ローカル ポリシーの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

ローカル ポリシー設定の制約事項

controllerでサポートされているポリシー マップの属性は、QoS、VLAN、セッション タイムアウト、および ACL です。

ローカル ポリシーの設定に関する情報

ローカル ポリシーは、HTTP と DHCP に基づいてデバイスをプロファイリングして、ネットワーク上のエンド デバイスを識別することができます。 ユーザは、デバイス ベースのポリシーを設定し、ネットワーク上でユーザまたはデバイス ポリシーごとにポリシーを適用できます。

ローカルポリシーにより、モバイルデバイスのプロファイリングと、特定のVLANへのプロファイリングされたデバイスの基本的なオンボーディングが可能になります。 また、ACLおよびQoSを割り当てたり、セッション タイムアウトを設定します。

2 つの個別のコンポーネントとしてローカル ポリシーを設定できます。

- ネットワークに参加するクライアントに固有のサービステンプレートとしてのポリシー属性の定義およびポリシー一致基準の適用。
- ポリシーへの一致基準の適用。

次のポリシー一致属性は、ローカル ポリシーを設定するために使用されます。

- デバイス：デバイスのタイプを定義します。 Windowsベースのコンピュータ、スマートフォン、iPad や iPhone などの Apple デバイス。
- ユーザ名：ユーザのユーザ名を定義します。
- ユーザ ロール：学生や従業員など、ユーザ タイプまたはユーザが属するユーザ グループを定義します。
- MAC：エンド ポイントの mac-address を定義します。
- MAC OUI：mac-address OUI を定義します。

エンドポイントごとにこれらのパラメータに対応する一致がcontrollerにあると、ポリシーを追加できます。 ポリシーの適用により、次のセッション属性に基づいてモバイルデバイスの基本的なデバイス オンボーディングが可能になります。

- VLAN
- QoS
- ACL
- Session timeout

これらのポリシーを設定して、指定されたポリシーでエンドポイントを適用できます。 ワイヤレス クライアントは、MAC OUI、DHCP および HTTP ユーザ エージェント（正常な HTTP プロファイリングには有効なインターネットが必要です）に基づいてプロファイリングされます。 controller は、これらの属性と事前定義された分類プロファイルを使用してデバイスを識別します。

デフォルトのプロファイル テキスト ファイルの置き換え

新しいデバイスが分類されていない場合は、デバイスの MAC アドレスを使用してシスコ サポート チームにお問い合わせください。 シスコ サポート チームにより、新しい **dc_default_profile.txt** ファイルが提供されます。そのファイルにはMACアドレスが含まれています。 **dc_default_profile.txt**

ファイルを以前のファイルと置き換える必要があります。 **dc_default_profile.txt** ファイルを変更するには、次の手順に従ってください。

1. 次のコマンドを入力して、デバイスの分類子を停止します。
   controller**(config)# no device classifier**
2. 次のコマンドを入力して、ファイルをコピーします。
   controller**# device classifier profile location** *filepath*
3. 次のコマンドを入力して、デバイスの分類子を開始します。
   controller**(config)# device classifier**

トランク ポートのセッション モニタのディセーブル化

アップリンク トランク ポートでは、セッション モニタリングを作成しないでください。 デフォルトでは、セッション モニタリングがイネーブルになっています。 セッション モニタリングをディセーブルにする必要があります。

1. 次のコマンドを入力して、グローバル コンフィギュレーション モードを開始します。
   controller**# configure terminal**
2. 次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。
   controller**(config)# interface** *interface-id*
3. 次のコマンドを入力して、セッション モニタリングをディセーブルにします。
   controller**(config-if)# no access-session monitor**

ローカル ポリシーの設定方法

ローカル ポリシーの設定（CLI）

ローカル ポリシーを設定するには、次の手順を完了します。

1. サービス テンプレートを作成します。
2. パラメータ マップを作成します。
3. ポリシー マップを作成します。
4. WLAN でローカル ポリシーを適用します。

サービス テンプレートの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**service-template** *service-template-name*
	
	例：
	
	`ControllerDevice(config)# service-template cisco-phone-template`
	`ControllerDevice(config-service-template)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

