SISFベースのデバイストラッキングの設定

SISF ベースのデバイストラッキングに関する情報

SISF ベースのデバイストラッキングの概要

スイッチ統合セキュリティ機能ベース（SISF ベース）のデバイストラッキング機能は、一連のファースト ホップ セキュリティ機能の一部です。

この機能の主な役割は、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡することです。SISF は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ（MAC と IP アドレス）を抽出して、バインディングテーブルに保存します。Cisco TrustSec、IEEE 802.1X、LISP、web 認証などの多くの機能は、この情報の正確性に依存して正常に動作します。

SISF ベースのデバイストラッキングは、IPv4 と IPv6 の両方をサポートします。

SISF ベースのデバイストラッキングが導入されても、レガシーデバイストラッキング CLI（IP デバイストラッキング（IPDT）および IPv6 スヌーピング CLI）は引き続き使用できます。スイッチをブートアップすると、使用可能なコマンドのセットは既存の設定によって異なり、次のいずれかのみが使用可能です。

- SISF ベースのデバイストラッキング CLI、または
- IPDT および IPv6 スヌーピング CLI

（注） IPDT および IPv6 スヌーピングコマンドは廃止されましたが、引き続き使用できます。SISF ベースのデバイストラッキングにアップグレードすることを推奨します。

IPDT および IPv6 スヌーピング CLI を使用していて、SISF ベースのデバイストラッキングに移行する場合、詳細については「レガシー *IPDT* と *IPv6* スヌーピングから *SISF* ベースのデバイストラッキングへの移行」を参照してください。

SISF ベースのデバイストラッキングは、手動で（**device-tracking** コマンドを使用して）、またはプログラムで（デバイス トラッキング サービスを他の機能に提供する場合に）有効にできます。

複数の IA_NA および IA_PD のサポート

場合によっては、ネットワークデバイスが DHCP サーバから複数の IPv6 アドレスを要求して受信することがあります。これは、レジデンシャルゲートウェイがアドレスをその LAN クライアントに配布することを要求する場合など、デバイスの複数のクライアントにアドレスを提供するために実行できます。デバイスが DHCPv6 パケットを送信すると、パケットにはデバイスに割り当てられているすべてのアドレスが含まれます。

SISF は DHCPv6 パケットを分析する際に、パケットの IA_NA（Identity Association-Nontemporary Address）および IA_PD（Identity Association-Prefix Delegation）コンポーネントを検査し、パケットに含まれる各 IPv6 アドレスを抽出します。SISF は、抽出された各アドレスをバインディングテーブルに追加します。

SISF ベースのデバイストラッキングを有効にするオプション

デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。

これを有効にするには、デバイス トラッキング ポリシーを定義し、そのポリシーを特定のターゲットに適用します。

（注） ターゲットは、インターフェイスまたは VLAN です。

SISF ベースのデバイストラッキングの手動による有効化

- オプション 1：**default** デバイス トラッキング ポリシーをターゲットに適用します。

  インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで、**device-tracking** コマンドを入力します。次に、システムは **default** ポリシーをインターフェイスまたは VLAN に適用します。

  （注） **default** ポリシーは、デフォルト設定の組み込みポリシーです。**default** ポリシーの属性は変更できません。デバイス トラッキング ポリシーの属性を設定できるようにするには、カスタムポリシーを作成する必要があります。「オプション *2*：カスタム設定でカスタムポリシーを作成します」を参照してください。

- オプション 2：カスタム設定でカスタムポリシーを作成します。

  グローバル コンフィギュレーション モードで device-tracking policy コマンドを入力し、続けてカスタムポリシー名を入力します。システムにより、指定した名前のポリシーが作成されます。その後、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用可能な設定を行い、指定したターゲットにポリシーを適用できます。

プログラムによる SISF ベースのデバイストラッキングの有効化

一部の機能はデバイストラッキングに依存し、SISF ベースのデバイストラッキングが構築および維持するバインディングエントリの信頼性のあるデータベースを利用します。これらの機能は、デバイス トラッキング クライアントとも呼ばれ、プログラムによりデバイストラッキングを有効にします（デバイス トラッキング ポリシーを作成して適用します）。

