WithSecure Elements Identity Security for Entra ID

2026-10-30

目次

第 章1: Entra ID のWithSecure Elements アイデンティティ セキュリティ、概要 4

1.1 製品を使用するには 6
1.2 WithSecure Elementsの検出と対応機能の使用 7
1.3 導入されたインフラストラクチャの概要 8
1.4 IDセキュリティとクラウドセキュリティの仕組み 11
1.5 前提条件 11

第 章2: オンボーディング構成 12

2.1 Azureテナントを追加する 13
2.2 Connect Identity Inventory 13
2.3 セキュリティ機能を追加する 14
2.4 Azure環境を準備する 15
2.5 リソースをデプロイする 16
2.6 導入後の検証 17
2.7 AzureをElements Cloudに接続する 19
2.8 検出機能が正常に動作することを確認してください。 19
2.9 オンボーディングを完了する 20
2.10 メールレポートの設定 20
2.11 セキュリティイベント用のカスタムビューを作成する 21

第 章3: 継続的な管理 22

3.1 スクリプトを再実行するタイミング 23
3.2 新しいテナントが作成されたとき 23
3.3 イベントハブの容量を確認する 23
3.4 スクリプトの定期的なリリース 24
3.5 検出モジュールの概要 24
3.6 更新通知の受信者 24

付録 A: デプロイされたリソースをオフボードする 26

付録 B: トラブルシューティング 29

B.1 接続状態を確認してください 30

付録 C: WithSecure Elementsソリューションの紹介 31

C.1 WithSecure Elementsセキュリティセンターを使用する.....32
Glossary.....66
索引.....71

第 章1

Entra ID のWithSecure Elements アイデンティティセキュリティ、概要

トピック :

- WithSecure Elements IDセキュリティを始めましょう
- WithSecure Elementsの検出と対応機能の使用
- 導入されたインフラストラクチャの概要
- IDセキュリティとクラウドセキュリティの仕組み
- 前提条件

Entra ID のWithSecure Elements アイデンティティ セキュリティ、概要

WithSecure MicrosoftテナントからEntra ID ログを取得できるようにするための設定が必要です。

WithSecure Elements Identity Security for Entra ID Microsoft クラウド エコシステム内のユーザー、サービス、リソースの ID およびアクセス管理に Entra ID を使用する組織向けに設計された基本モジュールです。

WithSecure Identity Security for Entra ID脅威アクターによる初期アクセスを示唆する可能性のある異常なサインインアクティビティを検出することで、EntraIDユーザーを保護するように設計されています。これらの検出は、以下のような様々なリスク要因に基づいています。

- 新しいデバイス、IP アドレス、国、都市からのサインイン
- サインイン間の時間と距離 (不可能な移動を検出するため)
- 疑わしいアプリケーションやメールクライアントへのアクセス

これらのシグナルを用いてリスクを評価し、「危険なサインイン」と呼ばれる単一の検出を生成します。リスクのレベルは、観測された異常の組み合わせによって異なります。当社の調査によると、堅牢な検出には、通常とは異なるサインイン行動とあり得ない移動の両方を含める必要があります。ルールがトリガーされるには、両方の条件が満たされている必要があります。

検出された異常の詳細を理解するには、Elements 内の検出タイトルをクリックして [**検出コンテキスト**]を確認してください。

誤検知やノイズを減らすため、個人ユーザーと組織の両方についてサインイン行動をプロファイリングします。これにより、VPNの使用など、想定されるアクティビティを考慮に入れます。また、エンドポイント検出と同様のロジックを適用します。つまり、繰り返し同じ検出が発生する場合は、想定される行動を示しているため、システムはそれを抑制します。

サインイン時の異常だけでなく、権限昇格や防御回避など、潜在的な攻撃者の行動を可視化するのに役立つその他の攻撃手法も検出します。これにより、Elementsユーザーは、侵害された可能性のあるID全体にわたる不審なアクティビティを評価できます。

同じ時間枠内で同一の人物 (または主体) に関連するすべての検出結果は、行動相関検出 *(BCD)* としてグループ化され、事件の包括的な状況把握が可能になります。

事例例 :

重篤 / 重症 このアクティビティは攻撃の一部である可能性が非常に高いです。



注 : 現在、重大な検出機能は稼働していません。

ロシアや中国などの高リスク国からの不審なログインに対して、重大な警告を発する機能強化を計画しています。

高 このアクティビティは攻撃の一部である可能性があります。

例としては以下のようなものがあります。

- 3 つ以上のリスク要因がある疑わしいサインイン
- 不審なメールクライアントへのサインインとあり得ない移動の組み合わせ
- 定義された閾値を超えるブルートフォース攻撃
- Azure での診断設定の削除
- 偽の第一当事者プリンシパルの作成

中 これは攻撃の一部である可能性のある疑わしいアクティビティです。

- ブルートフォース攻撃（高リスク閾値未満）
- レガシープロトコルを使用したデバイスコードログイン
- 条件付きアクセスポリシーの無効化

低 このアクティビティは攻撃を示すものではないかもしれませんが、調査には役立つ可能性があります。

- ROPC（リソース所有者パスワード資格情報）サインイン
- プリンシパルへの役割の割り当て
- ユーザーの同意設定が緩和される

情報 このアクティビティは必ずしも疑わしいものではありませんが、役立つコンテキストを提供する可能性があります。

- 新しい認証フローの有効化
- 不審なサインイン試行の失敗



注：

*Microsoft Entra ID P1*または*P2*ライセンスをお持ちのお客様の場合、リスクの高いサインインレポートをEntra IDから直接取り込みます。これらのレポートは大量に届くことがあり、異常な特徴や複数の異常一致（IPアドレス、ホスト、時間など）に基づく検出結果が含まれていることがよくあります。従来、このようなシグナルはノイズが多く、具体的なリスクを示すものではない場合がありました。

明確さを確保し、アラート疲労を軽減するには:

- 明確な主要リスクが示されていない報告は、自動的に却下します。
- 当社のシステムは、独自のモデリングに基づいた追加のフィルタリングを適用することで、マイクロソフトから受信するテレメトリデータに含まれるノイズを低減します。
- 重要な点として、当社が取り込むリスクイベントは[、**EntraIDのリスクイベントブレード**]に表示される内容と必ずしも完全に一致するとは限りません。これは、Microsoftが生のテレメトリデータとUIに表示される内容の間に独自のノイズ抑制メカニズムを適用しているためです。

1.1 WithSecure Elements IDセキュリティを始めましょう

Azureテナントをオンボーディングすることで、WithSecure Elements IDセキュリティの利用を開始できます。

WithSecure™にアクセスするには、WithSecure™ビジネスアカウントが必要です。Elements Security Centerこれは、すべてのWithSecure™ Elements製品を管理するための統合管理プラットフォームです。シナリオは2つあります。

- 製品を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一時パスワードとログインするためのリンク Elements Security Center。
- 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。

Elementsのエンドポイント検出および応答も設定する必要があります。

このクイックスタートガイドでは、Azureテナントをオンボーディングすることで、WithSecure Elements Identity Securityの利用を開始する手順を説明します。

1. ログイン Elements Security Centerそして、Azureテナントのオンボーディングを開始します。
   a) ログイン Elements Security Center Elements Endpoint Detection and Responseで使用している既存の認証情報を使用します。
   b) Elements XDR Cloud Security for Azure のサブスクリプションがあることを確認したら、次の場所へ移動してください。**環境** > **クラウド**テナントを追加するには、**[Microsoft テナントと Azure サブスクリプションを]**使用します。
2. デプロイされたインフラストラクチャと前提条件を確認します。
   詳細については、「前提条件」を参照してください。
3. Azure テナントを追加する Elements Security Centerオンボーディングを開始する。
   詳細については、「オンボーディング構成」を参照してください。
4. オンボーディング スクリプトを実行するために必要なアクセス許可があることを確認して、Azure 環境を準備します。
   詳細については、「Azure 環境の準備」を参照してください。
5. リソースを展開します。
   詳細については、「リソースのデプロイ」を参照してください。
6. デプロイ後の検証手順を完了します。
   詳細については、「展開後の検証」を参照してください。
7. 戻る Elements Security CenterElements Security CloudをAzureテナントに接続するための接続文字列を追加します。
   Elements Cloud は現在、*Azure* テナントからデータを受信しています。
8. 検出が機能しているかテストします。
   詳細については、「検出機能が動作することを確認する」を参照してください。
9. オンボーディング セッションを終了します。
   詳細については、「オンボーディングの終了」を参照してください。

問題が発生した場合は トラブルシューティングを参照してください。それでも問題が解決しない場合は、カスタマーケアに問い合わせてください。



注 : Cloud Broad Context Detections (BCD) を表示するために必要な追加ロールはありません。

1.2 WithSecure Elementsの検出と対応機能の使用

WithSecure Elements Identity SecurityでWithSecure ElementsのWithSecureおよび応答機能を使用するには、エンドポイントにエンドポイントセンサーをデプロイしてください。

Elements Identity Security効果的に使用するには、エンドポイントに Elements Detection and Response導入する必要があります。

エンドポイントセンサーは軽量で目立たず、管理対象組織内のすべての関連コンピュータに展開されます。センサーはエンドポイントデバイスから動作データを収集し、攻撃に耐性があります。WithSecure

