EJBCA with GemSAFE Toolbox Part3 SSL

Introduction

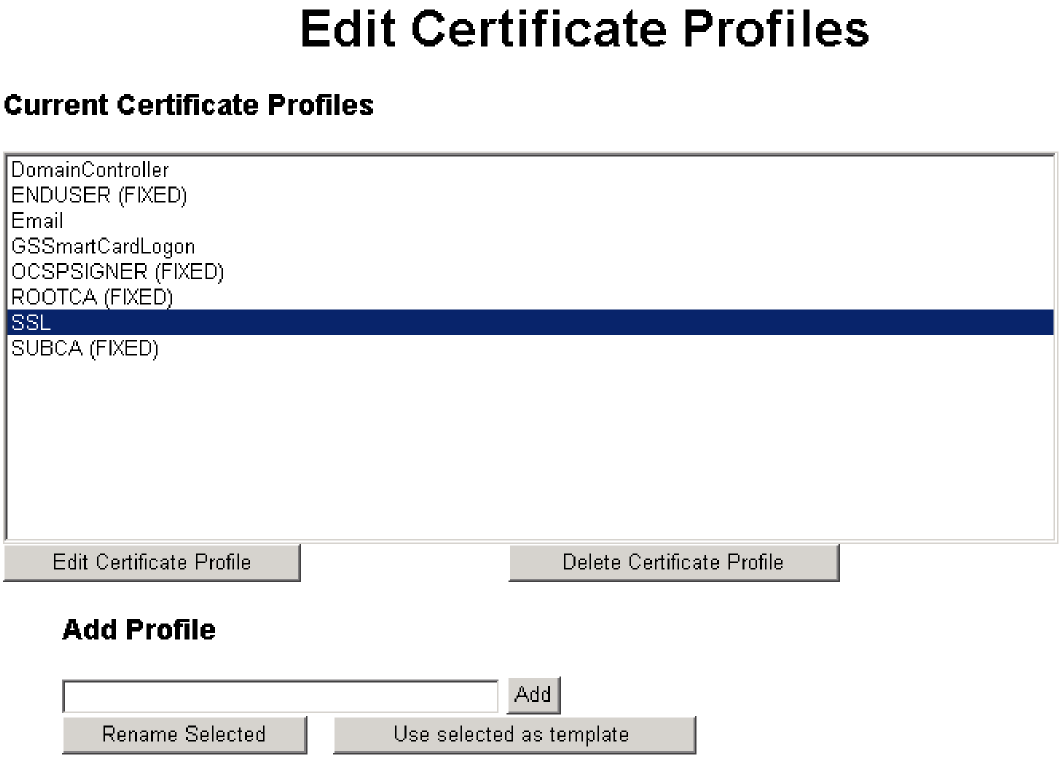
This document is a continuation form 2 documents namely “EJBCA with GemSAFE Toolbox Part1 workstation logon” and “EJBCA with GemSAFE Toolbox Part2 sign and encrypt email”. This is the last document in the series.

The way to request SSL server certificate from EJBCA was described in sequential manner. But most of the EJBCA setting and configuration were described in the previous documents.

Table of Content

1 -- Create SSL Certificate Profile

1. Go to EJBCA Administration GUI
2. Click “Edit Certificate Profiles”
3. Type "SSL" in the text box under “Add Profile”. Click “Add”
4. Choose “SSL” under “Current Certificate Profiles”

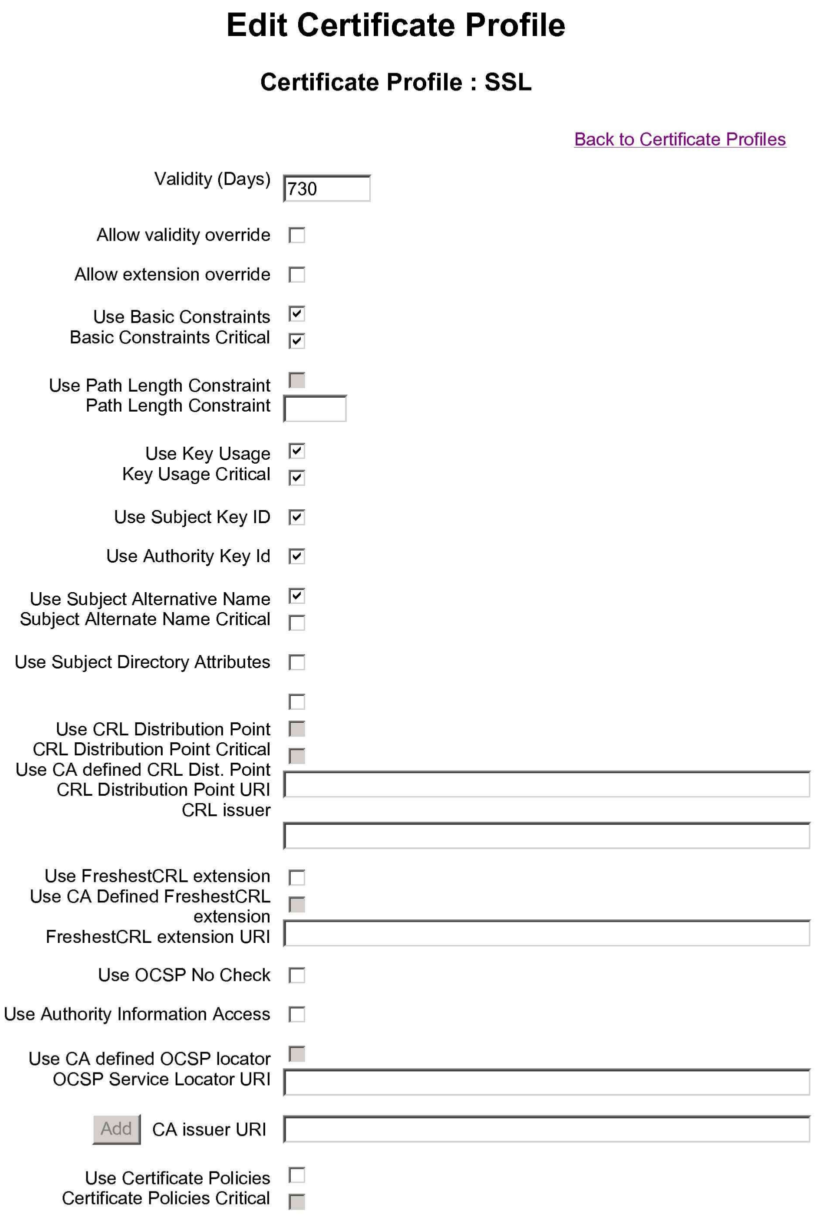


Edit Certificate Profiles

Current Certificate Profiles

DomainController
ENDUSER (FIXED)
Email
GSSmartCardLogon
OCSPSIGNER (FIXED)
ROOTCA (FIXED)
SSL
SUBCA (FIXED)

5. Click “Edit Certificate Profiles”
6. Set SSL certificate’s profile’s parameters
   a) Under key usage, select “Key agreement”
   b) Under available CAs, Select only “GS_SCL_CA_v1”
7. leave all other setting by default and click “Save”
8. The following is the screen capture of the settings

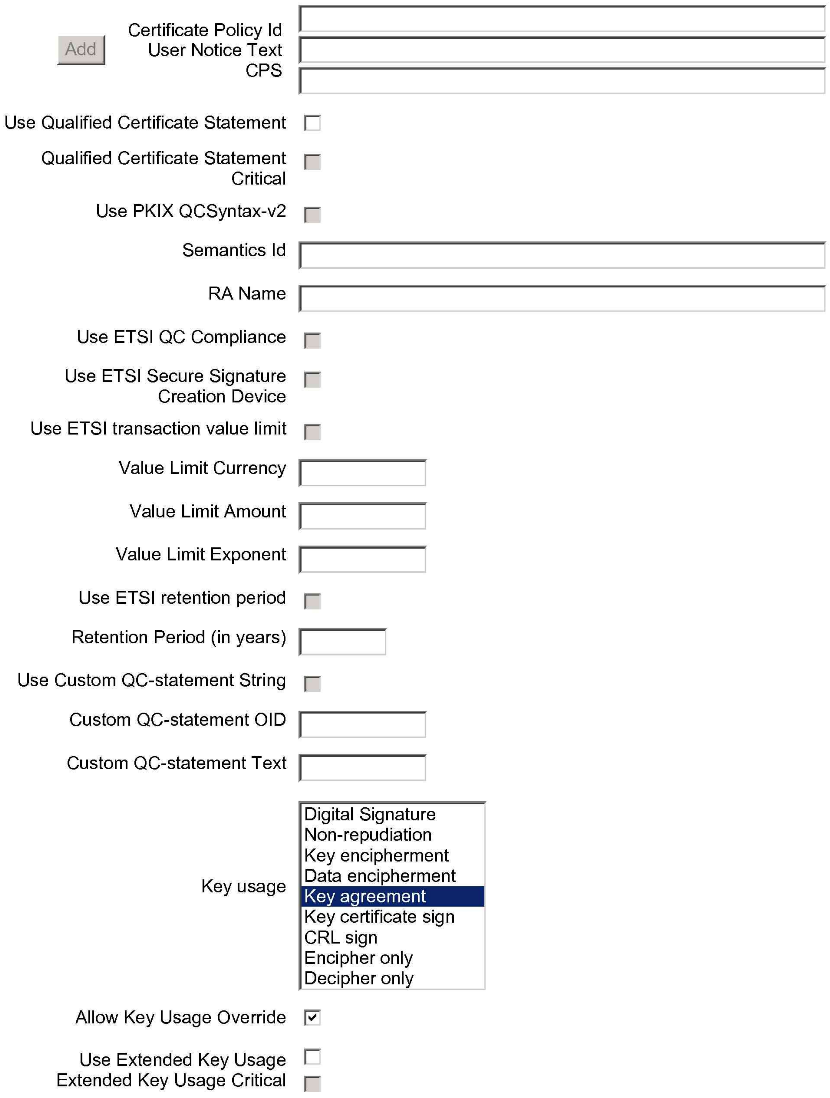


Edit Certificate Profile

Certificate Profile : SSL

Back to Certificate Profiles

Validity (Days)	730
Allow validity override	☐
Allow extension override	☐
Use Basic Constraints	☑
Basic Constraints Critical	☑
Use Path Length Constraint	☐
Path Length Constraint	
Use Key Usage	☑
Key Usage Critical	☑
Use Subject Key ID	☑
Use Authority Key Id	☑
Use Subject Alternative Name	☑
Subject Alternate Name Critical	☐
Use Subject Directory Attributes	☐
Use CRL Distribution Point	☐
CRL Distribution Point Critical	☐
Use CA defined CRL Dist. Point	☐
CRL Distribution Point URI	
CRL issuer	
Use FreshestCRL extension	☐
Use CA Defined FreshestCRL extension	☐
FreshestCRL extension URI	
Use OCSP No Check	☐
Use Authority Information Access	☐
Use CA defined OCSP locator	☐
OCSP Service Locator URI	
Add CA issuer URI	
Use Certificate Policies	☐
Certificate Policies Critical	☐



