

ゲストアクセスを許可するためのセキュアWebアプライアンスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[シナリオ概要](#)

[設定手順](#)

[ステップ 1: IDプロファイルを作成します。](#)

[ステップ2: \(オプション\) 許可URLとブロックURLのカスタムURLカテゴリを作成する](#)

[ステップ3管理対象デバイスの復号化ポリシーの作成](#)

[ステップ4管理対象外デバイスの復号化ポリシーの作成](#)

[ステップ5管理対象デバイスのアクセスポリシーの作成](#)

[ステップ6管理対象外デバイスのアクセスポリシーの作成](#)

[ステップ7: \(オプション\) 管理対象デバイス用のシスコデータセキュリティポリシーの作成](#)

[ステップ8: \(オプション\) 管理対象外デバイス用のCiscoデータセキュリティポリシーの作成](#)

[ステップ9変更の保存](#)

[関連情報](#)

はじめに

このドキュメントでは、復号化証明書をインストールしていないユーザがSecure Web Appliance(SWA)経由でインターネットにアクセスできるようにする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 物理または仮想SWAがインストールされている。
- ライセンスがアクティブ化またはインストールされていること。
- セットアップウィザードが完了しました。
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの

ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

シナリオ概要

この記事では、10.10.10.0/24 Wi-Fiサブネット内のネットワークアクセスコントロール(NAC)のシナリオについて説明します。この環境は、異なるセキュリティポリシーとアクセスポリシーを必要とする2つのユーザグループで構成されます。

- 管理対象デバイス：完全に認証され、SWA復号化証明書がインストールされている会社支給のラップトップ。これらのデバイスは信頼でき、通常は標準の企業アクセスポリシーの対象となります。
- アンマネージド/ゲストデバイス：認証されておらず、SWA復号化証明書を持たない個人用ラップトップおよびモバイルデバイス。

目標:

この企業は、管理対象外デバイスに制限のあるWebアクセスポリシーを実装し、企業リソースの安全性を維持しながら、その接続を許可されるURLの特定のサブセットに制限することを目指しています。

 注：復号化証明書はアンマネージドデバイスでは信頼されないため、HTTPSトラフィックを復号化することはできず、アクションをパススルーに設定する必要があります。

設定手順

ステップ 1：IDプロフィールを作成します。	ステップ 1.1：SWAのGUIで、Web Security Managerに移動し、Identification Profileを選択します。 ステップ 1.2：Add Identification Profileをクリックします。 ステップ 1.3：プロフィールの名前を定義します。 ステップ 1.4：(オプション)説明を定義する。 ステップ 1.5：Identification and AuthenticationでAuthenticate Usersを選択します。 ステップ 1.6：Select a Realm or SequenceからActive Directoryレームを選択します。
------------------------	--

ステップ 1.7 : Select a Schemeから、必要な認証プロトコルを選択します。

 ヒント: Select a SchemeリストではBasic Authenticationを選択しないでください。

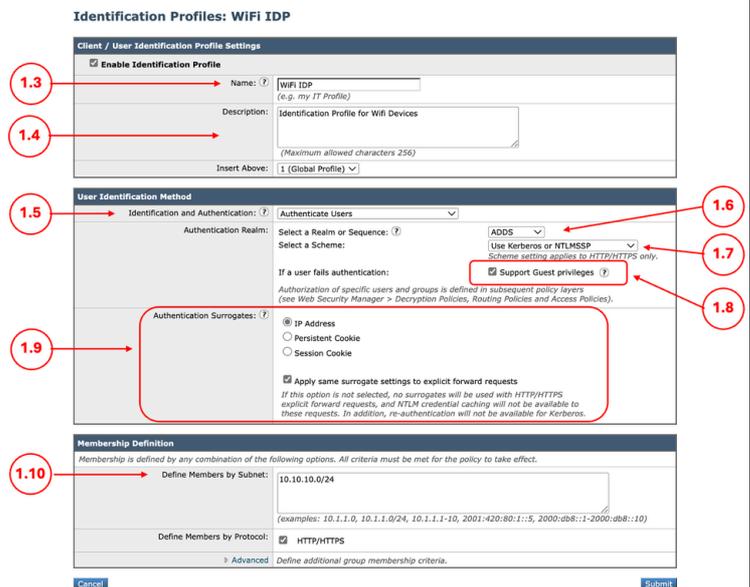
ステップ 1.8 : Support Guest privilegesのチェックボックスをオンにします。