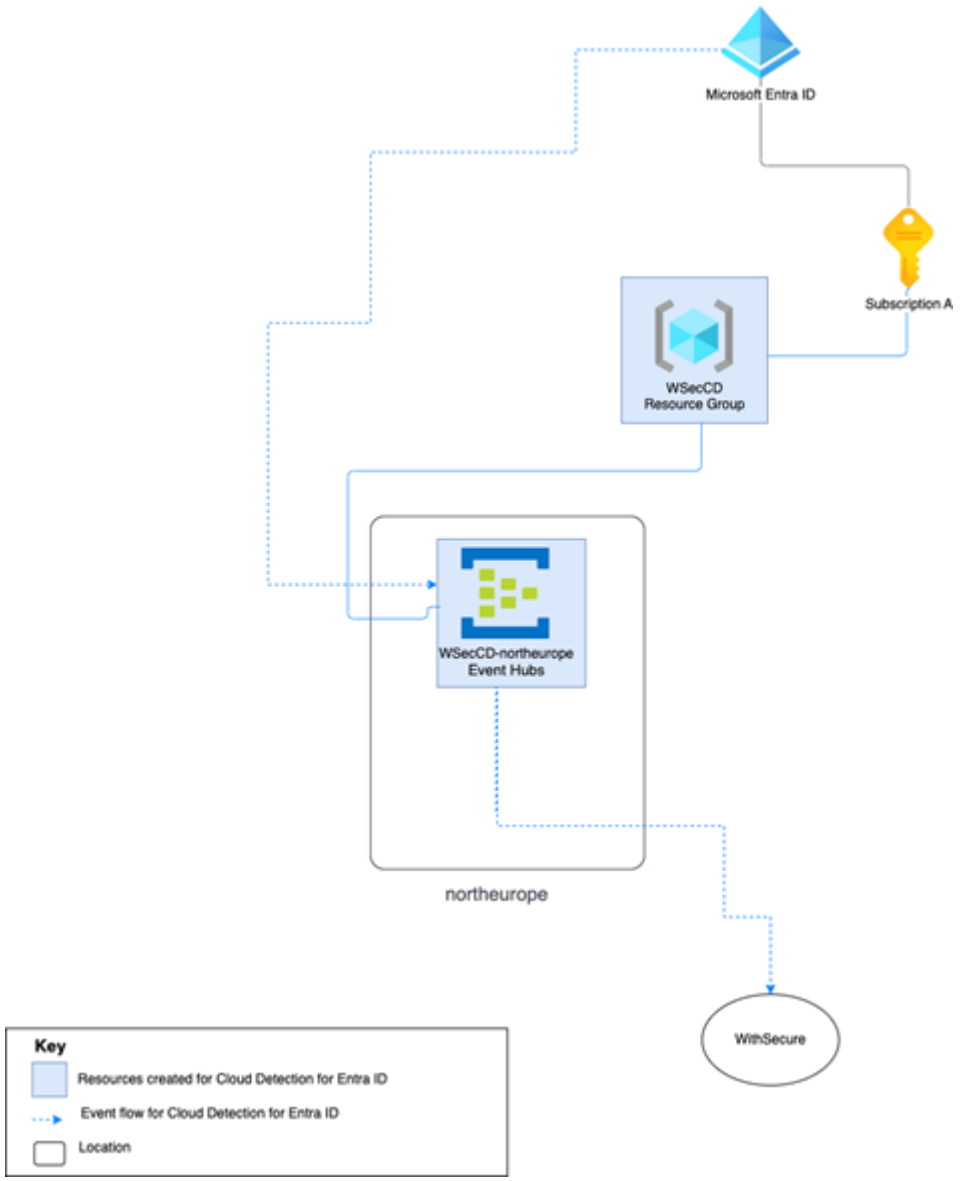
Elements Endpoint Detection and WithSecureをセットアップするには、エンドポイントセンサーのインストールパッケージが必要です。このパッケージには、バイナリインストーラファイルとWithSecure Elements Endpoint Detection and Response のアクティベーションコードが含まれています。

インストールパッケージを配布し、コンピュータにソフトウェアをインストールすると、WithSecure Elements Security Centerは、管理対象ホストごとに検出結果と統計情報を表示します。

1.3 導入されたインフラストラクチャの概要

Infrastructure as Code (IaC) テンプレートを使用して、環境に展開できます。テンプレートは、必要なすべてのインフラストラクチャ要素をコード化された形式で定義し、一貫した展開を保証します。

この図は、オンボーディングプロセス中に使用される WithSecure Entra ID構成スクリプトの効果を示しています。



このプロセスでは、次のインフラストラクチャが作成、構成、および展開されます。

- ターゲットテナントにリソースグループが作成され、その中にはWithSecure Entra ID 構成スクリプトによってデプロイされたすべてのリソース (イベントハブ、アラート、アクショングループ) が含まれます。これらはまとめて次の目的で使用されます。WithSecureログデータ収集。

- Standardレベルのイベントハブがデプロイされています。イベントハブはテレメトリイベントを24時間保持するように構成されています。監視対象リソースの数とそのアクティビティは、イベントハブの負荷に影響を与えます。
- イベント ハブが最大容量に達した場合に、イベント ハブが負荷を処理できないことを通知する電子メール アラート。この場合、一部のテレメトリ データが失われる可能性があるため、問題を可視化するためにアラートが展開されます。



注 : TU 数が増加するとアラートがトリガーされます。

- すべての Entra ID ログをイベント ハブに転送する診断設定が生成されます。これらは次のとおりです。
  - 監査ログ
  - サインインログ
  - 非対話型ユーザーのサインインログ
  - サービス プリンシパル サインイン ログ
  - マネージド ID サインイン ログ
  - プロビジョニングログ
  - ADFS サインイン ログ
  - 危険なユーザー
  - ユーザーリスクイベント
  - ネットワーク アクセス トラフィック ログ
  - 危険なサービスプリンシパル
  - サービスプリンシパルリスクイベント
  - 強化されたOffice365監査ログ
  - Microsoft Graph アクティビティ ログ



注 : 管理対象組織が P1/P2 ライセンス (Microsoft 365 E3/E5 プランに含まれています) を保有している場合、本ソリューションは Microsoft が生成するリスク レポートを収集し、独自の検出ロジックと組み合わせます。また、本ソリューションは条件付きアクセスを無効にするための検出機能も提供します。条件付きアクセスは、Azure Active Directory Premium P1 または P2 ライセンス (それぞれ E3 プランと E5 プランに含まれています) 専用の機能です。

次の表は、EntraID モジュールの一部として収集される主要なログ ソースの使用について説明しています。

表1:ログカテゴリ

ログカテゴリ	説明
監査ログ	アプリケーション、ユーザー、テナント構成の変更を監視するために必要です。たとえば、アプリケーション登録のアクセス許可の変更や、新しい条件付きアクセスポリシーの作成/変更などです。
サインインログ	テナントの認証および承認イベントが含まれます。たとえば、サインインイベントや、ユーザー ログインに関連付けられたメタデータなどです。
非対話型ユーザーのサインインログ	人間による操作がないシステム アクティビティに関する情報が含まれます。サービス アカウントは攻撃者の標的となる可能性があります。

ログカテゴリ	説明
サービス プリンシパル サインイン ログ	攻撃者がMicrosoft プリンシパルを悪用して目的を達成できるサービス プリンシパル アクティビティに関する情報が含まれています。
マネージド ID サインイン ログ	マネージド ID を使用するアプリケーション、サービス、またはシステムの相互作用に関する情報が含まれます。マネージド ID を監視すると、攻撃者による承認済みアクセスを検出できます。
危険なユーザー ユーザーリスクイベント	M365 Defenderによって危険と判断された「危険なユーザー」および関連イベントに関する情報を提供します。例えば、不審なログオンや、不正な形式または不審なトークンの提供などが挙げられます。
リスクのあるサービスプリンシパル サービスプリンシパルリスクイベント	M365 Defenderによって危険と判断された「危険なサービスプリンシパル」および関連イベントに関する情報を提供します。

設定が完了したら、データは収集および分析できます。WithSecure検出範囲を確保するため。

複数のテナントがいる場合は、各テナントごとにこのガイドに記載されている手順に従ってください。WithSecure各テナントのイベントハブごとに接続文字列が必要です。例えば、3つのテナントに対してそれぞれ固有の接続文字列を用意する必要があります。



注 : このドキュメントでは、コンテンツの重複を避けるために、多くの箇所で Azure ドキュメントを参照しています。

関連するMicrosoftコスト

デプロイされたイベントハブ構成では、標準ティアのイベントハブを使用しており、リージョンごとに1つのイベントハブをプロビジョニングし、イベントの保持期間を24時間に設定することで最適化されています。

イベントハブの料金は、スループットユニット (TU) あたり月額約22ユーロです。必要なTU数は、受信イベントの量によって異なります。システムはイベント負荷に応じて最大40TUまで拡張可能です。TU料金に加えて、受信イベント100万件あたり0.026ユーロのデータ入力料金が発生します。

シナリオ例:

- 中規模顧客は通常、月間約1億件のイベントを生成し、一般的に1TU以下しか必要としません。月額費用は約25ユーロと見積もられています。
- 大規模顧客の場合、月間約3億件のイベントが発生することがありますが、これは通常1TUの容量内に収まります。この場合の月額費用はおよそ30ユーロと見積もられます。

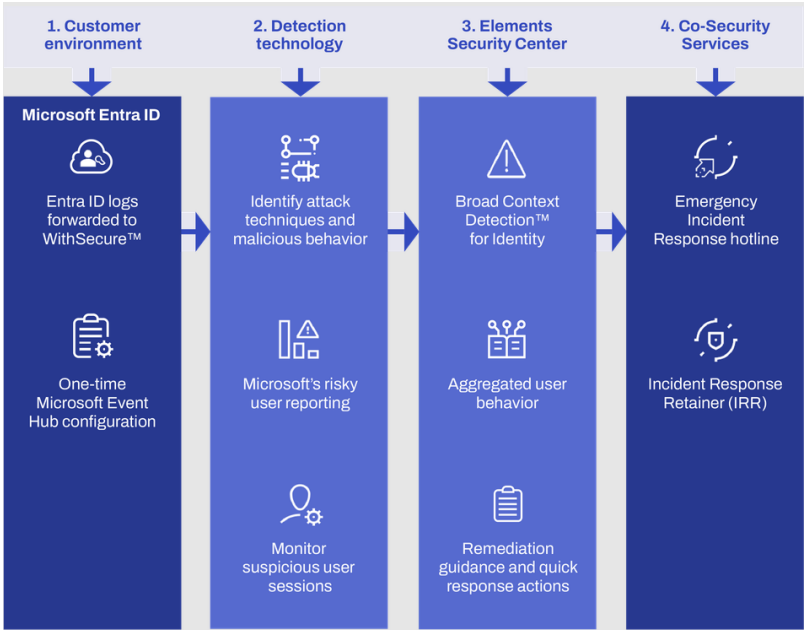


注 : 外部からの分散型サービス拒否 (DDoS) 攻撃が発生すると、イベントの総数は2億件増加し、1秒あたりのイベント数は10倍に増加する可能性があります。その場合、月額費用は約250ユーロにまで上昇する可能性があります。

予期せぬコストを削減するために、Azureのコストおよび請求に関するアラートを設定することをお勧めします。これらのアラートは、そのような事態が発生した後にTU (トランザクションユニット) を迅速に縮小するのに役立ちます。