（注） ここでの例外は、IEEE 802.1X、web 認証、Cisco TrustSec、IP ソースガード（IPSG）です。これらもデバイストラッキングに依存しますが、有効にはしません。これらのデバイストラッキング クライアントでは、**ip dhcp snooping vlan** *vlan* コマンドを入力して、プログラムにより特定のターゲットでデバイストラッキングを有効にする必要があります。

プログラムによる SISF ベースのデバイストラッキングの有効化については、次の点に注意してください。

- デバイス トラッキング クライアントでは、デバイストラッキングを有効にする必要があります。

  複数のデバイス トラッキング クライアントが存在するため、複数のプログラムポリシーを作成できます。各ポリシーの設定は、ポリシーを作成するデバイス トラッキング クライアントによって異なります。

- 作成されるポリシーとその設定はシステム定義です。

  設定可能なポリシー属性は、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用でき、リリースごとに異なります。設定不可能な属性を変更しようとすると、設定変更は拒否され、エラーメッセージが表示されます。

プログラムによって作成されたポリシーのリリース固有の情報については、マニュアルの必要なバージョンの「*Cisco IOS XE <release name> <release number>* での *SISF* ベースのデバイストラッキングのプログラムによる有効化」を参照してください。

レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドはCLIを異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。

（注） 古い IPDT と IPv6 スヌーピング CLI を SISF ベースのデバイストラッキング CLI と併用することはできません。

IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作に制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースのデバイス トラッキング コマンドに変換します。変換後は、新しいデバイス トラッキング コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースのデバイストラッキング CLI コマンドは使用できません。

IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI コマンドに変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IPDT 設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースのデバイス トラッキング コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

SISF ベースのデバイストラッキングの設定方法

SISF ベースのデバイストラッキングの手動による有効化

ターゲットへのデフォルト デバイス トラッキング ポリシーの適用

デフォルトのデバイス トラッキング ポリシーをインターフェイスまたは VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	インターフェイスまたは VLAN を指定します。 • **interface** *interface* • **vlan configuration** *vlan_list* 例： `Device(config)# interface gigabitethernet 1/1/4`	**interface** *type number*：インターフェイスを指定し、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。デバイス トラッキング ポリシーは、指定されたインターフェイスに適用されます。

	コマンドまたはアクション	目的
	OR Device(config)# **vlan configuration 333**	**vlan configuration** *vlan_list*：VLANを指定し、VLAN機能コンフィギュレーション モードを開始します。デバイス トラッキング ポリシーは、指定されたVLANに適用されます。
ステップ 4	**device-tracking** 例： Device(config-if)# **device-tracking** OR Device(config-vlan-config)# **device-tracking**	SISF ベースのデバイストラッキングを有効にし、デフォルトポリシーをインターフェイスまたはVLANに適用します。 デフォルトポリシーは、デフォルト設定の組み込みポリシーです。デフォルトポリシーの属性は変更できません。
ステップ 5	**end** 例： Device(config-if)# **end** OR Device(config-vlan-config)# **end**	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 VLAN機能コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show device-tracking policy** *policy-name* 例： Device# **show device-tracking policy default**	デバイストラッキング ポリシーの設定と、それが適用されるすべてのターゲットを表示します。

カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成

デバイス トラッキング ポリシーを作成して設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： Device# **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。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_policy`	ポリシーを作成し、デバイストラッキング コンフィギュレーション モードを開始します。

ステップ 4	[**data-glean** | **default** | **destination-glean** | **device-role** | **distribution-switch** | **exit** | **limit** | **no** | **prefix-glean** | **protocol** | **security-level** | **tracking** | **trusted-port** | **vpc**]
	例：
	`Device(config-device-tracking)# destination-glean log-only`
		システムプロンプトに疑問符（?）を入力すると、このモードで使用できるオプションのリストが表示されます。IPv4 と IPv6 の両方に対して以下を設定できます。
		• （任意）**data-glean**：ネットワーク内の送信元からスヌーピングされたデータパケットからのアドレスの学習を有効にし、データトラフィックの送信元アドレスとともにバインディングテーブルを読み込みます。次のいずれかのオプションを入力します。
		  • log-only：データパケット通知時に syslog メッセージを生成します。
		  • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**NDP**または**DHCP**の入力。
		• （任意）**default**：ポリシー属性をデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。**data-glean**、**destination-glean**、**device-role**、**limit**、**prefix-glean**、**protocol**、**security-level**、**tracking**、**trusted-port**。
		• （任意）**destination-glean**：データトラフィックの宛先アドレスを収集して、バインディングテーブルを読み込みます。次のいずれかのオプションを入力します。