ステップ1.9. (オプション) 設計に応じて、「明示的な転送リクエストに同じサロゲート設定を適用」を有効にすることで、サロゲートを有効にできます。

 注意 : トラフィックの復号化はできないため、透過的導入ではPersistent CookieもSession Cookieも選択しないでください。

ステップ 1.10 : でIPアドレスサブネットを定義し、サブネットでメンバを定義します。

ステップ 1.11 : 変更を [Submit] して [Commit] します。



イメージ - 識別プロファイルの定義

ステップ2: (オプション) 許可URLとブロックURLのカスタムURLカテゴリを作成する

ステップ2.1:GUIからWeb Security Managerに移動し、Custom and External URL Categoriesを選択します。

ステップ2.2 : カテゴリの追加をクリックして、新しいカスタムURLカテゴリを作成します。

ステップ2.3:新しいカテゴリの名前を入力します。

ステップ2.4:アクセスをブロックするWebサイトのドメインまたはサブドメイン (あるいはその両方) を定義します。

ステップ2.5:変更を送信します。

ステップ 2.6 : 同じ手順を使用して、アクセスを許可するWebサイトのURLカテゴリを作成します。

The figure shows two screenshots of the 'Edit Custom and External URL Category' interface. The top screenshot shows the 'Blocked WiFi Access' category with 'example.com, _example.com' in the Sites field. The bottom screenshot shows the 'Allowed WiFi Access' category with 'cisco.com, _cisco.com' in the Sites field. Red circles with numbers 2.3 and 2.4 point to the Category Name and Sites fields respectively.

図 - カスタムURLカテゴリの定義

ステップ 3 管理対象デバイスの復号化ポリシーの作成

ステップ 3.1 : GUIから、Web Security Managerに移動し、chooseDecryption Policiesを選択します。

ステップ3.2:Add Policyをクリックします。

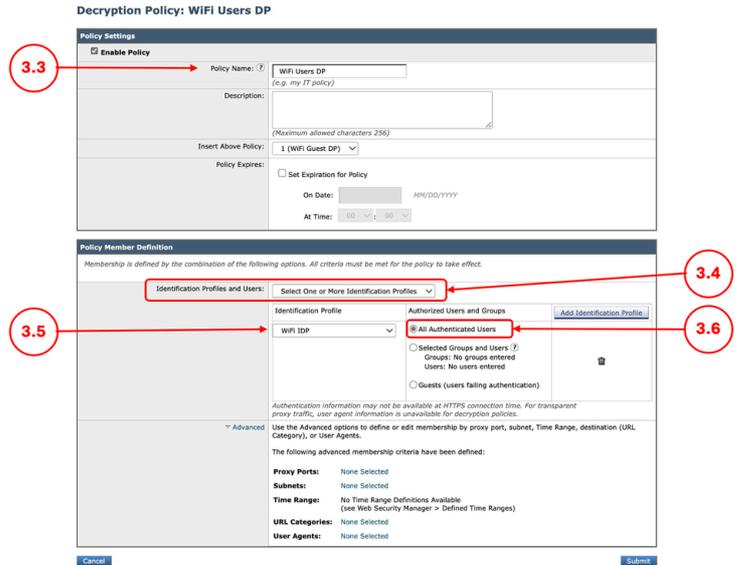
ステップ3.3 : 新しいポリシーのNameを入力します。

ステップ 3.4 : Identification Profiles and Usersドロップダウンメニューから、Select One or more Identification Profilesを選択します。

