–10
配布証明書 95

汎用インストーラー 97
 美術学修士 9–10
 評判に基づくブラウジング 163, 209
 保護されたフォルダー 179
 保護されていないデバイス 222
 保護ステータス 250
 保存されたビュー 242
 北中部 231–232
 未分類 246
 未満 181
 名前を変更する 21
 問題ページ 286
 役割の権限 17
 要素コネクタ 146
 連邦ドメイン 8, 29–30
 連邦制の廃止 30
 露出管理 12, 217

A

access rights 6, 11–12, 19
 account creation 20
 account levels 16
 Active Directory 37, 60, 73, 133, 222
 AD group 133
 AD groups 37
 adding devices 30, 32
 administrator account 6, 11, 19–20
 Agent 50, 58, 63–64, 68, 70, 95, 149, 222, 233, 258, 282
 Agent for Computers 31, 230, 282
 Agent for Computers (Mac) 282
 Agent for Computers」 69
 Agent for Servers 31, 96–97
 Agent for Servers」 69
 Agent for Windows 39
 Agent の再起動 189
 Agent は 148
 Agent を 144
 Agentを 50, 68, 127, 132, 222, 258
 AirWatch 98, 101
 alerting 239
 Android and iOS 107, 113, 120
 Android app 103, 105, 110, 122
 Android app configuration 106
 Android Enterprise 104–106, 111, 114, 119
 Androidアプリ 100, 114–115, 117, 119, 125–126
 Androidアプリの設定 101
 Androidアプリ管理 118
 Android端末 212–213
 AntiVirus class 269
 app assignment 102
 App Catalog 119
 app configuration 108–109
 app deployment 101, 103, 105, 107, 110, 113, 116, 119–120, 122
 app distribution 114
 app list 104
 App Store 116, 120, 123
 app-layer firewall 194, 196
 Apple Business Manager 123
 Apple Firewall 194
 Apple製品 86
 application blocking 180
 Application Control 42, 180–181, 183
 application rules 180–181
 audit logs entry 12
 Auth0Guardian認証アプリのプッシュ通知機能を使えば9

automated tasks 173, 246
 automatic updates 200, 246

B

BCD 255
 behavior-based protection 157
 BitLockerの管理 143
 BitLocker管理 142
 block page 280
 blocked website 280
 Broad Context Detection 255
 browser extension 90–91
 browsing protection 193
 Browsing protection 90–91, 279
 Browsing Protection 277, 280
 Browsing Protection extension 277

C

change subscription 26
 Chrome OS 100
 Citrix 69
 client applications 265
 client customization 263
 Client Security 282
 Client Security for Mac 89
 Client Security for Macを 282
 clone profile 189, 199
 codesign 197
 Collaboration Protection 17
 computer profile 141, 189, 199
 Computer Protection 50
 Computer Protection for Mac 233
 configuration designer 109
 configuration keys 106, 109, 113, 116–117, 121
 connection control 193
 connectivity status 218
 Connector 26, 31, 36, 143, 147, 201
 Connector の 31
 Connector は 147
 Connector」 の 147
 Connectorが 147
 Connectorを 147, 199, 251
 content categories 210, 277, 279
 create profile 141, 189, 199
 CSV reports 240
 custom profile 263
 custom services 230–231
 customer company 11, 23, 261
 customization 261

D

dark mode 22
 DataGuard 42, 178–180
 DataGuard Vault 179
 DataGuard は 178, 180
 DataGuardが 178, 241
 DataGuardに 178
 DataGuardは 178
 DataGuardを 178, 180
 Datto 225
 Datto RMM 233
 Datto RMMを 233, 235
 DeepGuard 42, 157, 178

