統合

この章で説明する内容は、次のとおりです。

- Cisco Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）の統合 （1 ページ）
- Cisco SecureX および Cisco Threat Response との統合 （19 ページ）
- Cisco Secure Web Appliance と Cisco Umbrella の統合 （29 ページ）

Cisco Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）の統合

この章で説明する内容は、次のとおりです。

- Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要 （1 ページ）
- ISE/ISE-PIC の証明書 （5 ページ）
- フォールバック認証 （6 ページ）
- ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）
- ISE-SXP 統合の設定 （16 ページ）
- ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証 （18 ページ）
- Identity Services Engine に関する問題のトラブルシューティング （19 ページ）

Identity Services Engine（ISE）/ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要

Cisco Identity Services Engine（ISE）は、ID 管理を向上させるためにネットワーク上の個々のサーバーで実行されるアプリケーションです。 Secure Web Applianceは、ISE または ISE-PIC の

サーバーからユーザーアイデンティティ情報にアクセスできます。ISE または ISE-PIC のいずれかが設定されている場合は、適切に設定された識別プロファイルに対してユーザー名および関連するセキュリティ グループ タグが ISE から、ユーザー名および Active Directory グループが ISE-PIC からそれぞれ取得され、それらのプロファイルを使用するように設定されたポリシーで透過的ユーザー識別が許可されます。

- セキュリティ グループ タグと Active Directory グループを使用してアクセス ポリシーを作成できます。
- ISE/ISE-PIC による透過的な識別に失敗したユーザーの場合、Active Directory ベースのレルムを使用してフォールバック認証を設定できます。「フォールバック認証 （6 ページ）」を参照してください。
- 仮想デスクトップ環境（Citrix、Microsoft 共有/リモート デスクトップ サービスなど）でユーザーの認証を設定できます。「ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証 （18 ページ）」を参照してください。

（注）

- ISE/ISE-PIC サービスはコネクタ モードでは使用できません。
- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- Secure Web Applianceの Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE または ISE-PIC を設定する手順は似ています。ISE-PIC に固有の詳細が適宜記載されています。

Cisco Secure Web Appliance ISE バージョンのサポートマトリックスの詳細については、『ISE Compatibility Matrix Information』を参照してください。

表 *1：Secure Web Appliance-ISE* スケール サポート マトリックス

モデル	AD グループが有効になっていないセッションスケール	AD グループが有効になっているセッションスケール	
-	サポートされている最大アクティブセッション数	サポートされている最大アクティブセッション数	サポートされている最大エンドポイント数 （各ユーザーの AD グループエントリと ISE データベース内のエンドポイント）
S680*、S690、S695	200K	125K	400K
S380*、S390、S600V	150K	50K	150K
S190、S195、S300V	50K	50K	75K
S100V	50K	40K	50K

（注） *S190、S390、および S690 モデルはサポートされていません。

関連項目

- pxGrid について （4 ページ）
- ISE/ISE-PIC サーバーの展開とフェールオーバーについて （4 ページ）

pxGrid について

シスコの Platform Exchange Grid（pxGrid）を使用すると、セキュリティ モニターリングとネットワーク検出システム、ID とアクセス管理プラットフォームなど、ネットワーク インフラストラクチャのコンポーネントを連携させることができます。これらのコンポーネントはpxGridを使用して、パブリッシュまたはサブスクライブ メソッドにより情報を交換します。

以下の 3 つの主要 pxGrid コンポーネントがあります：pxGrid パブリッシャ、pxGrid クライアント、pxGrid コントローラ。

- pxGrid パブリッシャ：pxGrid クライアントの情報を提供します。
- pxGrid クライアント：パブリッシュされた情報をサブスクライブする任意のシステム（Secure Web Applianceなど）。パブリッシュされる情報には、セキュリティグループタグ（SGT）、Active Directory グループ、ユーザーグループおよびプロファイルの情報が含まれます。
- pxGrid コントローラ：クライアントの登録/管理およびトピック/サブスクリプション プロセスを制御する ISE/ISE-PIC pxGrid ノードが該当します。

各コンポーネントには信頼できる証明書が必要です。これらの証明書は各ホストプラットフォームにインストールしておく必要があります。

ISE/ISE-PIC サーバーの展開とフェールオーバーについて

単一の ISE/ISE-PIC ノードのセットアップはスタンドアロン展開と呼ばれ、この 1 つのノードによって、管理およびポリシー サービスが実行されます。フェールオーバーをサポートし、パフォーマンスを向上させるには、複数の ISE/ISE-PIC ノードを分散展開でセットアップする必要があります。 Secure Web Applianceで ISE/ISE-PIC フェールオーバーをサポートするために必要な最小限の分散 ISE/ISE-PIC 構成は以下のとおりです。

- 2 つの pxGrid ノード
- 2 つの管理ノード
- 1 つのポリシー サービス ノード

この構成は、『*Cisco Identity Services Engine Hardware Installation Guide*』では「中規模ネットワーク展開」と呼ばれています。詳細については、『Installation Guide』のネットワーク展開に関する項を参照してください。

関連項目

- ISE/ISE-PIC の証明書 （5 ページ）
- ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）
- ISE/ISE-PIC サービスへの接続 （9 ページ）
- Identity Services Engine に関する問題のトラブルシューティング （19 ページ）

ISE/ISE-PIC の証明書

（注） このセクションでは、ISE/ISE-PIC 接続に必要な証明書について説明します。ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）では、これらの証明書に関する詳細情報を提供します。証明書の管理（Certificate Management）は、AsyncOS の証明書の一般的な管理情報を提供します。

Secure Web Applianceと各 ISE/ISE-PIC サーバー間で相互認証と安全な通信を行うには、一連の 2 つの証明書が必要です。

- **Web Appliance クライアント証明書**： Secure Web Applianceを認証するために ISE/ISE-PIC サーバーで使用されます。
- **ISE pxGrid 証明書**： Secure Web Appliance-ISE/ISE-PIC データサブスクリプション（ISE/ISE-PIC サーバーに対する進行中のパブリッシュ/サブスクライブクエリー）向けに ISE/ISE-PIC サーバーを認証するためにポート 5222 で Secure Web Applianceによって使用されます。

この 2 つの証明書は、認証局（CA）による署名でも自己署名でもかまいません。CA 署名付き証明書が必要な場合、AsyncOS には自己署名 Web Appliance クライアント証明書、または証明書署名要求（CSR）を生成するオプションがあります。同様に ISE/ISE-PIC サーバーにも、CA 署名付き証明書が必要な場合に、自己署名 ISE/ISE-PIC pxGrid 証明書、または CSR を生成するオプションがあります。

関連項目

- 自己署名証明書の使用 （5 ページ）
- CA 署名付き証明書の使用 （6 ページ）
- Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要 （1 ページ）
- ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）
- ISE/ISE-PIC サービスへの接続 （9 ページ）

自己署名証明書の使用

自己署名証明書が ISE/ISE-PIC サーバーで使用される場合は、ISE/ISE-PIC サーバーで開発された ISE/ISE-PIC pxGrid 証明書、 Secure Web Applianceで開発された Web Appliance クライアント証明書を、ISE/ISE-PIC サーバー上の信頼できる証明書ストアに追加する必要があります（**ISE** の場合は [管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]、**ISE-PIC** の場合は [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]）。

注意 認証に自己署名証明書を使用するのは、他の認証方法ほど安全ではないためお勧めしません。また、自己署名証明書は失効ポリシーをサポートしていません。

CA 署名付き証明書の使用

CA 署名付き証明書の場合：

- ISE/ISE-PIC サーバーで、Web Appliance クライアント証明書に適した CA ルート証明書が信頼できる証明書ストアにあることを確認します（[管理（Administration）] > [証明書（Certificates）] > [信頼できる証明書（Trusted Certificates）]）。
- Secure Web Applianceで、適切な CA ルート証明書が信頼できる証明書リストにあることを確認します（[ネットワーク（Network）] > [証明書管理（Certificate Management）] > [信頼できるルート証明書の管理（Manage Trusted Root Certificates）]）。
- [Identity Services Engine] ページ（[ネットワーク（Network）] > [Identity Services Engine]）で、ISE/ISE-PIC pxGrid 証明書用の CA ルート証明書がアップロードされていることを確認します。

フォールバック認証

ISE/ISE-PIC で利用できないユーザー情報については、フォールバック認証を設定できます。フォールバック認証が成功するには、次のものが必要です。

- Active Directory ベースのレルムのフォールバックオプションで設定された識別プロファイル。
- フォールバックオプションを含む正しい識別プロファイルを使用したアクセスポリシー。

ISE/ISE-PIC サービスを統合するためのタスク

（注）
- ISE/ISE-PIC バージョン 2.4、および PxGrid バージョン 2.0 がサポートされます。
- ISE-PIC で既存のアクセス ポリシーの使用を続行するには、ISE-PIC を使用する各識別プロファイルを編集してユーザーを透過的に識別する必要があります。これは、CDA を使用した識別プロファイルに適用されます。CDA 識別から ISE-PIC ベースの識別に移行している場合は、それぞれの識別プロファイルを編集する必要があります。

（注）

- AsyncOS 11.5 以前のバージョンから AsyncOS 11.7 以降のバージョンにアップグレードする場合は、 Secure Web Applianceで ISE を再設定します。
- 証明書は ISE/ISE-PIC デバイスを介して生成する必要があり、生成された証明書は Secure Web Applianceにアップロードする必要があります。

ステップ	タスク	トピックおよび手順へのリンク
1	ISE/ISE-PIC デバイスを介した証明書の生成。	ISE/ISE-PIC を介した証明書の生成 （8 ページ）
2	Secure Web Applianceにアクセスするために ISE/ISE-PIC を設定する。	Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定 （8 ページ）
3	Secure Web Applianceで ISE/ISE-PIC サービスを設定および有効にする。	ISE/ISE-PIC サービスへの接続 （9 ページ）
4	Secure Web Appliance クライアント証明書が自己署名済みの場合は、 ISE/ISE-PIC にインポートする。	自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート （12 ページ） 自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート （12 ページ）
5	必要に応じて、 Secure Web Applianceでロギングを設定する。	ISE/ISE-PIC へのロギングの設定 （14 ページ）
6	ISE/ISE-PIC ERS サーバーの詳細を取得します。	ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得 （15 ページ）