Add

Certificate Policy Id ____

User Notice Text ____

CPS ____

Use Qualified Certificate Statement ☐

Qualified Certificate Statement Critical ☐

Use PKIX QCSyntax-v2 ☐

Semantics Id ____

RA Name ____

Use ETSI QC Compliance ☐

Use ETSI Secure Signature Creation Device ☐

Use ETSI transaction value limit ☐

Value Limit Currency ____

Value Limit Amount ____

Value Limit Exponent ____

Use ETSI retention period ☐

Retention Period (in years) ____

Use Custom QC-statement String ☐

Custom QC-statement OID ____

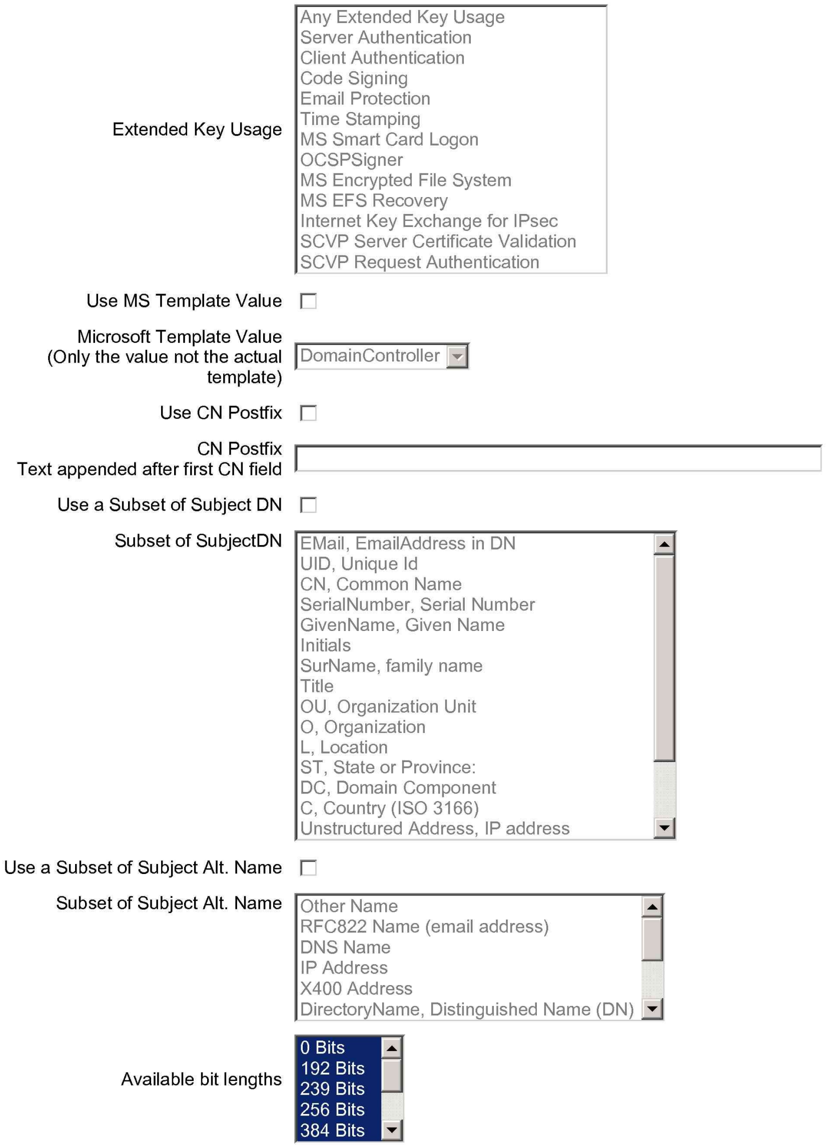
Custom QC-statement Text ____

Key usage
- Digital Signature
- Non-repudiation
- Key encipherment
- Data encipherment
- [✓ Key agreement]
- Key certificate sign
- CRL sign
- Encipher only
- Decipher only

Allow Key Usage Override ☑

Use Extended Key Usage ☐

Extended Key Usage Critical ☐



Extended Key Usage
- Any Extended Key Usage
- Server Authentication
- Client Authentication
- Code Signing
- Email Protection
- Time Stamping
- MS Smart Card Logon
- OCSPSigner
- MS Encrypted File System
- MS EFS Recovery
- Internet Key Exchange for IPsec
- SCVP Server Certificate Validation
- SCVP Request Authentication

Use MS Template Value □

Microsoft Template Value (Only the value not the actual template): DomainController

Use CN Postfix □

CN Postfix
Text appended after first CN field:

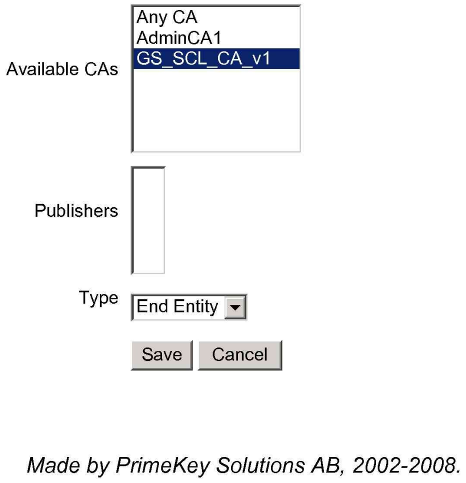
Use a Subset of Subject DN □

Subset of SubjectDN
- EMail, EmailAddress in DN
- UID, Unique Id
- CN, Common Name
- SerialNumber, Serial Number
- GivenName, Given Name
- Initials
- SurName, family name
- Title
- OU, Organization Unit
- O, Organization
- L, Location
- ST, State or Province:
- DC, Domain Component
- C, Country (ISO 3166)
- Unstructured Address, IP address

Use a Subset of Subject Alt. Name □

Subset of Subject Alt. Name
- Other Name
- RFC822 Name (email address)
- DNS Name
- IP Address
- X400 Address
- DirectoryName, Distinguished Name (DN)

Available bit lengths
- 0 Bits
- 192 Bits
- 239 Bits
- 256 Bits
- 384 Bits



Available CAs: Any CA, AdminCA1, GS_SCL_CA_v1 (selected)

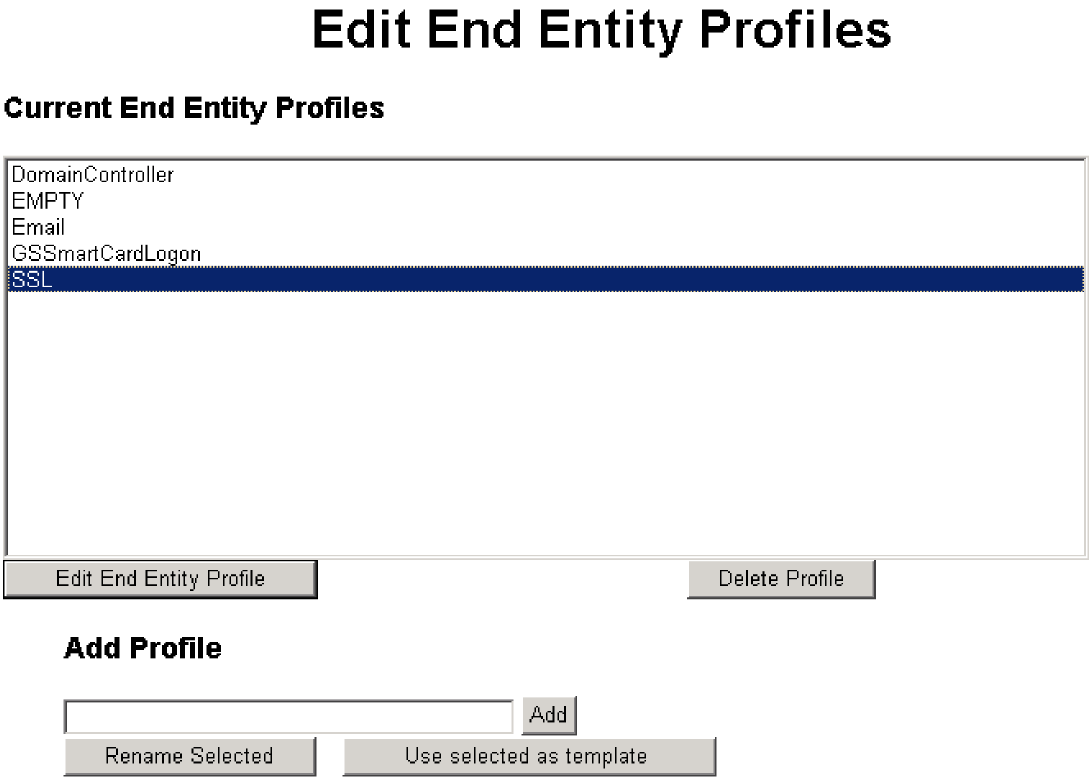
Publishers:

Type: End Entity

Made by PrimeKey Solutions AB, 2002-2008.

2 -- Create SSL End Entity profile

1. Go to EJBCA Administration GUI
2. Click “Edit End Entity Profiles”
3. Type "SSL" in the text box under “Add Profile”. Click “Add”
4. Choose “SSL” under “Current End Entity Profiles”



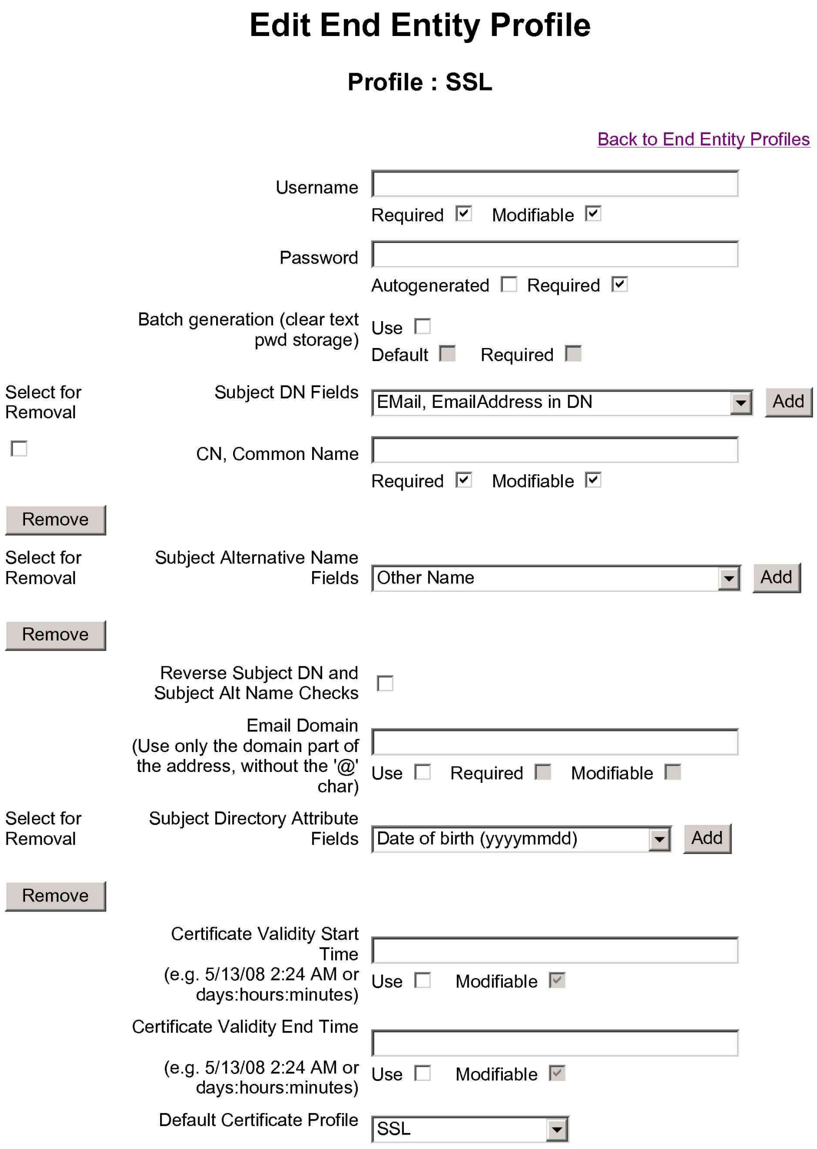
Edit End Entity Profiles

Current End Entity Profiles

DomainController
EMPTY
Email
GSSmartCardLogon
SSL

Add Profile

5. Click “Edit Certificate Profile”
6. Set SSL certificate’s profile’s parameters
   a) Under “Email Domain (Use only the domain part of the address, without the '@' char)” uncheck “Use”
   b) Under “Default Certificate Profile” choose “SSL”
   c) Under “Available Certificate Profile” choose “SSL”
   d) Under “Default CA” choose “GS_SCL_CA_v1”
   e) Under “Available CAs” choose only “GS_SCL_CA_v1”
7. leave all other setting by default and click “Save”
8. The following is the screen capture of the settings