ステップ3.5:ステップ1で作成したIDプロファイルを選択します。

ステップ 3.6 : All Authenticated Usersを選択します。

ステップ3.7:ClickSubmitをクリックします。



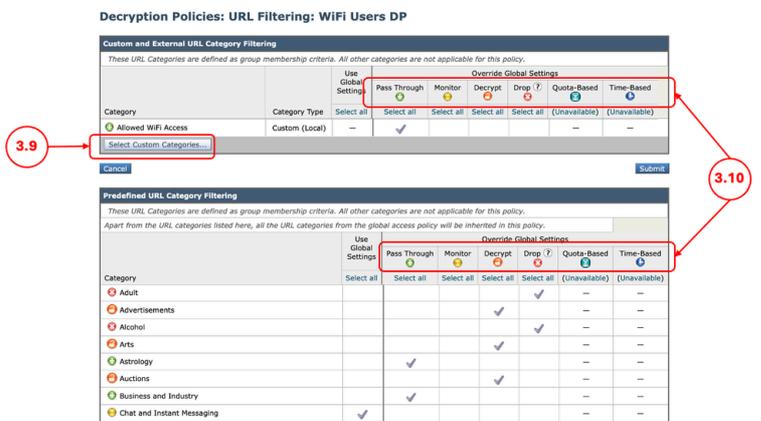
管理対象デバイスの復号化ポリシーの作成

ステップ 3.8 : Decryption Policiesページで、新しいポリシーに対するURL Filteringからのリンクをクリックします。

ステップ3.9. (オプション) カスタムURLカテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックし、「ポリシーに含める」を選択します

ステップ 3.10 : 各カスタムおよび外部URLカテゴリフィルタリングと事前定義されたURLカテゴリフィルタリングのアクションを設定します。

ステップ 3.11 : [Submit] をクリックします。



イメージ : 復号化ポリシーのアクションの設定

ステップ 4.1 : GUIから、Web Security Managerに移動し、chooseDecryption Policiesを選択します。

ステップ4.2:Add Policyをクリックします。

ステップ4.3 : 新しいポリシーのNameを入力します。

ステップ 4.4 : Identification Profiles and Users ドロップダウンメニューから、Select One or more Identification Profilesを選択します。

ステップ4.5:ステップ1で作成したIDプロフィールを選択します。

ステップ 4.6 : Guests (users failing authentication)を選択します。

ステップ4.7:ClickSubmitをクリックします。

ステップ 4 管理対象外デバイスの復号化ポリシーの作成

Decryption Policy: WIFI Guest DP

Policy Settings

Enable Policy

Policy Name: WIFI Guest DP
(e.g. my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: 00:00

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WIFI IDP

Authorized Users and Groups: Add Identification Profile

All Authenticated Users

Selected Groups and Users (?)
Groups: No groups entered
Users: No users entered

Guests (users failing authentication)

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(Use Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel Submit

管理対象外デバイスの復号化ポリシーの作成

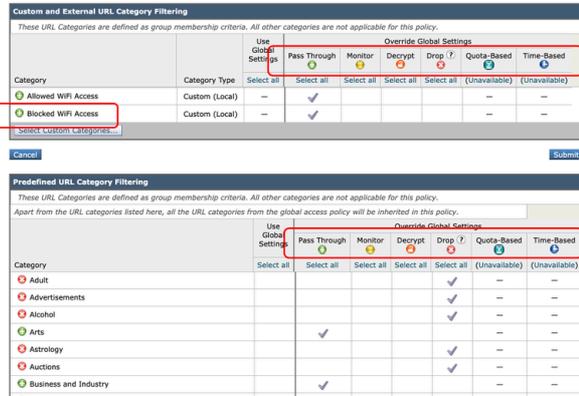
ステップ 4.8 : Decryption Policies ページで、新しいポリシーに対する URL Filtering からのリンクをクリックします。

ステップ4.9. (オプション) カスタム URL カテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックし、「ポリシーに含める」を選択します

ステップ 4.10 : 各カスタムおよび外部 URL カテゴリフィルタリングと事前定義された URL カテゴリフィルタリングのアクションを設定します。

 注:SWA復号化証明書はアンマネージドデバイスでは信頼されないため、Decryptをアクションとして使用しないでください。

Decryption Policies: URL Filtering: WiFi Guest DP



Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop (?)	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blocked WiFi Access	Custom (Local)	Select all	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Predefined URL Category Filtering

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings					
		Pass Through	Monitor	Decrypt	Drop (?)	Quota-Based	Time-Based
Adult	Select all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Advertisements	Select all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alcohol	Select all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Arts	Select all	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Astrology	Select all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Auctions	Select all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Business and Industry	Select all	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

イメージ - アンマネージドデバイスの暗号化解除操作

ステップ 4.11 : Uncategorized URLsセクションをスクロールダウンして、適切なアクションを選択します。



Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs:

Default Action for Update Categories:

画像 - 未分類のURL

 ヒント : セキュリティの観点からは、アクションをドロップに設定するのが最適です。任意のURLでアクセスが必要になった場合は、ポリシーに割り当てられたカスタムURLカテゴリに追加できます。