1.4 IDセキュリティとクラウドセキュリティの仕組み

WithSecure Elements Identity Security for Entra IDおよび ログを送信します。WithSecureこのサービスは、不審な行動や潜在的な脅威を検出します。WithSecure Elements Security CenterはWithSecureユーザーの行動を分析し、対策を提案します。



オンボーディング中に、Microsoft Event Hub のワンタイム構成により、Microsoft Entra ID ログが次の場所に送信されます。WithSecure。WithSecureログを利用して攻撃手法を特定し、悪意のある動作を検出し、侵害された可能性のあるアカウントにフラグを立てます。また、不審なユーザーセッションを監視して異常なアクティビティを検出します。

WithSecure Elements Identity Security and Cloud Securityは、ユーザーの行動を組み合わせてIDとクラウドの脅威を評価します。これらの脅威は 「広範なコンテキスト検出」として報告され、修復ガイダンスと対応策も提供されます。

インシデント対応リテーナーは、セキュリティインシデントへの備えと対応を支援します。緊急インシデント対応ホットラインは、インシデント発生時に迅速なサポートを提供します。

1.5 前提条件

構成を開始する前に、次の前提条件を満たしている必要があります。

- 組織は WithSecure Elements Endpoint Protectionおよび WithSecure Elements Endpoint Detection and Responseのサブスクリプションを保有している必要があります。オンボーディング時には WithSecure Elements Endpoint Protection管理者ロールが必要です。
- Azure Cloud Shellでスクリプトを実行するには、Azure アカウントにグローバル管理者としてサインインできる必要があります。
- デプロイを開始する前に、テナント ID、サブスクリプション ID、およびデプロイ場所を把握して準備しておく必要があります。手順については、「Azure Portal でサブスクリプションとテナント ID を取得する」を参照してください。
- サブスクリプションは、Azure Management Groupに割り当てる必要があります。Azure Azure Management Groupを設定するには、「管理グループの作成」を参照してください。

第 章2
オンボーディング構成

トピック :

- Azureテナントを追加する
- Connect Identity Inventory
- Azureテナントにセキュリティ機能を追加する
- Azure環境を準備する
- リソースをデプロイする
- 導入後の検証
- AzureをElements Cloudに接続する
- 検出機能が正常に動作することを確認してください。
- オンボーディングを完了する
- メールレポートの設定
- セキュリティイベント用のカスタムビューを作成する

オンボーディング構成

WithSecure Azureログデータの収集を開始できるように、クラウド環境をオンボーディングする手順は以下のとおりです。

Identity Securityで Azureログデータの収集を開始するには、クラウド環境をオンボーディングする必要があります。オンボーディングには、以下のタスクが含まれます。

- クラウドサブスクリプションを追加してください。
- 環境を準備します。
- 必要なリソースをデプロイします。
- デプロイメントを確認してください。
- 要素に接続します。
- メール通知を設定する。

WithSecure XDR 用の Entra ID レスポンス アクションのオンボーディング手順については、Entra ID レスポンス アクションのオンボーディング ビデオをご覧ください。

2.1 Azureテナントを追加する

WithSecure Elementsセキュリティセンターに新しいAzureテナントを追加します。

新しい Azure テナントを追加するには:

1. WithSecure Elements セキュリティ センターで、**[環境]** > **[クラウド]** > **[Microsoft テナントと Azure サブスクリプション]**に移動します。
2. [**Azure テナントの追加を**]選択します。
3. **テナント情報**ページで、以下の詳細を入力し、[**次へ**]を選択してください。
   - [**表示名**]: WithSecure Elements セキュリティ センターに表示される新しい Azure テナントの名前を入力します。
   - [**テナントID**]： Azureポータルからテナント IDを貼り付けてください。
   - [**組織**]：テナントに対して WithSecure Elements Security Center組織を選択します。
4. 次のページで、以下を入力して [**次へ**]を選択してください。
   - [**重要度**]：クラウドアカウントの重要度を設定します。重要度はリスク評価に使用されます。
   - [**ビジネスコンテキスト**]：テナントのビジネスコンテキストを提供します。

   テナントが追加され、*Connect Identity Inventory*の機能ページが開きます。

> 👉 **重要 :** 他の機能を追加する前に、必ずIDインベントリを設定する必要があります。「IDインベントリの接続」を参照してください。

2.2 Connect Identity Inventory

Azureテナントの IDインベントリを接続します。

> 👉 **注 :** テナントの作成方法については、以下を参照してください。Azureテナントを追加するページ13。

> 👉 **重要:** テナントに他の機能を追加する前に、必ずIDインベントリを設定する必要があります。

Identity Inventoryを接続するには：

1. [**セキュリティ機能**]で、[**IDインベントリ**]を選択します。
2. [**今すぐ接続**]を選択してください。
3. はじめにおよび手順を読み、確認用のチェックボックスを選択してから、[**開始**]を選択してください。
4. IDインベントリ機能に必要な権限を付与してください。
   - Azureテナント管理者である場合は、[**アクセス許可の承認**]を選択し、必要なアクセス許可を承認してください。
   - 権限を付与できない場合は、[**URLをコピー**]を選択してURLをコピーし、Azure管理者に送信してください。

Identity Inventoryは接続されており、必要な権限が付与されています。

2.3 Azureテナントにセキュリティ機能を追加する

WithSecure Elements セキュリティ センターで、Azure テナントにセキュリティ機能を追加します。

セキュリティ機能を追加する前に、Azure テナントを追加してください。Azure テナントの追加を参照してください。



重要： IDインベントリは必須です。他の機能を追加する前に、必ず接続してください。「IDインベントリの接続」を参照してください。

テナントを追加してIdentity Inventoryに接続したら、テナントにセキュリティ機能を追加します。

1. **[セキュリティ機能]**で、[**ID セキュリティ**][]選択します。
2. [**追加**] を選択します。
3. **接続詳細**ページに次の情報を入力します。
   - [**デプロイ サブスクリプション ID**]: 新しいリソースが作成される Azure portalからのサブスクリプション ID を貼り付けます。まだサブスクリプションを使用していない場合は、新しいサブスクリプションを作成することをお勧めします。手順については、「EAサブスクリプションの作成」を参照して、Enterprise Agreement サブスクリプションを作成してください。
   - [**デプロイ場所**]:新しいリソースが作成されるリージョンを選択します。既に使用している場所を選択することをお勧めします。
   - [**通知用の電子メール アドレス**]: イベント ハブの容量に達した場合に Microsoft が通知を送信するアドレスを入力します。

     注： メールアドレスを入力したら、`Enter` キーを押して保存します。

4. オンボーディングの `WithSecure Elements XDR Identity Security for Entra ID.zip`ファイルをダウンロードします。

セキュリティ機能が追加され、オンボーディングパッケージがダウンロードされます。

次に、Azureでインフラストラクチャを構成します。

2.4 Azure環境を準備する

構成スクリプトが必要とする、管理者権限とオンボーディングファイルを使用して、Azureテナントを準備します。

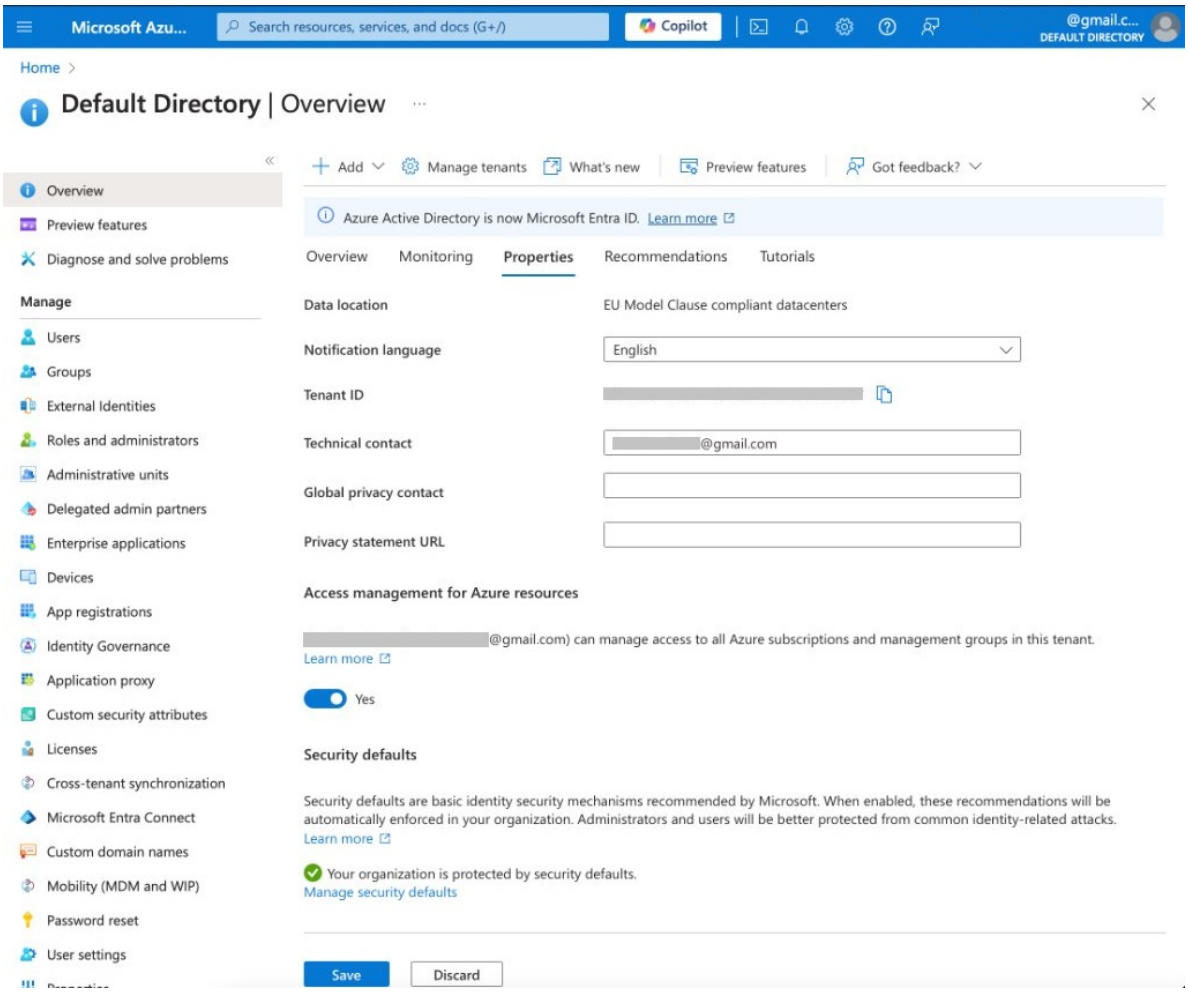
開始する前に、Azure の [**アクセス権限昇格**]機能を使用できる役割 (通常は Microsoft Entra ID のグローバル管理者役割) でサインインしていること、およびこの統合のためのオンボーディング パッケージを既にダウンロードしていることを確認してください。

