identity profile ～ ip device tracking probe

identity profile

アイデンティティプロファイルを作成し、アイデンティティプロファイル コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **identity profile** コマンドを使用します。 アイデンティティ プロファイルをディセーブルにするには、このコマンドの **no** 形式を使用します。

identity profile {**default| dot1x| eapoudp| auth-proxy**}

no identity profile {**default| dot1x| eapoudp| auth-proxy**}

構文の説明

default	サービス タイプはデフォルトです。
dot1x	802.1X のサービス タイプ。
eapoudp	Extensible Authentication Protocol over UDP（EAPoUDP）のサービス タイプ。
auth-proxy	認証プロキシのサービス タイプ。

コマンド デフォルト

アイデンティティ プロファイルは作成されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.3(8)T	**eapoudp** キーワードが追加されました。
12.4(6)T	**dot1x** キーワードが削除されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。

リリース	変更内容
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

identity profile コマンドおよび **default** キーワードにより、802.1X をサポートしないクライアントコンピュータのスタティック MAC アドレスを設定し、これらのクライアント コンピュータの許可または無許可を静的に切り替えることができます。 **identity profile** コマンドおよび **default** キーワードを発行し、ルータがアイデンティティ プロファイル コンフィギュレーション モードになると、非認証サプリカント（クライアントコンピュータ）がマッピングされる仮想アクセスインターフェイスの作成に使用可能なテンプレートの設定を指定できます。

identity profile コマンドおよび **dot1x** キーワードはサプリカントとオーセンティケータによって使用されます。 **dot1x** キーワードを使用して、802.1X 認証用のユーザ名、パスワード、またはその他のアイデンティティ関連の情報を設定できます。

identity profile コマンドおよび **eapoudp** キーワードを使用して、デバイスの IP アドレス、MAC アドレス、またはタイプに基づいてデバイスの認証または非認証を静的に切り替えることができ、**identity policy** コマンドを使用して、対応するネットワーク アクセス ポリシーを指定できます。

例

次に、アイデンティティ プロファイルおよびその説明を指定する例を示します。

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

次に、EAPoUDP アイデンティティ プロファイルを作成する例を示します。

```
Router (config)# identity policy eapoudp
```

関連コマンド

コマンド	説明
debug dot1x	802.1X デバッグ情報を表示します。
description	802.1X プロファイルの説明を指定します。
device	静的に個々のデバイスを許可または拒否します。
dot1x initialize	すべての 802.1X 対応インターフェイスで 802.1X ステート マシンを初期化します。

コマンド	説明
dot1x max-req	ルータがクライアント PC に EAP 要求/アイデンティティ フレームを送信できる最大回数を設定します。
dot1x max-start	オーセンティケータがクライアントに EAP 要求/アイデンティティ フレームを送信する最大回数を設定します（応答が受信されないと仮定）。
dot1x pae	802.1X 認証中の PAE タイプを設定します。
dot1x port-control	制御ポートの許可ステートの手動制御をイネーブルにします。
dot1x re-authenticate	指定した 802.1X 対応ポートの再認証を手動で開始します。
dot1x re-authentication	802.1X インターフェイスのクライアント PC の定期的な再認証をグローバルでイネーブルにします。
dot1x system-auth-control	802.1X SystemAuthControl（ポートベース認証）をイネーブルにします。
dot1x timeout	再試行タイムアウトを設定します。
identity policy	アイデンティティ ポリシーを作成します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
template（アイデンティティ プロファイル）	コマンドをクローニングできる仮想テンプレートを指定します。

ip access-group

インターフェイスまたはサービス ポリシー マップに IP アクセス リストまたはオブジェクト グループ アクセス コントロール リスト（OGACL）を適用するには、適切なコンフィギュレーション モードで **ip access-group** コマンドを使用します。 IP アクセス リストまたは OGACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-group {*access-list-name*| *access-list-number*} {**in**| **out**}

no ip access-group {*access-list-number*| *access-list-name*} {**in**| **out**}

構文の説明

access-list-name	**ip access-list** コマンドで指定された既存の IP アクセスリストまたは OGACL の名前。
access-list-number	既存のアクセス リストの番号。 • 標準または拡張の IP アクセス リストの 1 から 199 の整数。 • 標準または拡張の IP 拡張アクセス リストの 1300 から 2699 の整数。
in	インバウンドパケットに対してフィルタリングします。
out	発信パケットをフィルタリングします。