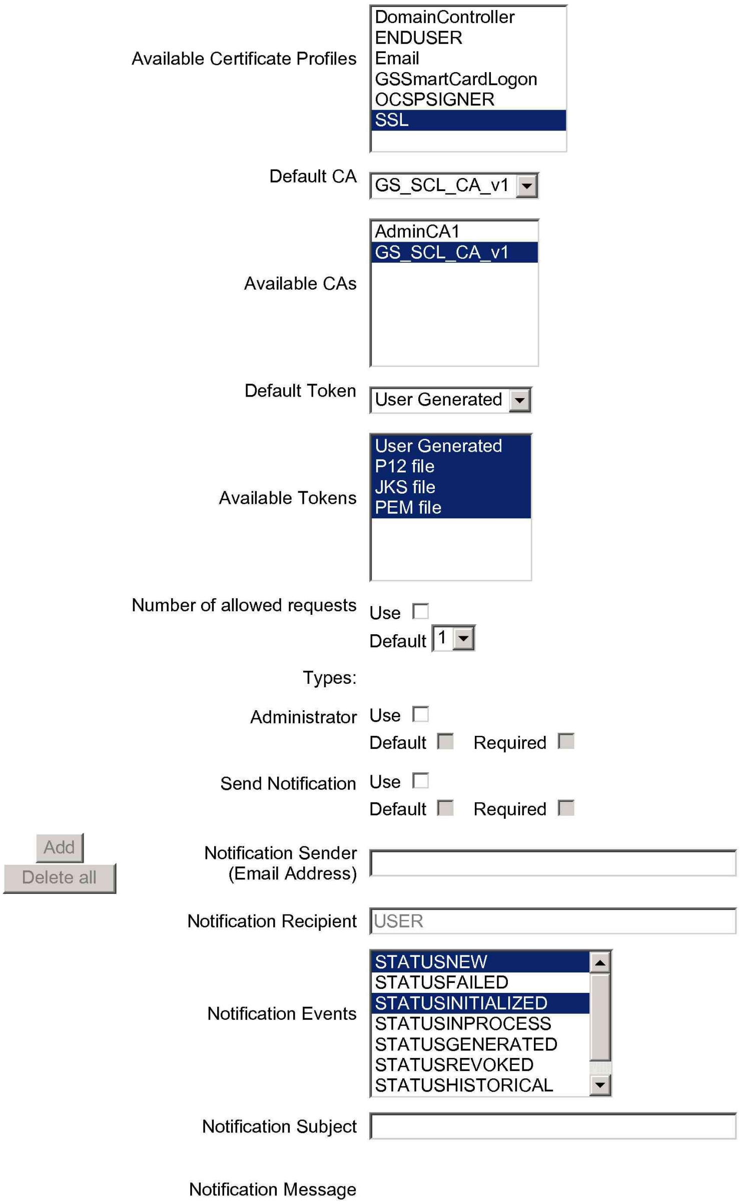


Edit End Entity Profile

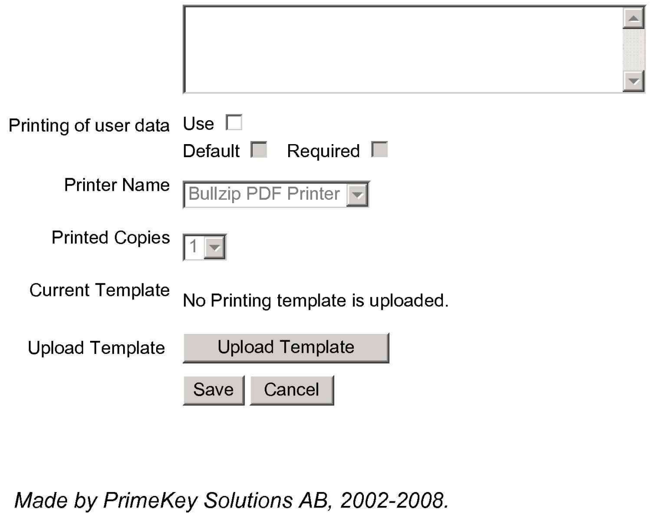
Profile : SSL

Back to End Entity Profiles

	Username	[ ] Required ☑ Modifiable ☑
	Password	[ ] Autogenerated □ Required ☑
	Batch generation (clear text pwd storage)	Use □ Default □ Required □
Select for Removal	Subject DN Fields	EMail, EmailAddress in DN ▾ Add
□	CN, Common Name	[ ] Required ☑ Modifiable ☑
Remove		
Select for Removal	Subject Alternative Name Fields	Other Name ▾ Add
Remove		
	Reverse Subject DN and Subject Alt Name Checks	□
	Email Domain (Use only the domain part of the address, without the '@' char)	[ ] Use □ Required □ Modifiable □
Select for Removal	Subject Directory Attribute Fields	Date of birth (yyyymmdd) ▾ Add
Remove		
	Certificate Validity Start Time (e.g. 5/13/08 2:24 AM or days:hours:minutes)	[ ] Use □ Modifiable ☑
	Certificate Validity End Time (e.g. 5/13/08 2:24 AM or days:hours:minutes)	[ ] Use □ Modifiable ☑
	Default Certificate Profile	SSL ▾



Available Certificate Profiles	DomainController ENDUSER Email GSSmartCardLogon OCSPSIGNER SSL
Default CA	GS_SCL_CA_v1
Available CAs	AdminCA1 GS_SCL_CA_v1
Default Token	User Generated
Available Tokens	User Generated P12 file JKS file PEM file
Number of allowed requests	Use □ Default 1
Types:	
Administrator	Use □ Default □ Required □
Send Notification	Use □ Default □ Required □
Notification Sender (Email Address)	
Notification Recipient	USER
Notification Events	STATUSNEW STATUSFAILED STATUSINITIALIZED STATUSINPROCESS STATUSGENERATED STATUSREVOKED STATUSHISTORICAL
Notification Subject	
Notification Message	

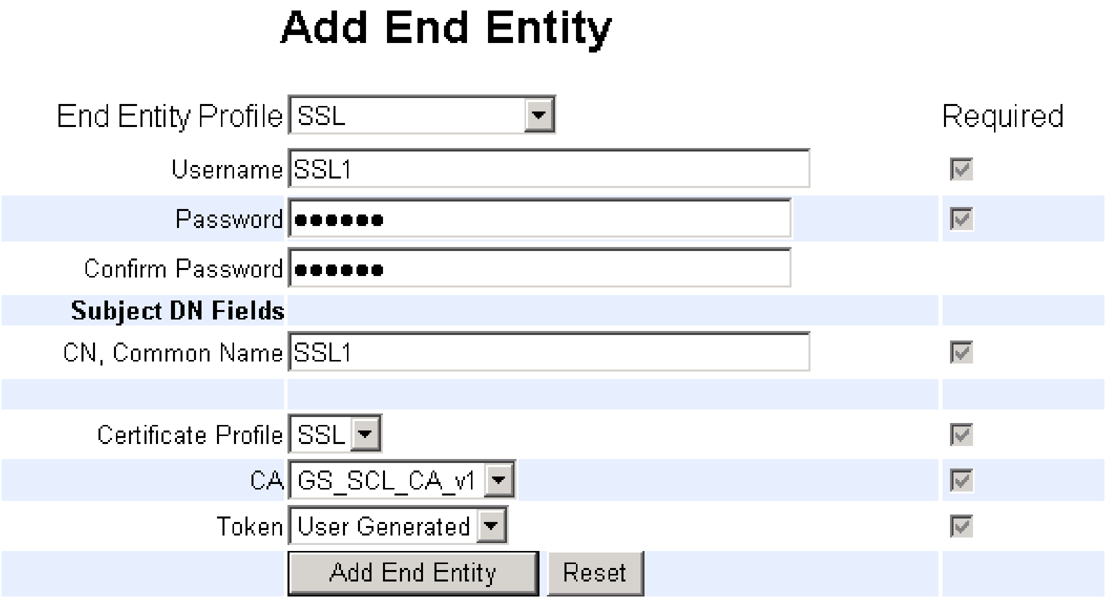


Printing of user data	Use □ Default □ Required □
Printer Name	Bullzip PDF Printer
Printed Copies	1
Current Template	No Printing template is uploaded.
Upload Template	

Made by PrimeKey Solutions AB, 2002-2008.

3 -- Create SSL End Entity

1. Go to EJBCA Administration GUI
2. Click “Add Edit Entity”
3. Set SSL end entity’s parameters
    a) End Entity Profile=SSL
    b) User Name=SSL1
    c) Password=foo123
    d) Confirm Password=foo123
    e) CN, Common Name=SSL1
4. leave all other setting by default and click “Add End Entity”
5. The following is the screen capture of the settings

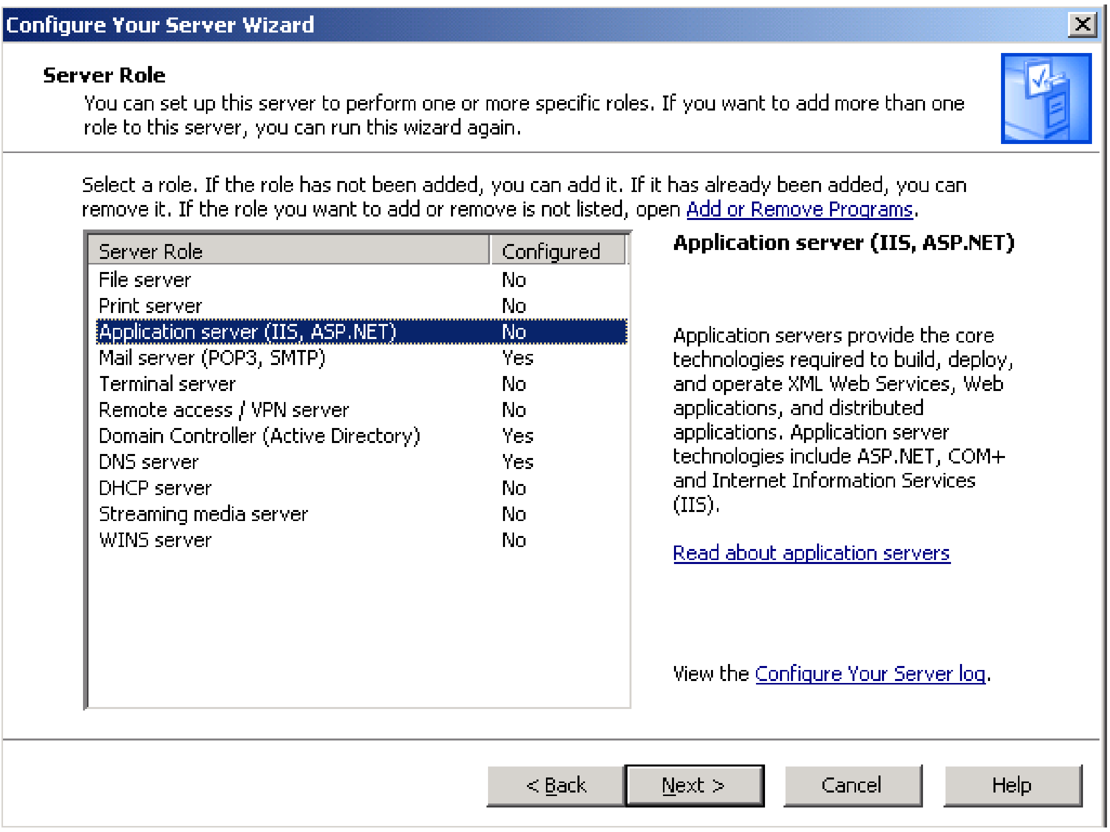


Add End Entity

End Entity Profile	SSL	Required
Username	SSL1	☑
Password	••••••	☑
Confirm Password	••••••	
Subject DN Fields		
CN, Common Name	SSL1	☑
Certificate Profile	SSL	☑
CA	GS_SCL_CA_v1	☑
Token	User Generated	☑
	Add End Entity Reset	