関連項目

- Identity Services Engine（ISE）/ ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要 （1 ページ）
- ISE/ISE-PIC の証明書 （5 ページ）
- Identity Services Engine に関する問題のトラブルシューティング （19 ページ）

ISE/ISE-PIC を介した証明書の生成

（注） ISE/ISE-PIC デバイスを介して生成される証明書は、PKCS12 形式である必要があります。

- **ISE/ISE-PIC**：

手順

ステップ 1 [ワークセンター（Work Centers）] > [PassiveID] > [サブスクライバ（Subscribers）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書のダウンロード形式（Certificate Download Format）] ドロップダウンリストから [PKCS12形式（PKCS 12 format）] を選択します。[証明書（Certificates）] タブでその他の必要な情報を入力し、pxGrid 証明書を生成します。

ステップ 3 次の `openssl` コマンドを使用して、生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出します。

- **ルート CA**： openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Web Appliance クライアント証明書**：openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Web Appliance クライアントキー**：openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

（注）
証明書パスワードは、手順 2 の実行中に ISE Web インターフェイスで入力したものを使用してください。

（注）
セカンダリ/フェールオーバー ISE サーバーを介してセカンダリルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成するには、同じ手順を実行します。

Secure Web Applianceにアクセスするための ISE/ISE-PIC サーバーの設定

- **ISE**
  - 識別トピックサブスクライバ（Secure Web Applianceなど）がリアルタイムでセッションコンテキストを取得できるように、各 ISE サーバーを設定する必要があります。
    1. **[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [設定（Settings）] > [pxGridの設定（pxGrid Settings）]** を選択します。
    2. **[新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）]** がオンになっていることを確認します。

ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

ISE サーバーのフッターが緑で、**「pxGrid に接続されました（Connected to pxGrid）」**と表示されていることを確認します。

- **ISE-PIC**
  - 識別トピックサブスクライバ（Secure Web Applianceなど）がリアルタイムでセッションコンテキストを取得できるように、各 ISE-PIC サーバーを設定する必要があります。
    1. **[サブスクライバ（Subscribers）] > [設定（Settings）]** を選択します。
    2. **[新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）]** がオンになっていることを確認します。

  ISE/ISE-PIC での認証に関与しない、設定済みの古い Secure Web Applianceをすべて削除します。

  ISE サーバーのフッターが緑で、**「pxGrid に接続されました（Connected to pxGrid）」**と表示されていることを確認します。

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

ISE/ISE-PIC サービスへの接続

（注） ISE 管理証明書、pxGrid 証明書、および MNT 証明書がルート CA 証明書によって署名されている場合は、アプライアンスで [ISE pxGrid ノード証明書（ISE pxGrid Node Certificate）] フィールドにルート CA 証明書自体をアップロードします（[ネットワーク（Network）] > [Identity Services Engine]）。

始める前に

- 各 ISE/ISE-PIC サーバーが Secure Web Applianceへのアクセス用に正しく設定されていることを確認します（ISE/ISE-PIC サービスを統合するためのタスク （6 ページ）を参照）。
- 有効な ISE/ISE-PIC 関連の証明書およびキーを取得します。関連情報については、ISE/ISE-PIC を介した証明書の生成 （8 ページ）を参照してください。
- 取得した RootCA.pem を Secure Web Applianceにインポートします（[ネットワーク（Network）] > [CertificateManagement] > [TrustedRootCertificate] > [ManageTrustedRootCertificate 上のクライアント（Client on ManageTrustedRootCertificate）]）。生成された XXX.pk12 ファイルからルート CA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを抽出するには、ISE/ISE-PIC を介した証明書の生成 （8 ページ）を参照してください。

（注） セカンダリ XXXX.pk12 ファイルから抽出された RootCA.pem について同じ手順に実行します（セカンダリ/フェールオーバー ISE サーバーが使用可能な場合）。

- Secure Web Applianceの Web インターフェイスで ISE 設定ページを使用して、ISE または ISE-PIC サーバーの設定、証明書のアップロード、ISE または ISE-PIC のいずれかのサービスへの接続を実行します。ISE と ISE-PIC を設定する手順は同じです。ISE-PIC 設定に固有の詳細が適宜記載されています。
- ISE/ISE-PIC が提供する Active Directory グループを使用してアクセスポリシーを構築する場合は、ERS を有効にします。
- AsyncOS 15.0 リリースの一部として、OpenSSL バージョン 1.1.1 およびライブラリは IP ベースの証明書を受け入れなくなりました。[テスト開始（Start Test）] が成功し、ISE が期待どおりに機能することを確認するには、SWA ISE 設定でホスト名のみを使用する必要があります。

手順

ステップ 1 [ネットワーク（Network）] > [Identification Service Engine] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ISE/ISE-PIC を初めて設定する場合は、[設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3 [ISEサービスを有効にする（Enable ISE Service）] をオンにします。

ステップ 4 ホスト名または IPv4 アドレスを使用して**プライマリ管理ノード**を特定し、 Secure Web Applianceの [プライマリ ISE pxGrid ノード（Primary ISE pxGrid Node）] タブに次の情報を入力します。

a) Secure Web Appliance-ISE/ISE-PIC データサブスクリプション（ISE/ISE-PIC サーバーに対して進行中のクエリー）用の **ISE pxGrid ノード証明書**を指定します。

プライマリ ISE サーバーからルート CA として生成される証明書（つまり、RootCA.pem）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、ISE/ISE-PIC を介した証明書の生成（8 ページ）を参照して [ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書およびキーのアップロードを参照してください。

ステップ 5 フェールオーバー用に 2 台目の ISE/ISE-PIC サーバーを使用している場合は、ホスト名または IPv4 アドレスを使用してその**プライマリ管理ノード**を特定し、ホスト名または IPv4 アドレスを使用して Secure Web Applianceの [セカンダリ ISE pxGrid ノード（Secondary ISE pxGrid Node）] タブに次の情報を入力します。

a) セカンダリ **ISE pxGrid ノード証明書**を入力します。

セカンダリ ISE サーバーからルート CA として生成される証明書（つまり、**RootCA.pem**）（または、すべての中間証明書を含む証明書チェーン）を参照して選択し、ISE/ISE-PIC を介した証明書の生成 （8 ページ）を参照して [ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書およびキーのアップロードを参照してください。

（注）
プライマリからセカンダリの ISE サーバーにフェールオーバーするときに、既存の ISE SGT キャッシュに含まれていないユーザーは、 Secure Web Applianceの設定に応じて、認証が必要になるか、またはゲスト認証が割り当てられます。ISE フェールオーバーが完了すると、通常の ISE 認証が再開されます。

ステップ 6 Secure Web Appliance-ISE/ISE-PIC サーバーの相互認証用の **Web Appliance クライアント証明書**を指定します。

- **[アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）]**

  証明書とキーの両方に対して、[選択（Choose）] をクリックして各ファイルを参照します。

  （注）
  ISE/ISE-PIC デバイスを介して生成された publicCert.pem と privateKey.pem を選択してアップロードします。「ISE/ISE-PIC を介した証明書の生成 （8 ページ）」を参照してください。

  キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] チェックボックスをオンにします。

  [ファイルのアップロード（Upload Files）] をクリックします。（このオプションの詳細については、証明書およびキーのアップロードを参照してください）。

ステップ 7 ISE SGT eXchange Protocol（SXP）サービスを有効にします。

Secure Web Applianceが ISE サービスから SXP バインディングトピックを取得する方法については、SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 （17 ページ）を参照してください。

ステップ 8 ISE 外部 Restful サービス（ERS）を有効にします。

- ERS 管理者のユーザー名とパスワードを入力します。ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得 （15 ページ）を参照。
- ERS が同じ ISE または ISE/ISE-PIC pxGrid ノードで使用可能な場合は、[ISE pxGrid ノードと同じサーバー名（Server name same as ISE pxGrid Node）] チェックボックスを確認します。同じノードで使用できない場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスを入力します。

ステップ 9 **[テスト開始（Start Test）]** をクリックして、ISE/ISE-PIC の pxGrid ノードと同じ接続をテストします。

ステップ 10 [送信（Submit）] をクリックします。

次のタスク

- ユーザーおよびクライアント ソフトウェアの分類

- インターネット要求を制御するポリシーの作成

関連情報

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html 特に「How To Integrate Cisco Secure Web Appliance using ISE/ISE-PIC and TrustSec through pxGrid..」。

自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC スタンドアロン展開へのインポート

基本的な手順は以下のとおりです。

- **ISE 管理ノード**
  - **[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

  次のオプションがオンになっていることを確認してください。
  - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
  - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
  - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

- **ISE-PIC 管理ノード**
  - **[証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

    次のオプションがオンになっていることを確認してください。
    - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
    - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
    - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

自己署名 Secure Web Appliance クライアント証明書の ISE/ISE-PIC 分散型展開へのインポート

基本的な手順は以下のとおりです。

- **ISE 管理ノード**：

- **[管理（Administration）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

次のオプションがオンになっていることを確認してください。

- [ISE内の認証用に信頼する（Trust for authentication within ISE）]
- [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
- [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

- **ISE-PIC 管理ノード**：
  - **[証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] > [インポート（Import）]** の順に選択します。

    次のオプションがオンになっていることを確認してください。
    - [ISE内の認証用に信頼する（Trust for authentication within ISE）]
    - [クライアント認証およびsyslog用に信頼する（Trust for client authentication and Syslog）]
    - [シスコサービスの認証用に信頼する（Trust for authentication of Cisco Services）]