コマンド デフォルト

アクセス リストは適用されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）サービス ポリシーマップ コンフィギュレーション（config-service-policymap）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
11.2	引数 *access-list-name* が追加されました。

リリース	変更内容
12.2(28)SB	このコマンドが、サービス ポリシーマップ コンフィギュレーション モードで使用可能になりました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	*access-list-name* キーワードが、OGACL の名前を受け入れるように変更されました。
Cisco IOS XE 3.3S	このコマンドが Cisco IOS XE Release 3.3S に統合されました。

使用上のガイドライン

指定したアクセス リストが存在しない場合は、すべてのパケットが通過します（警告メッセージは発行されません）。

インターフェイスへのアクセス リストの適用

アクセス リストまたは OGACL は、発信インターフェイスまたは着信インターフェイスに適用されます。 標準着信アクセス リストでは、インターフェイスがパケットを受信すると、Cisco IOS ソフトウェアがパケットの送信元アドレスをアクセス リストと比較して確認します。拡張アクセス リストまたは OGACL の場合は、ネットワーキング デバイスも宛先アクセス リストまたは OGACL を確認します。 アクセス リストまたは OGACL がアドレスを許可する場合は、ソフトウェアはパケットの処理を継続します。 アクセス リスト OGACL がアドレスを拒否している場合は、パケットを廃棄し、インターネット制御管理プロトコル（ICMP）ホスト到達不能メッセージを返します。

通常の発信アクセス リストでは、デバイスがパケットを受信して、それを制御されたインターフェイスへ送信した後、ソフトウェアがパケットの送信元アドレスをアクセス リストと比較して確認します。 拡張アクセス リストまたは OGACL の場合は、ネットワーキング デバイスも宛先アクセス リストまたは OGACL を確認します。 アクセス リストまたは OGACL がアドレスを許可した場合、ソフトウェアはパケットを送信します。 アクセス リストまたは OGACL がアドレスを拒否している場合は、パケットを廃棄し、ICMP ホスト到達不能メッセージを返します。

発信アクセス リストまたは OGACL をイネーブルにすると、そのインターフェイスの自律スイッチングは自動的にディセーブルになります。 任意の CBus インターフェイスまたは CxBus インターフェイス上で着信アクセス リストまたは OGACL をイネーブルにすると、すべてのインターフェイスの自律スイッチングが自動的にディセーブルになります（例外：簡易アクセス リストにより設定された Storage Services Enabler（SSE）は、出力に対してのみ、パケットのスイッチングを継続して行えます）。

サービス ポリシー マップへのアクセス リストまたは OGACL の適用

ip access-group コマンドを使用して、Intelligent Services Gateway（ISG）の加入者単位のファイアウォールを設定できます。 加入者単位のファイアウォールは Cisco IOS ACL IP アクセス リストま

たはOGACLであり、加入者、サービス、およびパススルートラフィックが特定のIPアドレスおよびポートにアクセスしないようにするために使用します。

ACLおよびOGACLは、認証、許可、およびアカウンティング（AAA）サーバ上のユーザ プロファイルまたはサービス プロファイル、またはISG上のサービス ポリシー マップで設定できます。 OGACLまたは番号付きまたは名前付きIPアクセス リストはISG上で設定でき、ACLステートメントまたはOGACLステートメントをプロファイル設定に含めることができます。

ACLまたはOGACLをサービスに追加すると、そのサービスのすべての加入者は、そのサービスによる指定されたIPアドレス、サブネットマスク、およびポートの組み合わせにアクセスできなくなります。

例

次に、イーサネット インターフェイス0から発信されるパケットに対して、リスト101を適用する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