4 -- Install IIS

1. Start\Manage Your Server\Add or remove a role\click “Next”\Choose “Application server(IIS, ASP.NET)”



Configure Your Server Wizard

Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	Yes
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	Yes
DNS server	Yes
DHCP server	No
Streaming media server	No
WINS server	No

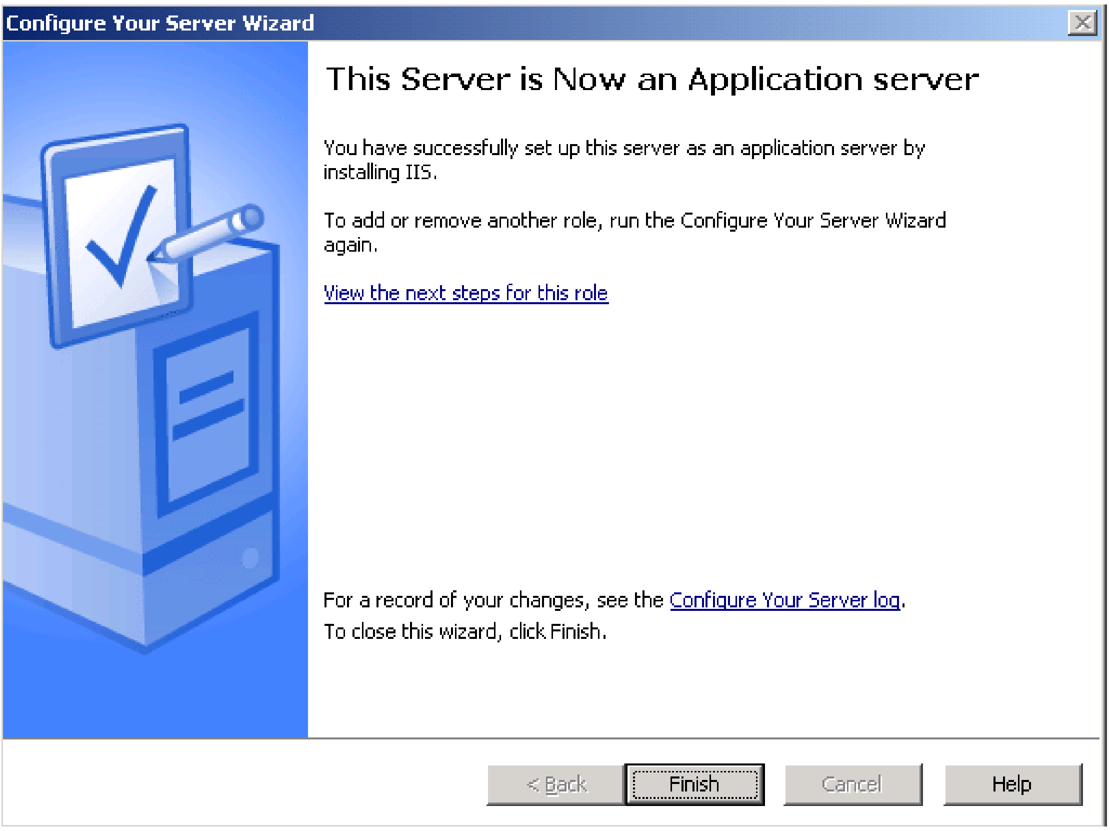
Application server (IIS, ASP.NET)

Application servers provide the core technologies required to build, deploy, and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+ and Internet Information Services (IIS).

Read about application servers

View the Configure Your Server log.

2. Click “Next” 3 times
3. You may be prompted to insert Windows 2003 server CD during installation process



This Server is Now an Application server

You have successfully set up this server as an application server by installing IIS.

To add or remove another role, run the Configure Your Server Wizard again.

View the next steps for this role

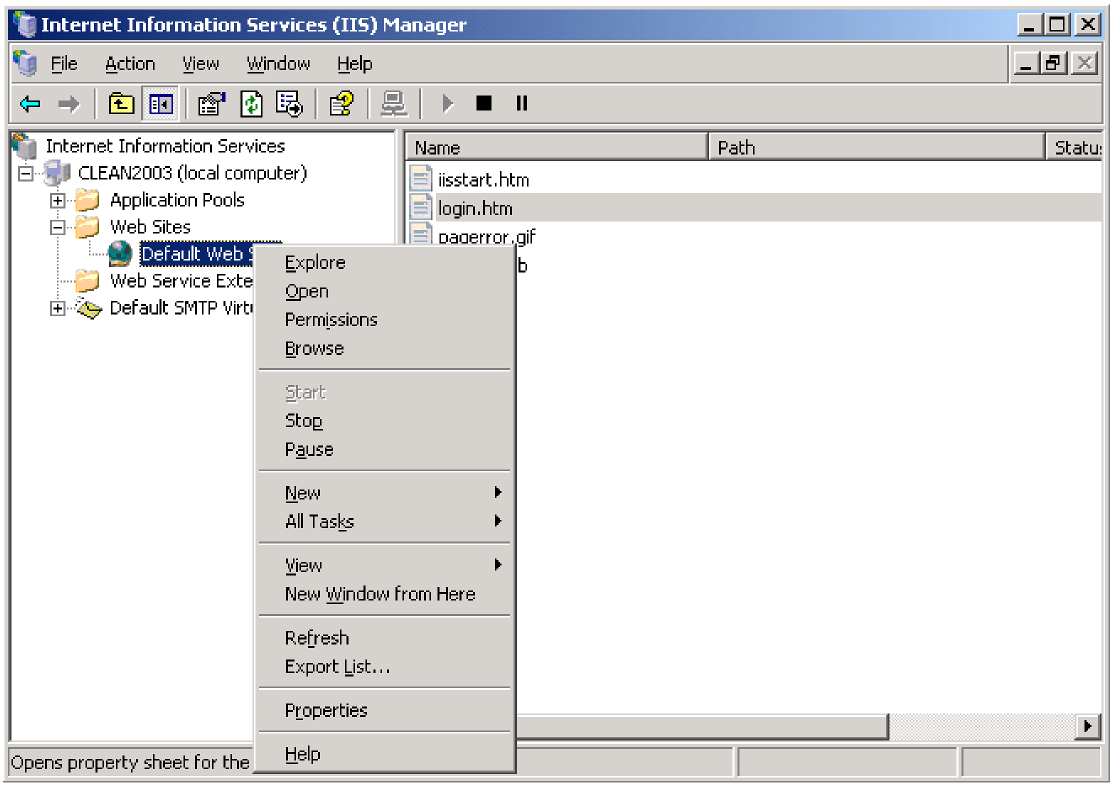
For a record of your changes, see the Configure Your Server log.

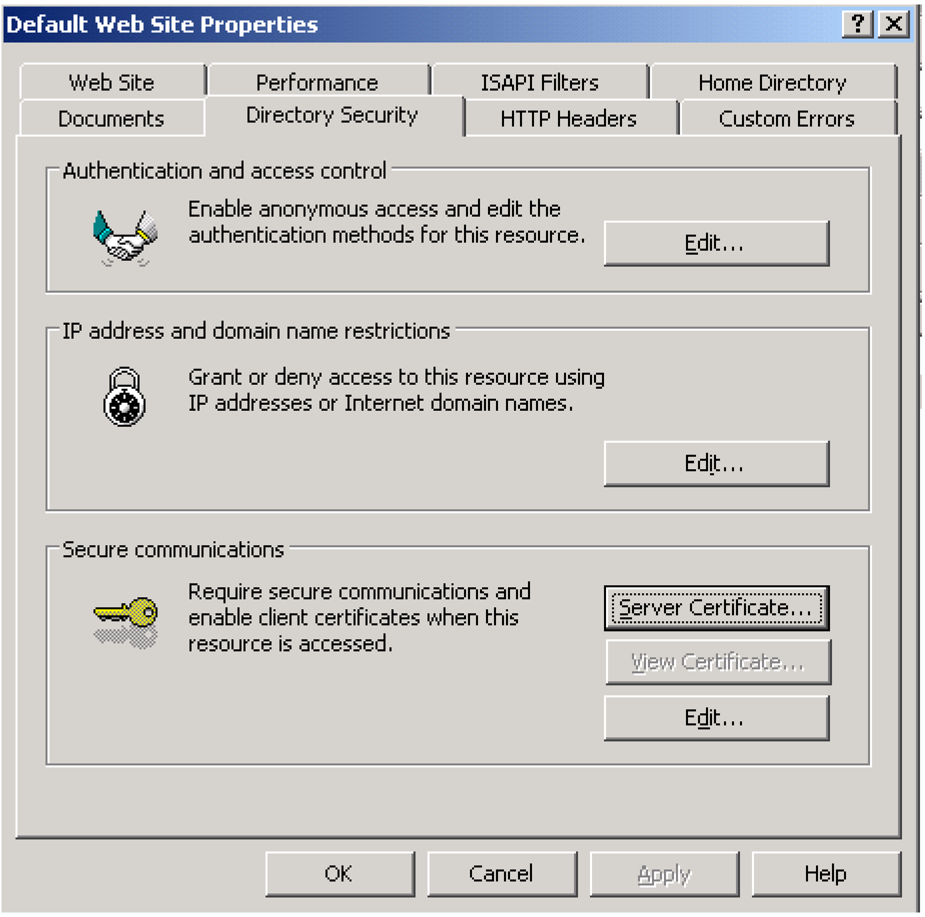
To close this wizard, click Finish.

