CHAPTER 7

Certificate Configuration

The Certificate Configuration page allows you to edit the Certificate information for an Ingrian i100/i140. You can access the Certificate Configuration Page from the Navigation Bar by selecting the Certificate icon in the Configuration folder. This chapter contains the following information:

Certificate Creation Overview

Certificates identify a web server to a client browser. The server's certificate is sent to the browser when the browser establishes a secure connection with the web server.

Before the Ingrian i100/i140 can respond to SSL requests from a client browser, the Ingrian i100/i140 must be configured with at least one certificate. To obtain a certificate, you must perform the following tasks from the Certificate Configuration page.

1. Create a certificate request on the Ingrian i100/i140.

   Use the **Create Certificate Request** fields on the bottom of the Certificate Configuration page. The new request will appear in the Certificate List portion of the page. Once created, the status of the new request shows as *Request Pending*.

2. Send the certificate request to a Certificate Authority (CA), such as VeriSign, Entrust, Equifax, or GlobalSign.

   Use the **Properties** button on the Certificate List section to view the newly created certificate request. The properties button displays the Certificate Information page. Use either of the following two methods to send the request to the CA:

   - Cut and paste the request from the certificate information page and send the request either via e-mail or paste it directly to the CA’s certificate request web page. Or
   - Use the download button on the Certificate Information page to download the certificate request to a file on your local machine. Then e-mail the file to the CA or upload the file to the CA's certificate request web page.

3. Receive the certificate from the Certificate Authority.

   The CA will e-mail you a certificate.

4. Install the certificate on the Ingrian i100/i140.

   Use the **Install Certificate** on the Certificate List section to install the certificate on the Ingrian i100/i140.

5. Use the certificate.

The certificate request is now an active certificate. It can be used in Forwarding Rules to establish SSL connections with client web browsers.

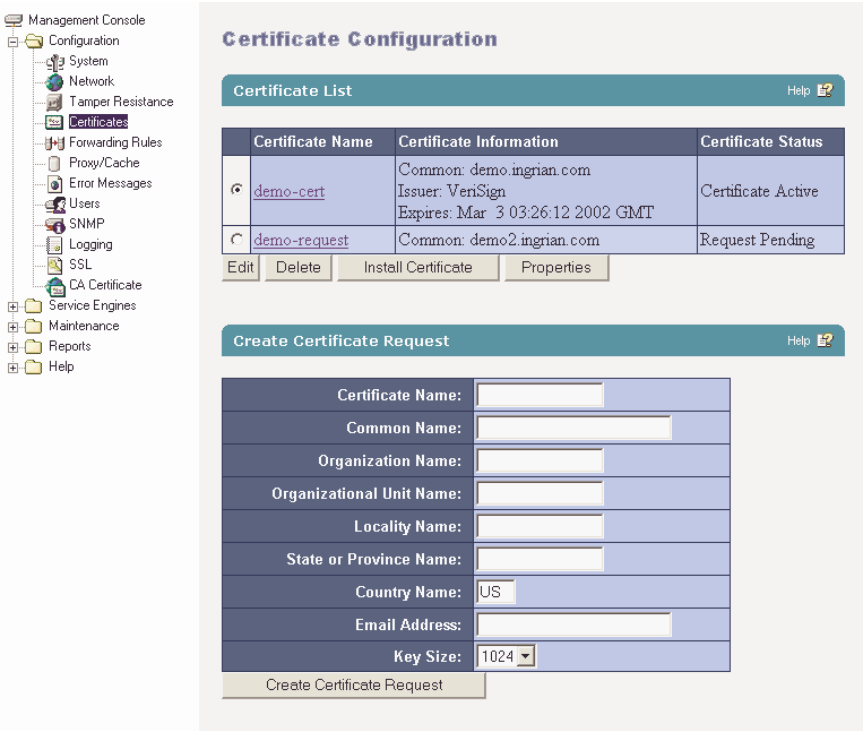


Fig. 7.1 Certificate Configuration

Server and Client Certificates

There are three kinds of certificates that are used in the Ingrian i100/i140 environment: server certificates installed on the Ingrian i100/i140, client certificates installed on the Ingrian i100/i140, and client certificates installed on the browsers of end users. These certificates are described below.