	コマンドまたはアクション	目的
		• **log-only**：データパケット通知時に syslog メッセージを生成します。 • **recovery**：プロトコルを使用してバインディングテーブルの回復を有効にします。**DHCP** を入力します。 • （任意）**device-role**：ポートに接続されているデバイスのロールを設定します。ノードまたはスイッチを指定できます。次のいずれかのオプションを入力します。 • node：接続されているデバイスをノードとして設定します。これがデフォルトのオプションです。 • switch：接続されているデバイスをスイッチとして設定します。 • （任意）**distribution-switch**：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 • **exit**：デバイストラッキング ポリシー コンフィギュレーション モードを終了します。 • **limit** address-count：ポートごとのアドレスカウント制限を指定します。有効な範囲は 1 ～ 32000 です。 • **no**：コマンドを無効にするか、デフォルト値を設定します。 • （任意）**prefix-glean**：IPv6 ルータアドバタイズメントまたは DHCP-PD のどちらかからのプレフィックスの学習を有効にします。次のオプションがあります。

	コマンドまたはアクション	目的
		• （任意）**only**：プレフィックスのみを収集し、ホストアドレスは収集しません。 • （任意）**protocol**：収集するプロトコルを設定します。デフォルトでは、すべて収集されます。次のいずれかのオプションを入力します。 • **arp** ［**prefix-list** *name*］：ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **dhcp4** ［**prefix-list** *name*］：DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **dhcp6** ［**prefix-list** *name*］：DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **ndp** ［**prefix-list** *name*］：NDP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。 • **udp** ［**prefix-list** *name*］：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 • （任意）**security-level**：この機能によって適用されるセキュリティのレベルを指定します。次のいずれかのオプションを入力します。 • **glean** ：アドレスをパッシブに収集します。

	コマンドまたはアクション	目的
		• **guard**：不正なメッセージを検査してドロップします。これはデフォルトです。 • **inspect**：メッセージを収集して検証します。 • （任意）**tracking**：トラッキングオプションを指定します。次のいずれかのオプションを入力します。 • **disable** ［**stale-lifetime** ［*1-86400-seconds* | **infinite**］ ］：デバイストラッキングをオフにします。 必要に応じて、エントリを削除するまで非アクティブにする期間を入力することも、永続的に非アクティブにすることもできます。 • **enable** ［**reachable-lifetime** ［*1-86400-seconds* | **infinite**］ ］：デバイストラッキングをオンにします。 必要に応じて、エントリを到達可能にする期間を入力することも、永続的に到達可能にすることもできます。 • （任意）**trusted-port**：信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。 • （任意）**vpc**：このオプションはCLIには表示されますが、サポート

	コマンドまたはアクション	目的
		されていません。行った設定は有効になりません。
ステップ 5	**end** 例： `Device(config-device-tracking)# end`	デバイストラッキングコンフィギュレーションモードを終了し、特権EXECモードに戻ります。
ステップ 6	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy example_policy`	デバイス トラッキング ポリシー設定を表示します。

次のタスク

ポリシーをインターフェイスまたは VLAN に適用します。

デバイス トラッキング ポリシーのインターフェイスへの適用

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** *interface* 例： `Device(config-if)# interface gigabitethernet 1/1/4`	インターフェイスを指定し、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。
ステップ 4	**device-tracking attach-policy** *policy name* 例： `Device(config-if)# device-tracking attach-policy example_policy`	インターフェイスにデバイス トラッキング ポリシーを適用します。デバイス トラッキングは、EtherChannel でもサポートされます。

	コマンドまたはアクション	目的
		（注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show device-tracking policies** [**interface** *interface*] 例： `Device# show device-tracking policies interface gigabitethernet 1/1/4`	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーの VLAN への適用