- default profile 131, 133
- delete profile 135
- device access rules 170–171
- device assignment 131
- device blocking 171
- device blocking rules 172
- device commands 36
- Device control 170–172
- Device Control 42
- device details 219
- device filtering 218
- device identification 117
- device information 219
- device isolation 169, 223
- device management 30, 35, 131, 216
- device operations 216
- device overview 217
- device protection status 219
- device reports 240
- device scan 249
- device search 219
- device security monitoring 217
- device statistics 239
- device updates 250
- device UUID 219
- device view 35, 37
- devices 26, 36, 135, 218
- Devices page 219
- diagnostic data 39
- distribution group 114
- downloading software 33
- Downloads page 33

E

- edit administrator 20
- edit profile 134
- EDR 26, 33
- EDR for Computers 26, 33
- EDR および EPP for Computers Premium 26
- EDR および EPP for Computers Premium まで 26
- EDR および EPP for Computers へ 26
- EDR および EPP for Servers Premium 26
- EDR と EPP for Computers 26
- EDR と EPP for Servers の 26
- EDRおよびEPP for Computers 26
- EDRおよびEPP for Computers Premium 26
- Element Security Center 51, 55
- Elements 6, 10, 17, 23, 27, 35, 42–43, 95, 119, 122, 258, 261, 286
- Elementsエージェント 233
- Elementsエージェントの 143
- Elementsエンドポイント保護 265
- Elementsコネクタ 145–146
- Elementsセキュリティセンター 6, 10, 21, 35, 98, 106, 119, 127, 185, 265, 275
- Elementsセキュリティセンターの 21, 71
- Elementsの 6, 17, 255
- Elementsモバイル保護 109, 113, 120
- email 121
- Email and Server Security 286
- email invitation 32
- EMM token 104
- Endpoint Detection and Response 42, 51
- Endpoint Protection 11, 17–18, 30, 42, 50–51, 69, 72, 74, 98, 186–187, 217, 219, 249, 285
- Endpoint Protection with EDR for Mac 89

- Endpoint Protection WithSecure 186
- Endpoint Protection の 116
- Endpoint Protectionの 135, 286
- Endpoint暗号化を 186
- enrollment 104
- env 121
- EPP for Computers 26, 36–37, 42, 60, 133, 141, 147, 178, 189, 225, 227, 230, 233, 263, 282, 287
- EPP for Computers (Mac) 92
- EPP for Computers Premium 26, 178, 180
- EPP for Computers Premium へ 26
- EPP for Computersは 60, 287
- EPP for Linux 198
- EPP for Servers 26, 36–37, 42, 133, 141, 178, 225, 263
- EPP for Servers Premium 26, 178, 180
- EPP for Servers Premium へ 26
- EPP for Servers に 42
- EPP for Servers は、 60
- EPP for Serversは 42
- EPP for Serversは、 42
- EPP subscription 26
- excluded paths 205
- exclusion rule 183
- exclusion rules 181
- EXE installer 50
- existing customer company 24
- exploit protection 157
- export rules 196
- Exposure Management 11, 17, 51

F

- F-Secure Linux Protection Monitor [LIN] 236
- file baseline 207
- file version 183
- firewall 194
- firewall configuration 166
- firewall profile 166–167, 169, 194–196
- firewall rule 167, 169
- firewall rules 166, 194–196
- firewall rules table 167
- forgot password 21
- frequently asked questions 285
- FSSO 27

G

- general settings 190
- global rule 180
- Google Chrome 72, 90–91, 100
- Google Play 117
- Google Playアプリ 114
- Google Playを管理 114, 125
- Google Workspace 100–101
- Google Workspace Endpoint Management 98
- GPO 60, 72–74
- GUTS2 updates 147

H

- hardware devices 170–171
- hardware ID 172
- Home page 217
- HTTP proxy 250

I

IAM role 11
 IBM MaaS360 113–115
 IBM Security MaaS360 42, 98
 import rules 196
 inbound connections 169
 infection activity 239
 installation link 32
 installation logs 245
 installation package 31, 33
 integration 265
 Integrity Checking 207
 IntuneWinAppUtil 67
 iOS 124, 128
 iOS app 101, 107, 113–114, 116, 120
 iOS app configuration 102, 121
 iOS app configuration policies 108
 iOS app management 116
 iOS store app 107
 iOSアプリ 123
 iOSアプリの設定 123
 iOSデバイス 209
 iPadOS 123
 Ivanti Endpoint Management 42, 98, 116–117, 119
 Ivanti Endpoint Management の 119
 Ivantiエンドポイント管理 117–119