ステップ 3	**access-group** *acl_list* 例： `ControllerDevice(config-service-template)# access-group foo-acl`	適用するアクセス リストを指定します。
ステップ 4	**vlan** *vlan_id* 例： `ControllerDevice(config-service-template)# vlan 100`	VLAN ID を指定します。 1 ～ 4094 の値を指定できます。
ステップ 5	**absolute-timer** *seconds* 例： `ControllerDevice(config-service-template)# absolute-timer 20`	サービス テンプレートのセッション タイムアウト値を指定します。 1 ～ 65535 の値を指定できます。
ステップ 6	**service-policy qos** {**input** | **output**} 例： `ControllerDevice(config-service-template)# service-policy qos input foo-qos`	クライアントの QoS ポリシーを設定します。
ステップ 7	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

パラメータ マップの作成（CLI）

クラス マップよりもパラメータ マップを使用することが推奨されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**parameter-map type subscriber attribute-to-service** *parameter-map-name* 例： `ControllerDevice(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* } 例： `ControllerDevice(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	パラメータ マップの属性フィルタ基準を指定します。

ステップ 4	**service-template** *service-template-name*
	
	例：
	
	`ControllerDevice(config-parameter-map-filter-submode)# service-template cisco-phone-template`
	`ControllerDevice(config-parameter-map-filter-submode)#`
		サービス テンプレート コンフィギュレーション モードを開始します。

ステップ 5	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クラス マップの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map type control subscriber** *class-map-name* { **match-all** | **match-any** | **match-first** } 例： `ControllerDevice(config)# class-map type control subscriber CLASS_AC_1 match-all`	クラス マップのタイプと名前を指定します。
ステップ 3	**match** {**device-type** | **mac-address** | **oui** | **username** | **userrole**} *filter-type-name* 例： `ControllerDevice(config-class-map)# match device-type Cisco-IP-Phone-7961`	クラス マップの属性フィルタ基準を指定します。
ステップ 4	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバルコンフィギュレーション モードを終了できます。

ポリシー マップの作成（CLI）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map type control subscriber** *policy-map-name* 例： `ControllerDevice(config)# policy-map type control subscriber Aironet-Policy`	ポリシー マップのタイプを指定します。

	コマンドまたはアクション	目的
ステップ 3	**event identity-update** {**match-all** | **match-first**} 例： `ControllerDevice(config-policy-map)# event identity-update match-all`	ポリシーマップに一致基準を指定します。
ステップ 4	*class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**} 例： `ControllerDevice(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	ローカルプロファイリングのポリシークラスマップ番号を設定し、操作の実行方法を指定します。クラス マップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • **always**：一致を行うことなく実行しますが、success を返します。 • **do-all**：すべてのアクションを実行します。 • **do-until-failure**：一致の失敗が発生するまですべてのアクションを実行します。 これはデフォルト値です。 • **do-until-success**：一致の成功が発生するまですべてのアクションを実行します。
ステップ 5	*action-index* **map attribute-to-service table** *parameter-map-name* 例： `ControllerDevice(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	使用するパラメータ マップ テーブルを指定します。
ステップ 6	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN 上のデバイスへのローカル ポリシーの適用（CLI）

はじめる前に

サービス ポリシーがパラメータ マップにデバイス タイプに基づくルールを含んでいる場合は、デバイスの分類子がすでにイネーブルになっていることを確認します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `ControllerDevice# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `ControllerDevice(config)# wlan wlan1`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**service-policy type control subscriber** *policymapname* 例： `ControllerDevice(config-wlan)# service-policy type control subscriber Aironet-Policy`	WLAN にローカル ポリシーを適用します。
ステップ 4	**profiling local http**（任意） 例： `ControllerDevice(config-wlan)# profiling local http`	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http**（任意） 例： `ControllerDevice(config-wlan)# profiling radius http`	ISE 上のデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： `ControllerDevice(config-wlan)# no shutdown`	WLAN をシャットダウンしないように指定します。
ステップ 7	**end** 例： `ControllerDevice(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ローカル ポリシーの設定（GUI）

ローカル ポリシーを設定するには、次の手順を完了します。

1. サービス テンプレートを作成します。
2. ポリシー マップを作成します。

3 ユーザが作成したローカル ポリシーを WLAN に適用します。

サービス テンプレートの作成（GUI）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Service Template] を選択し、[Service Template] ページを開きます。