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

（注） 分散型 ISE 展開では、 Secure Web Applianceは MNT、PAN、および PxGrid ノードと通信します。この場合、証明書またはすべての証明書の発行者が、「抽出されたルート証明書」（つまり、ISE/ISE-PIC デバイスを介して生成された RootCA）で使用できる必要があります。「ISE/ISE-PIC を介した証明書の生成 （8 ページ）」を参照してください。

手順

ステップ 1 ISE/ISE-PIC を介した証明書の生成 （8 ページ）の手順に従って、RootCA、Web Appliance クライアント証明書、および Web Appliance クライアントキーを生成します。

ステップ 2 **ISE/ISE-PIC 管理ノード**で、[ISE/ISE-PIC] > [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] から自己署名証明書を手動でエクスポートします。

1. [pxGrid]、[EAP認証（EAP Authentication）]、[管理（Admin）]、[ポータル（Portal）]、[RADIUS DTLS] のいずれかによって使用されている（Used by）証明書を選択します。
2. [エクスポート（Export）] をクリックし、生成された .pem ファイルを保存します。

すべての ISE/ISE-PIC 分散ノードについて上記の手順を繰り返します。

ステップ 3 `openssl` コマンドを使用して、ダウンロードした証明書ファイルを RootCA.pem に手動で追加します。ISE/ISE-PIC デバイスを介して RootCA.pem で証明書ファイルを生成および抽出する方法については、ISE/ISE-PIC を介した証明書の生成 （8 ページ）を参照してください。

1. ダウンロードした証明書に対して次のコマンドを実行します。

   ```
   Example:

   openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

   例（出力）：

   Issuer: CN=isehcamnt2.node
   Subject: CN=isehcamnt2.node
   ```

2. 内容を次のように変更します。

   ```
   Example:
   Subject=/CN=isehcamnt2.node
   Issuer=/CN=isehcamnt2.node
   ```

3. RootCA.pem に次の行を追加します。

   ```
   Bag Attributes: <Empty Attributes>
   ```

4. 手順 (2) のサブジェクトおよび発行者を RootCA.pem に（手順 (3) の行とともに）追加します。

   ```
   Example:
   Bag Attributes: <Empty Attributes>
   Subject=/CN=isehcamnt2.node
   Issuer=/CN=isehcamnt2.node
   ```

5. ダウンロードした証明書ファイルの内容全体をコピーし、RootCA の末尾（手順 (4) のデータの後）に貼り付けます。

   ダウンロードされたすべての分散型 ISE/ISE-PIC ノードの証明書について手順 (1) ～ (5) を繰り返し、変更された RootCA 証明書を保存します。

ステップ 4 Secure Web Applianceの ISE 設定ページで、変更された RootCA.pem をアップロードします。ISE/ISE-PIC サービスへの接続 （9 ページ） を参照してください。

ISE/ISE-PIC へのロギングの設定

- 認証メカニズムをログ記録するために、アクセスログにカスタムフィールド%mを追加します（アクセス ログのカスタマイズ）。
- ISE/ISE-PIC サービスログが作成されていることを確認します。作成されていない場合は作成します（ログ サブスクリプションの追加および編集）。
- ユーザーの識別と認証のために ISE/ISE-PIC にアクセスする識別プロファイルを定義します（「ユーザーおよびクライアントソフトウェアの分類」、117 ページ）。
- ISE/ISE-PIC ID を使用して、ユーザー要求の条件とアクションを定義するアクセスポリシーを設定します（「ポリシーの設定」、191 ページ）。

ISE/ISE-PIC からの ISE/ISE-PIC ERS サーバー詳細情報の取得

- ISE/ISE-PIC で Cisco ISE の REST API（API で HTTPS ポート 9060 を使用）を有効にします。

（注） グループに基づいてセキュリティポリシーを設定するには、Secure Web Applianceで ISE 外部 RESTful サービス（ERS）を有効にする必要があります（[ネットワーク（Network）] > [Identity Services Engine]）。これは、バージョン 11.7 以降に適用されます。

  - **ISE**
    - **[管理（Administration）] > [設定（Settings）] > [ERS設定（ERS Settings）] > [プライマリ管理ノードのERS設定（ERS settings for primary admin node）] > [ERSを有効化する（Enable ERS）]** を選択します。

      セカンダリ ノードがある場合は、**[その他すべてのノードの読み取り用ERS（ERS for Read for All Other Nodes）]** を有効にします。

  - **ISE-PIC**
    - **[設定（Settings）] > [ERS設定（ERS Settings）] > [ERSを有効化する（Enable ERS）]** を選択します。

- 正しい外部 RESTful サービス グループで ISE 管理者を作成していることを確認します。外部 RESTful サービス管理者グループには、ERS API へのフル アクセス（GET、POST、DELETE、PUT）が含まれています。このユーザーは、ERS API 要求を作成、読み取り、更新、および削除できます。外部 RESTful サービス オペレータ：読み取り専用アクセス（GET 要求のみ）。
  - **ISE**
    - **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザー（Admin Users）]** を選択します。

  - **ISE-PIC**
    - **[管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者ユーザー（Admin Users）]** を選択します。

ERS サービスが ISE/ISE-PIC pxGrid ノードではなく別のサーバーで使用可能な場合は、プライマリおよびセカンダリ（設定されている場合）サーバーのホスト名または IPv4 アドレスが必要です。

詳細については、Cisco *Identity Services Engine* のドキュメントを参照してください。

ISE-SXP 統合の設定

このセクションは、次のトピックで構成されています。

- SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて （16 ページ）
- 注意事項と制約事項 （16 ページ）
- 前提条件 （17 ページ）
- SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 （17 ページ）
- ISE-SXP プロトコルのコンフィギュレーションの確認 （18 ページ）

SGT から IP へのアドレスマッピングの ISE-SXP プロトコルについて

SGT Exchange Protocol（SXP）は、ネットワークデバイス間で IP-SGT バインディングを伝播するために開発されたプロトコルです。セキュリティグループタグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。

Cisco Identity Services Engine（ISE）の展開を Cisco Secure Web Applianceと統合して、パッシブ認証に使用できます。 Secure Web Applianceは、ISE から SXP マッピングをサブスクライブできます。ISE は SXP を使用して、SGT から IP へのアドレス マッピング データベースを管理対象デバイスに伝播します。ISE サーバーを使用するように Secure Web Appliance を設定する場合は、ISE から SXP トピックをリッスンするオプションを有効にします。これにより、 Secure Web Applianceは ISE から直接 SGT と IP アドレスマッピングについて学習します。

Secure Web Applianceは、ダミーのユーザー認証 IP アドレスを生成します。これには、ISE クラスタの IP アドレスとクライアントの IP アドレスが含まれます。したがって、複数のクライアント IP アドレスをクラスタ IP アドレスで認証できます。

注意事項と制約事項

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関するガイドラインと制限は次のとおりです。

- IPv6 対応のエンドポイントは、 Secure Web Appliance リリース 14.5 ではサポートされません。
- Secure Web Appliance リリース 14.5 では、ユーザー名とグループマッピングは、SGT から IP アドレスへのマッピングでは使用できません。したがって、管理者は Secure Web Applianceの ISE ユーザーおよびグループに基づいてポリシーを作成することはできません。ただし、SGT を使用してポリシーを作成できます。
- 一括ダウンロードプロセスの再起動タイムスタンプをスケジュールするには、isedプロセスを再起動する時刻を HH::MM 形式（24 時間）で設定する必要があります。

（注） ユーザー認証プロセスが示される時刻は 1 日の中で短時間に設定することをお勧めします。たとえば、00:00 時に設定します。

前提条件

SGT から IP アドレスへのマッピングの ISE-SXP プロトコルに関する前提条件は次のとおりです。

- 信頼できるルート証明書が必要です。信頼できるルート証明書を追加するには、「信頼できるルート証明書の管理」を参照してください。

SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化

SGT から IP アドレスへのマッピングを含む、ISE で定義されているすべてのマッピングは、SXP を介して公開できます。次のメカニズムを使用して、ISE-SXP 情報を取得できます。

- 一括ダウンロード：ised プロセスの再起動後、 Secure Web Applianceは、集約ノードで使用可能なすべての ISE-SXP エントリの情報を取得するために、一括ダウンロード要求を ISE アグリゲータノードに送信します。AsyncOS コマンドラインインターフェイス（CLI）を使用して、再起動のタイムスタンプをスケジュールできます。
- 差分更新： Secure Web Applianceは、WebSocket を介して登録し、差分更新メッセージを取得します。メッセージには次の 2 つのタイプがあります。
  - 作成：新しく作成されたすべてのエントリ
  - 削除：すべての SXP 更新エントリ

（注） Secure Web Applianceは、更新されたエントリごとに 2 つのメッセージ（「削除（Delete）」の後に「作成（Create）」）を受信します。

再起動をスケジュールすることができます。

手順

ステップ 1 **[ネットワーク（Network）] > [Identification Service Engine]**を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [ISEサービスを有効にする（Enable ISE Service）] をオンにします。

ステップ 4 Secure Web Applianceで ISE サービスから SXP バインディングトピックを取得できるようにするには、[有効（Enable）] をオンにします。

デフォルトでは、ISE SGT eXchange Protocol（SXP）サービスは無効になっています。

ステップ 5 [テスト開始（Start Test）] をクリックして接続をテストします。

（注）
SXP 情報は、ISE-SGT eXchange Protocol（SXP）サービスが有効になっている場合にのみ表示されます。

ステップ 6 **[送信（Submit）]** をクリックします。

ISE-SXP プロトコルのコンフィギュレーションの確認

次のいずれかの方法を使用して、ISE-SXP プロトコルのコンフィギュレーションを確認できます。

- SGT から IP へのアドレスマッピングの ISE-SXP プロトコルの有効化 （17 ページ） で [テスト開始（Start Test）] をクリックして、表示された情報を確認します。
- AsyncOS コマンド ライン インターフェース（CLI）の **ISEDATA** コマンドの下で **STATISTICS** コマンドを使用します。