4. Click “Finish”

5 -- Send SSL Certificate Request

1. Start\All Programs\Administrative tools\ Internet Information Services (IIS) Manager\CLEAN2003 (local computer)\ Web Sites\right click "Default Web Site"\Properties





Default Web Site Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

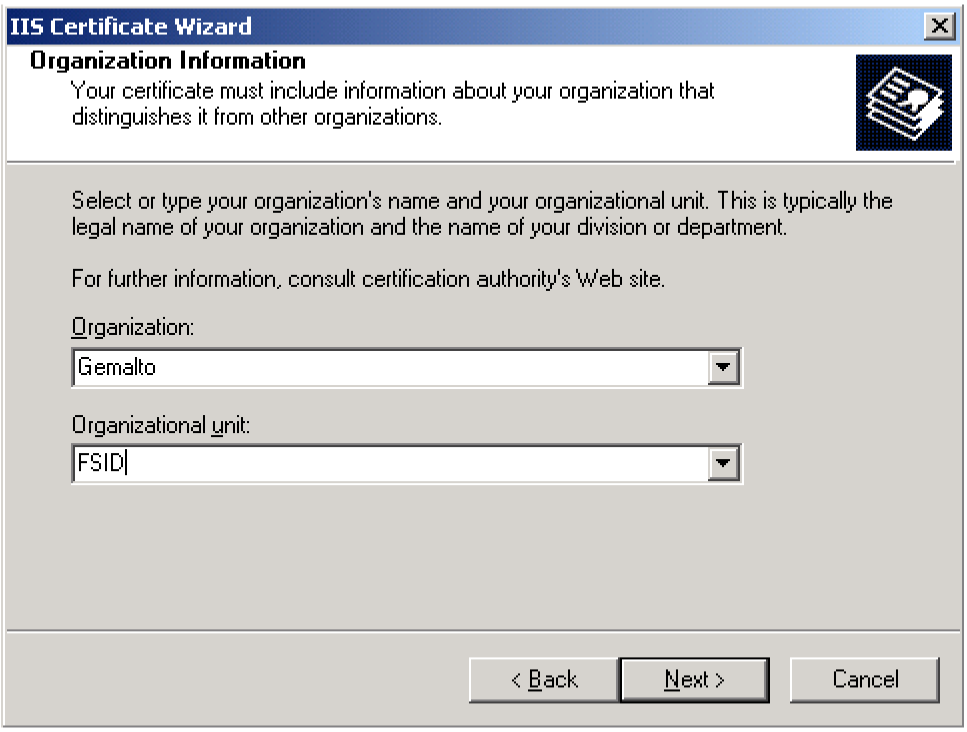
IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

2. Directory Security\Server Certificate…
3. Click “Next” 4 times
4. “Organization”= Gemalto
5. “Organization Unit”=FSID



IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

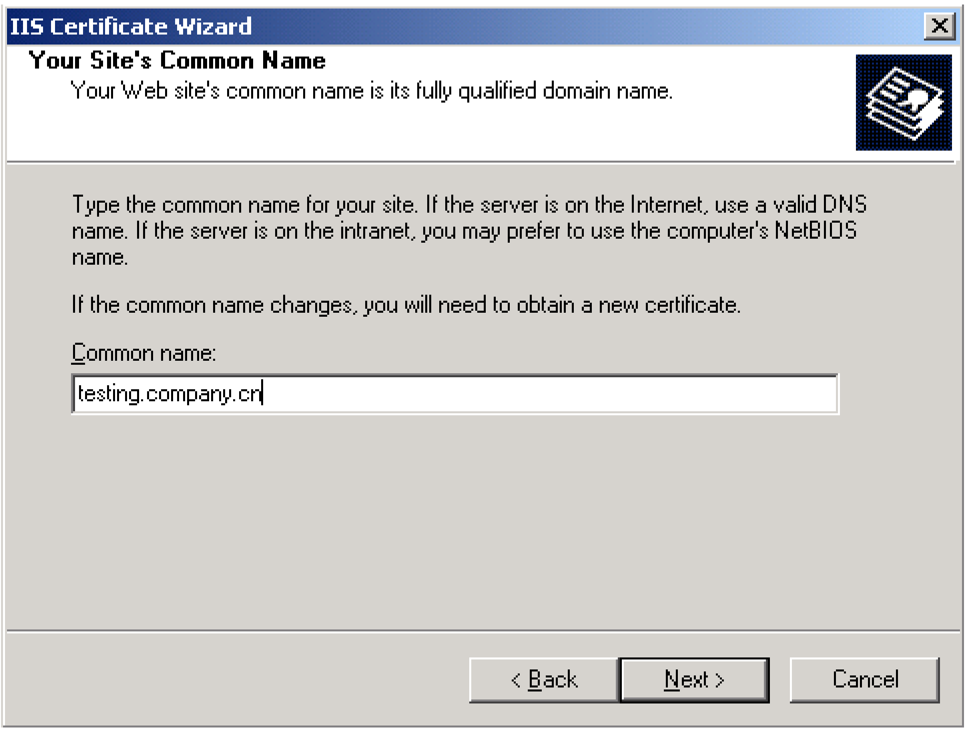
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization: Gemalto

Organizational unit: FSID

6. Click “Next”
7. Input website’s “common name”, here I use “testing.company.cn” as example



IIS Certificate Wizard

Your Site's Common Name

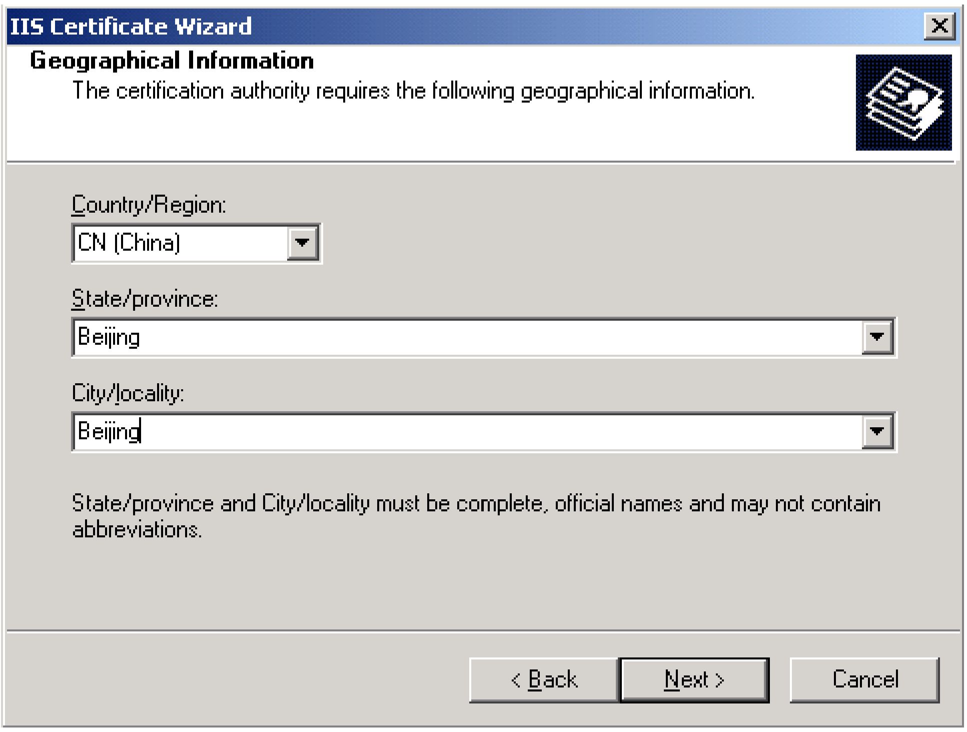
Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:
testing.company.cn

8. Click “Next”
9. “Country/Region”=(CN) China
10. “State”=Beijing
11. “City/locality”=Beijing



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

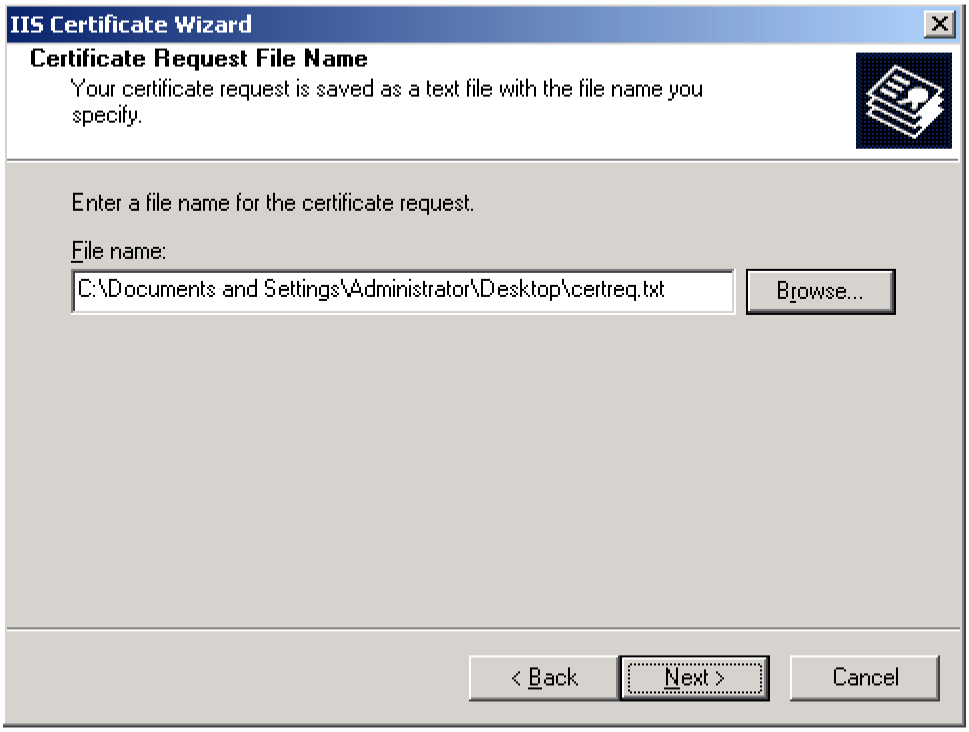
Country/Region:
CN (China)

State/province:
Beijing

City/locality:
Beijing

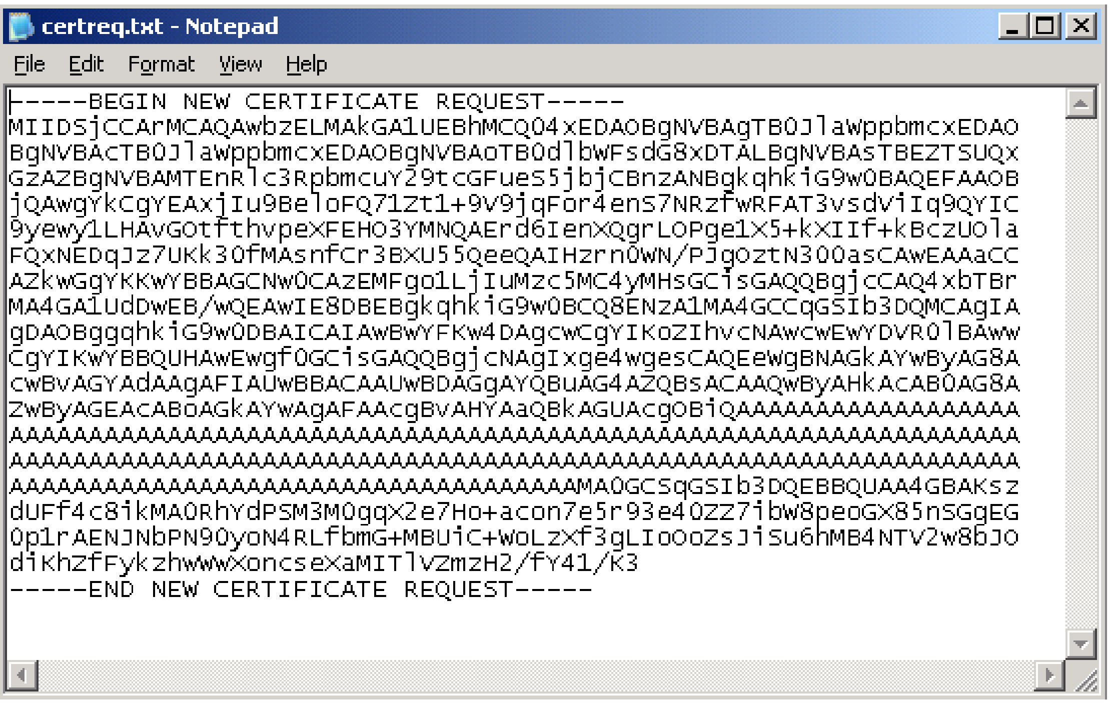
State/province and City/locality must be complete, official names and may not contain abbreviations.

