client ～ crl

client

デバイスに許可変更（CoA）および切断要求を送信する RADIUS クライアントを指定するには、動的許可ローカル サーバ コンフィギュレーション モードで **client** コマンドを使用します。 この指定を削除するには、このコマンドの **no** 形式を使用します。

client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

no client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

構文の説明

name	RADIUS クライアントのホスト名。
ip-address	RADIUS クライアントの IP アドレス。
key	（任意）デバイスと RADIUS クライアントの間で共有される RADIUS キーを設定します。
0	（任意）暗号化されていないキーが後ろに続くように指定します。
7	（任意）暗号化されたキーが後ろに続くように指定します。
word	（任意）暗号化されていないサーバ キー
vrf *vrf-id*	（任意）クライアントの仮想ルーティングおよびフォワーディング（VRF）ID。

コマンド デフォルト

CoA および切断要求はドロップされます。

コマンド モード

動的許可ローカル サーバ 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(28)SB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが、Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

デバイス（ルータなど）は、外部ポリシー サーバがルータに動的に更新を送信できるように設定できます。 この機能は、CoA RADIUS 拡張によって容易になります。 CoA は、RADIUS にピアツーピア機能を導入しました。これにより、ルータと外部ポリシー サーバをそれぞれ RADIUS クライアントとサーバとして機能させることができます。 **client** コマンドを使用して、ルータがサーバとして機能する RADIUS クライアントを指定します。

例

次に、ルータが、IP アドレス 10.0.0.1 の RADIUS クライアントから要求を受け入れるように設定する例を示します。

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

関連コマンド

コマンド	説明
aaa server radius dynamic-author	外部ポリシー サーバとの相互作用が容易になるように、ISG を AAA サーバとして設定します。

crl

公開キー インフラストラクチャ（PKI）トラストプールの証明書失効リスト（CRL）クエリーおよび CRL キャッシュ オプションを指定するには、ca-trustpool コンフィギュレーション モードで **crl** コマンドを使用します。 デフォルトの動作に戻し、証明書に埋め込まれている URL をルータが確認するようにするには、このコマンドの **no** 形式を使用します。

crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

no crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

構文の説明

cache	CRL キャッシュ オプションを指定します。
delete-after	タイムアウト後にキャッシュから CRL を削除します。
minutes	キャッシュから CRL を削除する前に待機する時間を分単位で指定します。範囲は 1 ～ 43200 分です。
none	CRLがキャッシュされないように指定します。
query *url*	CRL をクエリーするために認証局（CA）サーバによって発行される URL を指定します。

コマンド デフォルト

CRL はクエリーされません。CRL キャッシュ パラメータは設定されていません。

コマンド モード

ca-trustpool コンフィギュレーション（ca-trustpool）

コマンド履歴

リリース	変更内容
15.2(2)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

このコマンドを設定する前に、**crypto pki trustpool policy** コマンドをイネーブルにして ca-trustpool コンフィギュレーション モードを開始する必要があります。

crl query コマンドは、CDP が Lightweight Directory Access Protocol（LDAP）形式の場合に使用されます。これは、証明書内の CDP の場所が、ディレクトリ内の CRL 分散ポイント（CDP）が置かれている場所だけを示すことを意味します。つまり、CDP は実際のクエリーの場所を示しません。

Cisco IOS ソフトウェアでは、ピア証明書を確認するために証明書が取り消されないように CRL をクエリーします（たとえば、インターネット キー交換（IKE）または Secure Sockets Layer（SSL）ハンドシェイク中に）。 クエリーは、CRL のダウンロードに使用される証明書の CDP 拡張を探します。 このクエリーが失敗した場合は、CA サーバから直接 CRL をクエリーするために Simple Certificate Enrollment Protocol（SCEP）GetCRL メカニズムが使用されます（一部の CA サーバはこの方式をサポートしていません）。

Cisco IOS ソフトウェアは、次の CDP エントリをサポートしています。

- HTTP URL + ホスト名 （例：http://myurlname/myca.crl）。
- HTTP URL + IPv4 アドレス （例：http://10.10.10.10:81/myca.crl）。
- LDAP URL + ホスト名 （例：ldap://CN=myca、O=cisco）。
- LDAP URL + IPv4 アドレス （例：ldap://10.10.10.10:3899/CN=myca、O=cisco）。
- LDAP/X.500 DN （例：CN=myca、O=cisco）。

Cisco IOS には、CDP を検索するための完全な URL が必要です。

例

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

関連コマンド

コマンド	説明
cabundle url	PKI トラストプール CA バンドルをダウンロードする URL を設定します。
chain-validation	PKI トラストプールの、ピアの証明書からルート CA 証明書までのチェーン バリデーションをイネーブルにします。

コマンド	説明
crypto pki trustpool import	CA 証明書バンドルを PKI トラストプールに手動でインポート（ダウンロード）し、既存の CA バンドルを更新または置換します。
crypto pki trustpool policy	PKI トラストプールのポリシーパラメータを設定します。
default	ca-trustpool コンフィギュレーション コマンドの値をデフォルトにリセットします。
match	PKI トラストプールの証明書マップの使用をイネーブルにします。
ocsp	PKI トラストプールの OCSP 設定を指定します。
revocation-check	PKI トラストプール ポリシーが使用される場合の失効チェックをディセーブルにします。
show	ルータの PKI トラストプール ポリシーを ca-trustpool コンフィギュレーション モードで表示します。
show crypto pki trustpool	PKI トラストプールの CRL 取得、OCSP ステータス、または CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。
source interface	PKI トラストプールの CRL 取得、OCSP ステータス、または CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。
storage	ルータ上の、PKI トラストプール証明書が保存されるファイルシステムの場所を指定します。

コマンド	説明
vrf	CRL 取得に使用する VRF インスタンスを指定します。