- **Server certificates installed on the Ingrian i100/i140** allow the Ingrian i100/i140 to authenticate itself to a client browser during an SSL handshake.

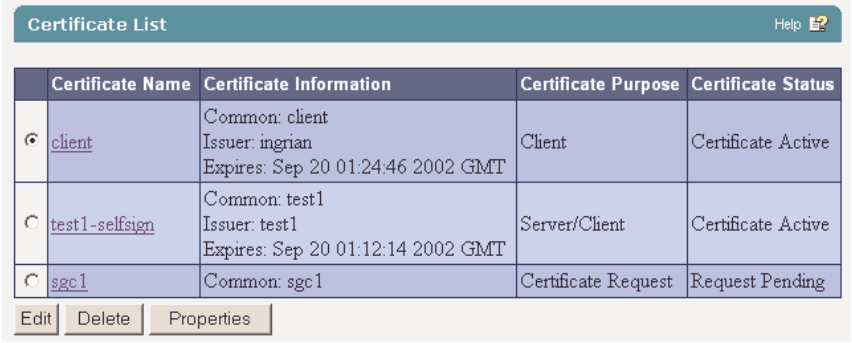
- **Client certificates installed on the Ingrian i100/i140** enable an Ingrian i100/i140 to authenticate itself to a backend web server during an SSL handshake. Client certificates provide an extra measure of security when you send decrypted text to a client, as is the case when you use Content Encryption.
- **Certificates installed on end user browsers** allow end users to authenticate themselves to the Ingrian i100/i140 during an SSL handshake.

Certificate List

The Certificate List displays the list of current certificates and certificate requests on the Ingrian i100/i140. Use the Certificate List section of the **Certificate Configuration** to view all installed certificates on the Ingrian i100/i140.

CLI: `hostname#` **show cert**

Fig. 7.2
View Certificate List



Certificate List Help

	Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
◉	client	Common: client Issuer: ingrian Expires: Sep 20 01:24:46 2002 GMT	Client	Certificate Active
○	test1-selfsign	Common: test1 Issuer: test1 Expires: Sep 20 01:12:14 2002 GMT	Server/Client	Certificate Active
○	sgc1	Common: sgc1	Certificate Request	Request Pending

Edit Delete Properties

Table 7.1
View Certificates

Components	Description
Certificate Name	The name of a certificate used by the Ingrian i100/i140. Click the hyperlinked certificate name to view properties and access the **Certificate Information Page**.
Certificate Information	A certification summary containing the following information: • Common Name: Name of entity to which certificate is issued. This is typically the domain name (e.g. www.xyz.com) of the site using the Ingrian i100/i140. • Issuer Name: Name of CA that issued the certificate (e.g. VeriSign). This information field is not displayed for certificate requests. • Expiration Date: The final date on which this certificate is valid. Following the expiration date, the certificate can only be renewed by obtaining a new certificate from the CA. This information field is not displayed for certificate requests.
Certificate Purpose	A certificate installed on the Ingrian i100/i140 can be client, server, or client/server. For more information, see **Server and Client Certificates**.
Certificate Status	Current state of the certificate, as one of the following: • Request Pending Certificate request generated. Waiting for certificate from CA. • Certificate Active Certificate is ready to be used. • Certificate Expires in x days Will expire in x days. This state appears when a certificate expires in less than 30 days. • Certificate Expired Certificate expiration date is earlier than current date. • Certificate Not Yet Active Certificate activation date is after the current date. • Invalid Certificate Certificate is improperly signed by CA. • Error in Certificate Malformed certificate.
Edit Button	Click to modify the certificate name.
Delete Button	Click to remove the specified certificate. `CLI: hostname (config)# no certificate <cert name>` If a certificate is bound to a currently configured Forwarding Rule it cannot be deleted.