12. Click “Next”
13. Save the certificate request at desktop



IIS Certificate Wizard
Certificate Request File Name
Your certificate request is saved as a text file with the file name you specify.
Enter a file name for the certificate request.
File name:
C:\Documents and Settings\Administrator\Desktop\certreq.txt
Browse...
< Back
Next >
Cancel

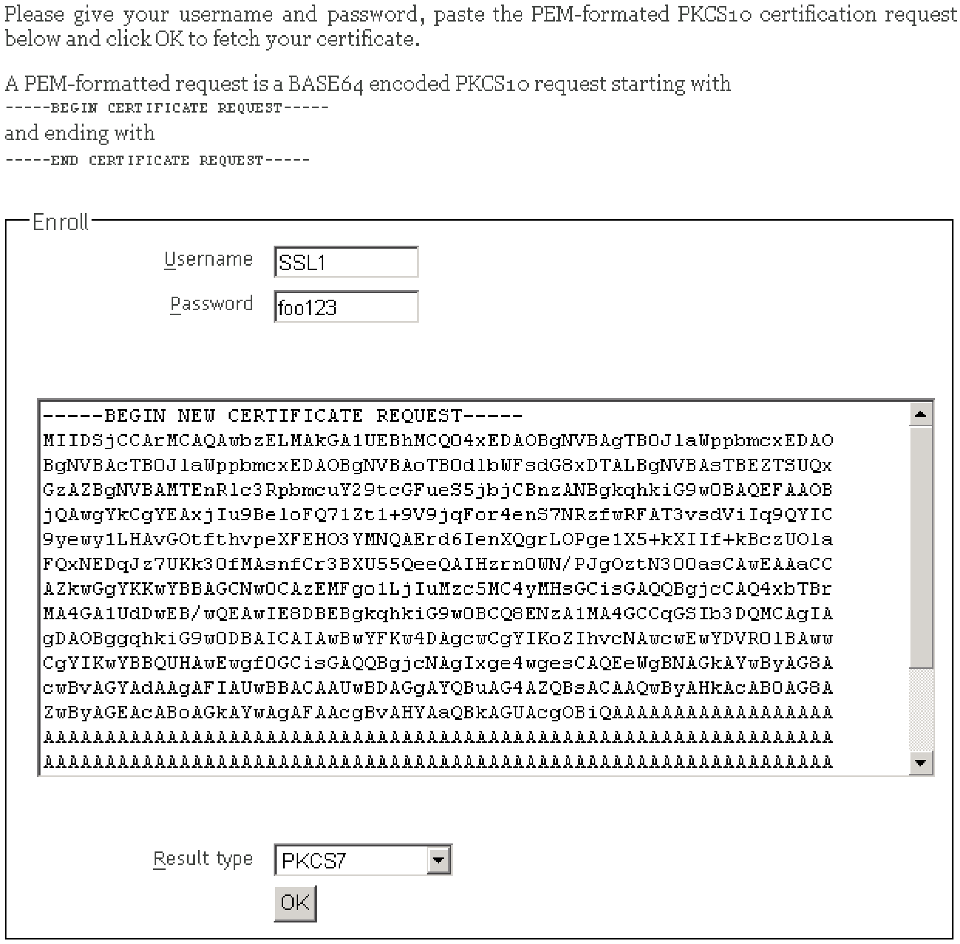
14. Click “Next” 2 times
15. Click “Finish”
16. A text file will be created at desktop
17. Open the text file, “certreq.txt”, copy the content, which is started by “-----BEGIN NEW CERTIFICATE REQUEST-----” and ended by “-----END NEW CERTIFICATE REQUEST-----”



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSjCCArMCAQAwbzELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB0JlaWppbmcxEDAO
BgNVBAcTB0JlaWppbmcxEDAOBgNVBAoTB0dlbWFsdG8xDTALBgNVBAsTBEZTSUQx
GzAZBgNVBAMTEnRlc3RpbmcuY29tcGFueS5jbjCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAxjIu9BeloFQ71Zt1+9V9jqFor4enS7NRzfwRFAT3vsdViIq9QYIC
9yewy1LHAvGOtfthvpeXFEHO3YMNQAErd6IenXQgrLOPge1X5+kXIIf+kBczUOla
FQxNEDqJz7UKk30fMAsnfCr3BXU55QeeQAIHzrn0WN/PJgOztN300asCAwEAAaCC
AZkwGgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBr
MA4GA1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIA
gDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAww
CgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8A
cwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8A
ZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAKsz
dUFf4c8ikMA0RhYdPSM3M0gqX2e7Ho+acon7e5r93e40ZZ7ibw8peoGX85nSGgEG
0p1rAENJNbPN90yoN4RLfbmG+MBUiC+WoLzXf3gLIoOoZsJiSu6hMB4NTV2w8bJO
diKhzfFykzhwwwXoncseXaMITlvZmzH2/fY41/K3
-----END NEW CERTIFICATE REQUEST-----
```

18. Go to EJBCA public webpage\Create Server Certificate
19. User name=SSL1
20. Password=foo123

21. Paste the request to the text area below
22. Select “Result type” as “PKCS7”



Please give your username and password, paste the PEM-formated PKCS10 certification request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded PKCS10 request starting with

```
-----BEGIN CERTIFICATE REQUEST-----
```

and ending with

```
-----END CERTIFICATE REQUEST-----
```

Enroll

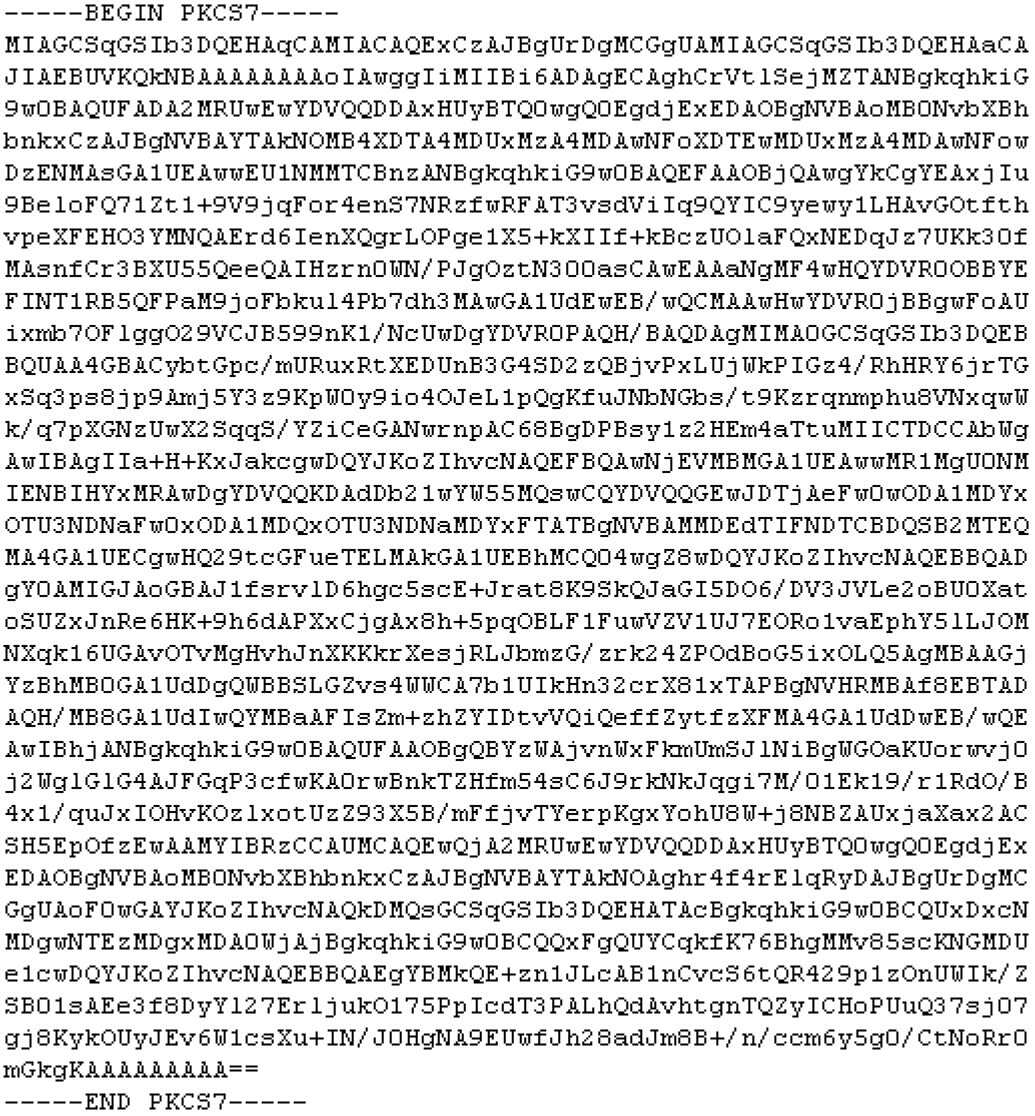
Username: SSL1

Password: foo123

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSjCCArMCAQAwbzELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB0JlaWppbmcxEDAO
BgNVBAcTB0JlaWppbmcxEDAOBgNVBAoTB0dlbWFsdG8xDTALBgNVBAsTBEZTSUQx
GzAZBgNVBAMTEnRlc3RpbmcuY29tcGFueS5jbjCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAxjIu9BeloFQ71Zt1+9V9jqFor4enS7NRzfwRFAT3vsdViIq9QYIC
9yewy1LHAvGOtfthvpeXFEHO3YMNQAErd6IenXQgrLOPge1X5+kXIIf+kBczUOla
FQxNEDqJz7UKk30fMAsnfCr3BXU55QeeQAIHzrn0WN/PJgOztN300asCAwEAAaCC
AZkwGgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBr
MA4GA1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIA
gDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAww
CgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8A
cwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8A
ZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Result type: PKCS7

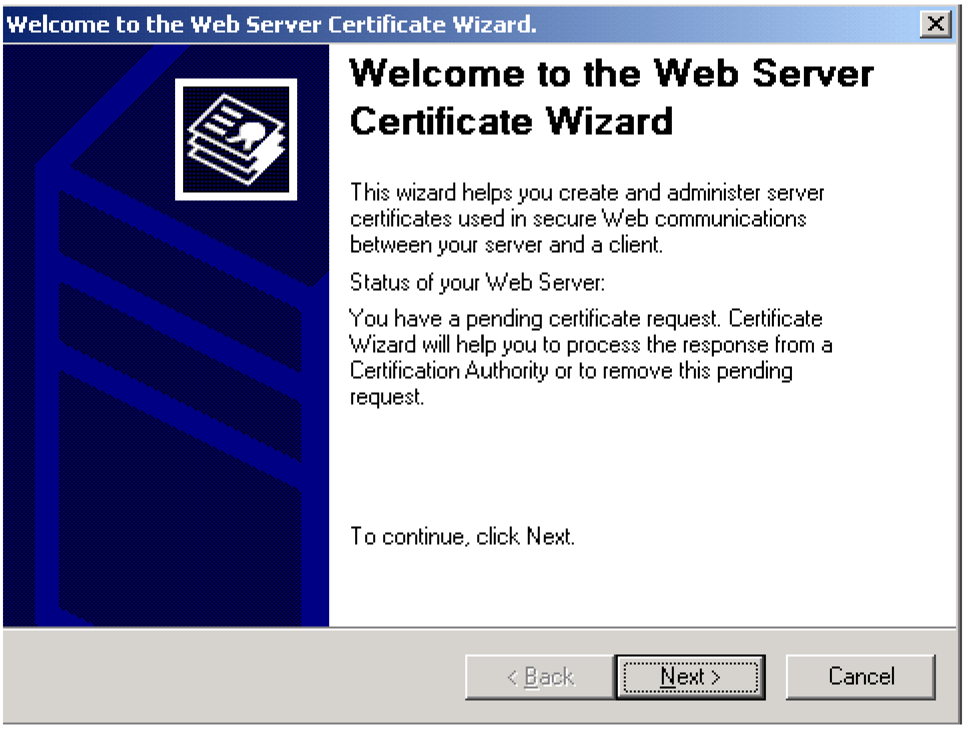
23. Click “OK”
24. A page of result will be shown.