関連コマンド

コマンド	説明
deny	名前付きIPアクセス リストまたはOGACLにおいて、パケットを拒否する条件を設定します。
ip access-list	IPアクセスリストまたはOGACLを名前または番号で定義します。
object-group network	OGACLで使用するネットワーク オブジェクト グループを定義します。
object-group service	OGACLで使用するサービス オブジェクト グループを定義します。
permit	名前付きIPアクセス リストまたはOGACLにおいて、パケットを許可する条件を設定します。
show ip access-list	IPアクセスリストまたはOGACLの内容を表示します。
show object-group	設定されているオブジェクト グループに関する情報を表示します。

ip access-list

IP アクセス リストまたはオブジェクト グループ アクセス コントロール リスト（ACL）を名前または番号で定義する、または IP ヘルパー アドレスの宛先を持つパケットのフィルタリングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip access-list** コマンドを使用します。 IP アクセス リストまたはオブジェクト グループ ACL を削除する、または IP ヘルパー アドレスの宛先を持つパケットのフィルタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

no ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

構文の説明

standard	標準 IP アクセス リストを指定します。
extended	拡張 IP アクセス リストを指定します。 オブジェクト グループ ACL に必要です。
access-list-name	IP アクセス リストまたはオブジェクト グループ ACL の名前。 名前には、スペースまたは引用符を含めることができず、番号付けされたアクセスリストと混乱しないように、英文字で始める必要があります。
access-list-number	アクセス リスト番号。 • 標準 IP アクセス リストの範囲は、1 ～ 99 または 1300 ～ 1999 です。 • 拡張 IP アクセス リストの範囲は、100 ～ 199 または 2000 ～ 2699 です。
helper egress check	IP ヘルパー機能によって宛先サーバ アドレスにリレーされるトラフィックに対して、インターフェイスに適用される発信アクセス リストの照合機能の許可または拒否をイネーブルにします。

コマンド デフォルト

IP アクセス リストまたはオブジェクト グループ ACL は定義されないため、発信 ACL は IP ヘルパーによってリレーされるトラフィックを照合またはフィルタリングしません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.2	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが変更されました。 **deny** コマンドおよび **permit** コマンドが標準 IP アクセスリスト コンフィギュレーション モードまたは拡張 IP アクセスリスト コンフィギュレーション モードで使用されている場合に、オブジェクト グループ ACL が受け入れられるようになりました。
Cisco IOS XE Release 3.2S	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.0(1)M5	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(1)SY	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(3)T3	このコマンドが変更されました。 **helper**、**egress**、および**check** キーワードが追加されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

名前付きまたは番号付き IP アクセス リストまたはオブジェクト グループ ACL を設定するには、このコマンドを使用します。 このコマンドにより、ルータはアクセス リスト コンフィギュレーション モードになります。その場合は、**deny** コマンドおよび **permit** コマンドを使用して、拒否または許可されるアクセス条件を定義する必要があります。

ip access-list コマンドで **standard** キーワードまたは **extended** キーワードを指定すると、アクセスリストコンフィギュレーションモードを開始したときに表示されるプロンプトが決定されます。オブジェクトグループACLを定義する場合は、**extended**キーワードを使用する必要があります。

オブジェクト グループおよびIPアクセス リストまたはオブジェクト グループACLは単独で作成できます。つまり、まだ存在していないオブジェクト グループ名を使用できます。

名前付きアクセス リストは、リリース 11.2 以前の Cisco IOS ソフトウェア リリースと互換性がありません。

ip access-group コマンドを使用して、アクセス リストをインターフェイスに適用します。

ip access-list helper egress check コマンドは、IP ヘルパー アドレス宛先を持つパケットの許可機能または拒否機能の発信 ACL 照合をイネーブルにします。 このコマンドとともに発信拡張 ACL を使用すると、送信元または宛先のユーザ データグラム プロトコル（UDP）ポートに基づいて IP ヘルパーによってリレーされたトラフィックを許可または拒否できます。 **ip access-list helper egress check** コマンドは、デフォルトでディセーブルです。出力 ACL は IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

例

次に、Internetfilter という名前の標準アクセス リストを定義する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

次に、プロトコル ポートが my_service_object_group で指定されたポートと一致した場合に、my_network_object_group のユーザからのパケットを許可するオブジェクト グループ ACL を作成する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

次に、ヘルパー アドレスの宛先を持つパケットの発信 ACL フィルタリングをイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

関連コマンド

コマンド	説明
deny	パケットを拒否する名前付き IP アクセス リストまたはオブジェクト グループ ACL の条件を設定します。
ip access-group	インターフェイスまたはサービス ポリシーマップに ACL またはオブジェクト グループ ACL を適用します。
object-group network	オブジェクト グループ ACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	オブジェクト グループ ACL で使用するサービス オブジェクト グループを定義します。