Components	Description
Install Certificate Button	Click to go to the **Certificate Installation** page. The install certificate button can be applied to either certificate requests or active certificates. • When applied to a certificate request the button is intended for transforming the certificate request into an active certificate. • When applied to an existing certificate the button is intended for reinstalling a certificate. Applying the install certificate button to a certificate should not be used under normal circumstances. See also “Install Certificate” on page 64.
Properties Button	Click to view the **Certificate Information Page**. See also “Properties” on page 68.

Install Certificate

Clicking the Install Certificate button invokes the certificate installation page. Use this page to install a certificate for a previously generated certificate request, or to reinstall a certificate for an active certificate. Paste the certificate received from the CA into the appropriate text field on the Certificate Installation page. Before accepting, the Ingrian i100/i140 verifies the validity of the newly installed certificate. If determined to be valid, the certificate appears as “Certificate Active” in the Certificate List.

```
CLI:  hostname (config)# cert install <req name>
```

Fig. 7.3 Certificate Installation

Table 7.2 Certificate Installation

Components	Description
Certificate Name	Name assigned to this certificate.
Key Size	Key size associated with this certificate.
Subject	Identity to which certificate is issued.
	CN = Common Name
	O = Organization
	OU = Organizational unit
	L = Locality
	ST = State
	C = Country

Installing a Certificate Chain

When CAs sign server certificates with an intermediate CA, it might be necessary for an Ingrian i100/i140 to send multiple certificates to a client to enable the client to verify the server certificate. A client connecting to a forward rule that uses such a chain will receive all certificates on the chain.

Certificate chains can be installed on the Ingrian i100/i140 through the Certificate Install Page. Follow the steps below to install a certificate chain.

1. Navigate to the Certificate Installation page shown in Figure 7.3, “Certificate Installation,” on page 65.

2. Append the intermediate CA certificate to the server certificate received from the CA.

   The combined certificates should be displayed in the Certificate Response field, as shown below:

Fig. 7.4 Certificate Response Field

Certificate Response:


```
w1OznpHuCC/lZknQeDVGij5GXPEmVuF2qe+Ei2ugqtKqB7Rbg9PH1KWaLa6tVKX3
Ul2pp9TXGNOB4wCBDRwGGYfKZW/1YSc4tkLpntusM8LvxwIDAQABoyAwHjAJBgNV
HRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQQFAAOBgQC6+dDe
E6e/48FxQR/CfDyCmxbTWP0qGNEZSJ2dz6c7IQtTYrc8cswig/YRiNGkhz9OEUrP
XJzVpKa25KphvFkGUrmLcKOwdu9SHVxJ3vSJCoj5ZVkK3+nO5AGxN1EgHk4JF1Ij
rXNiYxxobQxFsLvDJkqSDX1Te2KzgrWozXCojw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID7jCCA1egAwIBAgIBADANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEYMBYG
A1UEChMPSW5ncmlhbiBTeXNOZW1zMRQwEgYDVQQLEwtFbmdpbmVlcmluZzE1MCMG
A1UEAxMcSW5ncmlhbiBUZXNOIEludGVybWVkaWF0ZSBDQTEfMB0GCSqGSIb3DQEJ
ARYQaW5mb0BpbmdyaWFuLmNvbTAeFw0wMTA1MjYyMDAwMTZaFw0wNjA1MjcyMDAw
MTZaMIGxMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEVMBMGA1UE
BxMMUmVkd29vZCBDaXR5MRgwFgYDVQQKEw9JbmdyaWFuIFN5c3RlbXMxFDASBgNV
```


3. Click **Save**.

The combined certificates are shown below.