STATISTICS コマンドを使用すると、次の情報が表示されます。

- ERS ホスト名
- ERS 接続時間
- セッション一括ダウンロード
- グループ一括ダウンロード
- SGT 一括ダウンロード
- SXP 一括ダウンロード
- セッションの更新
- グループの更新
- SXP の更新
- Memory Allocation
- メモリの割り当て解除
- Total Session Count

ユーザー名は次の形式で生成されます。

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

例：isesxp_10.10.2.68_sgt18_10.10.10.10

ISE/ISE-PIC 統合での VDI（仮想デスクトップ インフラストラクチャ）ユーザー認証

使用される送信元ポートに基づいて VDI 環境のユーザーの ISE/ISE-PIC による透過的な識別を設定できます。

Cisco Terminal Services（TS）エージェントを VDI サーバーにインストールする必要があります。Cisco TS エージェントは、ISE/ISE-PIC にアイデンティティ情報を提供します。アイデンティティ情報には、ドメイン、ユーザー名、および各ユーザーが使用するポート範囲が含まれます。

- サポートサイト（https://www.cisco.com/c/en/us/support/index.html）から Cisco TS エージェントをダウンロードします。
- 詳細については、『Cisco Terminal Services (TS) Agent Guide』（https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html）を参照してください。
- Cisco TS エージェントと連携するように ISE/ISE-PIC API プロバイダを設定します。API コールの送信については、Cisco TS エージェントのドキュメントを参照してください。

（注）
- VDI 環境ユーザーのフォールバック認証はサポートされていません。
- シスコ ターミナル サービス エージェントと Microsoft サーバー設定で、リモート デスクトップセッションの最大数が同じであることを確認します。これにより、誤ったセッション情報が ISE から Secure Web Applianceに送信されないようにし、新しいセッションの誤認証が回避されます。

Identity Services Engine に関する問題のトラブルシューティング

- Identity Services Engine に関する問題
  - ISE 問題のトラブルシューティング ツール
  - ISE サーバーの接続に関する問題
  - ISE 関連の重要なログ メッセージ

Cisco SecureX および Cisco Threat Response との統合

この章で説明する内容は、次のとおりです。

- アプライアンスと Cisco SecureX および Cisco Threat Response の統合 （20 ページ）
- アプライアンスと Cisco SecureX および Cisco Threat Response の統合方法 （21 ページ）
- Secure Web Applianceでの Cisco Cloud Services ポータルの有効化 （24 ページ）
- Cisco Cloud Services ポータルへの Secure Web Applianceの登録 （24 ページ）
- Cisco SecureXRibbonを使用した脅威分析の実行 （25 ページ）

アプライアンスと Cisco SecureX および Cisco Threat Response の統合

Cisco SecureXは、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。これは新しいテクノロジーを導入する必要のないクラウドネイティブです。Cisco SecureX は、可視性を統合し、自動化を可能にして、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティを強化するプラットフォームを提供することで、脅威からの保護の要求を簡素化します。統合プラットフォームで技術を連携することで、Cisco SecureX は測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。Cisco SecureX では、セキュリティ インフラストラクチャを連携させて機能を拡張できます。

アプライアンスと Cisco SecureX および Cisco Threat Response の統合には、次のセクションが含まれています。

- アプライアンスと Cisco SecureX および Cisco Threat Response の統合方法 （21 ページ）
- Cisco SecureXRibbonを使用した脅威分析の実行 （25 ページ）

アプライアンスを Cisco SecureX および Cisco Threat Response と統合し、Cisco SecureX および Cisco Threat Response で以下のアクションを実行できます。

- 組織内の複数のアプライアンスから Web データを表示および送信します。
- Web レポートおよびトラッキングで検出された脅威を特定、調査、修正します。
- 侵害された URL または Web トラフィックをブロックします。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。
- 悪意のあるドメインのブロック、不審な観測対象の追跡、承認ワークフローの開始、または Web ポリシーを更新するための IT チケットの作成を行います。

Cisco SecureX および Cisco Threat Response には、次の URL を使用してアクセスできます。

https://securex.us.security.cisco.com/login

Cisco Secure Web Applianceは高度な脅威防御機能を備え、脅威を迅速に検出、ブロック、修復します。また、データの損失を防ぎ、送信中の重要情報をエンドツーエンドの暗号化によって保護します。 Secure Web Appliance モジュールで強化できる観測対象の詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動し、Cisco SecureX と統合するモジュールに移動して、**[詳細情報（Learn More）]** をクリックしてください。

Cisco Secure Web Appliance を SecureX と統合すると、Cisco Secure Web Appliance の Web トラッキングデータが検証されます。トランザクション タイムアウト（60 秒）は、Cisco Secure Web Appliance での処理遅延が原因で発生し、統合が失敗します。正常に統合するには、統合の時間制限をデフォルトの 30 日から 1 日または 2 日に短縮します。ただし、この短縮を行うと Cisco Secure Web Appliance のモニタリングの有効性に影響します。

アプライアンスと Cisco SecureX および Cisco Threat Response の統合方法

表 *2 :* アプライアンスと *Cisco SecureX* および *Cisco Threat Response* の統合方法

	操作手順	詳細
ステップ 1	前提条件を確認します。	前提条件 （21 ページ）
ステップ 2	Secure Web Applianceで、Cisco SecureX または Cisco Threat Response の統合を有効にします。	Cisco Secure Web Applianceでの Cisco SecureX または Threat Response の統合の有効化 （22 ページ）
ステップ 3	Cisco SecureX で、アプライアンスをデバイスとして追加し、登録して、登録トークンを生成します。	詳細については、次を参照してください。https://securex.us.security.cisco.com/help/settings-devices
ステップ 4	Secure Web Applianceで、Cisco SecureX または Cisco Threat Response の登録を完了します。	Cisco Secure Web Applianceでの Cisco SecureX または Cisco Threat Response の登録 （23 ページ）
ステップ 5	登録が成功したかどうかを確認します。	登録が成功したかどうかの確認 （23ページ）
ステップ 6	Cisco SecureX で、Web セキュリティ アプライアンス モジュールを追加します。	詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Secure Web Appliance モジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

前提条件

（注） すでに Cisco Threat Response のユーザーアカウントをお持ちの場合は、Cisco SecureX のユーザーアカウントを作成する必要はありません。Cisco Threat Response ユーザーアカウントのログイン情報を使用して Cisco SecureX にログインできます。

- 管理者アクセス権を使用して、Cisco SecureX でユーザアカウントを作成していることを確認します。新しいユーザーアカウントを作成するには、URL（https://securex.us.security.cisco.com/login）を使用して **Cisco SecureX のログイン**ページに

移動し、ログインページで**[SecureXサインオンアカウントの作成（Create a SecureX Sign-on Account）]**をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

- （プロキシサーバーを使用していない場合のみ。）ファイアウォールで HTTPS（インおよびアウト）443 ポートが次の FQDN に対してオープンになっていることを確認して、アプライアンスを Cisco SecureX または Cisco Threat Response に登録できるようにしてください。
  - api-sse.cisco.com（NAM ユーザのみに対応）
  - api.eu.sse.itd.cisco.com（欧州連合（EU）のユーザのみに対応）
  - api.apj.sse.itd.cisco.com（APJC ユーザのみに対応）
  - est.sco.cisco.com（APJC、EU、および NAM ユーザに対応）

Cisco Secure Web Applianceでの Cisco SecureX または Threat Response の統合の有効化

手順

ステップ 1 アプライアンスにログインします。

ステップ 2 [ネットワーク（Networks）] > [クラウドサービス設定（Cloud Service Settings）] を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 5 アプライアンスを Cisco SecureX または Cisco Threat Response に接続するために必要な Cisco SecureX または Cisco Threat Response サーバーを選択します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、[登録（Register）] ボタンがアプライアンスに表示されるかどうかを確認します。

次のタスク

アプライアンスを Cisco SecureX または Cisco Threat Response に登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動して、Cisco SecureX と統合するモジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

Cisco Secure Web Applianceでの Cisco SecureX または Cisco Threat Response の登録

手順

ステップ 1 [ネットワーク（Network）] > [クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [クラウドサービス設定（Cloud Services Settings）] に、登録トークンを入力し、[登録（Register）] をクリックします。

（注） CLI を使用して Cisco SecureX または Cisco Threat Response を登録するには、`cloudserviceconfig` コマンドを使用します。

次のタスク

登録が成功したかどうかの確認 （23 ページ）

登録が成功したかどうかの確認

- Security Services Exchange で、Security Services Exchange のステータスを確認して、正常に登録されたことを確認します。
- Cisco SecureX で、[デバイス（Devices）] ページに移動し、Security Services Exchange に登録されている Secure Web Appliance を表示します。

（注） 別の Cisco SecureX サーバーまたは Cisco Threat Response サーバー（欧州用の「api.eu.sse.itd.cisco.com」など）に切り替える場合は、最初に Cisco SecureX または Cisco Threat Response からアプライアンスの登録を解除して、アプライアンスと Cisco SecureX および Cisco Threat Response の統合方法 （21 ページ）のステップを実行する必要があります。

アプライアンスを Cisco SecureX または Cisco Threat Response と統合した後は、Cisco Security Management アプライアンスを Cisco SecureX または Cisco Threat Response と統合する必要はありません。

Security Services Excange にアプライアンスが正常に登録されたら、Cisco SecureX に Secure Web Appliance Web モジュールを追加します。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックしてページに記載されている手順を参照してください。

Secure Web Applianceでの Cisco Cloud Services ポータルの有効化

手順

ステップ 1 Secure Web Appliance にログインします。

ステップ 2 [ネットワーク（Networks）] > [クラウドサービス設定（Cloud Service Settings）] を選択します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 [Cisco Cloud Servicesの有効化（Enable Cisco Cloud Services）] チェックボックスをオンにします。