これにより、後の手順でWithSecure Identity Security構成スクリプトを実行する前に、Azureテナントに必要な昇格されたアクセス許可とオンボーディングファイルが準備されます。

1. Azure Portal で、テナントを管理するために一時的にアクセス権を昇格します。

   すべてのサブスクリプションを管理するためのアクセス権を一時的に昇格させるには、次のページに記載されている手順に従ってください。すべての Azure サブスクリプションと管理グループを管理するためのアクセス権の昇格 | Microsoft Learn。

2. サインアウト。
3. 再度ログインして、より高いアクセス権限でアクセスを更新してください。
4. [**Azure リソースのアクセス管理**]オプションを [**はい**]に切り替えます。



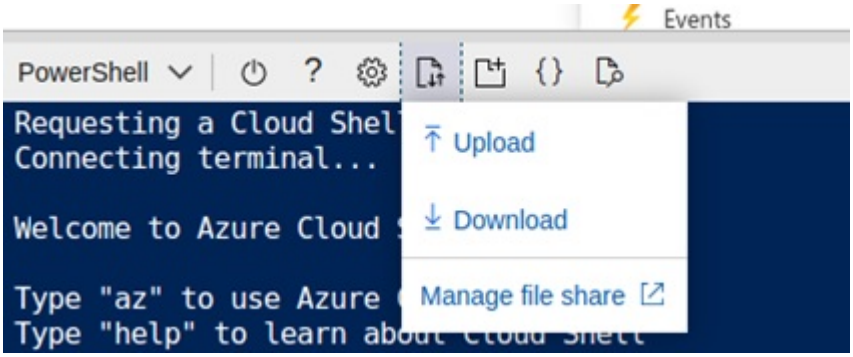
> 👉 **注 :** これにより 、Microsoft Defender for Cloud の警告が表示される可能性があります。

5. サインアウト。
6. 変更を有効にするには、再度ログインしてください。

7. PowerShellを使用して Azure Cloud Shellを開きます。

> **注：** Azure Cloud Shell では、ローカル ファイルを保存するためのストレージ アカウント インスタンスが必要です。インスタンスを作成する必要がありますが、これは通常、テナントで Azure Cloud Shell が以前に使用されたことがない場合に発生します。次のリンクでは、クラウド シェル用のストレージ アカウント インスタンスを作成する方法について説明しています: Cloud Shell の起動
>
> Microsoft からAzure Cloud Shellリソース プロバイダーへのサブスクリプションの登録を求められた場合は、次のリンクの手順に従ってください: Azure Cloud Shell へのサブスクリプションの登録

8. 先ほどダウンロードしたオンボーディング用のzipファイルを、Azure Cloud Shellの画面上部にあるアップロード機能を使ってアップロードしてください。ファイルは現在の作業ディレクトリにアップロードされます。



9. パッケージに対して `unzip`コマンドを使用してパッケージを解凍します。

```
unzip './WithSecure Elements XDR Identity Security for Entra ID.zip'
```

これにより、すべてのファイルが新しい *`withsecure`*フォルダーに解凍されます。

10. 解凍されたファイルがあるフォルダにディレクトリを変更します。

```
cd withsecure
```

11. Azure Cloud Shellで次のコマンドを実行して 、WithSecure Entra ID 構成スクリプトをデプロイする必要のあるプリンシパルに *Owner*割り当て、*[userId]*を [**(Azure から取得した) ユーザープリンシパル名**]に更新します。

```
New-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```

Azure環境はオンボーディングの準備が整っています。

2.5 リソースをデプロイする

環境の準備が完了したら、WithSecure configuration scriptを展開する準備が整います。

WithSecure構成スクリプトは、関連するEntra ID ログをEvent Hubに転送するために必要なリソースをデプロイします。WithSecure検出を実行するためのデータを収集できます。

次のコマンドを実行してリソースをデプロイします。