J

Jamf 86
 Jamf Pro 123–124
 JSON file 196

K

Kaseya 225
 Kaseya agent 227
 Kaseya RMM 225–229
 Kaseyaを 228

L

license 122, 128
 light mode 22
 Linux 229
 Linux profile 199–200, 204–205, 207
 Linux profiles 198
 Linux Protection 229, 231–232, 235
 Linux Protection が 236
 Linux Protection の 229
 Linux Protectionを 228, 235–236
 Linux WithSecure 231
 Linuxのインストール 96–97
 Linuxの展開 95
 Linuxの保護 228–229, 231–232, 235–236
 Linuxプロファイル 199–202
 List view 216
 lock profile settings 136
 login 8, 21
 login credentials 8
 logo 263
 Luminen 254–256
 Luminenは 254–255

M

Mac 227, 230–231
 Mac firewall 194
 Mac installation 233
 Mac profile 189–195
 Mac profiles 189
 Mac 用クライアントセキュリティ 282
 Mac 用コンピュータ保護 233
 macOS 83–85, 88–90, 95
 macOS application 197
 macOS Sequoia 87–88
 macOSへの展開 77
 Macの展開 74
 Macプロフィール 190, 192–193
 Macへのインストール 227
 malware definitions 200
 malware prevention 180
 malware scan 173, 192, 204–205
 managed applications 104
 managed companies 16
 Managed Google Play 110
 managed iOS devices 108
 manual deployment 50
 manual scanning 204–205
 MDM 75–76, 98, 100–104, 116–117, 121
 MDM deployment 101, 104, 107, 113–114, 116, 119–120
 Microsoft Configuration Manager 50, 63–64
 Microsoft Edge 73
 Microsoft Endpoint Manager 112
 Microsoft Entra Admin Center 27
 Microsoft Entra ID 27
 Microsoft Intune 42, 50, 66–68, 83–85, 98, 107–112
 Microsoft Intune の 109
 Microsoft updates 251
 Miradore 98, 120–122
 missing software updates 249
 missing updates 245, 250
 mobile devices 219
 mobile profile 210
 Mobile Protection 30, 36, 39, 42, 50, 66–67, 98, 100–101, 104–105, 107, 109–110, 113–114, 116–117, 119–120, 123–125, 128, 131, 208
 Mobile Protection with External MDM 106
 Mobile Protection」 108, 111
 Mobile Protectionが 118
 Mobile Protectionの 105, 111, 115, 119, 126
 Mobile Protectionは 42, 98, 110, 119
 Mobile Protectionは、 31
 Mobile Protectionを 98, 107
 MobileIron Cloud 98, 116
 monitoring 275
 Mozilla Firefox 74
 mpkgインストーラー 75
 msiexec 54

N

N-Central 230
 namespaces 269
 network attack 223
 network containment 223
 network isolation 169, 216, 223
 Network Reputation Service 277
 network traffic 194–196
 new customer company 24, 262
 non-federated domain 8

O

ordering products 24, 262
 Organization Settings 19–20
 Organizational view 216
 outbound connections 169

P

partner 20, 261
 Partner Portal 23–24, 261–262
 password recovery 21
 patch management 245
 Patch Management 245–246, 250
 permissions 12
 Pilot client 261
 pkgbuild 76
 Policy Manager migration 282
 portal customization 263
 PowerShell 266
 Premium subscription 26, 178, 180
 Pro 123
 product deployment 23
 product updates 200
 profile 131, 134–135, 141, 167, 173, 180–181, 250, 266, 279
 profile assignment 37, 131, 133, 135
 profile assignment rules 131
 profile management 141, 189, 198
 profile settings 134, 136
 protected folders 178, 180
 protection status 239
 Protection の 123
 proxy settings 199, 250
 publish profile 134