コマンド	説明
permit	パケットを許可する名前付き IP アクセス リストまたはオブジェクト グループ ACL の条件を設定します。
show ip access-list	IP アクセス リストまたはオブジェクト グループ ACL の内容を表示します。
show object-group	設定されているオブジェクト グループに関する情報を表示します。

ip access-list resequence

アクセス リストのアクセス リスト エントリにシーケンス番号を適用するには、グローバル コンフィギュレーション モードで **ip access-list resequence** コマンドを使用します。

ip access-list resequence *access-list-name* **starting-sequence-number** *increment*

構文の説明

access-list-name	アクセス リストの名前。 名前にスペースや引用符を含めることはできません。
starting-sequence-number	アクセス リストのエントリは、この初期値を使用して、並べ直されます。 デフォルト値は 10 です。 可能なシーケンス番号の範囲は 1 ～ 2147483647 です。
increment	シーケンス番号が変更される幅の数値。 デフォルト値は 10 です。 たとえば、increment 値が 5 で開始シーケンス番号が 20 の場合、以降のシーケンス番号は 25、30、35、40 と続きます。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(14)S	このコマンドが導入されました。
12.2(15)T	このコマンドが、Cisco IOS Release 12.2(15)T に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドにより、指定されたアクセス リストの **permit** エントリおよび **deny** エントリを、*starting-sequence-number* 引数により決定され初期シーケンス番号値で並べ直すことができ、これは、*increment* 引数に決定された増分により増え続けます。最も大きいシーケンス番号が使用可能な最大シーケンス番号を超える場合は、シーケンシングが発生しません。

以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は 10 ずつ増分されます。 最大シーケンス番号は 2147483647 です。 生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。

（シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。

既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。

分散サポートが提供されます。ルート プロセッサ（RP）とラインカード（LC）にあるエントリのシーケンス番号は、常に同期されます。

シーケンス番号は NVRAM に保存されません。 つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号と増分に戻されます。

このコマンドは、名前付きの標準および拡張 IP アクセス リストと連動します。 アクセス リストの名前は番号として指定できるため、番号、名前付きアクセス リスト コンフィギュレーション モードで入力されている限り、番号を名前として使用できます。

例

次に、kmd1 という名前のアクセス リストを並べ直す例を示します。 開始シーケンス番号は 100、増分値は 5 です。

```
ip access-list resequence kmd1 100 5
```

関連コマンド

コマンド	説明
deny（IP）	パケットが名前付き IP アクセス リストを通過しない条件を設定します。

コマンド	説明
permit（IP）	パケットが名前付き IP アクセス リストを通過する条件を設定します。

ip admission

インターフェイスに適用されるレイヤ 3 ネットワーク アドミッション コントロール ルールを作成する、または認証、許可、アカウンティング（AAA）サーバが到達不能な場合にインターフェイスに適用できるポリシーを作成する場合は、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。ネットワーク アクセス デバイスに適用できるグローバル ポリシーを作成するには、グローバル コンフィギュレーション モードで**任意のキーワード**および引数**を指定して ip admission コマンド**を使用します。アドミッション コントロール ルールを削除するには、このコマンドの **no** 形式を使用します。

ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

構文の説明

admission-name	認証ルールまたは許可ルールの名前。
event timeout aaa policy identity	AAA サーバが到達不能である場合に適用される認証ポリシーを指定します。
identity-policy-name	AAA サーバが到達不能の場合に適用される認証ルールまたは許可ルールの名前。

コマンド デフォルト

ネットワーク アドミッション コントロール ルールは、インターフェイスには適用されません。

コマンド モード

インターフェイス コンフィギュレーション（config）グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.4(11)T	このコマンドが、**event timeout aaa policy identity** キーワードおよび *identity-policy-name* 引数を含むように変更されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

許可ルールは、アドミッション コントロールを適用する方法を定義します。

任意のキーワードおよび引数は、AAA サーバが到達不能な場合にネットワーク アクセス デバイスまたはインターフェイスに適用されるネットワーク アドミッション ポリシーを定義します。このコマンドを使用して、デフォルトのアイデンティティ ポリシーを Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）セッションに関連付けることができます。

例

次に、「nacrule1」という名前のネットワーク アドミッション コントロール ルールをインターフェイスに適用する例を示します。

```
Router (config-if)# ip admission nacrule1
```