Fig. 7.5
Combined Certificates


```
-----BEGIN CERTIFICATE-----
MIIC6DCCAlGgAwIBAgIBAjANBgkqhkiG9wOBAQQFADCBsTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEYMBYG
A1UEChMPSW5ncmlhbiBTeXNOZW1zMRQwEgYDVQQLEwtFbmdpbmVlcmluZzElMCMG
A1UEAxMcSW5ncmlhbiBUZXNOIEludGVybWVkaWFOZSBDQTEfMBOGCSqGSIb3DQEJ
ARYQaW5mbOBpbmdyaWFuLmNvbTAeFwOwMTA1MjYyMDAxNThaFwOwMjA1MjcyMDAx
NThaMIGfMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEVMBMGA1UE
BxMMUmVkd29vZCBDaXR5MRgwFgYDVQQKEw9JbmdyaWFuIFN5c3RlbXMxDjAMBgNV
BAsTBVNhbGVzMRkwFwYDVQQDExBkZW1vLmluZ3JpYW4uY29tMR8wHQYJKoZIhvcN
AQkBFhBpbmZvQGluZ3JpYW4uY29tMIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCuQI1UVNKPsHXOhUHKHZRGcdMT/M4mOcIqObkLC9b3PaIS8fPuBMOfgAUbiP+V
w1OznpHuCC/lZknQeDVGij5GXPEmVuF2qe+Ei2ugqtKqB7Rbg9PH1KWaLa6tVKX3
Ul2pp9TXGNOB4wCBDRwGGYfKZW/1YSc4tkLpntusM8LvxwIDAQABoyAwHjAJBgNV
HRMEAjAAMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9wOBAQQFAAOBgQC6+dDe
E6e/48FxQR/CfDyCmxbTWPOqGNEZSJ2dz6c7IQtTYrc8cswig/YRiNGkhz9OEUrP
XJzVpKa25KphvFkGUrmLcKOwdu9SHVxJ3vSJCoj5ZVkK3+nO5AGxN1EgHk4JF1Ij
rXNiYxxobQxFsLvDJkqSDX1Te2KzgrWozXCojw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID7jCCA1egAwIBAgIBADANBgkqhkiG9wOBAQQFADCBsTELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEYMBYG
A1UEChMPSW5ncmlhbiBTeXNOZW1zMRQwEgYDVQQLEwtFbmdpbmVlcmluZzElMCMG
A1UEAxMcSW5ncmlhbiBUZXNOIEludGVybWVkaWFOZSBDQTEfMBOGCSqGSIb3DQEJ
ARYQaW5mbOBpbmdyaWFuLmNvbTAeFwOwMTA1MjYyMDAwMTZaFwOwNjA1MjcyMDAw
MTZaMIGxMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEVMBMGA1UE
BxMMUmVkd29vZCBDaXR5MRgwFgYDVQQKEw9JbmdyaWFuIFN5c3RlbXMxFDASBgNV
BAsTCOVuZ2luZWVyaW5nMSUwIwYDVQQDExxJbmdyaWFuIFRlc3QgSW5OZXJtZWRp
YXRlIENBMR8wHQYJKoZIhvcNAQkBFhBpbmZvQGluZ3JpYW4uY29tMIGfMAOGCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDDx4GpHtTR8RWIbICnTWaaMAgcNNPh7otA/kmr
T8vBPE2OHYkONguyQB+iUv/bN6SWwwOwebgQOTqT+6kDARW5s6HZtLZN8k+Rr3wt
/PU978b86RHVLI/TjkwsyK3iWrhONz4wlF//Gdg3x51OHpKTTIUr/XxUUExUM8zW
sQSmHQIDAQABo4IBEjCCAQ4wHQYDVROOBBYEFO3b4sMKjROyesO5kqt1W8QoZwz9
MIHeBgNVHSMEgdYwgdOAFO3b4sMKjROyesO5kqt1W8QoZwz9oYG3pIGOMIGxMQsw
CQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEVMBMGA1UEBxMMUmVkd29v
ZCBDaXR5MRgwFgYDVQQKEw9JbmdyaWFuIFN5c3RlbXMxFDASBgNVBAsTCOVuZ2lu
ZWVyaW5nMSUwIwYDVQQDExxJbmdyaWFuIFRlc3QgSW5OZXJtZWRpYXRlIENBMR8w
HQYJKoZIhvcNAQkBFhBpbmZvQGluZ3JpYW4uY29tggEAMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEEBQADgYEAANcnTX2K/Hg6bhzQMq36Odc57RmGmQpkkbVAV4kE
LOl+GoLtDvS1D6npb669KMfRf1BXGj4nevhXIJo4ZwNUxa+hOdYlwkC8OqrTHW69
64zxmRiX+ZLlvn52ljW3CPgtCX9rvyGuWl2aKJbnd/EQ7TmCh7682E4E+JQzwIm3
r88=
-----END CERTIFICATE-----
```


