



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	<code>sntp server ip_address</code>	Sntp サーバの IP アドレスを指定します。
ステップ 2	<code>crypto key generate rsa general-keys label RSA_keypair_label exportable</code>	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	<code>ip http server</code>	HTTP サーバをイネーブルにします。
ステップ 4	<code>crypto pki server server_name</code>	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	<code>no database archive</code>	フラッシュ メモリのみ書き込むすべてのデータベース エントリを設定します。

	コマンド	目的
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。
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 <i>name_of_trustpoint</i>	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 <i>number</i>	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 <i>minutes</i>	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 <i>http://ip-address:subnet</i>	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、 <i>http://CA_name</i> という形式にする必要があります。ここで、 <i>CA_name</i> 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 <i>none</i>	
ステップ 6	auto-enroll <i>60</i>	
ステップ 7	crypto pki authenticate <i>CA name of the CA</i>	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 <i>name of the CA</i>	CA 証明書を取得します。
ステップ 9	crypto pki trustpoint <i>CA server name</i>	
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 <i>none</i>	
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。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。