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	デバイス トラッキング ポリシーを適用する VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**device-tracking attach-policy** *policy_name* 例： `Device(config-vlan-config)# device-tracking attach-policy example_policy`	すべてのスイッチインターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 5	**do show device-tracking policies vlan** *vlan-ID* 例： `Device(config-vlan-config)# do show device-tracking policies vlan 333`	VLAN インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが指定された VLAN に割り当てられていることを確認します。
ステップ 6	**end** 例： `Device(config-vlan-config)# end`	VLAN機能コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

Cisco IOS XE Fuji 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化

表 *1 : Cisco IOS XE Fuji 16.9.x* 以降のリリースでの *SISF* ベースのデバイストラッキングのプログラムによる有効化

SISF ベースのデバイストラッキングを有効にできるデバイス トラッキング クライアント機能	Cisco IOS XE Fuji 16.9.x 以降のリリースでは、次の機能について SISF ベースのデバイストラッキングをプログラムで有効にできます。 • IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能：**ip dhcp snooping vlan** *vlan* コマンドを入力します。 • Cisco Locator/ID Separation Protocol（LISP）。 • EVPN on VLAN （注） プログラムによって作成されたポリシーが複数ある場合は、優先順位が最も高いポリシーが有効になります。

ポリシー名	• IEEE 802.1X、web 認証、Cisco TrustSec、および IPSG 機能は、ポリシー `DT-PROGRAMMATIC` を使用します。 • LISP 機能は、`LISP-DT-GUARD-VLAN` または `LISP-DT-GLEAN-VLAN` を作成します。 • EVPN on VLAN 機能は `evpn-sisf-policy` を作成します 設定のリストは、各プログラムポリシーによって異なります。詳細については、例を参照してください。
ユーザ オプション	• ポリシーの優先順位がサポートされます。優先順位は、ポリシーの作成方法によって決まります。手動で作成されたポリシーが最も優先されます。これにより、プログラムで生成されたポリシーとは異なるポリシー設定を適用できます。 • 複数のポリシーを同じ VLAN に適用できます。 • 優先順位が異なる複数のポリシーが同じ VLAN に適用されている場合、優先順位が最も高いポリシーの設定が有効になります。ここでの例外は **limit address-count for IPv4 per mac** と **limit address-count for IPv6 per mac** の設定です。優先順位が最も低いポリシーの設定が有効になります。 • デバイストラッキング クライアント機能の設定が削除されない限り、ポリシーは削除できません。 • ポリシー属性は変更できません。 • MAC ごとのアドレスカウント制限は変更できません。これは **limit address-count for IPv4 per mac** および **limit address-count for IPv6 per mac** コマンドに該当します。 • VLANのポリシー設定を変更するには、カスタマイズされたデバイストラッキング ポリシーを作成し、VLAN に適用します。 • デバイストラッキング ポリシーが VLAN のインターフェイスに適用されると、インターフェイスのポリシー設定がVLANのポリシー設定よりも優先されます。ここでの例外は、**limit address-count for IPv4 per mac** と **limit address-count for IPv6 per mac** の値で、インターフェイスと VLAN の両方のポリシーから集約されます。

トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定

マルチスイッチネットワークでは、SISFベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインディング テーブル エントリを分散できます。バインディングエン

トリは、ホストがアクセスポートに表示されるスイッチでのみ作成されます。トランクポート経由で表示されるホストのエントリは作成されません。これは、**trusted-port** および **device-role switch** オプションを使用してポリシーを設定し、トランクポートに適用することで実現されます。

重要 ポリシーで、**trusted-port** および **device-role switch** オプションの両方を設定する必要があります。

さらに、SISF ベースのデバイストラッキングが有効になっているデバイス側のポートに、このようなポリシーを適用することを推奨します。

次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_trusted_policy`	指定されたポリシーのデバイストラッキング ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**device-role switch** 例： `Device(config-device-tracking)# device-role switch`	ポートに接続されているデバイスのロールを指定します。デフォルトは node です。ポートのバインディングエントリの作成を停止する **device-role switch** オプションを入力します。
ステップ 5	**trusted-port** 例： `Device(config-device-tracking)# trusted-port`	信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-device-tracking)# exit`	デバイストラッキング ポリシー コンフィギュレーションモードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *interface* 例： `Device(config)# interface gigabitethernet 1/0/25`	インターフェイスを指定し、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。
ステップ 8	**device-tracking attach-policy** *policy-name* 例： `Device(config-if)# device-tracking attach-policy example_trusted_policy`	デバイス トラッキング ポリシーをインターフェイスまたはそのインターフェイス上で指定された VLAN にアタッチします。
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SISF ベースのデバイストラッキングの設定例