次に、AAA サーバが到達不能な場合に「example」という名前のアイデンティティ ポリシーをデバイスに適用する例を示します。

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```

関連コマンド

コマンド	説明
interface	インターフェイスを定義します。

ip admission proxy http

Web ベース認証中のカスタム認証プロキシ Web ページの表示を指定するには、グローバル コンフィギュレーション モードで **ip admission proxy http** コマンドを使用します。 デフォルトの Web ページの使用を指定するには、このコマンドの **no** 形式を使用します。

ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

no ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

構文の説明

login	ログイン時に表示される、ローカルに保存された Web ページを指定します。
success	ログインが成功した場合に表示される、ローカルに保存された Web ページを指定します。
failure	ログインが失敗した場合に表示される、ローカルに保存された Web ページを指定します。
login expired	ログインが期限切れになった場合に表示される、ローカルに保存された Web ページを指定します。
device	カスタム HTML ファイルが保存されているスイッチのメモリ ファイル システムのディスクまたはフラッシュ メモリを指定します。
file-name	指定した条件において、デフォルトの HTML ファイルの代わりに使用するカスタム HTML ファイルの名前を指定します。
success redirect *url*	ログインが成功した場合に表示される、外部 Web ページを指定します。

コマンド デフォルト

Web ベース認証時には、デフォルトの内部認証プロキシ Web ページが表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

カスタマイズされた認証プロキシ Web ページの使用を設定する場合は、次の注意事項を考慮してください。

- カスタム Web ページ機能をイネーブルにするには、4 つのすべてのカスタム HTML ファイルを指定する必要があります。 4 つ未満のファイルが指定されている場合は、内部デフォルト HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルはスイッチのディスクまたはフラッシュに存在している必要があります。 各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のイメージは、アクセス可能な HTTP サーバ上になければなりません。 HTTP サーバにアクセスできるように、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム ページからのすべての外部リンクでは、アドミッション ルール内で代行受信 ACL を設定する必要があります。
- 外部リンクまたは画像に必要なすべての名前解決では、有効な DNS サーバにアクセスするためにアドミッション ルール内で代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルである場合、成功ログイン機能のリダイレクション URL は利用不可能です。
- カスタム ログイン ページはパブリック Web 形式であるため、このページについて次の注意事項に留意してください。
  - ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを uname および pwd として POST する必要があります。
  - カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。
- ログイン成功時のリダイレクション URL を設定する場合、次の注意事項に従ってください。
  - カスタム認証プロキシ Web ページ機能がイネーブルである場合、リダイレクション URL 機能はディセーブルに設定され、CLI で利用できなくなります。 リダイレクションはカスタム ログイン成功ページ内で実行できます。
  - リダイレクション URL 機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。

例

次に、カスタム認証プロキシ Web ページを設定する例を示します。

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

次に、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
Router# show ip admission configuration
Authentication proxy webpage
 Login page          : disk1:login.htm
 Success page        : disk1:success.htm
 Fail Page           : disk1:fail.htm
 Login expired Page : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

次に、ログイン成功時のリダイレクション URL を設定する例を示します。

```
Router(config)# ip admission proxy http success redirect www.example.com
```

次に、ログイン成功時のリダイレクション URL を確認する例を示します。

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.example.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

関連コマンド

コマンド	説明
ip http server ip https server	スイッチ内の HTTP サーバをイネーブルにします。
show ip admission configuration	Web ベース認証 IP アドミッションの設定を表示します。

ip device tracking probe

デバイス プローブのトラッキングをイネーブルにするには、コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。 デバイス プローブをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking probe {**count** *count*| **delay** *delay*| **interval** *interval*}

構文の説明

count *count*	1 ～ 5 の IP トラッキング プローブの数を指定します。
delay *delay*	1 ～ 120 秒の IP トラッキング プローブの遅延時間を指定します。
interval *interval*	30 ～ 300 分の IP トラッキング プローブの間隔を指定します。

コマンド デフォルト

デバイス プローブ トラッキングはディセーブルです。

コマンド モード

コンフィギュレーション モード（config #）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	このコマンドが導入されました。

例

次に、プローブの数を 5 に設定する例を示します。

```
Router(config)# ip device tracking probe count 5
```

次に、遅延時間を 60 に設定する例を示します。

```
Router(config)# ip device tracking probe delay 60
```

次に、間隔を 35 に設定する例を示します。

```
Router(config)# ip device tracking probe interval 35
```

関連コマンド

コマンド	説明
show ip device tracking	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。