R

ransomware 157
 ransomware protection 178, 180
 read-only profile 136
 real-time scanning 191, 205
 remote device management 36
 remote request 39
 removable devices 170
 removable storage 170
 remove administrator 20
 remove profile 135
 report export 240
 reports 239
 Reports 239
 reputation analysis 277
 reset password 21
 RMM component 233
 RMM integration 225, 230, 233
 RMM tools 225, 265
 role 12
 role assignment 11

S

Safari 90–91
 Samsung Knox 98, 125
 scan exclusions 204
 scan schedule 192
 scanning exclusions 205
 scheduled reports 239

scheduled scan 173, 192, 205
 scope selector 6, 16, 25, 217, 249, 261
 scp 75
 search criteria 219
 Secure Browsing 91
 security administrator 11, 19
 Security Administrators 20
 Security Center 6, 8–9, 11, 16–17, 19, 22–24, 27–28, 30, 33–37, 39, 43, 50–51, 55, 58, 64, 66–67, 69–71, 74–75, 88, 92–93, 95–98, 102, 106, 123, 131, 133, 135, 140, 152, 172, 174, 186, 189, 191, 194, 216–218, 220, 222, 224–225, 229, 235, 245, 249, 255, 258, 261–263, 265–266, 285–287
 Security Center の 7, 39
 Security Center は 222
 Security Center に 6, 8, 43
 Security Center の 263, 285
 Security Center は 6, 51, 222
 Security Center は、 258
 Security Center を 263
 Security Cloud 191, 199
 Security Cloud は、 191
 security monitoring 216
 security settings 131
 security status 217, 239
 security updates 246
 sensor 45
 Server Protection 50, 187–189
 Server Security 42, 282
 Server Share Protection 187
 service partner account 20
 Signing Identifier 197
 silent activation 110
 software distribution 31
 software installation 32
 Software Updater 245–246, 249–251
 software updates 240, 245–246, 250
 SolarWinds 225
 SolarWinds MSP 230–232
 SolarWinds RMM 230–232
 Solution Provider 16, 23, 261
 status information 265, 269
 status monitoring 231
 status reporting 230
 subscription 23–24, 30, 261–262
 subscription assignment 23, 261
 subscription details 219
 subscription key 23, 25–26, 31, 50, 261
 subscription upgrade 26
 subscriptions 23, 25
 Subscriptions view 25
 support 39, 285
 support link 263
 supported browsers 45
 supported operating systems 45
 system requirements 45

T

Team Identifier 197
 third-party software 245
 troubleshooting 285
 trusted applications 178
 Trusted by WithSecure setting 196

U

unauthorized modifications 207
 uninstallation 190
 unknown connections 169
 update caching 147
 update categories 246
 upgrading options 26
 USB devices 170
 USB storage 170
 User Access Control 280
 user management 11
 user permissions 136, 190
 uuidgen 77

V

VDI 69–70
 vendor 246
 view mode 22
 VMware Horizon 69
 VMware Workspace ONE 98, 101–106
 VMware Workspace ONEを 104
 Vulnerability Management: 17
 Vulnerabilityエージェント 42
 vulnerable application 183