ステップ 4.12 : [Submit] をクリックします。

ステップ 5管理対象デバイスのアクセスポリシーの作成

ステップ 5.1 : GUIから、Web Security Managerに移動し、Access Policiesを選択します。

ステップ5.2:Add Policyをクリックします。

ステップ5.3 : 新しいポリシーのNameを入力します。

ステップ 5.4 : Identification Profiles and Usersドロップダウンメニューから、Select One or more Identification Profilesを選択します。

ステップ5.5:ステップ1で作成したIDプロファイルを選択します。

ステップ 5.6 : All Authenticated Usersを選択します。

ステップ5.7:ClickSubmitをクリックします。

Access Policy: WiFi Users AP

Policy Settings

Enable Policy

Policy Name: WiFi Users AP
(e.g. my IT policy)

Description:

Insert Above Policy: 1 (WiFi Guest AP)

Policy Expires:

Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: HH:MM:SS

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: All Authenticated Users

Selected Groups and Users (Groups: No groups entered, Users: No users entered)

Guests (users failing authentication)

Advanced: Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel Submit

イメージ - 管理対象デバイスのアクセスポリシー

ステップ 5.8 : アクセスポリシーページで、新しいポリシーのURLフィルタリングからのリンクをクリックします。

ステップ5.9. (オプション) カスタムURLカテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックして「ポリシーに含める」を選択します

ステップ 5.10 : 各カスタムおよび外部URLカテゴリフィルタリングと事前定義されたURLカテゴリフィルタリングのアクションを設定します。

Access Policies: URL Filtering: WiFi Users AP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings						
			Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
Adult	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Advertisements	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Alcohol	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Arts	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Astrology	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Auctions	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Business and Industry	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

図 - 管理対象デバイスのアクセスポリシーURLフィルタリング

ステップ 5.11 : [Submit] をクリックします。

ステップ 6.1 : GUIから、Web Security Managerに移動し、Access Policiesを選択します。

ステップ6.2:Add Policyをクリックします。

ステップ6.3 : 新しいポリシーのNameを入力します。

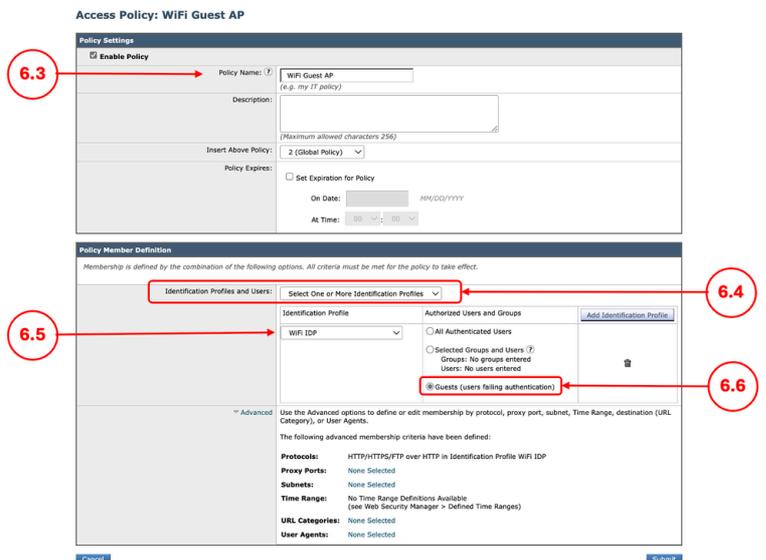
ステップ 6.4 : Identification Profiles and Users ドロップダウンメニューから、Select One or more Identification Profilesを選択します。

ステップ6.5:ステップ1で作成したIDプロフィールを選択します。

ステップ 6.6 : Guests (users failing authentication)を選択します。

ステップ6.7:ClickSubmitをクリックします。

ステップ 6 管理対象外デバイスのアクセスポリシーの作成



イメージ - 管理対象外デバイスのアクセスポリシー

ステップ 6.8 : アクセスポリシーページで、新しいポリシーのURLフィルタリングからのリンクをクリックします。

ステップ6.9. (オプション) カスタムURLカテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックして「ポリシーに含める」を