```
./deploy.ps1
```

リソースはAzure環境にデプロイされます。

2.6 導入後の検証

デプロイメントが期待どおりに機能することを確認するための検証方法。

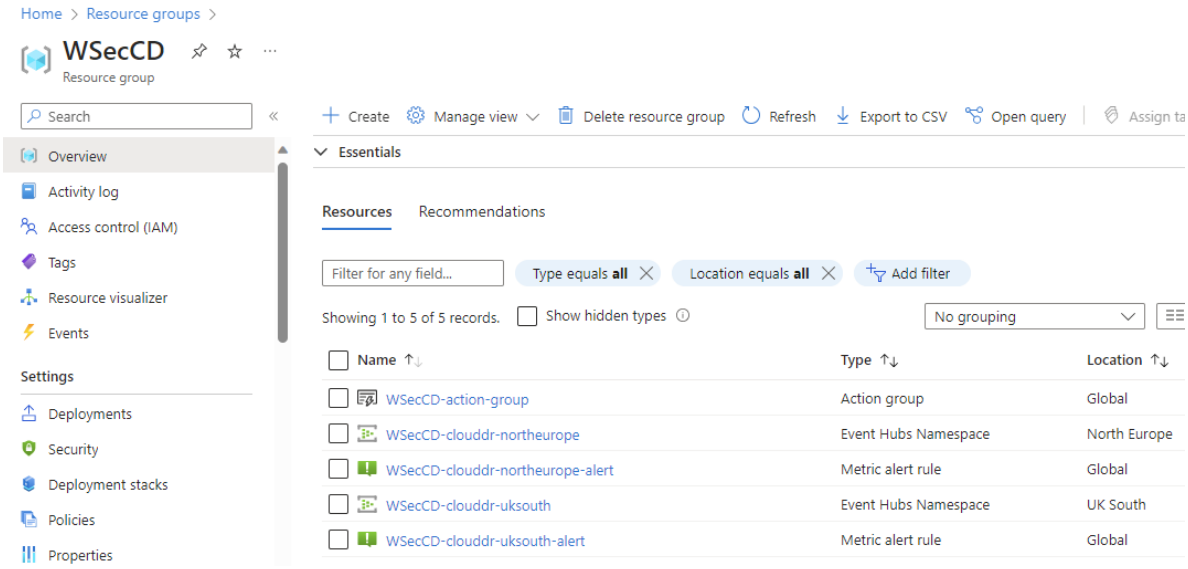
必要なリソースをデプロイしたら、デプロイが想定どおりに機能することを確認してください。検証には、イベントハブがイベントを受信していること、および 診断設定がログを アイデンティティセキュリティに転送していることを確認することが含まれます。

2.6.1 イベントハブを検証する

イベントハブが作成され、イベントを受信していることを検証します。

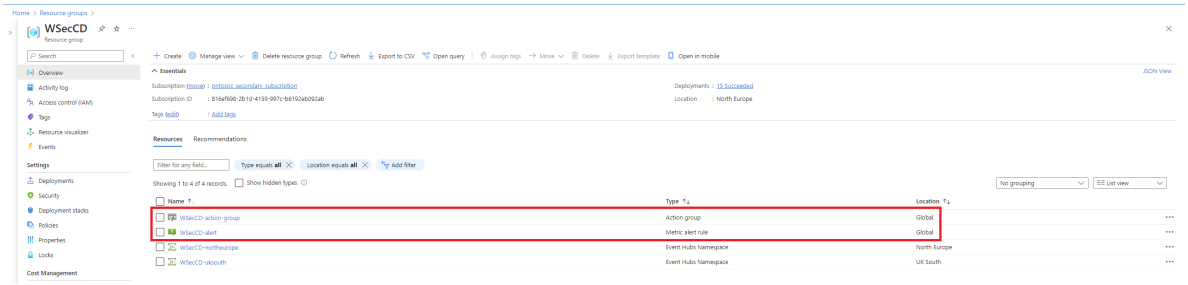
Event Hubs を検証するには:

1. *WSecCD*というリソースグループをチェックして、イベントハブが作成されたことを確認します。



イベントハブが存在する必要があります。

2. アラートが存在すること、およびアクションに正しいメールアドレスが含まれていることを確認してください。アラートは、イベントハブの容量が上限に達したときに通知します。



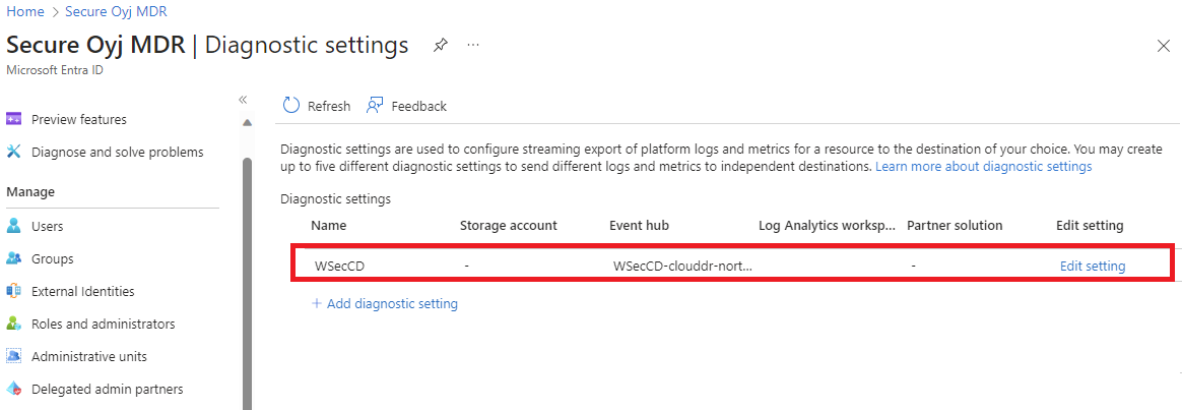
イベントハブには、正しい受信者メールアドレスを含むテストアラートが表示され、イベントが正しく配信されていることが確認できます。

2.6.2 診断設定を検証する

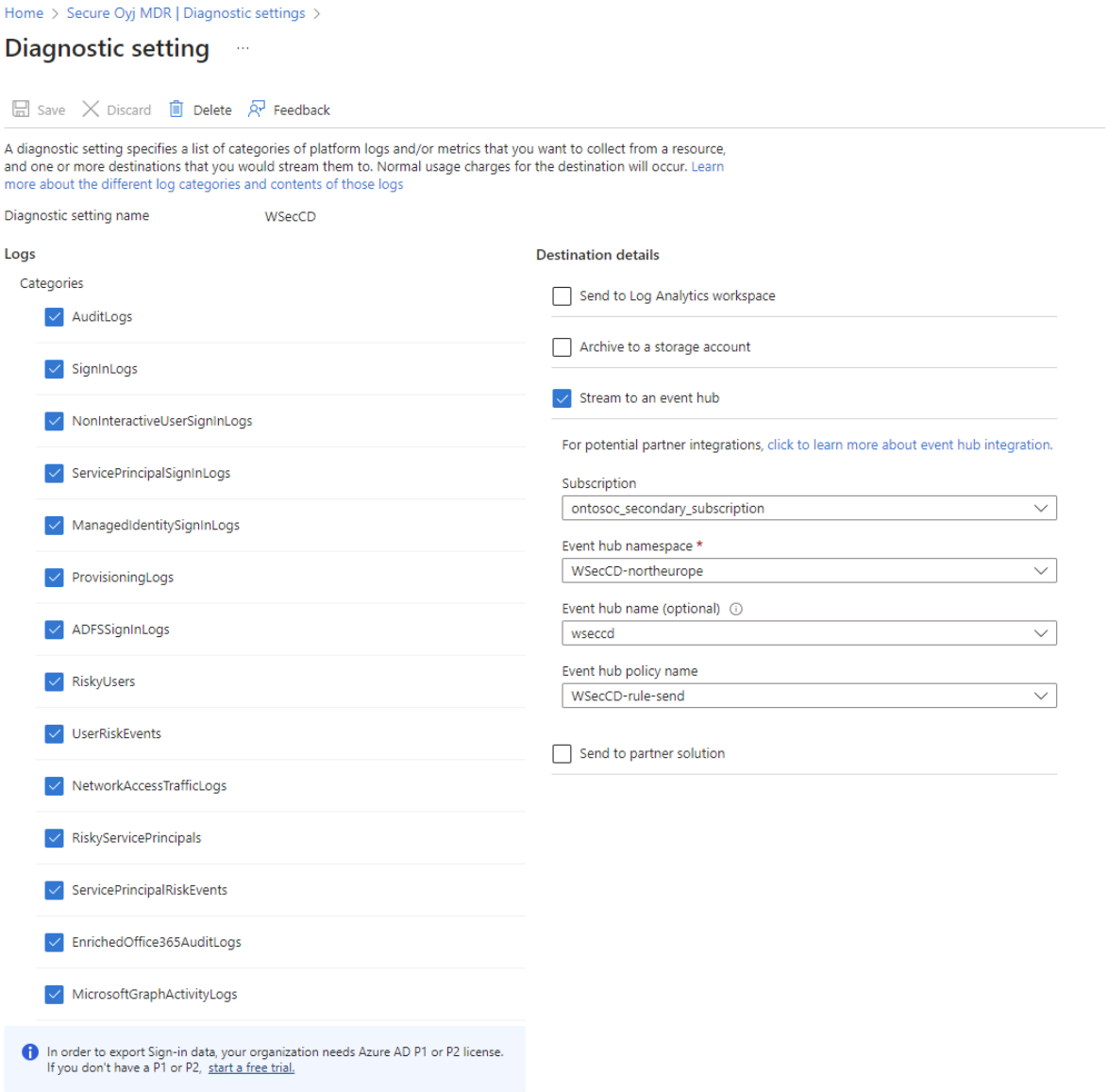
イベントハブにログをストリーミングする診断設定を検証します。

診断設定を検証するには:

1. Entra IDの診断設定を確認してください。WSecCD *WSecCD*名前の診断設定があるはずです。



2. [**設定の編集**]をクリックして、**診断設定**画面を開きます。



診断設定が検証され、必要な修復措置が一覧表示されます。

2.7 AzureをElements Cloudに接続する

WithSecure Elements Security Centerで Microsoft テナントを Elements Cloud に接続します。

展開が完了したら、次の手順に従ってください。

1. WithSecure Elements セキュリティ センターで、**[環境]** > **[クラウド]** > **[Microsoft テナントと Azure サブスクリプション]**に移動します。
2. リストから Azure テナントを選択します。
3. **[セキュリティ機能]**ページで、[**接続文字列の追加**]を選択します。
4. AzureCLIから`Endpoint=sb://`を含む接続文字列全体をコピーして貼り付け、[**追加**]を選択します。

> 👉 **注：** このプロセスには最大 5 分かかる場合があります。

接続が機能している場合、ステータスは*[***テナントは保護されています**」に変わり、緑色のチェックマークが表示されます。

テナントが複数ある場合は、**クラウド環境**ビューに戻り、**Microsoft テナント**タブに移動して別のテナントを構成します。

デプロイメントが成功したら、デプロイメント後の検証に進みます。

> 👉 **注:** デプロイメントが失敗した場合は、WithSecureカスタマーケアのチケットを作成してください。

> 👉 **重要：** 次の場合には、WithSecure Elements Security Centerから新しい展開スクリプトをダウンロードしてください。
>
> - 新しいテナントを作成する場合。
> - もし WithSecureセキュリティのベストプラクティスに準拠するために、クラウドプラットフォームまたはスクリプトに変更を加える。

2.8 検出機能が正常に動作することを確認してください。

Elements CloudをEntra IDテナントに接続した後、`onboarding.zip`ファイル内のスクリプトを実行することで、Entra ID向けWithSecure Elements Identity Securityとインストールが成功したことを確認できます。

このスクリプトは新しいアプリ登録を作成し、広範なコンテキスト検出 (BCD) をトリガーします。Elements Security Centerそして、クリーンな環境を維持するためにアプリの登録を削除します。

ID セキュリティ検出機能を確認するには:

1. クラウド シェル内で、次のコマンドを実行します。

```
./WithSecureIdentitySecurityTestingTool.ps1
```

2. スクリプトの実行が完了するまでお待ちください。
3. アプリケーションの登録が正しく作成され、かつ削除されていることを確認してください。
4. Elements Security Centreに移動し、**イベント** > **広範なコンテキスト検出**このアクティビティに対して、広範なコンテキスト検出が作成されていることを確認する。

   広範なコンテキスト検出には、`WithSecure test detection add application`と呼ばれる検出が含まれています。

5. 広範なコンテキスト検出を閉じる。

Elementsでは広範囲な文脈検出機能が表示され、検出機能が正常に動作していることが確認された。

2.9 オンボーディングを完了する

ロールの割り当てとサブスクリプション アクセスを調整して、オンボーディング プロセスを完了します。

デプロイメントを検証し、接続文字列を WithSecure Elementsセキュリティセンターに追加したら、役割とアクセス権限を次のように調整します。

1. Cloud Shell で次のコマンドを実行して WithSecure Entra ID configuration scriptデプロイに必要な昇格されたアクセスを取り消します。

```
Remove-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```

[**ユーザー プリンシパル名を**]*userId*として使用します。

2. Microsoft の手順に従って、[**すべてのサブスクリプションへのアクセス権の昇格**]オプションを無効にしてください: すべての Azure サブスクリプションと管理グループを管理するためのアクセス権の昇格

オンボーディングセッションは終了しました。

検出機能を導入したので、サイバー攻撃時の脅威の影響を最小限に抑えるために、ID対応機能を追加できます。

2.10 メールレポートの設定

自動メールレポートは、以下の [**メール通知とレポート**]機能を使用して設定できます。**レポート**。

セキュリティイベントのテンプレートとして使用するには、カスタムビューが必要です。

カスタム ビューを作成した後、電子メール レポートを追加、構成、スケジュールし、受信者を定義できます。

1. 新しい電子メールレポートを追加して構成するには、次の手順を実行します。
   a) 選択[**レポート**]左側のナビゲーションペインに表示されます。
   b) オン**レポート**ページを開き、[**メール通知とレポート**]タブに移動してください。
   c) [**電子メールレポートの追加**]を選択します。
   新しい電子メールレポートの追加ペインが開きます。
   d) レポートの名前を入力してください (例： `Entra ID`レポート) 。
   e) **データ ソース**ドロップダウン メニューから、[**セキュリティ イベント**]を選択します。



注： データソースとして [**セキュリティイベントを**]選択すると、受信者に送信されるメールには、Elements Security Centerの**セキュリティイベント**ビューへのリンクが含まれます。[**マイ レポート**]データソースとして、受信者に送信されるメールには、レポートをPDFファイルとしてダウンロードするためのリンクが含まれています。レポートの内容は、選択されたテンプレートを使用してカスタマイズされます。

   f) **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の**ページで既に作成済みのテンプレート (例： [**Entra IDイベント**]) を選択します。
   g) レポートに使用する言語を選択してください。
2. スケジュールと受信者を構成するには、次の手順を実行します。
   a) デフォルトでは、[**スケジュール**]の [**レポートにコンテンツがある場合のみ送信**]がオンになっています。イベントがない場合でもレポートを受信するには、オフにしてください。

セキュリティ イベントのレポートは 10 分ごとに送信されます。



注: 最初のレポートには過去 24 時間のデータが含まれます。後続のレポートには過去 10 分間のデータが含まれます。

b) [**受信者**]に、電子メール アドレスをコンマで区切って入力します。

3. [**保存**] を選択します。

メールレポートの設定が保存されました。

2.11 セキュリティイベント用のカスタムビューを作成する

[Entra ID]セキュリティイベント用のカスタムビューを作成し、例えばメールレポートの設定時などに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. [**表示**]ドロップダウン メニューを開き、**[Entra ID]**を選択します。
3. [**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。たとえば、「Entra ID events」などです。
4. [**保存**] を選択します。
   カスタムビューは、リストの一番上にある **「マイビュー」** の下に表示されます。

第 章3
継続的な管理

トピック :

- スクリプトを再実行するタイミング
- 新しいテナントが作成されたとき
- イベントハブの容量を確認する
- スクリプトの定期的なリリース
- 検出モジュールの概要
- 更新通知の受信者

