



Enrolling for Digital Certificates

This chapter describes how to enroll for a digital certificate using ASDM. Once enrolled, you can use the certificate to authenticate VPN LAN-to-LAN tunnels and remote access tunnels. If you intend to use only preshared keys to authenticate, you do not need to read this chapter.

This chapter includes the following sections:

- [Overview of Configuration Procedure, page 1-1](#)
- [Understanding Key Pairs, page 1-2](#)
- [Generating an RSA Key Pair, page 1-2](#)
- [Creating the Trustpoint, page 1-3](#)
- [Obtaining Certificates with SCEP, page 1-4](#)
- [Enrolling with the Certificate Authority, page 1-5](#)
- [Managing Certificates, page 1-5](#)



Note

As you following the instructions in this chapter, click **Help** for more information about the attributes shown in the ASDM windows.

Overview of Configuration Procedure

To enroll with a CA and get an identity certificate for authenticating tunnels, complete the following tasks.



Note

This example shows automatic (SCEP) enrollment.

1. Create a key pair for the identity certificate. The key pair can be either RSA or DSA. However, for automatic enrollment, you must use RSA keys. The instructions in the sections that follow show how to generate an RSA key pair.
2. Create a trustpoint. The name of the trustpoint in this example is newmsroot.
3. Configure an enrollment URL. The URL this example uses is `http://10.20.30.40/certsrv/mscep/mscep.dll`.
4. Authenticate the CA.
5. Enroll with the CA, which gets an identity certificate onto the ASA.

Understanding Key Pairs

Each peer has a key pair containing both a public and a private key. These keys act as complements; any communication encrypted with one can be decrypted with the other.

Key pairs can be either RSA keys or DSA keys. Support for these two types of keys differs as follows:

- DSA keys cannot be used for SSH or SSL. To enable SSH or SSL access to a security appliance, use RSA keys.
- SCEP enrollment supports only the certification of RSA keys. If you use DSA keys, you must use manual enrollment.
- For the purposes of generating keys, the maximum key modulus for RSA keys is 2048, and the maximum key modulus for DSA keys is 1024. The default size for either is 1024 bits.
- For signature operations, the maximum key sizes are 4096 bits for RSA keys and 1024 bits for DSA keys.
- You can generate a *general purpose* RSA key pair used for both signing and encryption, or *usage* RSA key pairs separated for each respective purpose, thus requiring two certificates for the corresponding identity. The default setting is general purpose. This topic does not apply to a DSA key pair because it is only for signing.

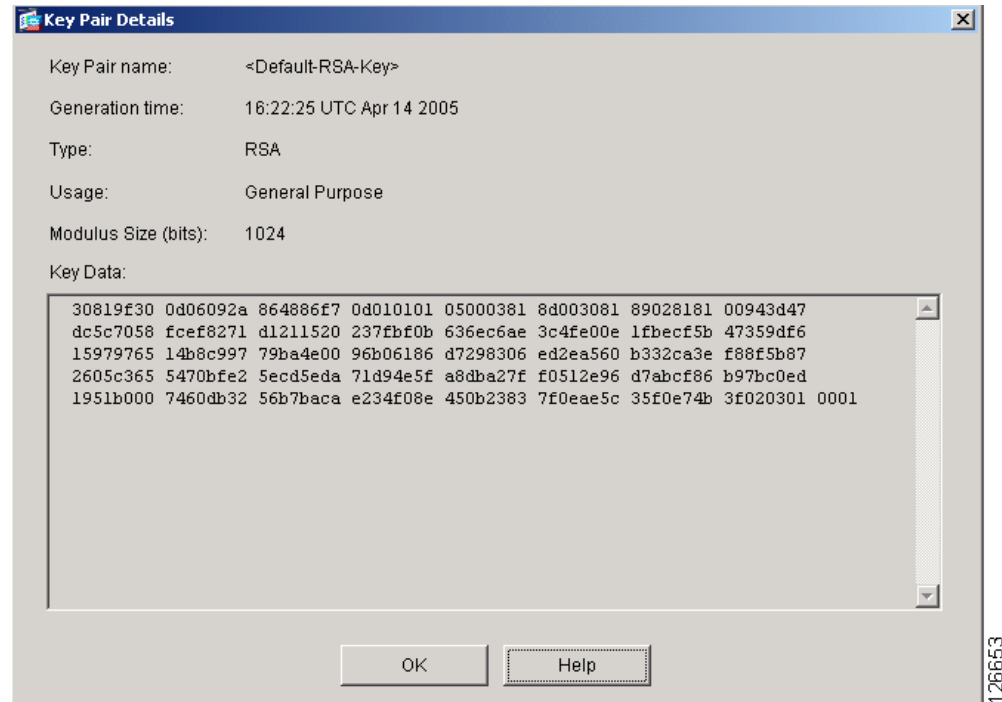
To configure a key pair for a certificate, you specify the labels to identify the key pair to be generated. The following sections show how to generate an RSA key pair with a specified label using ASDM, and use the default settings for the other parameters.