ステップ 5 必要な Cisco Secure サーバーを選択して、 Secure Web Applianceを Cisco Cloud Services ポータルに接続します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、[登録（Register）] ボタンが [クラウドサービス設定（Cloud Services Settings）] ページに表示されるかどうかを確認します。

（注） CLI を使用して Cisco Cloud Services ポータルを有効にするには、`cloudserviceconfig` コマンドを使用します。

次のタスク

Cisco Cloud Services ポータルに Secure Web Applianceを登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックしてページに記載されている手順を参照してください。

Cisco Cloud Services ポータルへの Secure Web Applianceの登録

手順

ステップ 1 [ネットワーク（Network）] > [クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [クラウドサービス設定（Cloud Services Settings）] の下に、登録トークンを入力し、**[登録（Register）]** をクリックします。

（注） CLI を使用して Secure Web Applianceを Cisco Cloud Services ポータルに登録するには、`cloudserviceconfig` コマンドを使用します。

アプライアンスにスマートライセンスが登録されている場合は、Cisco Cloud サービスを無効化または登録解除できません。

Cisco SecureXRibbonを使用した脅威分析の実行

（注） AsyncOS 14.0 以前のバージョンからダウングレードする場合、**ケースブック**は Cisco SecureX Ribbon の一部となります。

Cisco SecureX は、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能をサポートします。Cisco SecureX の分散機能は、SecureX リボンでアプリケーションおよびツールの形式で利用できます。

この章で説明する内容は、次のとおりです。

- Cisco SecureX Ribbon へのアクセス （26 ページ）
- Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （27 ページ）

Cisco SecureX Ribbon はページの下部ペインにあり、ダッシュボードと環境内の他のセキュリティ製品間を移動しても保持されます。Cisco SecureX Ribbon は、次のアイコンと要素で構成されています。

- [リボンの展開/縮小（Expand/Collapse Ribbon）]
- Home
- ケースブックアプリ
- Incidents アプリ
- Orbital アプリ
- [エンリッチメント（Enrichment）] 検索ボックス
- 観測対象の検索
- 設定

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Ribbon へのアクセス

始める前に

前提条件 （21 ページ）に記載されているすべての前提条件を満たしていることを確認してください。

（注） AsyncOS の以前のバージョンで**ケースブック**を設定していたものとします。次の手順で説明するように、追加のスコープを持つ Cisco SecureX API クライアントで新しい [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成する必要があります。

ボタンを使用して、ページの下部ペインにある Cisco SecureX リボンを右からドラッグできます。

手順

ステップ 1 アプライアンスの新しいWebインターフェイスにログインします。詳細については、新しいWebインターフェイスの Web レポート ページの概要を参照してください。

ステップ 2 [Cisco SecureX Ribbon] をクリックします。

ステップ 3 **SecureX API クライアント**で[クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成します。API クライアントのクレデンシャルを生成する方法の詳細については、「Creating an API Client」を参照してください。

クライアント ID とクライアントパスワードの作成時には、次の範囲を選択してください。

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (アクセス権がある場合)

ステップ 4 アプライアンスの **[SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）]** ダイアログボックスのステップ 3 で取得したクライアント ID とクライアントパスワードを入力します。

ステップ 5 [SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）] ダイアログボックスで必要な Cisco SecureX サーバを選択します。

ステップ 6 [認証（Authenticate）] をクリックします。

（注）
クライアントID、クライアントパスワード、およびCisco SecureXサーバを編集する場合は、Cisco SecureXリボンを右クリックして詳細を追加します。

次のタスク

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （27 ページ）

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加

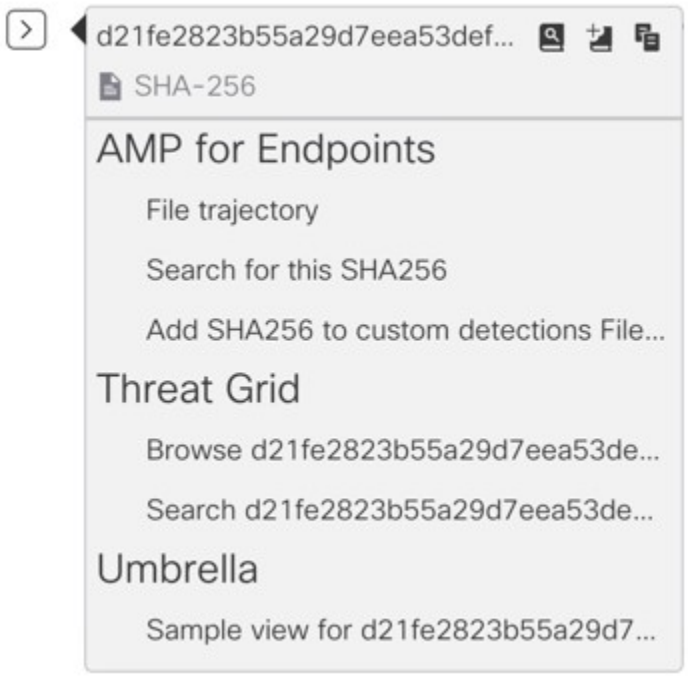
始める前に

アプライアンスの Cisco SecureX Ribbon とピボット メニュー ウィジェットにアクセスするには、クライアントID とクライアントパスワードを取得します。詳細については、Cisco SecureX Ribbon へのアクセス （26 ページ）を参照してください。

手順

ステップ 1 アプライアンスの新しいWebインターフェイスにログインします。詳細については、新しいWebインターフェイスの Web レポート ページの概要を参照してください。

ステップ 2 [Web レポート（Web Reporting）] ページへ移動して、該当する観測対象（bit.ly など）の横にあるピボットメニュー ボタンをクリックします。



次の手順を実行します。

- アクティブなケースに観測対象を追加するには、 ボタンをクリックします。
- 新しいケースに観測対象を追加するには、 ボタンをクリックします。

（注）

ピボットメニュー ボタンを使用して、ポータルに登録された他のデバイスの観測対象（ AMP for Endpoints など）をピボットし、攻撃分析の調査を実行します。

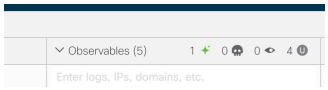
ステップ 3 アイコンにカーソルを合わせ、 ボタンをクリックして**ケースブック**を開きます。観測対象が新しいまたは既存のケースに追加されたかどうかを確認します。

ステップ 4 （オプション） ボタンをクリックして、タイトル、説明、またはメモを**ケースブック**に追加します。

（注） 脅威分析の観測対象を検索するには、次の 2 つの方法があります。

- Cisco SecureX の[エンリッチメント（Enrichment）] 検索ボックスをクリックし、観測対象を検索します。

- Cisco SecureX Ribbon 内の [ケースブック（Casebook）] アイコンをクリックし、



フィールドで観測対象を検索します。

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco Secure Web Appliance と Cisco Umbrella の統合

この章で説明する内容は、次のとおりです。

- Cisco Secure Web Appliance（SWA）と Cisco Umbrella について （29 ページ）
- 統合のためのガイドライン （30 ページ）
- エンドツーエンドの手順 （30 ページ）
- Cisco Secure Web Appliance と Cisco Umbrella を統合する方法 （30 ページ）
- Web ポリシーと接続先リストの設定 （34 ページ）
- AD ユーザーまたは AD グループの設定 （38 ページ）
- Microsoft 365 の互換性の設定 （39 ページ）
- ポリシーの競合管理とポリシーの順序付け （39 ページ）
- ブロックされているページの管理 （40 ページ）
- Cisco Umbrella シームレス ID （40 ページ）

Cisco Secure Web Appliance（SWA）と Cisco Umbrella について

Umbrella は、シスコのクラウドベース Secure Internet Gateway（SIG）プラットフォームです。インターネットベースの脅威に対する防御を複数のレベルで提供します。Umbrella は、セキュア Web ゲートウェイ、ファイアウォール、DNS レイヤセキュリティ、およびクラウド アクセス セキュリティ ブローカ（CASB）機能を統合して、システムを脅威から保護します。

Cisco Umbrella と Cisco Secure Web Appliance の統合により、Cisco Umbrella から Cisco Secure Web Appliance への共通 Web ポリシーの展開が容易になります。Cisco Umbrella ダッシュボードを使用してポリシーを設定したり、ログを表示したりできます。

Cisco Umbrella ダッシュボードで共通 Web ポリシーを設定すると、ポリシーは Cisco Secure Web Appliance にプッシュされます。これらの設定された Web ポリシーのレポートデータは Cisco Umbrella に送り返され、Cisco Umbrella ダッシュボードで使用できます。レポートデータには、参照された URL、その IP アドレス、URL が許可されたかブロックされたかなどの情報が含まれます。

次の URL を使用して Cisco Umbrella にアクセスできます。

https://login.umbrella.com/umbrella

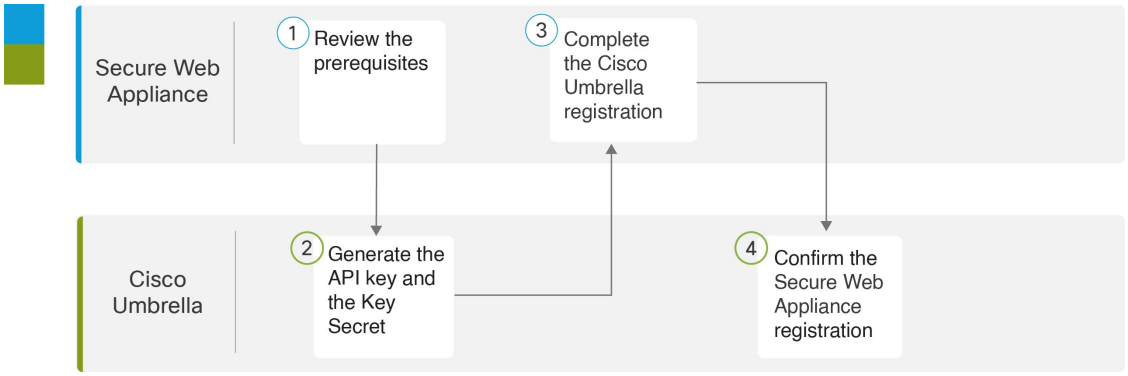
詳細については、『Umbrella Integration with Secure Web Appliance』を参照してください。