ステップ 2 次のようにして、新しいテンプレートを作成します。

a) [New] をクリックして、[Service Template] > [New] ページを開きます。
b) [Service Template name] テキスト ボックスに、新しいサービス テンプレート名を入力します。
c) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。 値の範囲は 1 ～ 4094 です。
d) [Session timeout] テキスト ボックスに、最大時間を秒単位で入力します。この後、クライアントは強制的に再認証されます。 値の範囲は、1 ～ 65535 秒です。
e) [Access control list] ドロップダウン リストから、ポリシーにマッピングされるアクセス コントロール リストを選択します。
f) [Ingress QoS] ドロップダウン リストから、適用させる入力 QoS ポリシーを選択します。
g) [Egress QoS] ドロップダウン リストから、適用させる出力 QoS ポリシーを選択します。
h) [Apply] をクリックして、設定を保存します。

ステップ 3 次のようにサービス テンプレートを編集します。

a) [Service Template] ページから、サービス テンプレートをクリックして [Service Template] > [Edit] ページを開きます。
b) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。 値の範囲は 1 ～ 4094 です。
c) [Session timeout] テキスト ボックスに、最大時間を秒単位で入力します。この後、クライアントは強制的に再認証されます。 値の範囲は、1 ～ 65535 秒です。
d) [Access control list] ドロップダウン リストから、ポリシーにマッピングされるアクセス コントロール リストを選択します。
e) [Ingress QoS] ドロップダウン リストから、適用させる入力 QoS ポリシーを選択します。
f) [Egress QoS] ドロップダウン リストから、適用させる出力 QoS ポリシーを選択します。
g) [Apply] をクリックして、設定を保存します。

ステップ 4 次のようにサービス テンプレートを削除します。

a) [Service Template] ページから、サービス テンプレートを選択します。
b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します。

ポリシー マップの作成（GUI）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Policy Map] を選択し、[Policy Map] ページを開きます。

ステップ 2 新しいポリシー マップを次のように作成します。

a) [New] をクリックして、[Policy Map] > [New] ページを開きます。
b) [Policy Map name] テキスト ボックスに、新しいポリシー マップの名前を入力します。
c) [Add] をクリックして、[Match Criteria] 領域を開きます。
d) [Device Type] ドロップダウン リストから、デバイス タイプを選択します。 デバイス タイプの一致基準は、選択しているデバイス タイプごとに、eq、not-eq、または regex を指定できます。
e) [User Role] ドロップダウン リストから、一致基準を eq、not-eq、または regex から選択し、ユーザ タイプまたはユーザのユーザ グループ（たとえば、学生、教員など）を入力します。
f) [Service Template] ドロップダウン リストから、ポリシーにマッピングされるサービス テンプレートを選択します。
g) [Add] をクリックします。 一致基準が一致基準リストに追加されます。
h) [Match Criteria Lists] 領域で、[Add] をクリックしてポリシーに一致基準を追加します。
i) [Apply] をクリックして、設定を保存します。

ステップ 3 ポリシー マップを次のように編集します。

a) [Policy Map] ページで、編集するポリシー マップを選択し、[Edit] をクリックして [Policy Map] > [Edit] ページを開きます。
b) [Match Criteria] 領域で、[Device Type] ドロップダウン リストからデバイス タイプを選択します。 デバイス タイプの一致基準は、選択しているデバイス タイプごとに、eq、not-eq、または regex を指定できます。
c) [Match Criteria] 領域で、[User Role] ドロップダウン リストからユーザ ロールを選択します。 一致基準を eq、not-eq、または regex から選択し、ユーザ タイプまたはユーザのユーザ グループを入力します。
d) [Service Template] ドロップダウン リストから、ポリシーにマッピングされるサービス テンプレートを選択します。
e) 設定を保存するには [Ok] を、または設定を破棄するには [Cancel] をクリックします。
f) デバイスタイプ、ユーザ ロール、サービステンプレートに基づいて追加の一致基準をポリシーに追加するには、[Add] をクリックします。
g) [Match Criteria Lists] 領域で、一致基準を選択し、[Move to] をクリックして行テキスト ボックスに入力した値に対して一致基準を移動させます。
h) 一致基準をリストの上に移動させるには、一致基準を選択し、[Move up] をクリックします。
i) 一致基準をリストの下に移動させるには、一致基準を選択し、[Move down] をクリックします。
j) ポリシー マップ リストから一致基準を削除するには、一致基準を選択し、[Remove] をクリックします。
k) [Apply] をクリックして、設定を保存します。