Download | Install Certificate | Back

Properties

Clicking the Properties button in the Certificate List displays the Certificate Information Page, which you can use the to view information associated with a specific certificate.

```
CLI:  hostname# show cert <cert name>
```

The top portion of the Certificate Information page contains the configured elements of the certificate. The lower portion of this page contains the X509 certificate data encoded in PEM format.

Fig. 7.6
Certificate Information Page

Certificate Information — Help

Certificate Name:	demo-cert
Key Size:	1024
Start Date:	Oct 24 23:50:32 2000 GMT
Expiration:	Oct 25 23:50:32 2001 GMT
Issuer:	CN: Self Signed Certificate O: Ingrian Systems OU: E-Commerce L: Redwood City ST: California C: US Email: certs@ingrian.com
Subject:	C: US ST: California L: Redwood City O: Ingrian Systems OU: E-Commerce CN: demo.ingrian.com Email: certs@ingrian.com


```
-----BEGIN CERTIFICATE-----
MIIC6TCCAlKgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBrDEgMB4GA1UEAxMXU2Vs
ZiBTaWduZWQgQ2VydGlmaWNhdGUxGDAWBgNVBAoTD0luZ3JpYW4gU3lzdGVtczET
MBEGA1UECxMKRS1Db21tZXJjZTEVMBMGA1UEBxMMUmVkd29vZCBDaXR5MRMwEQYD
VQQIEwpDYWxpZm9ybmlhMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJARYRY2Vy
dHNAaW5ncmlhbi5jb20wHhcNMDAxMDI0MjM1MDMyWhcNMDExMDI1MjM1MDMyWjCB
pTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFTATBgNVBAcTDFJl
ZHdvb2QgQ2l0eTEYMBYGA1UEChMPSW5ncmlhbiBTeXN0ZW1zMRMwEQYDVQQLEwpF
LUNvbW1lcmNlMRkwFwYDVQQDExBkZW1vLmluZ3JpYW4uY29tMSAwHgYJKoZIhvcN
AQkBFhFjZXJOcOBpbmdyaWFuLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAr/LkUq+0YswwFg6Emh3hY7/cYOgCwbpXkK4Iwbze+91TiywNRmfiFDZKOIRO
g73ir7hd4vNFzy+yKGCSbzZ54airAak6FSOHIcxcJhk/wvzY8oPejE6qB8pKX6oY
rPyJIrTZeMol8ByBJxe0vZiOAtDkfmSNtUeATA3iCLN8aRcCAwEAAaMgMB4wCQYD
VROTBAIwADARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcNAQEEBQADgYEAIL1a
meLrPnDTS5lQgHB1lk5A5KFpuqEvM1p68+1cxxEKND9kpFoq8k4Wjz8iTB6iGxwo
8eZUdYVOVUApjxguVtmeD41nJWxSbIafM7KLGGMENrk+5MHI8XmefeOKkTWBzwei
zPQwaIlmq8Cs1tkIlckFMMFr9h8yZKcDjhXz3Gk=
-----END CERTIFICATE-----
```


Download | Install Certificate | Back

When applied to a certificate request, the Certificate Information page presents only the Certificate Name, Key Size, and Subject fields above the X509 certificate request data. The X509 data is encoded in PEM format. An active certificate presents Certificate Name, Key Size, Start Date, Expiration, Issuer, and Subject above the X509 certificate data.