W

web content control 193, 210
 Web content control 277, 279
 web filtering 277
 website blocking 210
 Win32アプリ 67–68
 Windows 230, 233
 Windows Device Manager 172
 Windows Firewall 166
 Windows installation 50
 Windows Management Instrumentation 265, 269
 Windows profile 141
 Windows profiles 141
 Windows registry 275
 Windows updates 251
 Windowsイベントログ 185
 Windowsエンドポイントクライアント 142, 145, 148, 150, 152–153, 158–159, 161, 165
 Windowsシステムイベント 186
 Windowsプロファイル 136, 142–144, 149, 151, 163, 168
 Windows展開 50
 With Secure Mobile Protection 123
 WithSecure 7–8, 16, 18, 23, 43, 72, 222, 261
 WithSecureエレメント付き 6
 WithSecureパートナーポータル 24, 262
 WithSecureパートナーポータルに 24, 262
 WithSecureパートナーポータルへのアクセス 24
 WithSecureモバイル保護 128
 WithSecureモバイル保護の 122
 WMI 265
 WMI classes 269, 275
 WMI integration 265, 269
 WMI interface 265
 WMI properties 266
 WMI Provider 266, 275
 Workspace ONE 42
 WSDIAG file 39

X

XFence 191

Z

zero-touch deployment 110

あ

アーカイブスキャン 152
 アイテム保持 150
 アイデンティティとアクセス管理 17
 アイデンティティプロバイダー 27
 アカountの詳細 21
 アカount連携 27
 アクセス管理 17–18
 アクセス権限 20
 アクティベーショントークン 93
 アクティベーションリマインダー 209
 アクティベーターツール 75–76, 92–93
 アップデイトスキャン 175, 249
 アップデイトを除外する 249
 アプリカタログ 114–115
 アプリケーションの起動 184
 アプリケーションの起動とモジュールの読み込み 184
 アプリケーション制御 184
 アプリケーション制御ルール 184
 アプリのインストール 128
 アプリの権限 112
 アプリの設定 115, 119, 126
 アプリの展開 117, 125
 アプリの有効化 128
 アプリの例外 212
 アプリ課題 126
 アプリ構成ポリシー 111
 アプリ配信 115
 アンインストール 144
 アンインストールコマンド 54
 アンドロイド 105, 112, 128

い

イベントタイプ 184
 イベントの詳細 221
 イベントフィルタリング 222, 242
 インストーラ 50, 181
 インストーラーパッケージ 95
 インストーラーファイル名 93
 インストーラー準備スクリプト 76
 インストーラの開始 184
 インストールタグ 92
 インストールパラメータ 55
 インストールリンク 34, 127
 インターネットトラフィック 209
 インポートプロファイル 135

う

ウェブコンテンツフィルタリング 161
 ウェブコンテンツ管理 163
 ウェブサイトのブロック 163
 ウェブサイトの例外 164, 210
 ウェブトラフィックスキャン 156
 ウェブトラフィック監視 211
 ウェブブラウザ 72

え

エージェント 68, 233
 エージェントのインストール 74
 エージェントバージョン 139
 エージェントパッケージ 229
 エージェント手順 226–229
 エージェント通知 90
 エクスポージャー管理 217
 エクスポージャー管理の 217
 エクスポートプロファイル 134
 エグゼクティブサマリー 255–256
 エレメンツサービス 40
 エレメンツセキュリティセンター 7–8, 30, 43, 177, 189, 208, 224, 239, 258, 285–286
 エLEMENTアカウント 29
 エLEMENTエージェント 50, 58, 63–64, 70, 95, 127, 144, 258
 エLEMENTコネクタ 143, 145–146, 199, 201, 251
 エンドポイント暗号化 186
 エンドポイント構成 133
 エンドポイント保護 6, 30
 エンドポイント保護クライアント 151
 エンドポイント保護は 42

お

オフラインインストール 54
 オフラインデバイス 33, 37
 オンラインバンキングの保護 165

か

が 180
 カスタマイズされたインストーラー 58
 カスタムウィジェット 256
 カスタムサービス 231–232
 カスタムパッケージ 75–76
 カスタムビュー 241–242
 カスタムプロファイル 286
 カスタムラベル 34
 カセヤエージェント 229

く

クイックスタート 7
 クライアントアップグレード 286
 クライアントステータス 228
 クライアントセキュリティ for Mac 282
 クライアントソフトウェアへのアクセス 139, 142, 200
 クライアントのインストール 132
 クライアント設定 131
 クラウド分析 153
 グループポリシー 60, 74
 クローンプロファイル 208