ステップ 4 ポリシー マップを次のように削除します。

a) [Policy Map] ページから、ポリシー マップを選択します。

b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します。

WLAN へのローカル ポリシーの適用（GUI）

ステップ 1 [Configuration] > [Wireless] > [WLAN] を選択して、[WLANs] ページを開きます。

ステップ 2 対応する WLAN プロファイルをクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Policy-Mapping] タブをクリックします。

ステップ 4 [Device Classification] チェックボックスをオンにして、デバイス タイプに基づいた分類をイネーブルにします。

ステップ 5 [Local Subscriber Policy] ドロップダウン リストから、WLAN に適用させるポリシーを選択します。

ステップ 6 [Local HTTP Profiling] を選択して、HTTP に基づいてデバイスのプロファイリングをイネーブルにします（任意）。

ステップ 7 [Radius HTTP Profiling] を選択して、RADIUS に基づいてデバイスのプロファイリングをイネーブルにします（任意）。

ステップ 8 [Apply] をクリックして、設定を保存します。

ローカル ポリシーのモニタリング

次のコマンドを使用して、controllerで設定されたローカル ポリシーを監視できます。

表 *1*：ローカル ポリシーのモニタリング コマンド

コマンド	目的
show access-session	表示される各クライアントまたは MAC アドレスの承認ステータス、方式、およびドメインを含むアクセスセッションのサマリーを表示します。
show access-session cache	クライアントの最新の分類を表示します。
show device classifier attached detail	Mac、DHCP、HTTP などのパラメータに基づいてクライアントの最新の分類を表示します。

show access-session mac *mac-address* **details**	マッピングされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。
show access-session mac *mac-address* **policy**	マッピングされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。 また、次の情報を表示する [Resultant Policy] も確認できます。 • セッションが属性をローカルで設定している場合にセッションに適用された最終属性。 • サーバから適用された属性。

例：ローカル ポリシーの設定

次に、サービス テンプレートを作成する例を示します。

```
ControllerDevice(config)# service-template test3
ControllerDevice(config-service-template)# access-group josephacl
ControllerDevice(config-service-template)# vlan 137
ControllerDevice(config-service-template)# absolute-timer 500
ControllerDevice(config-service-template)#  service-policy qos input qosingress
ControllerDevice(config-service-template)# end
```

次に、パラメータ マップを作成する例を示します。

```
ControllerDevice(config)# parameter-map type subscriber attribute-to-service apple-tsim-param
ControllerDevice(config-parameter-map)# 1 map device-type eq "Apple-Device"
ControllerDevice(config-parameter-map)# 1 service-template test1
ControllerDevice(config-parameter-map)# 2 map device-type eq "Apple-Ipad"
ControllerDevice(config-parameter-map)# 1 service-template test2
ControllerDevice(config-parameter-map)# 3 map device-type eq "Android"
ControllerDevice(config-parameter-map)# 1 service-template test3
ControllerDevice(config-parameter-map)# end
```

次に、ポリシー マップを作成する例を示します。

```
ControllerDevice(config)# policy-map type control subscriber apple-tsim
ControllerDevice(config-policy-map)# event identity-update match-all
ControllerDevice(config-policy-map)# 1 class always do-until-failure
ControllerDevice(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
ControllerDevice(config-policy-map)# end
```

次に、WLAN 上のデバイスにポリシーを適用する例を示します。

```
ControllerDevice(config)# wlan wlan1
ControllerDevice(config-wlan)# client vlan VLAN0054
ControllerDevice(config-wlan)# profiling local http
ControllerDevice(config-wlan)# service-policy type control subscriber apple-tsim
ControllerDevice(config-wlan)# no shutdown
ControllerDevice# end
```

ローカル ポリシーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*（セキュリティ コマンド リファレンス ガイド、*Cisco IOS XE Release 3SE*（*Cisco WLC 5700* シリーズ））

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ローカル ポリシーの設定の実行に関する機能履歴

リリース	機能情報
Cisco IOS XE 3E	この機能が導入されました。