Table 7.3
Certificate Detail

Components	Description
Certificate Name	Configured name of the certificate.
Key Size	Size of the key associated with this certificate.
Start Date	The activation date for the certificate. The certificate cannot be used before the activation date.
Expiration	The expiration date for the certificate. The certificate cannot be used after the expiration date.
Issuer	Full information about the CA who issued the certificate.
Subject	Full information about the entity to whom the certificate is issued. This information commonly identifies the web site to which the certificate is issued.
Download Button	Click to download the certificate request data or the certificate data onto your web browser. Once downloaded into a file the certificate request can be E-mailed to the CA.
Install Certificate Button	Click to install a new certificate received from the CA. *See also "Install Certificate".*
Back Button	Click to return to the Certificate list.

Create Certificate Request

The Create Certificate Request is used to create certificate requests. From the command line, you can create a certificate request with the command below. Once you have entered the command, you are prompted for the information shown in the fields below.

```
CLI:  hostname# cert request
```

Fig. 7.7
Create Certificate Request

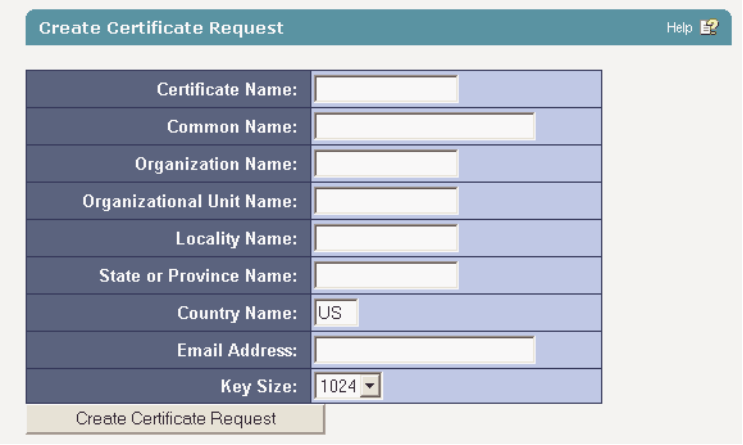


Table 7.4
Certificate Request Fields

Field	Description
Certificate Name	Internal name of a newly generated certificate request. This name will be used when referring to this certificate request in other parts of the administrative interface.
Common Name	Domain name of the web site using this certificate (for example, www.xyz.com). When a web browser establishes a secure SSL connection with the Ingrian i100/i140, the web browser compares the common name in the certificate to the domain name in the requested URL. If the two differ the web browser displays an error message and the connection is severed.
Organization Name	Name of the organization that owns this certificate. • Example: XYZ Co.
Organizational Unit Name	Name of the unit within the organization requesting the certificate. • Example: E-commerce Group
Locality Name	Name of city to which the certificate is being issued. • Example: San Francisco

Field	Description
State or Province Name	Name of state where request is issued. • Example: California
Country Name	Two-character ISO 3166 code of country where request is issued. • Example: US (United States)
Email Address	E-mail address of person requesting the certificate.
Key Size	Size of key being generated. The Ingrian i100/i140 supports 768-bit, 1024-bit, and 2048-bit key sizes. 1024-bit is the most commonly used key size.
Create Certificate Request Button	Click this button to create the certificate request. Once created, the request appears as a "Request Pending" on the Certificate List section. See also "Certificate Status".

Create Self-signed Certificate

The Ingrian i100/i140 allows you to test the network configuration without waiting for a certificate from the CA. To create a temporary test certificate, you can create an active certificate by using the "Create Self Sign Certificate" button on the Certificate Information page. This button can only be applied to existing certificate requests. The resulting test certificate can be bound to forwarding rules in the same way as a regular certificate.

When applying the "Create Self Sign Certificate" button to a certificate request, the Ingrian i100/i140 performs the following steps:

1. The certificate request "certreq" is copied into a new certificate request called "certreq-selfsign."
2. The Ingrian i100/i140 transforms "certreq-selfsign" into an active certificate by generating a self signed certificate.
3. The test self signed certificate is presented as an Active Certificate in the Certificate List section. This certificate can be used in forwarding rules. An attempt to connect with an Ingrian i100/i140 using a test self-signed certificate will display a warning message in the user's browser window.