選択します

ステップ 6.10 : 各カスタムおよび外部URLカテゴリフィルタリングと事前定義されたURLカテゴリフィルタリングのアクションを設定します。

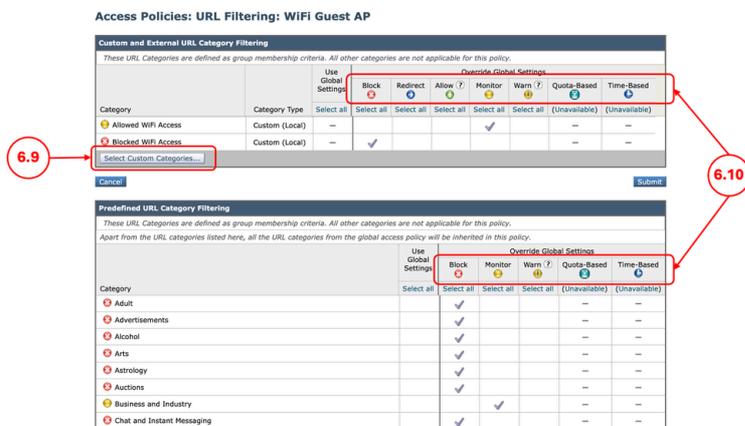


図 - 管理対象外デバイスのアクセスポリシーURLフィルタリング

ステップ 6.11 : Uncategorized URLsセクションをスクロールダウンして、適切なアクションを選択します。

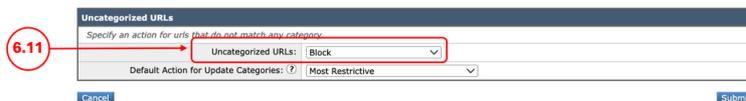


図 - アクセスポリシーの未分類のURL

 ヒント : セキュリティの観点からは、アクションをブロックに設定するのが最適です。任意のURLでアクセスが必要になった場合は、ポリシーに割り当てられたカスタムURLカテゴリに追加できます。

ステップ 6.12 : [Submit] をクリックします。

ステップ7: (オプション) 管理対象デバイスのCiscoデータセキュリティポリシーを作成します

ステップ 7.1 : GUIから、Web Security Managerに移動し、Cisco Data Securityを選択します。

ステップ7.2:Add Policyをクリックします。

ステップ7.3 : 新しいポリシーのNameを入力します。

ステップ 7.4 : Identification Profiles and Usersドロップダウンメニューから、Select One or more

 注 : 管理対象デバイスのアップロードトラフィックをフィルタリングしない場合は、このステップを省略できます。

Identification Profilesを選択します。

ステップ7.5:ステップ1で作成したIDプロフィールを選択します。

ステップ 7.6 : All Authenticated Usersを選択します

。

ステップ7.7:ClickSubmitをクリックします。

Cisco Data Security Policy: Add Group

Policy Settings

Enable Policy

Policy Name: ? Wifi Users Upload
(e.g. my IT policy)

Description:

Insert Above Policy: 1 (Global Policy)

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: All Authenticated Users

Selected Groups and Users (?): Groups: No groups entered
Users: No users entered

Guests (users falling authentication)

Cancel Submit

図 - 管理対象デバイス用のCiscoデータセキュリティポリシー

ステップ 7.8 : Cisco Data Security Policiesページで、新しいポリシーのURL Filteringからのリンクをクリックします。

ステップ7.9. (オプション) カスタムURLカテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックして「ポリシーに含める」を選択します

ステップ 7.10 : 各カスタムおよび外部URLカテゴリフィルタリングと事前定義されたURLカテゴリフィルタリングのアクションを設定します。

Cisco Data Security Policies: URL Filtering: Wifi Users Upload

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings		
			Allow ?	Monitor	Block
Allowed Wifi Access	Custom (Local)	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select Custom Categories...					

