CHAPTER 21

SCEP の設定

SCEP の概要

Simple Certificate Enrollment Protocol は、ネットワーク機器およびソフトウェアの製造業者が使用するプロトコルであり、一般ユーザの大規模導入に対する証明書の処理を簡素化します。このプロトコルは、標準ネットワーク ユーザが電子的かつできるだけ容易にデジタル署名を要求できるよう、デジタル証明書の発行ができるだけスケーラブルになるように設計されています。

Cisco Aironet Autonomous アクセス ポイントでは、このプロトコルは、大規模導入で自動登録とデジタル署名の更新を行うために実装されています。

SCEP サーバの設定

グローバル コンフィギュレーション モードを開始し、次のコマンドを実行して SCEP サーバを設定します。

	コマンド	目的
ステップ 1	**sntp server** *ip_address*	SNTP サーバの IP アドレスを指定します。
ステップ 2	**crypto key generate rsa general-keys label** *RSA_keypair_label* **exportable**	**general-keys** 引数は汎用キー ペアが生成されることを指定します。これがデフォルト設定です。 *RSA_keypair_label* は、RSA キー ペアをエクスポートするときにそのキー ペアに使用する名前を指定します。 **exportable** 引数は、ルータなどの別のシスコ デバイスに RSA キー ペアをエクスポートできることを指定します。
ステップ 3	**ip http server**	HTTP サーバをイネーブルにします。
ステップ 4	**crypto pki server** *server_name*	認証局（CA）サーバを有効にして設定します。 SCEP は CA 証明書を使用して、メッセージ交換を保護します。証明書サーバでは、手動で生成された RSA キー ペアと同じ名前を使用する必要があります。
ステップ 5	**no database archive**	フラッシュ メモリのみに書き込むすべてのデータベース エントリを設定します。
ステップ 6	**issuer-name CN=***CA_certificate_issuer_name* **L=***Locality* **C=***Country*	CA 証明書の発行元の名前、地域、および CA 証明書の国を設定します。

	コマンド	目的
ステップ 7	**grant auto**	証明書の自動認可を設定します。
ステップ 8	**lifetime certificate**	証明書の有効期限を指定します。
ステップ 9	**lifetime ca-certificate** *number_of_days*	日数を指定して、CA 証明書の有効期限を指定します。
ステップ 10	**end**	設定を終了します。

SCEP クライアントの設定

グローバル コンフィギュレーション モードを開始し、次のコマンドを実行して SCEP クライアントを設定します。

	コマンド	目的
ステップ 1	**sntp server** *ip_address*	SNTP サーバの IP アドレスを指定します。
ステップ 2	**crypto key generate rsa**	R2 キー ペアを生成します。
ステップ 3	**crypto ca trustpoint cisco**	AP が使用する必要がある CA サーバ（Cisco IOS CA など）に宣言すると、その後のコマンドでトラストポイント CA の特性を指定できます。 **crypto ca trustpoint** コマンドは、既存の **crypto ca identity** コマンドと **crypto ca trusted-root** コマンドを統合し、これによって、1 つのコマンドで複合的な機能が提供されます。
ステップ 4	**enrollment retry count** 5	
ステップ 5	**enrollment retry period** 3	
ステップ 6	**enrollment url** http://175.68.186.79:80	
ステップ 7	**revocation-check none**	
ステップ 8	**auto-enroll** 60	
ステップ 9	**crypto ca authenticate cisco**	CA サーバからルート証明書を取得します。ここでは、**cisco** はトラストポイント ラベルです。
ステップ 10	**crypto ca enroll cisco**	CA 証明書を登録および生成します。ここでは、**cisco** はトラストポイント ラベルです。
ステップ 11	**end**	設定を終了します。

Cisco IOS CA サーバに正常に登録された後、**show crypto ca certificates** コマンドを使用すると発行された証明書を確認できます。

ワークグループ ブリッジの設定

グローバル コンフィギュレーション モードを開始し、次のコマンドを実行してワークグループ ブリッジを設定します。

	コマンド	目的
ステップ 1	**crypto pki trustpoint** *name_of_trustpoint*	トラストポイントを作成し、名前を指定します。 このコマンドをイネーブルにすると、ca-trustpoint コンフィギュレーション モードが開始されます。
ステップ 2	**enrollment retry count** *number*	以前の要求への応答が得られない場合に、スイッチが証明書要求を再送信する回数を指定します。1 ～ 100 回の再試行を指定できます。デフォルトは 10 回です
ステップ 3	**enrollment retry period** *minutes*	証明書要求の次の再試行までの待機時間を分単位で指定します。1 ～ 60 分の待機時間を指定できます。デフォルトは 1 分です。
ステップ 4	**enrollment url** *http://ip-address:subnet*	スイッチが証明書要求を送信する CA の URL を指定します。URL は、*http://CA_name* という形式にする必要があります。ここで、*CA_name* は CA のホスト DNS 名または IP アドレスです。
ステップ 5	**revocation-check none**	
ステップ 6	**auto-enroll** *60*	
ステップ 7	**crypto pki authenticate CA** *name of the CA*	CA の証明書を取得することによって、CA を認証します。
ステップ 8	**crypto pki enroll** *name of the CA*	CA 証明書を取得します。
ステップ 9	**crypto pki trustpoint** *CA server name*	
ステップ 10	**enrollment terminal pem**	PEM 形式の証明書要求をコンソール端末に対して生成するようトラストポイントを設定します。 証明書を手動でコピーして貼り付けて、登録を行う必要があります。証明書要求はコンソール端末上に表示されます。これを手動でコピーする必要があります。
ステップ 11	**revocation-check none**	
ステップ 12	**crypto pki authen radiuscert**	CA 証明書を取得して、認証します。
ステップ 13	**crypto pki export cisco pem terminal**	コンソール端末で証明書を手動でエクスポートして貼り付けます。