次の例は、デバイストラッキングの設定例と、特定の状況で推奨される、または関連するその他の設定を示しています。

例：Cisco IOS XE Everest 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化

この出力例は、プログラムによって作成されたポリシーのさまざまな設定を示しています。

デバイス トラッキング クライアント：VLAN での LISP

LISP を設定したら、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された `LISP-DT-GUARD-VLAN` ポリシーと対応する設定を表示します。

```
Device> enable
Device# show device-tracking policy LISP-DT-GUARD-VLAN

Policy LISP-DT-GUARD-VLAN configuration:
  security-level guard (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4 (*)
```

```
  limit address-count for IPv6 per mac 12 (*)
  tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target      Type    Policy                  Feature           Target range
vlan 10     VLAN    LISP-DT-GUARD-VLAN      Device-tracking   vlan all
  note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer:   30 minutes (*)
```

デバイス トラッキング クライアント：VLAN での LISP

LISP を設定したら、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された `LISP-DT-GLEAN-VLAN` ポリシーと対応する設定を表示します。

```
Device# show device-tracking policy LISP-DT-GLEAN-VLAN

Policy LISP-DT-GLEAN-VLAN configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4 (*)
  limit address-count for IPv6 per mac 12 (*)
  tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target     Type   Policy                Feature           Target range
vlan 10    VLAN   LISP-DT-GLEAN-VLAN    Device-tracking   vlan all

  note:
  Binding entry Down timer: 10 minutes (*)
  Binding entry Stale timer:   30 minutes (*)
```

デバイス トラッキング クライアント：VLAN での EVPN

EVPN を設定した後、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された `evpn-sisf-policy` ポリシーとポリシーに応じて行った設定を表示します。

```
Device# show device-tracking policy evpn-sisf-policy

Policy evpn-sisf-policy configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy evpn-sisf-policy is applied on the following targets:
Target      Type    Policy                  Feature           Target range
vlan 10     VLAN    evpn-sisf-policy        Device-tracking   vlan all
  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

デバイス トラッキング クライアント：IEEE 802.1X、web 認証、Cisco TrustSec、IPSG

グローバル コンフィギュレーション モードで **ip dhcp snooping vlan** *vlan* コマンドを設定して、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能のデバイストラッキングを有効にします。特権 EXEC モードで **show device-tracking policy** コマンドを入力し、作成された DT-PROGRMMATIC ポリシーとポリシーに応じて行った設定を表示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end
Device# show device-tracking policy DT-PROGRAMMATIC

Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type    Policy               Feature            Target range
vlan 10     VLAN    DT-PROGRAMMATIC      Device-tracking    vlan all


  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

ターゲットに複数のポリシーが適用されている場合のアクティブポリシーの識別

この例では、複数のポリシーが同じ VLAN に適用されている場合にアクティブポリシーを指定する方法を示します。

この例では、2 つのポリシーが VLAN 10 に適用されており、LISP-DT-GUARD-VLAN がアクティブポリシーです。

```
Device# show device-tracking policies

Target               Type  Policy                Feature        Target range
vlan 10              VLAN  DT-PROGRAMMATIC       Device-tracking vlan all
vlan 10              VLAN  LISP-DT-GUARD-VLAN    Device-tracking vlan all

Device# show device-tracking capture-policy vlan 10

 HW Target vlan 10 HW policy signature 0001DF9F policies#:2 rules 14 sig 0001DF9F
                SW policy DT-PROGRAMMATIC feature Device-tracking -

                SW policy LISP-DT-GUARD-VLAN feature Device-tracking - Active
```

例：ターゲットでの IPv6 デバイストラッキングの無効化

デフォルトでは、SISF ベースのデバイストラッキングは IPv4 と IPv6 の両方をサポートします。次の設定例は、必要な場合に IPv6 デバイストラッキングを無効にする方法を示しています。

ターゲットがカスタムポリシーに適用されている場合の IPv6 デバイストラッキングの無効化：