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy. Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings	
		Monitor	Block
Adult	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Advertisements	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alcohol	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Arts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Astrology	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Auctions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Cancel Submit

イメージ - 管理対象デバイスのアップロードアクション

ステップ 7.11 : [Submit] をクリックします。

ステップ 8.1 : GUIから、Web Security Managerに移動し、Cisco Data Securityを選択します。

ステップ8.2:Add Policyをクリックします。

ステップ8.3 : 新しいポリシーのNameを入力します。

ステップ 8.4 : Identification Profiles and Users ドロップダウンメニューから、Select One or more Identification Profilesを選択します。

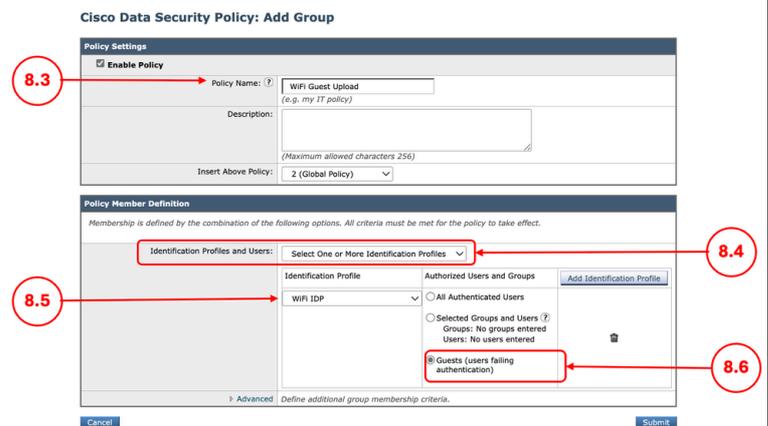
ステップ8.5:ステップ1で作成したIDプロフィールを選択します。

ステップ 8.6 : All Authenticated Usersを選択します。

ステップ8.7:ClickSubmitをクリックします。

ステップ8: (オプション) 管理対象外デバイス用のCiscoデータセキュリティポリシーの作成

 注 : 管理されていないデバイスのアップロードトラフィックをフィルタリングしない場合は、このステップを省略できます。



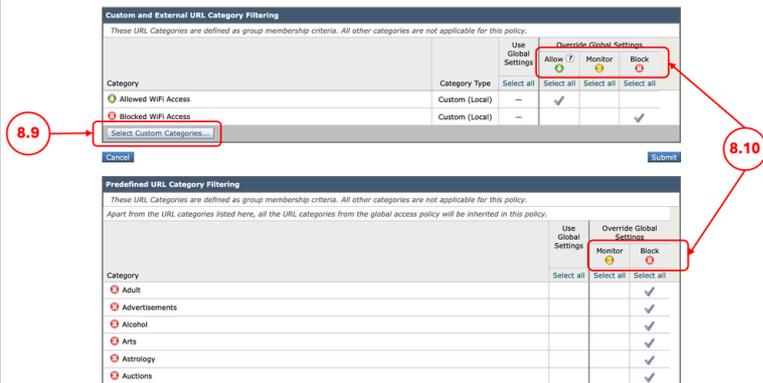
イメージ - アンマネージドデバイス用のCiscoデータセキュリティポリシー

ステップ 8.8 : Cisco Data Security Policies ページで、新しいポリシーのURL Filteringからのリンクをクリックします。

ステップ8.9. (オプション) カスタムURLカテゴリを追加するには、カテゴリ名の前に「カスタムカテゴリの選択」をクリックして「ポリシーに含める」を選択します

ステップ 8.10 : 各カスタムおよび外部URLカテゴリフィルタリングと事前定義されたURLカテゴリフィルタリングのアクションを設定します。

Cisco Data Security Policies: URL Filtering: WiFi Guest Upload



イメージ - アンマネージドデバイスのアップロードアクション

ステップ 8.11 : Uncategorized URLsセクションをスクロールダウンして、適切なアクションを選択します。



イメージ : 未分類のURLに対するアップロードアクション

 ヒント : セキュリティの観点からは、アクションをブロックに設定するのが最適です。任意のURLでアクセスが必要になった場合は、ポリシーに割り当てられたカスタムURLカテゴリに追加できます。

ステップ 8.12 : [Submit] をクリックします。

ステップ 9変更の保存

ステップ 9.1 : 変更を保存します。

関連情報

- [AsyncOS 15.0 for Cisco Secure Web Appliance ユーザガイド - LD \(限定導入 \) - トラブルシューティング...](#)
- [SWAでの実行可能ファイルのダウンロードのブロック](#)
- [セキュアWebアプライアンスでのアップロードトラフィックのブロック](#)
- [Secure Web Applianceでのトラフィックのブロック](#)
- [Secure Web Applianceでの認証のバイパス](#)
- [SWAでのMicrosoft O365テナント制限の設定](#)
- [セキュアなWebアプライアンスの初期設定の設定](#)
- [Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。