統合のためのガイドライン

- Cisco Umbrella でデバイスの登録を正常に完了するには、Cisco Umbrella 組織で有効な範囲の API キーとキーシークレットを取得します。
- Web ポリシーを正しく変換するには、証明書バンドルとカテゴリを Cisco Secure Web Appliance の最新のカテゴリに更新します。

エンドツーエンドの手順

次のフローチャートは、Cisco Secure Web Appliance と Cisco Umbrella を統合するためのワークフローを示しています。



Cisco Secure Web Appliance と Cisco Umbrella を統合する方法

表 *3 : Cisco Secure Web Appliance* と *Cisco Umbrella* を統合する方法

	操作手順	詳細
ステップ 1	Cisco Secure Web Appliance で、前提条件を確認します。	前提条件 （31 ページ）
ステップ 2	Cisco Umbrella で、API キーとキーシークレットを生成します。	「Generate API Keys and Key Secret」
ステップ 3	Cisco Secure Web Appliance で、シスコ登録を完了します。	「Cisco Secure Web Appliance を Cisco Umbrella に登録する」
ステップ 4	Cisco Umbrella で、Cisco Secure Web Appliance の登録を確認します。	「登録が成功したかどうかの確認」

前提条件

Cisco Secure Web Appliance で以下を実行します。

- Cisco Umbrella に正しく接続するには、Cert バンドル（シスコの信頼できるルート証明書バンドル：2.2）を更新します。
- Cisco Umbrella からの変換されたポリシーを正常に設定するには、コンテンツカテゴリ（107）を更新します。
- Cisco Umbrella のルールセットで HTTPS インスペクションが有効になっている場合は、Cisco Secure Web Appliance で HTTPS プロキシを手動で有効にします。
- Cisco Umbrella のルールで選択したアプリケーション設定を正常に変換するには、Cisco Secure Web Appliance で**[セキュリティサービス（Security Services）]** > **[使用許可コントロール（Acceptable Use Controls）]**に移動し、[アプリケーションの検出と制御（ADC）（Application Discovery and Control (ADC)）] を有効にします。
- AD が Cisco Umbrella に統合されている場合は、Cisco Secure Web Appliance で Active Directory（AD）レルムを設定します。正常な AD コネクタとドメインコントローラを使用することをお勧めします。
- AsyncOS バージョン 15.1 にアップグレードするには、スマートライセンスをアクティブにする必要があります。
- 内部ネットワークがパブリックネットワークに関連付けられていること、または Active Directory が Cisco Umbrella と統合されていることを確認します。

Cisco Umbrella で以下を実行します。

Cisco Umbrella の [キースコープ（Key Scopes）] を使用して、[APIキー（API Key）] と [キーシークレット（Key Secret）] を生成します。キーの生成手順については『Cisco Umbrella SIG User Guide』を参照してください。

（注）

- [APIキー（API Key）] と [キーシークレット（Key Secret）]（**[管理（Admin）]** > **[APIキー（API Keys）]**）を生成する際に、特定の組織について、[認証（Auth）]（読み取り専用）として [キースコープ（Key Scope）] を選択し、[展開または登録済みアプライアンス（Deployments/Registered Appliances）]（読み取りまたは書き込み）として [登録済みアプライアンス（Registered Appliances）] を選択していることを確認します。
- [登録済みアプライアンス（Registered Appliance）] ページは、有効なサブスクリプションでのみ表示できます。

Cisco Umbrella から Cisco Secure Web Appliance ポリシーを設定および管理できます。

Cisco Secure Web Appliance を Cisco Umbrella に登録する

手順

ステップ 1 Cisco Secure Web Appliance にログインします。

ステップ 2 **[ネットワーク（Network）] > [Umbrella設定（Umbrella Settings）]**を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [Umbrella設定（Umbrella Settings）] で、[APIキー（API Key）]、[APIシークレット（API Secret）] を入力し、[登録（Register）] をクリックします。

Cisco Secure Web Appliance が登録されると、成功メッセージが表示されます。

（注）
M1 インターフェイスを介してインターネットにアクセスできない場合、パブリック ドメイン（api.umbrella.com）へのアクセスはブロックされ、Umbrella への登録も失敗します。

ステップ 5 Cisco Secure Web Appliance と Cisco Umbrella 間の接続を開始するには、ハイブリッドポリシーを有効にする必要があります。有効にするには、[ハイブリッドポリシー（Hybrid Policy）] チェックボックスをオンにします。

ステップ 6 Cisco Umbrella で設定された Web ポリシーレポートデータを Cisco Secure Web Appliance から Cisco Umbrella レポートダッシュボードに送信するには、[ハイブリッドレポート（Hybrid Reporting）] チェックボックスをオンにします。Cisco Umbrella ダッシュボードは、外部クライアントの IP アドレスに基づいて Cisco Secure Web Appliance レポートデータをフィルタ処理します。

（注）
ハイブリッドポリシーを無効にすると、ハイブリッドレポートも無効になります。

ステップ 7 [ソースインターフェイス（Source Interface）] ドロップダウンリストから [管理（Management）] または [データ（Data）] を選択します。Cisco Secure Web Appliance は、[データポート（Data Port）] がインターフェイスとして設定されている場合にのみ、[データ（Data）] インターフェイスを表示します。

ステップ 8 変更を送信し、保存します。

次のタスク

登録が成功したかどうかの確認 （33 ページ）

（注）

- [ハイブリッドポリシー（Hybrid Policy）] チェックボックスを有効にすると、ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。ポリシーのプッシュが失敗すると、ユーザーは電子メールで通知を受けることができます。この通知は、**[システム管理（System Administration）]** > **[アラート（Alerts）]**で [システム（System）] アラートとして設定できます。
- ハイブリッドレポートを有効にすると、Cisco Umbrella で設定されたポリシーの Cisco Secure Web Appliance レポートデータのみが Cisco Umbrella レポートに送信されます。レポートデータが Cisco Secure Web Appliance によって送信されない場合、ユーザーは電子メールで通知を受けることができます。この通知は、**[システム管理（System Administration）]** > **[アラート（Alerts）]**で [システム（System）] アラートとして設定できます。

登録が成功したかどうかの確認

Cisco Umbrella で、**[展開（Deployments）]** > **[コアアイデンティティ（Core Identities）]** > **[登録済みのアプライアンス（Registered Appliances）]**ページに移動し、Cisco Umbrella に登録されている Cisco Secure Web Appliance デバイスを表示します。

（注）

- 登録済みの Cisco Secure Web Appliance のステータスは、Cisco Secure Web Appliance の [Umbrella設定（Umbrella Settings）] ページで [ハイブリッドポリシー（Hybrid Policy）] チェックボックスをオンにした場合にのみ、アクティブになります。それ以外の場合、Cisco Secure Web Appliance デバイスのステータスはオフラインです。
- Cisco Secure Web Appliance の [Umbrella設定（Umbrella Settings）] ページで [ハイブリッドポリシー（Hybrid Policy）] と [ハイブリッドレポート（Hybrid Reporting）] のチェックボックスをオンにした場合、Cisco Umbrella のハイブリッドレポートのステータスは**アクティブ**になります。
- ポリシー同期のステータスが**失敗**の場合、ステータスにカーソルを合わせるとエラーメッセージが表示されます。
- ポリシー同期のステータスが警告アイコンの付いた**成功**である場合、ステータスにカーソルを合わせると次の警告メッセージが表示されます：「**一部のユーザー/グループが正常な状態でないADコネクタまたはドメインコントローラのルール/ルールセットで選択されている場合は、[展開（Deployments）] > [設定（Configuration）] > [サイトとActive Directory（Sites and Active Directory）] に移動してエラーの詳細を確認し、修正してください。（If a few users/groups have been selected in rules/rulesets from AD Connectors or Domain Controllers which are not in a healthy state, navigate to Deployments > Configuration > Sites and Active Directory to see the error details and fix it.）**」AD の詳細と選択されたユーザー/グループの情報も、警告メッセージで確認できます。

Cisco Umbrella UI の [登録済みアプライアンス（Registered Appliances）] ページにある [ポリシーのプッシュ（Policy Push）] オプションを使用すると、設定した Web ポリシーを選択した Cisco Secure Web Appliance にプッシュできます。

Cisco Umbrella からの Cisco Secure Web Appliance の登録解除

手順

ステップ 1 Cisco Secure Web Appliance にログインします。

ステップ 2 **[ネットワーク（Network）]** > **[Umbrella設定（Umbrella Settings）]**を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 **[ハイブリッドポリシー（Hybrid Policy）]** および **[ハイブリッドレポーティング（Hybrid Reporting）]** チェックボックスをオンにして無効にします。

ステップ 5 変更を保存します。

ステップ 6 **[APIキー（API Key）]**、**[APIシークレット（API Secret）]** を入力し、**[登録解除（Deregister）]** をクリックします。

Cisco Umbrella がプッシュしたポリシーを保持するか削除するかを尋ねられます。[はい（Yes）] を選択すると、Cisco Umbrella がプッシュしたポリシーは、変更がコミットされた後に Cisco Secure Web Appliance から削除されます。

Cisco Umbrella レポーティング ダッシュボードの表示

Cisco Secure Web Appliance は、Cisco Umbrella が設定したポリシー レポーティング データを Cisco Umbrella ダッシュボードに送信します。このレポーティングデータを Cisco Umbrella で表示するには、**[レポーティング（Reporting）]** > **[アクティビティ検索（Activity Search）]**に移動し、**[IDタイプ（Identity Type）]** として **[Cisco Secure Web Appliance（Secure Web Appliance）]** を選択します。