```
-----BEGIN PKCS7-----
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAaCA
JIAEBUVKQkNBAAAAAAAAoIAwggIiMIIBi6ADAgECAghCrVtlSejMZTANBgkqhkiG
9w0BAQUFADA2MRUwEwYDVQQDDAxHUyBTQ0wgQ0EgdjExEDAOBgNVBAoMB0NvbXBh
bnkxCzAJBgNVBAYTAkNOMB4XDTA4MDUxMzA4MDAwNFoXDTEwMDUxMzA4MDAwNFow
DzENMAsGA1UEAwwEU1NMMTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxjIu
9BeloFQ71Zt1+9V9jqFor4enS7NRzfwRFAT3vsdViIq9QYIC9yewy1LHAvGOtfth
vpeXFEHO3YMNQAErd6IenXQgrLOPge1X5+kXIIf+kBczUOlaFQxNEDqJz7UKk3Of
MAsnfCr3BXU55QeeQAIHzrnOWN/PJgOztN3OOasCAwEAAaNgMF4wHQYDVR0OBBYE
FINT1RB5QFPaM9joFbkul4Pb7dh3MAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU
ixmb7OFlggO29VCJB599nK1/NcUwDgYDVR0PAQH/BAQDAgMIMA0GCSqGSIb3DQEB
BQUAA4GBACybtGpc/mURuxRtXEDUnB3G4SD2zQBjvPxLUjWkPIGz4/RhHRY6jrTG
xSq3ps8jp9Amj5Y3z9KpW0y9io4OJeL1pQgKfuJNbNGbs/t9Kzrqnmphu8VNxqwW
k/q7pXGNzUwX2SqqS/YZiCeGANwrnpAC68BgDPBsy1z2HEm4aTtuMIICTDCCAbWg
AwIBAgIIa+H+KxJakcgwDQYJKoZIhvcNAQEFBQAwNjEVMBMGA1UEAwwMR1MgU0NM
IENBIHYxMRAwDgYDVQQKDAdDb21wYW55MQswCQYDVQQGEwJDTjAeFw0wODA1MDYx
OTU3NDNaFw0xODA1MDQxOTU3NDNaMDYxFTATBgNVBAMMDEdTIFNDTCBDQSB2MTEQ
MA4GA1UECgwHQ29tcGFueTELMAkGA1UEBhMCQ04wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ1fsrvlD6hgc5scE+Jrat8K9SkQJaGI5DO6/DV3JVLe2oBUOXat
oSUZxJnRe6HK+9h6dAPXxCjgAx8h+5pqOBLF1FuwVZV1UJ7EORo1vaEphY5lLJOM
NXqk16UGAvOTvMgHvhJnXKKkrXesjRLJbmzG/zrk24ZPOdBoG5ixOLQ5AgMBAAGj
YzBhMB0GA1UdDgQWBBSLGZvs4WWCA7b1UIkHn32crX81xTAPBgNVHRMBAf8EBTAD
AQH/MB8GA1UdIwQYMBaAFIsZm+zhZYIDtvVQiQeffZytfzXFMA4GA1UdDwEB/wQE
AwIBhjANBgkqhkiG9w0BAQUFAAOBgQBYzWAjvnWxFkmUmSJlNiBgWGOaKUorwvjO
j2WglGlG4AJFGqP3cfwKAOrwBnkTZHfm54sC6J9rkNkJqgi7M/O1Ek19/r1RdO/B
4x1/quJxIOHvKOzlxotUzZ93X5B/mFfjvTYerpKgxYohU8W+j8NBZAUxjaXax2AC
SH5EpOfzEwAAMYIBRzCCAUMCAQEwQjA2MRUwEwYDVQQDDAxHUyBTQ0wgQ0EgdjEx
EDAOBgNVBAoMB0NvbXBhbnkxCzAJBgNVBAYTAkNOAghr4f4rElqRyDAJBgUrDgMC
GgUAoF0wGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcN
MDgwNTEzMDgxMDA0WjAjBgkqhkiG9w0BCQQxFgQUYCqkfK76BhgMMv85scKNGMDU
e1cwDQYJKoZIhvcNAQEBBQAEgYBMkQE+zn1JLcAB1nCvcS6tQR429p1zOnUWIk/Z
SBO1sAEe3f8DyYl27ErljukO175PpIcdT3PALhQdAvhtgnTQZyICHoPUuQ37sjO7
gj8KykOUyJEv6W1csXu+IN/JOHgNA9EUwfJh28adJm8B+/n/ccm6y5gO/CtNoRrO
mGkgKAAAAAAAAA==
-----END PKCS7-----
```

6 -- Fetch SSL Certificate

1. Copy the result and save it in a text file at desktop with a name of SSL1.text
2. Change the text file extension from txt to cer so SSL1.text becomes SSL1.cer
3. Go to Start\All Programs\Administrative tools\ Internet Information Services (IIS) Manager\ CLEAN2003 (local computer)\ Web Sites\right click “Default Web Site”\Properties\ Directory Security\Server Certificate…



Welcome to the Web Server Certificate Wizard

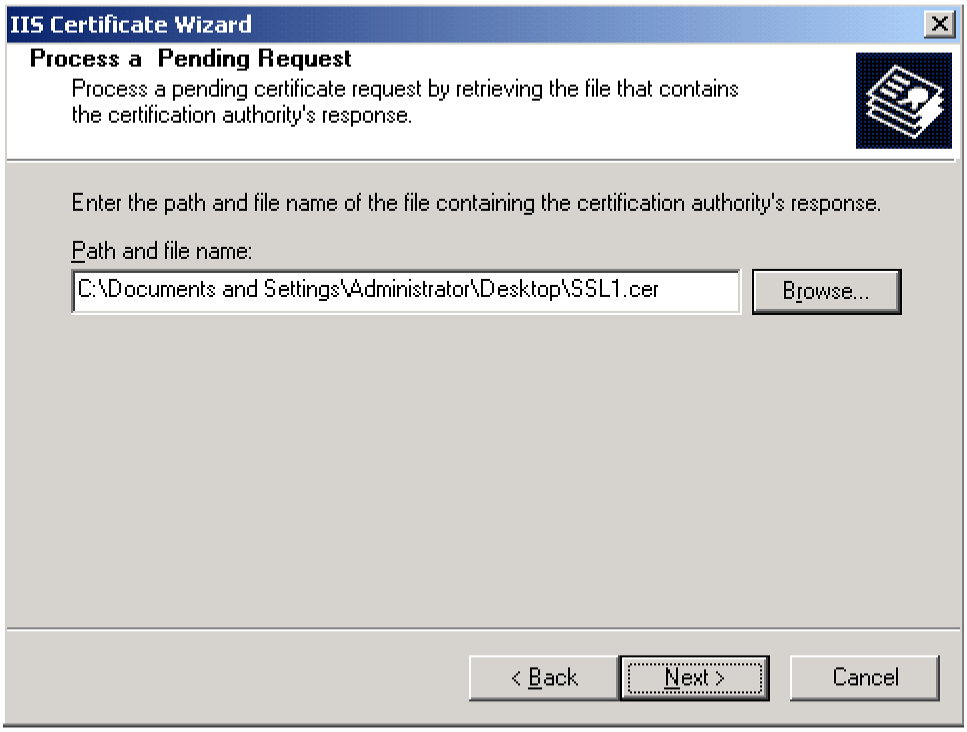
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web Server:

You have a pending certificate request. Certificate Wizard will help you to process the response from a Certification Authority or to remove this pending request.

To continue, click Next.

4. Click “Next >” 2 times



Process a Pending Request

Process a pending certificate request by retrieving the file that contains the certification authority's response.

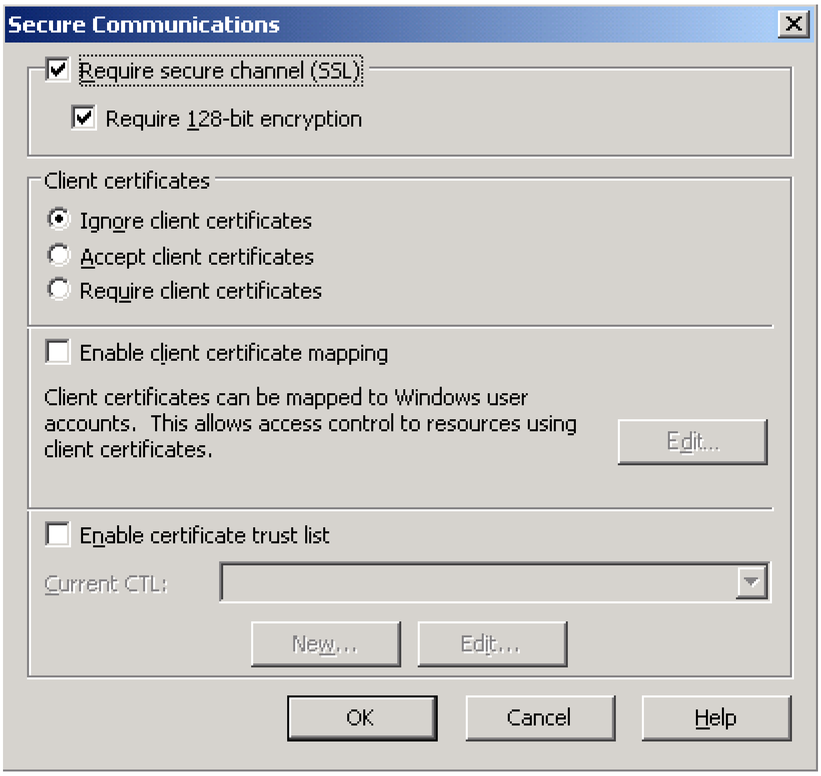
Enter the path and file name of the file containing the certification authority's response.

Path and file name: C:\Documents and Settings\Administrator\Desktop\SSL1.cer

5. Browse to SSL1.cer