継続的な管理

アイデンティティセキュリティを接続状態に保ち、期待されるサービスレベルで動作させるために必要な保守作業。

導入後、アイデンティティセキュリティが接続され、期待されるサービスレベルで動作し続けるように、継続的なメンテナンスを実施します。メンテナンス活動には以下が含まれます。

- クラウド環境が変更された場合にデプロイスクリプトを再実行する
- 新規テナントの受け入れ
- イベントハブの容量を監視する
- デプロイメントスクリプトの新しいリリースを適用する
- 通知受信者を更新しています

3.1 スクリプトを再実行するタイミング

オンボーディング プロセス中に実装される診断設定とポリシーにより、クラウド環境の一部が変更されます。

初期オンボーディング プロセスの後、診断設定とポリシーは、クラウド環境の一部の変更を自動的に検出して処理するように設計されています。ただし、これらの設定とポリシーでカバーされていない重要な変更や更新がある場合は、スクリプトを再実行する必要があります。

3.2 新しいテナントが作成されたとき

新しいテナントが作成されたら、それを Elements Security Centerに追加し、デプロイスクリプトを実行してオンボーディングします。

新しいテナントが作成されたら、オンボーディング設定を完了して、新しいテナントをElements Security Centerに追加し、新しい `.zip`ファイルをダウンロードしてください。

新しいテナントをオンボーディングするには、最初のリソース展開時と同じように、展開スクリプト（`deploy.ps1`）を再度実行します。

3.3 イベントハブの容量を確認する

オンボーディング プロセス中に、スクリプトは、イベント ハブが処理できる数を超えるイベントを受信したときにアラートを作成します。

イベントハブの容量を確認するには、以下の手順を実行してください。

1. Azure portalの検索バーに 「`Event Hubs`」と入力して、Event Hub の概要ページに移動します。
2. イベントハブの名前を選択してください。
3. 概要ページで、[**スループット単位」の**]値を確認してください。
   [**スループットユニット**]数が40の場合、またはアラートが間もなく解決されることを示すメールが届かない場合は、 WithSecureカスタマーケアにお問い合わせください。

イベントハブの概要画面にはスループットユニットの値が表示され、その容量を確認できます。

3.4 スクリプトの定期的なリリース

イベント ハブ、診断設定、およびポリシーを構成するために使用されるスクリプトは、時間の経過とともに変更や改善が必要になる場合があります。

検出範囲の拡張、最新のクラウドのベストプラクティスへの適合、または基盤となるクラウド プラットフォームの変更により、変更が必要になる場合があります。

最新バージョンのファイルが展開されていない場合、WithSecure Elements Security Centerで [**オンボードファイルの**]ステータスを確認できます。再展開するには、最新バージョンのスクリプトをダウンロードし、コマンド `deploy.ps1 -update $true`を使用してください。

3.5 検出モジュールの概要

アイデンティティセキュリティは、危険なサインインと潜在的な権限昇格を特定します。検出モジュールは、これを基に、攻撃者が盗んだ認証情報を使用した後の攻撃者の活動について、より詳細な情報を提供します。

検出モジュールは 、Elements Endpoint Protection、Elements Endpoint Detection and Response、および Elements Identity Securityと連携して動作します。これにより、攻撃者が盗んだ認証情報を使用した後の攻撃者の行動をより詳細に把握できます。

検出モジュールは、IDセキュリティと 検出の両方から検出結果を収集します。そして、疑わしいアクティビティをまとめて、広範なコンテキスト検出 (BCD) として表示します。

検出モジュールは、次の Azure クラウド サービスを監視します。

- Azure Key Vault：機密性の高いキーやシークレットへの不正アクセスを検出します。攻撃者はこれらを利用して攻撃をエスカレートさせる可能性があります。
- ネットワークセキュリティグループ：ネットワーク経路を開放する変更を特定します。攻撃者はこれらの経路を利用して機密情報を盗み出す可能性があります。
- Azure 仮想マシン (VM)：仮想マシンの起動時に実行される有害なコードを監視します。また、クリプトジャッキングの兆候も監視します。クリプトジャッキングとは、攻撃者が組織のシステムを利用して、秘密裏に仮想通貨をマイニングする行為です。
- Azure Storage：管理者が Cloud Shell を開いたときに実行されるセットアップスクリプトの変更を検出します。これらの変更により、攻撃者は管理者レベルの権限を取得し、コードを密かに実行できるようになります。

3.6 更新通知の受信者

Elements Security Centerでは通知の受信者を更新できません。受信者リストを変更するには、Azure ポータルでアクション グループを編集してください。

通知受信者は、オンボーディングスクリプトによって配信されるメールアラート (例えば、イベントハブが容量に達したときに発生するアラートなど) を受け取ります。

1. Azure ポータルにサインインし、[**リソース グループ**]に移動します。
2. *WSecCD*という名前のリソース グループを開きます。
3. **概要**セクションの [**リソース**]で、*WsecCD-action-group*という名前のアクショングループを選択します。
4. アクショングループを編集して、通知の受信者を追加または削除します。



重要 : これらの変更は Elements Security Centerには表示されません。

通知の受信者は、アクショングループ内で更新されます。

付録 A
デプロイされたリソースをオフボードする

デプロイされたリソースをオフボードする

Azure 環境から、デプロイ済みの Entra ID 用WithSecure Identity Securityリソースを削除します。

これは、次のいずれかの場合に実行する必要があります。

- 展開プロセスで問題が発生したため、展開をやり直す必要がある、または
- サービスをオプトアウトし、監視リソースを削除します。

リソースを削除するには、次の手順に従います。

1. **テナント詳細**ビューにある最新の *onboarding script*をダウンロードしてください。**環境** > **クラウド** > **[Microsoft テナントと Azure サブスクリプションの]**タブ。
2. Azure Portal で、テナントを管理するために一時的にアクセス権を昇格します。

   すべてのサブスクリプションを管理するためのアクセス権を一時的に昇格させるには、次のページに記載されている手順に従ってください。すべてのAzureサブスクリプションと管理グループを管理するためのアクセス権の昇格 | Microsoft Learn。
3. Azure ポータルに移動し、[**Azure リソースのアクセス管理**]オプションを [**はい**]に切り替えます。
4. PowerShell で Azure Cloud Shell を開きます。
5. シェル画面の上部にある **[ファイルの管理と]** > **[アップロード]**を使用して、手順 1 でダウンロードした *onboarding script* zip ファイルを Azure Cloud Shell にアップロードします。
   オンボーディング *zip* ファイルが現在の作業ディレクトリにアップロードされます。
6. パッケージの `unzip`コマンドを使用してパッケージを解凍します。

```
unzip './WithSecure Elements XDR Identity Security for Entra ID.zip'
```

   これにより、すべてのファイルが新しい *`withsecure`*フォルダーに解凍されます。
7. 解凍されたデプロイメント ファイルが含まれるディレクトリに移動します。

```
cd withsecure
```

8. Azure Cloud Shellで次のコマンドを実行して、WithSecure Entra ID構成スクリプトをデプロイする必要があるプリンシパルに *Owner*を割り当て、*[userId]*を [**ユーザー プリンシパル名**]で更新します。

```
New-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```

   > 👉 **注：** これにより、Microsoft Defender for Cloud アラートが作成される場合があります。

9. リソースを削除するには、`withsecure`ディレクトリ内から次のコマンドを実行します。