こ

コマンドプロンプト 54, 69
 コマンドラインインストール 132
 コマンドラインインターフェース 88
 コマンドラインパラメータ 51
 コミュニケーション設定 145–146
 コンテンツカテゴリ 163
 コンテンツタイプのフィルタリング 164
 コンテンツフィルタリング 83

コンテンツ制限 90
 コンピュータ 282
 コンピュータ用WithSecure Elements Agent 230
 コンピュータ用ELEMENTエージェント 282
 コンプライアンス状況 220

さ

サーバー展開 70
 サイバーセキュリティ 254
 サイレントアクティベーション 112
 サイレントアップグレード 190
 サイレントアンインストール 54
 サブスクリプション 7, 33, 282
 サブスクリプションキー 51, 54–55, 58, 75–76, 88, 92–93, 101, 115, 117–118, 285–287
 サブスクリプションシート 224
 サブスクリプションの有効化 92
 サポート終了 140
 サポート対象外のクライアント 286
 サムスン・ノックス 125–126

し

システムイベント検出 185–186
 システム拡張 87, 89
 システム拡張機能 85–86
 システム設定 87, 89
 ジャムフ 86–88
 シングルサインオン 8, 27–28, 30

す

スキャン結果 248–249
 スキャン周波数 158
 スキャン除外 148–149, 155, 159, 177, 192, 286
 スキャン設定 148, 152
 スクリーンタイム 90
 スクリプトスキャン 153
 スケジュールされたスキャン 158, 172, 175, 213
 スケジュールされたタスク 174
 スコープセクター 19, 23, 35, 217, 256, 261
 スコープセクターが 25, 32, 36, 127, 219, 249
 スコープセクターで 32, 127
 スコープセクターを 6, 25, 217, 240
 ステータス監視 232, 236
 ステータス報告 231
 スマートグループ 88
 スマートフォンまたはその他のデバイス 9

せ

セーフサーチ 161
 セキュリティ センター 133
 セキュリティアップデート 174
 セキュリティイベント 185–187, 211, 221–222, 241–242, 254
 セキュリティイベントページ 222
 セキュリティセンター 50, 101, 282
 セキュリティに関する推奨事項 220
 セキュリティの役割 17
 セキュリティプロファイル 286
 セキュリティポリシー 133
 セキュリティレポート 241, 254–256
 セキュリティ以外のアップデート 249
 セキュリティ以外の更新プログラム 250

セキュリティ意識向上アシスタント 254
 セキュリティ関連 246
 セキュリティ機能 144, 202
 センサー統合 143, 201

そ

ソフトウェアアップデート 146, 174–176, 247–249, 251
 ソフトウェアアップデートは 245
 ソフトウェアのインストール 50, 229, 235
 ソフトウェアを再初期化する 287
 ソフトウェア署名 95
 ソフトウェア展開 60
 ソフトウェア配布 75

た

ダウンロードブロック 164

て

ディスク暗号化 143, 186
 データガード 177, 179
 データ復旧 40
 テーブルデータのインポート 137
 テーブルデータのエクスポート 137
 テーブルデータを置換する 138
 テーブルの列 38
 デバイス 133, 189
 デバイスアクセスルール 171
 デバイスグループ 88
 デバイスグループ分け 34–35
 デバイススキャン 222
 デバイスターゲット 115
 デバイスのセキュリティ 83
 デバイスのセキュリティ態勢 220
 デバイスの種類 222
 デバイスの生体認証 9
 デバイスの展開 127
 デバイスビュー 38
 デバイスフィルター 38
 デバイスページ 36
 デバイスマスク 171
 デバイスラベル 34–35
 デバイスリスト 35
 デバイスを取り外す 224
 デバイスを追加する 36, 43
 デバイス割り当て 36
 デバイス管理 33–35, 37–38, 224
 デバイス検出 222
 デバイス除外 171
 デバイス招待状 34
 デバイス制御 170–171
 デバイス制御の 170
 デバイス生体認証 11
 デバイス登録 106, 114
 デフォルトプロファイル 71, 92
 デプロイメント 66, 68