Web ポリシーと接続先リストの設定

統合が成功すると、Web ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。

統合してハイブリッドレポートを有効にしている場合、Cisco Secure Web Appliance は Cisco Umbrella ポリシーに基づいて生成されたレポートデータを Cisco Umbrella レポートダッシュボードに送信します。

次のプロファイルとポリシーは、Cisco Secure Web Appliance に変換されます。

- 識別プロファイルの設定 （35 ページ）
- カスタムおよび外部 URL カテゴリの設定 （35 ページ）

• アクセスポリシーの設定 （35 ページ）
• 復号ポリシーの設定 （36 ページ）
• アクセスポリシーでのアプリケーションの設定 （37 ページ）

識別プロファイルの設定

認証オプション（AD が Cisco Umbrella に統合されている場合）または認証を免除オプション（AD が Cisco Umbrella に統合されていない場合）を持つグローバル識別プロファイルは 1 つだけです。

Cisco Umbrella でルールセットアイデンティティを作成するには、[Webポリシー（Web Policy）] に移動し、ルールセットアイデンティティとして [ネットワーク（Networks）] または [ADユーザー（AD Users）] または [ADグループ（AD Groups）] を選択します。詳細については、https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy#setupを参照してください。

（注） ネットワークアイデンティティに関連付けられた内部ネットワークがあることを確認してください。

Cisco Umbrella で内部ネットワークを作成し（**[展開（Deployments）] > [設定（Configuration）] > [内部ネットワーク（Internal Networks）]**）、パブリックネットワークに関連付けることができます。内部ネットワークは、Cisco Secure Web Appliance のアクセスポリシーおよび復号ポリシーでサブネットとして変換されます。

カスタムおよび外部 URL カテゴリの設定

Cisco Umbrella の接続先リストは、Cisco Secure Web Appliance のカスタムおよび外部 URL カテゴリとして変換されます（**[Webセキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）]**）。

Cisco Umbrella で接続先リストを作成し（**[ポリシー（Policy）] > [ポリシーコンポーネント（Policy Components）] > [接続先リスト（Destination Lists）]**）、Web ポリシーに関連付けます。詳細については、https://docs.umbrella.com/umbrella-user-guide/docs/add-a-destination-listを参照してください。

アクセスポリシーの設定

Cisco Umbrella の Web ポリシー（規則）は、Cisco Secure Web Appliance のアクセスポリシーとして変換されます。

パブリックネットワーク（内部ネットワークが関連付けられている）、内部ネットワーク、AD ユーザー、およびルールアイデンティティとして設定された AD グループを使用して、Cisco Umbrella でルールを作成します。[コンテンツカテゴリ（Content Categories）] または [接続先リスト（Destination Lists）] を使用して接続先を設定します。

詳細については、https://docs.umbrella.com/umbrella-user-guide/docs/add-rules-to-a-ruleset#procedure を参照してください。

変換されたルールを Cisco Secure Web Appliance で表示できます（**[Webセキュリティマネージャ（Web Security Manager）]** > **[アクセスポリシー]** > **[URLフィルタリング（URL Filtering）]**）。

アクセスポリシーについて、[Umbrellaルール（Umbrella Rules）] から選択した [コンテンツカテゴリ（Content Categories）] を **[URLフィルタリング（URL Filtering）]** > **[定義済みURLカテゴリフィルタリング（Predefined URL Category Filtering）]** で表示できます。また、[接続先リスト（Destination lists）] を **[URLフィルタリング（URL Filtering）]** > **[カスタムおよび外部URLカテゴリフィルタリング（Custom and External URL Category Filtering）]** で表示できます。

ルールセットで選択したアイデンティティに基づいて、すべての接続先をモニターする追加のアクセスポリシーが作成されます。

（注）
- 変換するアイデンティティの選択に基づいて、Cisco Umbrella ルールから Cisco Secure Web Appliance アクセスポリシーへの 1 対 1 のマッピングまたは 1 対多のマッピングが作成されます。
- ルールセットで選択したアイデンティティに基づいて、すべての接続先をモニターする追加のアクセスポリシーが作成されます。

復号ポリシーの設定

Cisco Umbrella の [HTTPSインスペクション（HTTPS Inspection）] ポリシーは、アイデンティティとともに使用できるように、Cisco Secure Web Appliance の [復号ポリシー（Decryption policies）] として変換されます。

（注） Cisco Secure Web Appliance で [HTTPSプロキシ（HTTPS Proxy）] が有効になっている場合にのみ、Cisco Umbrella から復号ポリシーを設定できます。

Cisco Umbrella で HTTPS インスペクションを有効にします（**[ポリシー（Policies）]** > **[管理（Management）]** > **[Webポリシー（Web Policy）]** > **[ルールセット設定（Ruleset Settings）]** > **[HTTPSインスペクション設定（HTTPS Inspection Settings）]**）。

[選択的復号リスト（Selective Decrpytion List）] で [なし（None）] を選択すると、すべての事前定義されたコンテンツカテゴリが復号されます。ドロップダウンから選択的復号リストを選択して、HTTPS インスペクションをバイパスします。

Cisco Umbrella の [選択的復号リスト（Selective Decryption List）] からの変換されたコンテンツカテゴリは、**[URLフィルタリング（URL Filtering）]** > **[事前定義されたURLカテゴリフィルタリング（Predefined URL Category Filtering）]** に表示され、Cisco Umbrella の [選択的復号リスト（Selective Decrpytion List）] からのドメインは、復号ポリシーの **[URLフィルタリング**

（URL Filtering）]>[カスタムおよび外部URLカテゴリフィルタリング（Category Filtering）] に表示されます。

Cisco Umbrella の HTTPS インスペクション設定は、次のように Cisco Secure Web Appliance に変換されます。

- 有効にすると、[ドメイン（Domains）] と、[選択的復号リスト（Selective Decryption List）] の [コンテンツカテゴリ（Content Categories）] は、Cisco Secure Web Appliance で [パススルー（Passthrough）] に設定され、残りのカテゴリは [復号する（Decrypt）] に設定されます。
- 無効にすると、[復号ポリシー（Decryption Policies）] は、すべての事前定義された URL カテゴリフィルタリングが [モニター（Monitor）] として、Cisco Secure Web Appliance に表示されます。
- [HTTPS経由でブロックされているページを表示（Display Block Page Over HTTPS）] が選択されている場合、[復号ポリシー（Decryption Policies）] は、すべての事前定義された URL カテゴリフィルタリングが [モニター（Monitor）] として、Cisco Secure Web Appliance に表示されます。

詳細については、「Add a Ruleset to the WebPolicy」を参照してください。

（注）

- Cisco Umbrella の [選択的復号リスト（Selective Decryption List）] の [アプリケーション（Applications）] を Cisco Secure Web Appliance の [復号ポリシー（Decryption Policies）] に変換することはサポートされていません。
- ルールセットアイデンティティでネットワークとともに AD ユーザーまたは AD グループが選択されると、追加の復号ポリシーが作成されます。
- Cisco Umbrella から変換された復号ポリシーのデフォルトアクションは、[復号する（Decrypt）] に設定されます。
- Cisco Secure Web Appliance では、Cisco Umbrella から変換された [復号ポリシー（Decryption Policies）] に対して WBRS が無効になっています。

アクセスポリシーでのアプリケーションの設定

Cisco Umbrella で CASI とも呼ばれる [アプリケーション設定（Application Settings）] は、Cisco Secure Web Appliance のアクセスポリシーで [ADCアプリケーション（ADC Applications）] として変換されます。

Cisco Umbrella ルールでアプリケーションカテゴリまたは特定のアプリケーションを選択でき、Cisco Secure Web Appliance でアクセスポリシーのアプリケーションに同じルールアクションが適用されます。ルール内で選択されていないアプリケーションはグローバル設定を継承します。

選択したアプリケーションのドメインで構成されるカスタム URL カテゴリが作成され、Cisco Secure Web Appliance にプッシュされます。これを表示するには、**[URLフィルタリング（URL**

Filtering）] > **[カスタムおよび外部URLカテゴリのフィルタリング（Custom and External URL Category Filtering）]** に移動し、アクセスポリシーの [URLフィルタリング（URL Filtering）] セクションで [アクション（Action）] を [モニター（Monitor）] として選択します。

詳細については、「Manage Application Settings on Umbrella」を参照してください。

これらのルールは、Cisco Secure Web Appliance に変換されると、**[Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] > [アプリケーション（Applications）]**に移動して表示できます。

重要選択したアプリケーションを含むアプリケーションルールを Cisco Umbrella から Cisco Secure Web Appliance に正常に変換するには、[アプリケーションの検出および制御（ADC）（Application Discovery and Control (ADC)）] を有効にする必要があります。

詳細については、「AVC または ADC エンジンを有効にする」を参照してください。

（注） Cisco Umbrella のアプリケーションポリシーは、Cisco Secure Web Appliance で復号ポリシーとして変換されません。

AD ユーザーまたは AD グループの設定

Cisco Umbrella Web ポリシーの AD ユーザーまたは AD グループは、**ポリシーメンバー定義セクション**の [選択されたグループおよびユーザー（Selected Groups and Users）] として Cisco Secure Web Appliance ポリシーで設定する必要があります。

Cisco Umbrella では、AD が統合されている場合 （**[展開（Deployments）] > [構成（Configuration）] > [サイトおよびアクティブディレクトリ（Sites and Active Directory）]**）、レルムを [すべてのレルム（All Realms）] として、[ケルベロス、NTLMSSPまたは基本を使用する（Use Kerberos or NTLMSSP or Basic）] をスキーマとして、[IPアドレス（IP Address）] を認証サロゲートとして作成するグローバル ID プロファイルは 1 つだけです。**[セキュリティサービス（Security Services）] > [プロキシ設定（Proxy Settings）] > [Webプロキシ設定（Web Proxy Settings）] > [基本設定（Basic Settings）] > [プロキシモード（Proxy Mode）]** で、[Web プロキシモード（Web Proxy Mode）] が [透過的（Transparent）] である場合、Cisco Secure Web Appliance で [同じサロゲート設定を明示的な転送要求に適用する（Apply same surrogate settings to explicit forward requests）] チェックボックスが有効になります。