```
Device(config)# device-tracking policy example-policy
 Device(config-device-tracking)# no protocol ndp
 Device(config-device-tracking)# no protocol dhcp6
 Device(config-device-tracking)# end
```

ターゲットがプログラムによるポリシーに適用されている場合の IPv6 デバイストラッキングの無効化：

Cisco IOS XE Everest 16.6.x では、プログラムによるポリシーを変更することで、IPv6 デバイストラッキングを無効にできます。

```
Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

ネットワークで IPv6 が有効になっており、VLAN 上でスイッチ仮想インターフェイス（SVI）が設定されている場合は、SVI 設定に次の内容を追加することを推奨します。これにより、SVI はリンクローカルアドレスを自動的に取得できます。このアドレスは SISF プローブの送信元 IP アドレスとして使用されるため、重複 IP アドレスの問題を防止できます。

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

例：IPv4 重複アドレスの問題の緩和

次に、Microsoft Windows を実行しているクライアントによって発生した重複 IP アドレス 0.0.0.0 エラーメッセージの問題に対応する例を示します。

device-tracking tracking auto-source コマンドをグローバル コンフィギュレーション モードで設定します。このコマンドは、デバイストラッキング テーブル内のエントリを維持するために、スイッチがクライアントをプローブするよう送信するアドレス解決パケット（ARP）要求で使用される送信元 IP および MAC アドレスを決定します。その目的は、送信元 IP アドレスとして 0.0.0.0 を使用しないようにすることです。

（注） スイッチ仮想インターフェイス（SVI）が設定されていない場合に、**device-tracking tracking auto-source** コマンドを設定します。SVI が VLAN で IPv4 アドレスを使用して設定されている場合は、設定する必要はありません。

コマンド	アクション （デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するため）	注記
device-tracking tracking auto-source	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 0.0.0.0 を使用します	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。
device-tracking tracking auto-source override	• 存在する場合、VLAN SVI に送信元を設定します。 • 0.0.0.0 を使用します。	SVI がない場合は推奨しません。
ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。 計算された IPv4 アドレスは、クライアントまたはネットワークデバイスに割り当てることはできません。

コマンド	アクション （デバイストラッキング **ARP** プローブの送信元 **IP** および **MAC** アドレスを選択するため）	注記
device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0 override	• 存在する場合、VLAN SVI に送信元を設定します。 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します*。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。	

* クライアント IP アドレスによっては、IPv4 アドレスを送信元 IP 用に予約する必要があります。

予約済み送信元 IPv4 アドレス = (host-ip and mask) | client-ip

- クライアント IP = 192.0.2.25
- 送信元 IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP アドレス 192.0.2.1 をクライアントまたはネットワークデバイスに割り当てないでください。

例：短いデバイストラッキング バインディング到達可能時間の回避

以前のリリースから移行する場合、次の設定が存在している可能性があります。

```
device-tracking binding reachable-time 10
```

コマンドの **no** バージョンを入力して、これを削除します。

```
Device> enable
Device# configure terminal
Device(config)# no device-tracking binding reachable-time 10
Device(config)# end
```

SISF ベースのデバイストラッキングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	SISF ベースのデバイストラッキング	ネットワーク内のエンドノードの存在、ロケーション、移動を追跡します。この機能は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ（MAC と IP アドレス）を抽出して、バインディングテーブルに保存します。その他の機能（デバイス トラッキング クライアント）が適切に動作するには、この情報が正確である必要があります。 IPv4 および IPv6 のどちらもサポートされています。
Cisco IOS XE Fuji 16.9.1	ポリシーの優先順位	ポリシーの優先順位のサポートが導入されました。優先順位は、ポリシーの作成方法によって決まります。手動で作成されたポリシーが最も優先されます。これにより、プログラムで生成されたポリシーとは異なるポリシー設定を適用できます。 デバイス トラッキング クライアント機能が追加されました。プログラムで作成されるポリシーは、デバイス トラッキング クライアントごとに異なります。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.comに進みます。