6. Click “Next >”3 times
7. Click “Finish”

7 -- Configure IIS

1. Go to Start\All Programs\Administrative tools\ Internet Information Services (IIS) Manager\ CLEAN2003 (local computer)\ Web Sites\right click “Default Web Site”\Properties\ Directory Security\Secure Communications\Edit
2. Check “require secure Channel (SSL)”
3. Check “require 128-bit encryption”



Secure Communications

☑ Require secure channel (SSL)

☑ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

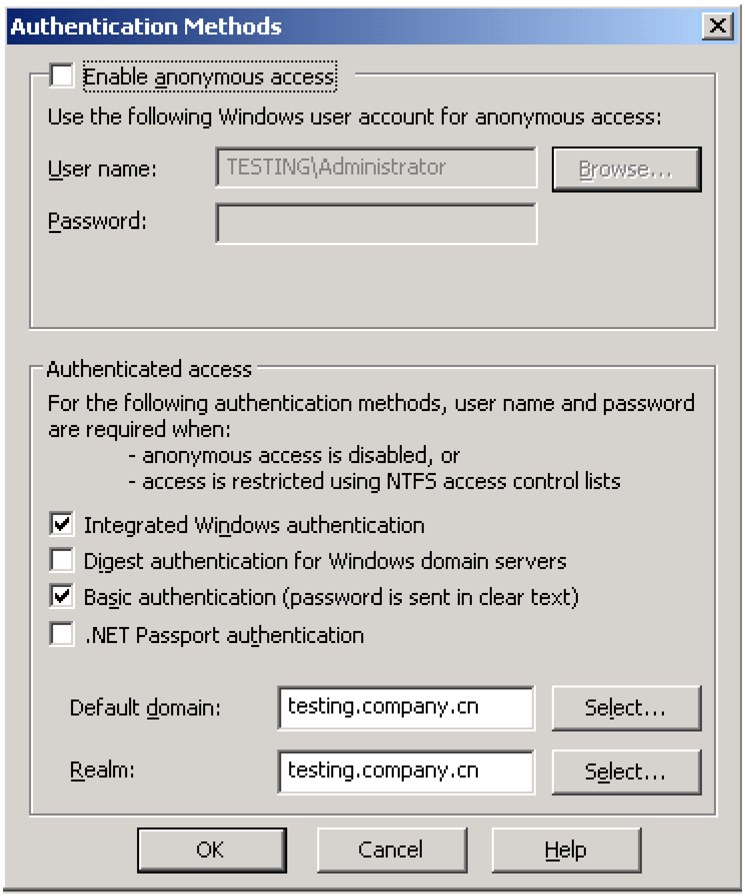
□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

Current CTL:

4. Click “OK”
5. Go to “Authentication and access control”\Edit…
6. Uncheck the “anonymous access”
7. User name:= TESTING\Administrator
8. Password=foo123
9. Check the “Basic authentication (password is sent in clear text)”
10. Choose “Yes” to the warning
11. Default Domain= testing.company.cn
12. realm= testing.company.cn



Authentication Methods

☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: TESTING\Administrator

Password:

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☑ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

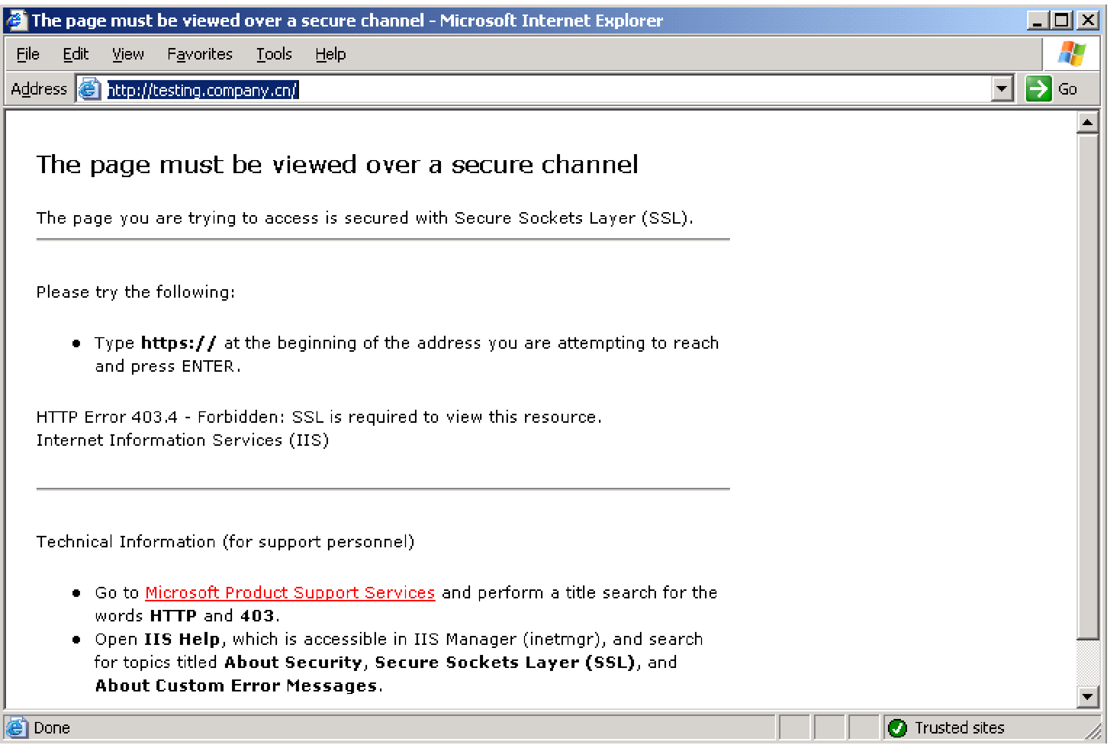
Default domain: testing.company.cn

Realm: testing.company.cn

13. Click “OK” 2 times

8 -- Test SSL

1. Open Internet Explorer, go to http://testing.company.cn/
2. You will not be able to access the default webpage



The page must be viewed over a secure channel - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://testing.company.cn/
Go

The page must be viewed over a secure channel

The page you are trying to access is secured with Secure Sockets Layer (SSL).

Please try the following:

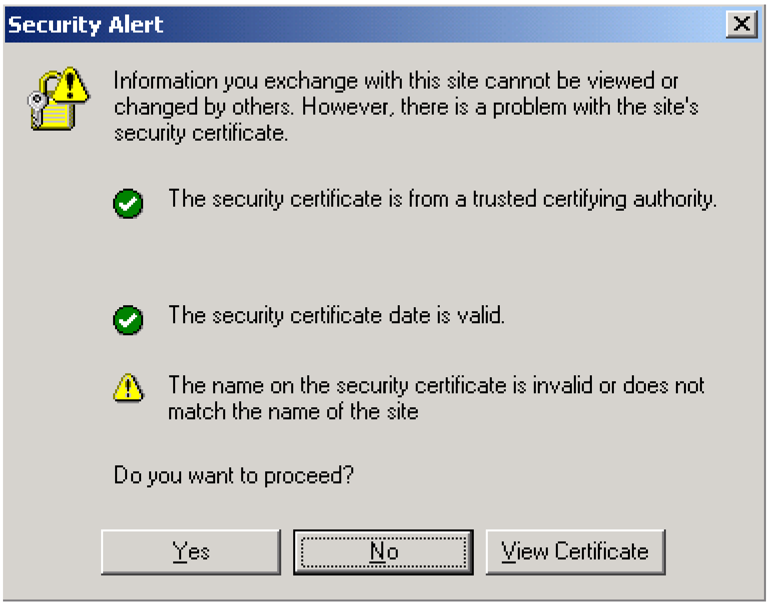
- Type **https://** at the beginning of the address you are attempting to reach and press ENTER.

HTTP Error 403.4 - Forbidden: SSL is required to view this resource.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Security**, **Secure Sockets Layer (SSL)**, and **About Custom Error Messages**.

3. Then try again with https://testing.company.cn/



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

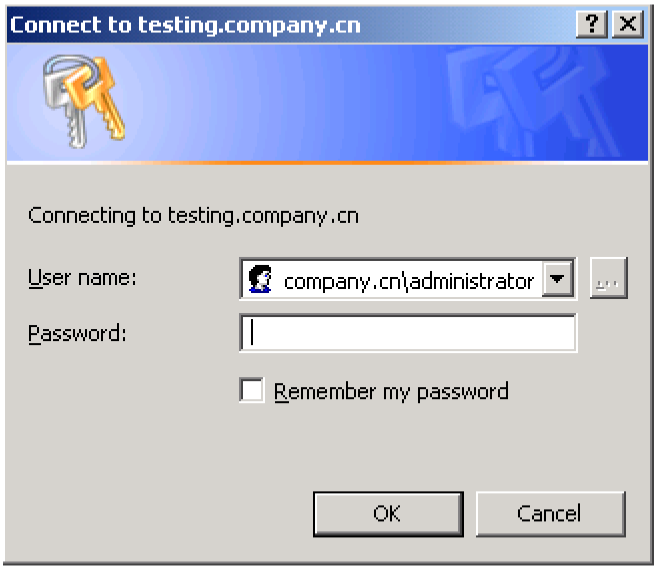
✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

4. Click "Yes"



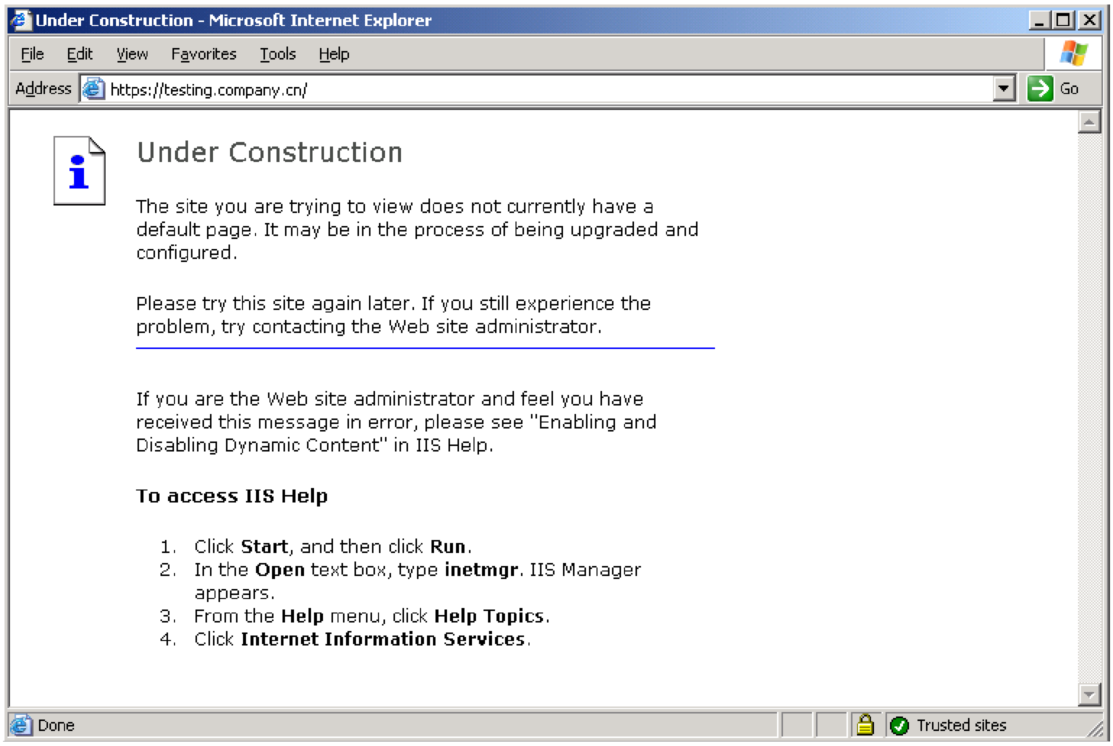
Connecting to testing.company.cn

User name: company.cn\administrator

Password:

□ Remember my password

5. Enter your account password, which you used to logon to server
6. Then you will be able to access the default webpage



Under Construction - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://testing.company.cn/
Go

Under Construction

The site you are trying to view does not currently have a default page. It may be in the process of being upgraded and configured.

Please try this site again later. If you still experience the problem, try contacting the Web site administrator.

If you are the Web site administrator and feel you have received this message in error, please see "Enabling and Disabling Dynamic Content" in IIS Help.

To access IIS Help

1. Click **Start**, and then click **Run**.
2. In the **Open** text box, type **inetmgr**. IIS Manager appears.
3. From the **Help** menu, click **Help Topics**.
4. Click **Internet Information Services**.

7. Notice that there is a lock sign 🔒 at the bottom of the web page

8. That means SSL is working