と

トップ 9
 ドメインフェデレーション 28
 ドライブ暗号化 186–187

に

に 7
 に等しい 181
 に等しくない 181

ね

ネットワークインストーラー 69
 ネットワークゲートウェイ 42, 209, 212
 ネットワークコンテンツフィルタリング 90
 ネットワークドライブ 153
 ネットワークルール 176
 ネットワーク拠点 176
 ネットワーク保護 209

は

は 178, 254
 は、 254
 バージョン固定 140
 パートナー 18, 256, 286
 パートナー ポータル 24, 262
 パートナーポータル 285–286
 はじめる 7
 バックアップ 40
 パッチ管理 6
 パフォーマンス設定 158

ひ

ビジネスアカウント 8, 43
 ビットロッカー 186–187

ふ

ファイアウォール 176
 ファイアウォールプロファイル 168
 ファイアウォールルール 286
 ファイアウォールルールアラート 168
 ファイル アクセス 184
 ファイルスキャン 153, 202, 212
 ファイルチェックサム 149
 ファイルの種類 164
 ファイルハッシュ 184
 ファイルボルト 187
 ファイル監視 152
 ファイル復元 177
 ファイル保持 193
 フェデレーション型シングルサインオン 27–28
 フォルダー除外 188
 プライバシーとセキュリティ 89
 ブラウザ拡張機能 72, 100
 ブラウザ保護拡張機能 73
 ブラウジング保護 72
 ブラウジング保護プラグイン 209
 ブラウジング保護拡張機能 72, 74
 フルディスクアクセス 85, 89
 プレミアム会員 185, 187
 プロキシ 199
 プロキシサーバー 145
 プロキシ設定 145, 251
 プログラム、「重大なセキュリティ更新プログラム 250
 ブロックされたウェブサイト 210
 ブロックされたドメイン 164
 ブロックされたページ 161

ブロックリスト 286
プロファイルテーブル 137
プロファイルのインポート 133
プロファイル割り当て 71, 132–133
プロファイル割り当てルール 35
プロファイル管理 133, 208
プロファイル設定をコピーする 136
プロファイル比較 136
プロフィール 43, 105, 131, 133–138, 186, 191, 208, 249, 251
プロフィールイベント 242
プロフィールエディター 172, 174–175
プロフィールを作成する 208
プロフィールを編集 21
プロフィール設定 220

へ

ペアレント 181
ペイロード識別子 77

ほ

ポータル言語 285
ポリシーマネージャー 135, 282

ま

マック 234, 282
マルウェアスキャン 158, 175, 202, 213
マルウェア検出 148, 152
マルウェア対策 212–213
マルウェア対策スキャンインターフェース 153

め

メールエイリアス 27
メールとサーバーのセキュリティ 285
メールレポート 241
メール招待状 34, 98, 127
メール設定 285

も

モジュールの読み込み 184
モバイルデバイスプロファイル 208
モバイルプロフィール 209–210, 212–213
モバイル展開 98
モバイル保護 98, 100, 106–107, 113, 123, 125

ゆ

ユーザーブロック 188
ユーザー権限 142
ユーザー除外 189
ユーザー名 21

よ

より大きい 181

ら

ライセンス有効期限通知 144
ラベル割り当て 35
ランサムウェア 188
ランサムウェア検出 187
ランサムウェア対策 177, 187

り

リアルタイムスキャン 152–153, 155–156, 202
リスクレベル 221
リムーバブルメディア 148
リモートインストール 229
リモート管理 189
リリースグループ 93, 139–140, 142, 200

る

ルミネン 254–255

れ

レポート 241, 256

ろ

ローカル除外リスト 177
ログアウトツール 70
ログイン 8
ログインセキュリティ 9
ログイン認証情報 8

を

を含む 181