Configuring SCEP

Understanding SCEP

Simple Certificate Enrollment Protocol is a protocol which is used by manufacturers of network equipment and software, to simplify the means of handling certificates for large-scale implementation to everyday users. The protocol is designed to make the issuing of digital certificates as scalable as possible, so that an standard network user should be able to request their digital certificate electronically and as easily as possible.

In the case of autonomous Cisco Aironet access points, this protocol is being implemented for automatic enrollment and renewal of digital certificates in large-scale deployments.

Configuring the SCEP Server

Start in global configuration mode and execute the following commands to configure the SCEP server.

	Command	Purpose
Step 1	**sntp server** *ip_address*	Specify the IP address of the SNTP server.
Step 2	**crypto key generate rsa general-keys label** *RSA_keypair_label* **exportable**	The **general-keys** argument specifies that a general-purpose key pair is to be generated. This is the default setting. The *RSA_keypair_label* specifies the name to be used for the RSA key pair when they are being exported. The **exportable** argument specifies that the RSA key pair can be exported to another Cisco device, such as a router.
Step 3	**ip http server**	Enable the HTTP server.
Step 4	**crypto pki server** *server_name*	Enable and configure the certificate authority (CA) server. SCEP uses the CA certificate in order to secure the message exchange. The certificate server must use the same name as the RSA key pair that was manually generated.
Step 5	**no database archive**	Set all database entries to be written to the Flash memory only.
Step 6	**issuer-name CN=***CA_certificate_issuer_name* **L=***Locality* **C=***Country*	Configure CA certificate issuer name, the locality, and country of the CA certificate.

	Command	Purpose
Step 7	**grant auto**	Set automatic grant of certificates
Step 8	**lifetime certificate**	Specify the lifetime of a certificate
Step 9	**lifetime ca-certificate** *number_of_days*	Specify the lifetime of a CA certificate, by specifying the number of days.
Step 10	**end**	Exit the configuration.

Configuring the SCEP Client

Start in global configuration mode and execute the following commands to configure the SCEP client.

	Command	Purpose
Step 1	**sntp server** *ip_address*	Specify the IP address of the SNTP server.
Step 2	**crypto key generate rsa**	To generate the R2 key pair.
Step 3	**crypto ca trustpoint cisco**	Declare to the CA server that your AP should use, for example, the Cisco IOS CA, and then you can specify characteristics for the trustpoint CA in the commands that follow. Note that the **crypto ca trustpoint** command unifies the existing **crypto ca identity** command and **crypto ca trusted-root** command, thereby providing combined functionality under a single command.
Step 4	**enrollment retry count** 5	
Step 5	**enrollment retry period** 3	
Step 6	**enrollment url** http://175.68.186.79:80	
Step 7	**revocation-check none**	
Step 8	**auto-enroll** 60	
Step 9	**crypto ca authenticate cisco**	To retrieve the root certificate from the CA server. Here, **cisco** is the trustpoint label.
Step 10	**crypto ca enroll cisco**	To enroll and generate the CA certificate. Here, **cisco** is the trustpoint label.
Step 11	**end**	Exit the configuration.

After successfully enrolling in the Cisco IOS CA server, you can see the issued certificates by using the **show crypto ca certificates** command.

Configuring the Workgroup Bridge

Start in global configuration mode and execute the following commands to configure the workgroup bridge.

	Command	Purpose
Step 1	**crypto pki trustpoint** *name_of_trustpoint*	Create and specify the name of a trustpoint. Enabling this command puts you in ca-trustpoint configuration mode.
Step 2	**enrollment retry count** *number*	Specify the number of times a switch should resend a certificate request when it does not receive a response from the previous request. You can specify from 1 to 100 retries. The default is 10 retries.
Step 3	**enrollment retry period** *minutes*	Specify the wait period, in minutes, between certificate request retries. You can specify an wait period from 1 to 60 minutes. The default is 1 minute.
Step 4	**enrollment url** *http://ip-address:subnet*	Specify the URL of the CA where your switch should send certificate requests. The URL must be in the form *http://CA_name*, where *CA_name* is the CA's host DNS name or IP address.
Step 5	**revocation-check none**	
Step 6	**auto-enroll** *60*	
Step 7	**crypto pki authenticate CA** *name of the CA*	Authenticate the CA by obtaining the certificate of the CA.
Step 8	**crypto pki enroll** *name of the CA*	Obtain the CA certificate.
Step 9	**crypto pki trustpoint** *CA server name*	
Step 10	**enrollment terminal pem**	Configures the trustpoint to generate PEM-formatted certificate requests to the console terminal. You will need to perform the manual copy-and-paste certificate enrollment method. The certificate request is displayed on the console terminal, and you need to manually copy it.
Step 11	**revocation-check none**	
Step 12	**crypto pki authen radiuscert**	Retrieves the CA certificate and authenticates it.
Step 13	**crypto pki export cisco pem terminal**	Exports and pastes a certificate manually at the console terminal.