Generating an RSA Key Pair

To generate an RSA key pair, perform the following steps.

-
- Step 1** In the **Configuration > Properties > Certificate > Key Pair** window, click **Add**.
- Step 2** Configure the information in the **Add Key Pair** dialog box:
- Name**—Click to use the default name, or type a name for the key pair(s). This example uses the default RSA key, but you could, instead, enter a name such as key1.
 - Size** list—For an RSA key pair, the **Size** list displays the options: 512, 768, 1024, or 2048. The default size is 1024. This example accepts the default setting.
 - Type** options—**Type** options are RSA and DSA. For this example, accept the default setting, RSA.
 - Usage** options—(Applicable only if the Type is RSA.) The options are General Purpose (one pair for both signing and encryption) and Special (one pair for each respective function). For this example, accept the default setting (General Purpose).
- Step 3** Click **Generate Now**.
- Step 4** To view the key pair generated, click **Show Details**. ASDM displays information about the key pair. [Figure 1-1](#) shows sample output.
-

Figure 1-1 Key-pair Details Display



Creating the Trustpoint

A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. Refer to the section that names the interface you want to use to create a trustpoint.

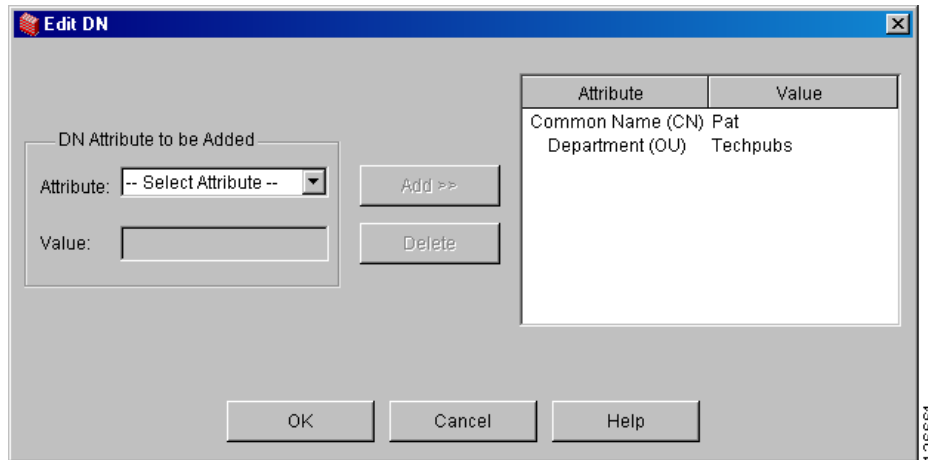
To create a trustpoint, perform the following steps.