（注） Cisco Umbrella に統合されているアクティブディレクトリは、Cisco Secure Web Appliance で手動で設定し、到達可能である必要があります。

Cisco Umbrella（**[ポリシー（Policies）] > [管理（Management）] > [Webポリシー（Web Policy）] > [ルールセットアイデンティティ（Ruleset Identities）]**）で、Cisco Umbrella の統合 AD から [ADユーザー（AD Users）] または [ADグループ（AD Group）] を選択します。ルールセット アイデンティティで選択した [ADユーザー（AD Users）] または [ADグループ（AD Groups）] は、Cisco Secure Web Appliance の復号ポリシーのメンバーシップセクション（**[Web**

セキュリティマネージャ（Web Security Manager）] > [復号ポリシー（Decryption Policies）] > [ポリシーメンバー定義（Policy Member Definition）]）にマップする必要があります。

Cisco Umbrella（**[ポリシー（Policies）] > [管理（Management）] > [Webポリシー（Web Policy）] > [ルールセット（Ruleset）] > [ルール（Rules）]**）で、[ADユーザー（AD Users）] として選択されたアイデンティティまたは選択されたルールアクションおよび接続先で [ADグループ（AD Groups）] でルールを作成します。ルールで選択された [ADユーザー（AD Users）] または [ADグループ（AD Groups）] は、Cisco Secure Web Appliance のアクセスポリシーのメンバーシップセクション（**[Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] > [ポリシーメンバー定義（Policy Member Definition）]**）にマップされます。

ルールセット アイデンティティの選択された [ADユーザー（AD Users）] または [ADグループ（AD Groups）] を使用して追加のポリシーが作成され、すべての事前定義されたコンテンツカテゴリが許可されます。

Microsoft 365 の互換性の設定

[Microsoft 365互換性（Microsoft 365 Compatibility）] 設定を Cisco Umbrella から Cisco Secure Web Appliance の [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）] に変換できます。

Cisco Umbrella では、[Microsoft 365互換性（Microsoft 365 Compatibility）] が有効になっている場合（**[ポリシー（Policies）] > [管理（Management）] > [Webポリシー（Web Policy）] > [グローバル設定（Global Settings）]**）、Cisco Secure Web Appliance の [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）] は、[カテゴリタイプ（Category Type）] が [外部ライブフィードカテゴリ（External Live Feed Category）] として、[フィードファイルの場所（Feed File Location）] が [Office 365 Webサービス（Office 365 Web Service）] として作成されます。このカテゴリは、Cisco Secure Web Appliance の [URLフィルタリング（URL Filtering）] セクションで、[アクション（Action）] を [パススルー（Passthrough）] として Cisco Umbrella から設定された復号ポリシーに対して選択されます。

（注） 復号ポリシーは、Cisco Secure Web Appliance で [HTTPSプロキシ（HTTPS Proxy）] が有効になっている場合にのみ設定されます。

ポリシーの競合管理とポリシーの順序付け

Cisco Umbrella の管理対象プロファイル、または識別プロファイル、アクセスポリシー、復号ポリシー、および Cisco Umbrella から Cisco Secure Web Appliance に設定されたカスタムおよび外部 URL カテゴリなどのポリシーを編集または削除することはできません。名前の先頭に「umbrella<space>」が付いたプロファイルまたはポリシーを作成することはできません（例：umbrella abc）。

（注）

- Cisco Secure Web Appliance で設定された Cisco Umbrella ポリシーをクローンすることはできません。
- Cisco Secure Web Appliance では、Cisco Umbrella から変換されたポリシーの順序を変更できません。
- Cisco Secure Web Appliance の **[ネットワーク（Network）]** > **[Umbrella設定（Umbrella Settings）]** でハイブリッド ポリシー オプションを無効化した後、Cisco Umbrella からプッシュされたポリシーを編集または削除できます。
- REST API を使用して、Cisco Umbrella からプッシュされたポリシーを編集および削除できます。

Cisco Umbrella のポリシー規則のシーケンスは、Cisco Secure Web Appliance へのポリシー変換中に保持されます。したがって、Cisco Secure Web Appliance 管理者が設定したポリシーまたはプロファイルは、Cisco Umbrella から変換されたポリシーよりも優先されます。

ブロックされているページの管理

最初のルールセットに関連付けられている Cisco Umbrella の [ブロックされているページ（Block Page）] 設定（**[ポリシー（Policies）]** > **[管理（Management）]** > **[ポリシーコンポーネント（Policy Components）]** > **[ブロックされているページの外観（Block Page Appearance）]**）を、Cisco Secure Web Appliance の [エンドユーザー通知（End-User Notification）] ページ（**[セキュリティサービス（Security Services）]** > **[エンドユーザー通知（End-User Notification）]**）に変換できます。

Cisco Umbrella で、Cisco Umbrella の [ブロックされているページ（Block Page）] 設定を変換するには、ブロックされているページを設定し、最初のルールセットでブロックされているページを選択します（**[ポリシー（Policies）]** > **[Webポリシー]**）。

（注） 最初のルールセットの選択された [ブロックされているページ（Block Page）] の変更は、3 時間ごとに Cisco Secure Web Appliance にプッシュされます。

詳細については、https://docs.umbrella.com/umbrella-user-guide/docs/create-a-custom-block-pageを参照してください。

Cisco Umbrella シームレス ID

Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ（SWG）にパスすることができます。Cisco Umbrella SWG は、 Secure Web Applianceから受信した認証済み識別情報に基づい

て、Active Directory のユーザー情報をチェックします。Cisco Umbrella SWG は、ユーザを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。

Secure Web Applianceは、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザー識別情報を渡します。

（注）
- Cisco Umbrella シームレス ID ヘッダーは、 Secure Web Appliance上の同じ名前のヘッダーを上書きします。
- Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine（ISE）、および Cisco Context Directory Agent（CDA）をサポートしていません。
- Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。

表 *4 : HTTPS* トラフィックの動作

構成モード	サロゲート	認証のための復号	Secure Web Appliance 認証	Cisco Umbrella シームレス ID の共有
Explicit	IP サロゲート	はい/いいえ	対応	対応
透過	IP サロゲート	対応	対応	対応
透過	IP サロゲート	非対応	認証をスキップ	非対応
Explicit	Cookie、クレデンシャルの暗号化なし	はい/いいえ	対応	対応
Explicit	Cookie、クレデンシャルの暗号化あり	はい/いいえ	対応	非対応
透過	Cookie、クレデンシャル暗号化あり/なし	はい/いいえ	認証をスキップ	非対応

（注） Secure Web Applianceは、認証されたユーザーの UPN 値を Active Directory から取得し、Cisco Umbrella シームレス ID でユーザーに正しい Web ポリシーを適用できるようにします。この機能を利用するには、すべての Active Directory ユーザーにデフォルトまたはカスタマイズされた UPN 値を割り当てる必要があります。

ここでは、次の内容について説明します。

• Cisco Umbrella シームレス ID の設定
• Cisco Umbrella SWG のルーティング先の設定

Cisco Umbrella シームレス ID の設定

始める前に

- **[ネットワーク（Network）]** > **[証明書の管理（Certificate Management）]** > **[信頼できるルート証明書の管理（Manage Trusted Root Certificates）]**を選択して、ルートまたはカスタムの Umbrella 証明書をアプライアンスに手動でアップロードします。「証明書の管理」を参照してください。
- 認証用の識別プロファイルが設定されていることを確認します。
- 設定済みの識別プロファイルを使用してルーティングポリシーを定義します。

手順

ステップ 1 **[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco UmbrellaシームレスID（Cisco Umbrella Seamless ID）]**を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 Cisco Umbrella SWG ホスト名または IP アドレスを入力します。

ステップ 4 HTTP および HTTPS トラフィック用の SWG のポート番号を入力します。

最大 6 つのポート番号を入力できます。

ステップ 5 （オプション）[接続テスト（Connectivity Test）] をクリックして、ポートを介した Cisco Umbrella SWG の接続と証明書の検証が正常に行われていることを確認します。

ステップ 6 Cisco Umbrella SWG の一意のカスタマー組織 ID を入力します。

ステップ 7 送信して確定します。

Cisco Umbrella SWG のルーティング先の設定

新しいルーティングポリシーを作成するには、「ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加」を参照してください。

。

手順

ステップ 1 **[Webセキュリティマネージャ（Web Security Manager）]** > **[ルーティングポリシー（Routing Policies）]**を選択します。

ステップ 2 [ルーティングポリシー（Routing Policies）] ページで、必要なポートを含む Cisco Umbrella シームレス ID を設定するルーティングポリシーの [ルーティング先（Routing Destination）] 列の下にあるリンクをクリックします。

ステップ 3 ポリシーのアップストリーム プロキシグ グループとして、ポートを含む適切な Cisco Umbrella シームレス ID を選択します。[アップストリームプロキシグループ（Upstream Proxy Group）] ドロップダウンリストには、**[Cisco Umbrellaシームレス ID（Cisco Umbrella Seamless ID）]** ページ（**[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco Umbrellaシームレス ID（Cisco Umbrella Seamless ID）]**）で設定したすべての Cisco Umbrella シームレス ID とポートが表示されます。

（注）
ルーティングポリシーにすでにリンクされているポート番号を持つ **Cisco Umbrella シームレス ID** を削除すると（**[Webセキュリティマネージャ（Web Security Manager）]** > **[Cisco Umbrellaシームレス ID（Cisco Umbrella Seamless ID）]**）、ルーティング先が [直接接続（Direct Connection）] に変わります。

ステップ 4 変更を送信し、保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。