```
./cleanup.ps1
```

   これにより、*Azure* 環境内の *WithSecure Identity Security for Entra ID*関連リソース *(WSecCD*リソース グループ、アクショングループ、イベントハブ名前空間、メトリックアラートルール*)* の *WithSecure Identity Security* が削除されます。
10. Elements Security Centerに戻り、関連する Azure テナント接続を削除します。WithSecure。
    a) WithSecure Elements セキュリティ センターで、**[環境]** > **[クラウド]** > **[Microsoft テナントと Azure サブスクリプション]**に移動します。
    b) 削除するテナントを選択します。

c) **[クイック アクション]**で、[**Azure テナントの削除**]を選択します。
d) 通知を読み、[**Event Hub 接続を削除する**]チェック ボックスを選択します。
e) [**削除**]を選択します。
テナント接続が正常に削除されたことを確認するメッセージが表示されます。

デプロイされたリソースは、お客様の環境から削除されます。

付録 B
トラブルシューティング

トピック :

- 接続状態を確認してください

トラブルシューティング

トラブルシューティング情報は、製品に関する問題を解決するのに役立ちます。

- デプロイが完了する前にクラウドシェルターミナルが閉じられた場合：リソースを再度デプロイする手順に従ってください。
- `deploy.ps1`スクリプトの実行中に、進行中のデプロイメントに関するエラーが発生した場合は、15 分待ってから再試行してください。
- サブスクリプションが名前空間 Microsoft.PolicyInsightsを使用するように登録されていないことを示すエラーが発生してデプロイが失敗した場合は、次の操作を行います。

  1. このサブスクリプション ページに移動し、[**リソース プロバイダー**]をクリックします。
  2. プロバイダー [**Microsoft.PolicyInsights**]をクリックし、[**登録**]または [**再登録を**]クリックします。
  3. 登録が完了したら、`./deploy.ps1`スクリプトを実行してプロセスを再起動します。

B.1 接続状態を確認してください

WithSecure Elements Security Centerで接続ステータスを確認できます

ID セキュリティ保護が非アクティブに見える場合は、各テナントの接続状態を確認してください。Elements Security Center。

1. WithSecure Elements セキュリティ センターで、**[環境]** > **[クラウド]** > **[Microsoft テナントと Azure サブスクリプション]**に移動します。
2. リストに表示される各テナントの [**ID セキュリティ**]ステータスを確認します。

各テナントごとに、IDセキュリティ接続の状態が表示されます。

付録 C
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、強靭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。

C.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。

C.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。

C.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. ユーザ名を入力して [**ログイン**] を選択します。

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

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

フェデレーションドメインにログインする

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）とも呼ばれ、システムへのログインプロセスにおけるセキュリティを高める方法です。

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



重要： WithSecure Elements Security Centerへのアクセスを保護するために、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もあります。そのため、安全な代替手段がない場合を除いて、SMSの使用を避けることをお勧めします。



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. 
   右上隅にある [**マイ設定**]を選択します。

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

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

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

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. 
   右上隅にある [**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。

C.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、スコープセレクター、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

スコープセレクターを使用して、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。

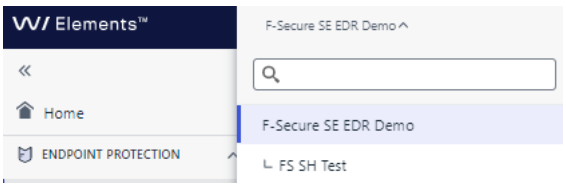
- ソリューションプロバイダー（SoP）は、サービスパートナーおよび企業グループを管理します。SoPは Elements Security Centerにアクセスして、自社が直接管理する企業、サービスパートナー、およびサービスパートナーの企業のセキュリティとサブスクリプションを管理できます。
- サービスパートナー（SeP）は、複数の企業グループを管理します。SePはElements Security Centerにアクセスして、直接管理する企業のセキュリティを管理できます。
- 各企業は単一の企業を管理します。SoPまたはSePによって管理されている企業はプロバイダーにアクセスを要求できますが、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。

特定の会社にスコープセレクタを重視するには

1. タイトルバーにある

   アイコンを選択してください。
   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）ロールを使用すると、IAM管理者は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ことができます。これは、IAM管理者自身の組織および関連組織内に適用されます。

概要

IAM の役割は、WithSecure Elementsセキュリティ機能とサービスの管理を効率化します。

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

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

セキュリティ管理者は 、Elements Security Center にアクセスするために以下の方法を使用します。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、およびサービスごとに管理されます。IAMロールを使用することで、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が簡素化されます。

利点

IAMロールには以下の利点があります。

- 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

組織内には、既にすべての従来のユーザーアクセス管理ロールを保有しているユーザーがいます。これらのユーザーの場合、IAMロールを取得しても権限は昇格しません。セキュリティ管理者ビューには、新しいIAM管理者ロールを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検討する必要があります。結果として、このオプションが利用可能になる前よりも、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WithSecureElements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ロールは引き続き有効ですが、最終的にはIAMロールを通じて管理されるようになります。IAMロールは、APIキーの設定など、現在他のロールによって管理されている機能へのアクセスも保護します。

IAM権限の移行

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

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

顧客企業向け	以下のレガシーロ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ロ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 ロールを要求するようにします。

IAM管理者候補が特定できない場合

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

IAM ロールに関するよくある質問

IAMロールに関するよくある質問への回答。

Q	A
パートナー(SOP/SEP)は、傘下のすべての企業に対して IAM ロールを作成できますか?	はい、パートナーレベルのIAM管理者は、XM/CPアクセスをSOPから分離することを選択した企業を除き、自身の組織とその傘下の組織を完全に管理できます。
企業がIAM期限(2025年4月末)に間に合わなかった場合、企業管理者は何をすべきでしょうか?	会社の管理者は、サービス パートナーに問い合わせてサポートを受けるか、WithSecureサポートに連絡する必要があります。
セルフ登録ポータルを使用して新しいユーザーを作成すると、最初の管理者は IAM ロールを自動的に取得しますか?	はい、最初の管理者には IAM ロールが自動的に付与されます。
最高レベルの管理者ロールを要求するときに、誤って [拒否] を選択した場合はどうなりますか?	ユーザーが誤って IAM ロールの要求を拒否した場合でも、必要に応じて他の IAM 管理者が IAM ロールを割り当てることができます。

Q	A
[**拒否**]を選択した Endpoint Protection 管理者ユーザーは、他の Endpoint Protection 管理者ユーザーを追加できますか?	はい、当面はまだ可能です。将来的には、すべてのユーザー管理アクション権限は IAM ロール所有者のみに制限されます。
1 つの組織に複数の IAM 管理者ユーザーを設定できますか?	はい、組織が持つことができる IAM 管理者の数に制限はありません。
一部の管理者ユーザーに請求および拒否のオプションが表示されないのはなぜですか?	最初の段階では、組織が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。
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？	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. スコープセレクターを使用して、新しい管理者アカウントを作成する組織レベルを選択します。
4. [**管理者の追加を**]選択します。
5. **管理者追加**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に制限されます。
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:

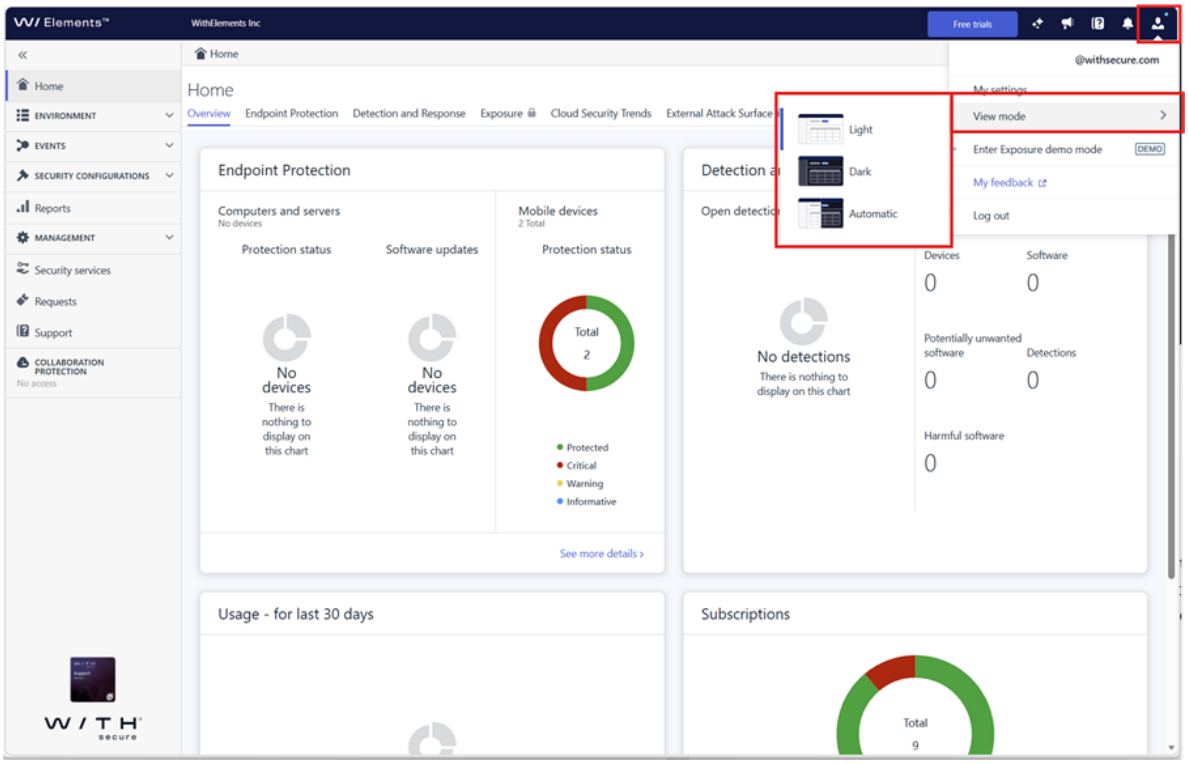
1.
   右上隅にある [**マイ設定**]を選択します。
2. [**詳細**]欄に、新しいユーザー名を入力してください。
3. [**保存**] を選択します。

C.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ァイ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。

C.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**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 WithSecure Partner Portalアカウントに新しい顧客として追加します。次に、少なくとも1つの製品を購入します。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。

まず、パートナーポータルアカウントから新規顧客の発注書を追加してください。発注書が正常に追加されると、その顧客は自動的に 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、購入した製品のサブスクリプションを管理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. スコープセレクターを使用して、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 ElementsWithSecure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 ElementsWithSecure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、[**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

利用可能の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： スコープセレ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、スコープセレクターを使用して、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アントについても、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。

C.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、ユーザーの身元を証明するデジタル署名付きトークンが生成されます。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と、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、アクセスを許可します。ユーザーは再度ログインする必要はありません。

FSSOはシステム間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、アプリケーションやサービス間を移動できます。また、FSSOはユーザーが複数回のログインを必要としないため、セキュリティとユーザーエクスペリエンスを向上させます。IDプロバイダーからユーザーを削除すると、そのユーザーは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。

3. 電子メールアドレスがドメインですでに認証されている場合は、IDリンクフローにリダイレクトされます。電子メールアドレスがドメインでまだ認証されていない場合は、ドメインパスワードの入力を求められます。

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

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

ドメインからフェデレーションを削除する

ドメインからシングルサインオンフェデレーションを削除します。

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:

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

C.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。
   デバイスページが表示されます。
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 [**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：** スコープセレ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。

C.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。

C.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 スコープセレクターまたは [**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ことができます。

Active Directory の構成に基づいてデバイスを表示するには

1. 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。

C.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。

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。

アクティベーションコード

アクティベーションコードとは、製品をインストールする際に入力するコードで、製品を有効化し、その設定を適用するために使用します。

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。

異常

予期されるシステムまたはユーザーの動作からの異常な逸脱。多くの場合、潜在的なセキュリティの脅威を示します。

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の使用です。

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。

ビジネスコンテキスト

資産の役割、重要性、ビジネス運営への関連性を把握するために資産に割り当てられる追加のメタデータ。

クラウドアカウント

クラウドアカウントは、クラウドプロバイダーによって管理されるクラウドコンピューティングサービスとリソースへのアクセスを許可するユーザーまたは組織のプロファイルです。

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。

侵害されたアカウント