-
- Step 1** In the **Configuration > Properties > Certificate > Trustpoint > Configuration** window, click **Add**.
- Step 2** Configure the basic information in the **Add Trustpoint Configuration** dialog box. For all other parameters, accept the default values.
- Trustpoint Name** field—Type the trustpoint name in the **Trustpoint Name** field. For this example, the name is `newmsroot`.
 - Enrollment URL** field—In the **Enrollment Settings** window, under the **Enrollment Mode** area, click the **Use automatic enrollment** option. Then type the enrollment URL in the field. For this example, type `10.20.30.40/certsrv/mscep/mscep.dll`.
- Step 3** Configure the subject name using the common name (CN) and the name of the organizational unit (OU):
- In the **Enrollment Settings** window, select the key pair you configured for this trustpoint in the **Key Pair** list. For this example, the key pair is `key1`.
 - In the **Enrollment Settings** window, click **Certificate Parameters**.
 - To add subject distinguished (X.500) name values, click **Edit** in the **Certificate Parameters** dialog box.

- d. In the **Edit DN** area under **DN Attribute to be Added**, select an attribute in the **Attribute** list and type a value in the **Value** field. Then click **Add**. After entering the DN information, click **OK**.

For this example, first select **Common Name (CN)**, type **Pat** in the **Value** field, and click **Add**; then select **Department (OU)** and type **Techpubs** in the **Value** field. [Figure 1-2](#) shows what you have entered in the **Edit DN** dialog box.

Figure 1-2 Subject Name Attributes and Values



- Step 4** After reviewing the dialog box, click **OK**, then click **OK** in the remaining two dialog boxes.

Obtaining Certificates with SCEP

This section shows how to configure certificates using SCEP. Repeat the instructions for each trustpoint you configure for automatic enrollment. As you complete the instructions for each trustpoint, the security appliance receives a CA certificate for the trustpoint and one or two certificates for signing and encryption purposes. If you do not follow these procedures, the security appliance prompts you to paste the base-64 formatted CA certificate into the text box.

If you use DSA keys, the certificate received is for signing only.

If you use general-purpose RSA keys, the certificate received is for signing and encryption. If you use separate RSA keys for signing and encryption, the security appliance receives separate certificates for each purpose.

To obtain certificates, perform the following steps.

- Step 1** Select the **Configuration > Properties > Certificate > Authentication** window.
- Step 2** In the **Trustpoint Name** list, select the name of the trustpoint. For this example, select **newsroot**.
- Step 3** Click **Authenticate**.
- Step 4** Click **Apply**. When ASDM displays the **Authentication Successful** dialog, click **OK**.

Enrolling with the Certificate Authority

After you configure the trustpoint and authenticate with it, you can enroll for an identity certificate by performing the following steps.

-
- Step 1** In the **Configuration > Properties > Certificate > Enrollment** window, select the trustpoint in the **Trustpoint Name** list. For this example, you would select **newmsroot**.
- Step 2** Click **Enroll**.
-

Managing Certificates

To manage certificates, use the **Configuration > Properties > Certificate > Manage Certificates** window.

You can use this window to add a new certificate and delete a certificate. You can also display information about a certificate by clicking **Show Details**. The Certificate Details dialog displays three tables: General, Subject, and Issuer.

The **General** table displays the following information:

- Type—CA, RA, or Identity
- Serial number—Serial number of the certificate
- Status—Available or pending
 - Available means that the CA has accepted the enrollment request and has issued an identity certificate.
 - Pending means that the enrollment request is still in process and that the CA has not yet issued the identity certificate.
- Usage—General purpose or Signature
- CRL distribution point (CDP)—URL for obtaining the CRL for validating the certificate
- Dates/times within which the certificate is valid—Valid from, valid to

The **Subject** table displays the following information:

- Name—The name of the person or entity that owns the certificate
- Serial number—The serial number of the ASA
- Distinguished (X.500) name fields for the subject of the certificate—cn, ou, etc.
- Hostname of the certificate holder

The **Issuer** table displays the distinguished name fields for the entity that granted the certificate.

- Common name (cn)
- Organizational unit or department (ou)
- Organization (o)
- Locality (l)
- State (st)
- Country code (c)

- E-mail address of the issuer (ea)