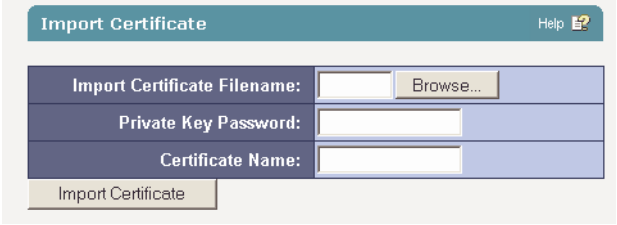
Note A self-signed certificate should be used for testing purposes only.

```
CLI:  hostname# cert selfsign install
```

Import Certificate

If you are adding an Ingrian i100/i140 to your existing web site infrastructure, you can easily import certificates and private keys to the device from the computers which comprise your server farm. The Ingrian i100/i140 can import certificates from most existing web servers (e.g. IIS, Apache, etc.) in PEM or PKCS #12 format. Import from iPlanet/Netscape servers is not supported.

Fig. 7.8
Import Certificate Screen



To import a Certificate:

1. Export Certificate and Private Key from your web server

   See “How to export a Certificate from an ApacheSSL server” on page 73” for detailed information on how to export from this type of web server.

   See “How to export a Certificate from a Stronghold server” on page 73” for detailed information on how to export from this type of web server.

   See “How to export a Certificate from an IIS (Windows 2000) server” on page 73 for detailed information on how to export from this type of web server.

2. Either type the path to the Certificate you want to import into the Import Certificate Filename field or press **Browse** to find the Certificate on your network.

3. Enter the password of the private key associated with the Certificate into the Private Key Password field.

4. Enter the name of the Certificate into the Certificate Name field.

5. Select **Import Certificate**.

The Certificate is imported into your Ingrian i100/i140.

How to export a Certificate from an ApacheSSL server

The key location is listed in the $APACHEROOT/conf/httpd.conf file. The default is $APACHEROOT/certs/*.key. Note the name and location.

The certificate location is also listed in the $APACHEROOT/conf/ httpd.conf file. The default is $APACHEROOT/certs/*.crt. Note the name and location.

How to export a Certificate from a Stronghold server

The key location is listed in the $STRONGHOLDROOT/conf/httpd.conf file. The default is $STRONGHOLDROOT/ssl/private/*.key. Note the name and location.

The certificate location is also listed in the $STRONGHOLDROOT/conf/ httpd.conf file. The default is $STRONGHOLDROOT/ssl/*cert. Note the name and location.

How to export a Certificate from an IIS (Windows 2000) server

1. Select “Start> Programs> Administrative Tools> Computer Management> Services and Applications> Internet Information Services.”
2. Find the site from which you wish to export a Certificate.
3. Right click on the site’s icon.
4. Select Properties from the popup menu.

   The Properties menu appears.
5. Select the Directory Security tab in the Properties menu.

   The Directory Security tab appears.
6. Select View Certificate.
7. Select Details.
8. Select Copy to File.

The Certificate Export Wizard appears.

9 Select Next to continue using the wizard.

10 Select the radio button associated with the phrase “Yes, export the private key.” (default)

11 Select Next.

The Personal Information Exchange page appears.

12 Select Next to enable the default options (Recommended).

The Password Verification page appears.

13 Enter the password associated with the private key in the Password field.

14 Copy and paste the password you entered into the Password field into the Confirm Password field.

15 Select Next.

The File to Export page appears.

16 Select Browse.

A Choose File or Save As popup window appears.

17 Navigate through your network to the directory in which you want to place the Certificate and its associated private key.

18 Select Open or Save.

The Choose File popup window disappears.

19 Select Next.

20 Select **Finish**.

The **Certificate Export Wizard** disappears. The certificate is exported.