侵害されたアカウントとは、攻撃者が許可なくアクセス、悪用、または乗っ取ったユーザーアカウントのことです。

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。

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。

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。

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。

ディスカバリースキャン

ディスカバリースキャンとは、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。

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。

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。

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。

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。

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。

Identity Response

Microsoft Entra IDと連携し、IDベースの脅威を検出・緩和するWithSecure Elementsのセキュリティ機能。

Identity Security

IDセキュリティとは、危険なサインイン、IDの不正使用、およびユーザーのIDやアクセスシステムに影響を与える権限関連の脅威を検出するセキュリティ機能です。

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。

Incident Response

インシデント対応とは、セキュリティインシデントを検知、封じ込め、調査、復旧し、被害を最小限に抑え、通常の業務を回復させるための組織的なプロセスである。

インシデント対応リテイナー

重大なセキュリティインシデントに対処するため、サイバーセキュリティの専門家へのアクセスを事前に確保・提供するサービス。

Infrastructure as Code (インフラのコード化) (IaC)

手動プロセスではなく、機械で読み取り可能な構成ファイルを通じてITインフラストラクチャを管理およびプロビジョニングします。

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。

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。

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。

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。

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。

オフボーディング

オフボーディングとは、製品、統合、サービス接続、または付与された権限が不要になった場合に、それらを環境から削除する管理されたプロセスのことです。

組織

Elements RBAC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。

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。

権限昇格

システム内で、当初許可されていたアクセスレベルよりも高いアクセス レベルを取得する行為。

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。

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。

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。

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。

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。

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。

スコープセレクター

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。

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。

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。

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。

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。

索引

記号

解決策。 まず、パートナーポータルアカウントから新規顧客の発注書を追加してください。発注書が正常に追加されると、その顧客は自動的に Elements Security Center 49
環境を整える 15
管理者アカウント 33
企業レベル 61–62
危険なサインイン 5, 24
緊急インシデント対応 11
継続的な管理 23
検出 7
検出の 24
検出モジュール 24
検出能力 19
検証 17
権限 13
広範なコンテキスト検出 5, 11, 19, 24
購読アクセス 20
高所へのアクセス 15, 20
再配置 24
指紋 37
私の設定 36, 47
資産グループ 61–62
自動削除 59, 62
招待待ち 60
侵害されたアカウント 11
新しい入居者 23
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ロールは引き続き有効ですが、最終的にはIAMロールを通じて管理されるようになります。IAMロールは、APIキーの設定など、現在他のロールによって管理されている機能へのアクセスも保護します。 IAM権限の移行 移行プロセスの目的は、従来の機能固有の IAM ロールから、より高い権限を付与する新しい Elements 43
診断設定 8, 17, 23
診断設定が 17
生体認証 37
脆弱性ロール 37
脆弱性管理 32
接続状態 30
接続性 23
接続文字列 19
設定スクリプト 16, 23–24
前提条件 11
組織設定 46–47, 61
多要素認証 33, 35–37
退職手続き 27
通知の受信者 20, 24
展開されたインフラストラクチャ 8
展開後の検証 17
電子メールアドレス 53
電子注文 49
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、強靭なビジネスの構築と維持を支援します。 WithSecure Elementsの特長 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、ビジネスの必要性応じてWithSecure Elements 32
二段階認証 35
認証アプリ 35–36
美術学修士 35–36
名前を変更する 47
役割の権限 43
役割割り当て 15, 20
容量アラート 23
要素 13
連邦ドメイン 34, 55–56
連邦制の廃止 56
露出管理 38

A

access rights 32, 37–38, 45
account creation 46
account levels 42
Active Directory 63
AD groups 63
adding devices 56, 58
administrator account 32, 37, 45–46
Agent for Computers 57
Agent for Windows 64
audit logs entry 38
Auth0 Guardian認証アプリのプッシュ通知機能を使えば 35
Azure 13, 20–21
Azure Cloud Shell 11, 15, 27
Azure Cloud Shell が 15
Azure Cloud Shell では、 15
Azure Cloud Shell を 27
Azure Cloud Shellの 15
Azure Key Vault 24
Azure Management Group 11
Azure portal 14, 23
Azure Storage 24
Azure テナント 6, 13–14, 19, 27, 30
Azure ポータル 24
Azure ログ収集 13
Azure 仮想マシン (VM) 24
Azure 管理グループ 11
Azureクラウドサービス 24
Azureポータル 13, 23–24

C

change subscription 52
Collaboration Protection 43
Connector 52, 57, 62
Connector の 57
customer company 37, 49

D

dark mode 48
deploy.ps1 -update $true 24
Detection and Response 7
device commands 62
device management 56, 61
device view 61, 63
devices 52, 62
diagnostic data 64
downloading software 59
Downloads page 59

E

edit administrator 46
EDR 52
EDR for Computers 52, 59
EDR および EPP for Computers Premium 52
EDR および EPP for Computers Premium まで 52
EDR および EPP for Computers へ 52
EDR および EPP for Servers Premium 52
EDR と EPP for Computers 52
EDR と EPP for Servers の 52
EDRおよびEPP for Computers 52
EDRおよびEPP for Computers Premium 52
Elements 36, 43, 49, 53, 60
Elementsセキュリティセンター 20, 32, 36, 47, 61
Elementsセキュリティセンターの 47
Elementsの 32, 43
email invitation 58
Endpoint Detection and Response 7, 11, 24
Endpoint Detection and Response の 7
Endpoint Detection and WithSecure 7
Endpoint Protection 11, 37, 43–44, 56
Entra ID 17, 20, 27
Entra ID configuration script 20
Entra ID 構成スクリプト 8
Entra ID構成スクリプト 8
EPP for Computers 52, 62–63
EPP for Computers Premium 52
EPP for Computers Premium へ 52
EPP for Servers 52, 62–63
EPP for Servers Premium 52
EPP for Servers Premium へ 52
EPP subscription 52
existing customer company 50
Exposure Management 37, 43

F

forgot password 47
FSSO 53

I

IAM role 37
Identity Security 7, 13, 24
Identity Security for Entra ID 5, 27
installation link 58
installation package 57, 59

L

light mode 48
login 34, 47
login credentials 34

M

managed companies 42
Microsoft Entra Admin Center 53
Microsoft Entra ID 53
Microsoft Entra ID P1またはP2ライセンスを 5
Microsoft から 15
Microsoft テナント 5
Microsoft.PolicyInsights 30
Mobile Protection 56, 62, 64

N

new customer company 50
non-federated domain 34

O

ordering products 50
Organization Settings 45–46

P

partner 46
Partner Portal 49–50
password recovery 47
permissions 38
PowerShell 15
Premium subscription 52
product deployment 49
profile assignment 63

R

remote device management 62
remote request 64
remove administrator 46
reset password 47
role 38
role assignment 37

S

scope selector 32, 42, 51
security administrator 37, 45
Security Administrators 46
Security Center 13, 19, 23–24, 27, 32, 34–35, 37, 42, 45, 48–50, 53–54, 56, 59–64
Security Center の 33, 64
Security Centerに 34
Security Centerは 7, 32
service partner account 46
software distribution 57
software installation 58
Solution Provider 42, 49

subscription 49–50, 56
subscription assignment 49
subscription key 49, 51–52, 57
subscription upgrade 52
subscriptions 49, 51
Subscriptions view 51
support 64

U

unzip 15, 27
upgrading options 52
user management 37

V

view mode 48
Vulnerability Management: 43

W

WithSecure 33–34, 42, 44, 49
WithSecureエレメント付き 32
WithSecureパートナーポータル 50
WithSecureパートナーポータルへのアクセス 50
WithSecure構成スクリプトは、 16
WSDIAG file 64
WSecCD 17, 24

あ

アイデンティティインベントリ 13–14
アイデンティティセキュリティ 5, 7, 11, 13, 17, 19, 23–24, 30
アイデンティティセキュリティが 23
アイデンティティとアクセス管理 43
アイデンティティプロバイダー 53
アカウントの詳細 47
アカウント連携 53
アクショングループ 24
アクセス管理 43–44
アクセス権限 46
アプリ登録 19
アラートルール 17

い

イベントハブ 8, 11, 13, 16–17, 23
イベントハブが 17
イベントハブの 23
イベントハブの容量 23
インシデント対応リテーナーは 11
インストールパッケージ 7
インストールリンク 60
インフラストラクチャ・アズ・コード 8

え

エレメンツクラウド 19
エレメンツサービス 65
エレメンツセキュリティセンター 6, 13–14, 19–20, 23–24, 30, 33–34, 56
エレメントアカウント 55
エンドポイントセンサー 7
エンドポイント保護 32, 56

お

オフラインデバイス 59, 62
オンボーディング 6, 13
オンボーディングスクリプト 15, 23
オンボーディングを完了する 20
オンボーディング設定 13

か

カスタムビュー 20–21
カスタムラベル 60

く

クイックスタート 33
クラウドアカウント 13–14
クラウドシェル 20, 30
クラウド環境 23
クリーンアップスクリプト 27
グローバル管理者 11

さ

サブスクリプション 11, 33, 59

し

シングルサインオン 34, 53–54, 56

す

スクリプトの更新 24
スクリプトの再実行 23
スコープセレクター 45, 49, 61
スコープセレクターが 51
スコープセレクターで 58
スコープセレクターを 32, 51
スマートフォンまたはその他のデバイス 35
スループットユニット 23

せ

セキュリティ センター 13
セキュリティイベント 20–21
セキュリティの役割 43
セキュリティ機能 13–14
セキュリティ機能とサービスの管理を効率化します。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 43

そ

そして、クリーンな環境を維持するためにアプリの登録を削除します。 ID セキュリティ検出機能を確認するには: クラウド シェル内で、次のコマンドを実行します。 ./WithSecureIdentitySecurityTestingTool.ps1 スクリプトの実行が完了するまでお待ちください。 アプリケーションの登録が正しく作成され、かつ削除されていることを確認してください。 Elements Security Centre 19

て

データ復旧 65
テーブルの列 64
テストツール 19
デバイスグループ分け 60–61
デバイスの生体認証 35
デバイスビュー 64
デバイスフィルター 64
デバイスページ 62
デバイスラベル 60
デバイスリスト 60
デバイスを追加する 62
デバイス割り当て 62
デバイス管理 59–62, 64
デバイス招待状 60
デバイス生体認証 37
デプロイされたリソース 27
デプロイメントスクリプト 23, 30

と

トップ 35
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 34
ドメインフェデレーション 54
トラブルシューティング 30

に

に 33

ね

ネットワークセキュリティグループ 24

は

パートナー 44
パートナー ポータル 50
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。一時パスワードと、 Elements Security Center 34
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 32
はじめる 6, 33
バックアップ 65
パッチ管理 32

ひ

ビジネスアカウント 6, 34
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 43

ふ

フェデレーション型シングルサインオン 53–54
プロファイル割り当てルール 61
プロフィールを編集 47

ほ

ポリシー 23
ポリシー遵守 17

め

メールアラート 24
メールエイリアス 53
メールレポート 20
メール招待状 60

ゆ

ユーザー名 47

ら

ラベル割り当て 60

り

リソースグループ 8, 17, 27
リソースの展開 16
リソースプロバイダー 30

ろ

ログイン 34
ログインセキュリティ 35
ログイン認証情報 34