Configuring a Secure Website with a Digital Certificate

This article will explain you different steps that can be taken to secure a web site in IIS5 with a third- party assigned certificate.

The whole practice consists of the following steps.

- Generating the CSR for a website named **Secure**.
- Requesting a trial certificate from Verisign.
- Obtaining the **Trial Certificate**.
- Installing the Trial Certificate.
- Enforcing SSL and Testing the Secure Website.

Note: This whole article assumes that you have already installed IIS 5 on your Windows 2000 computer and has configured a website named Secure.

Generating CSR:

A CSR (Certificate Signing Request) is basically a certificate that you generate on your server that validates the computer-specific information about your server when you request a certificate from a third-party CA. The CSR is simply an encrypted text message that is encrypted with a public/private key pair.

Typically, a CSR contains the following information about your computer.

- Organization
- Organizational unit
- Country
- State
- Locality

To begin the process to obtain the certificate, you must generate a CSR. Follow these steps to generate the CSR.

 Access the IIS Microsoft Management Console (MMC). To access it, right-click My Computer and click Manage. This opens the Computer Management Console. Expand the Services and Application section. Locate Internet Information Services and expand the IIS console.

📮 Computer Management	
$Action$ View \Rightarrow \Rightarrow \blacksquare	🗗 🖶 😫
Tree	Description
Services	🙈 Default Web Site
🖅 🚰 Indexing Service	ite 🔬 Administration Web Site
🖃 🍓 Internet Information Services	i Secure
🕀 🜏 Default Web Site	🌤 Default SMTP Virtual Serve
🕀 🧶 Administration Web Site	lefault NNTP Virtual Servε
🕀 Secure	
🕀 🌭 Default SMTP Virtual Server	
Default NNTP Virtual Server	
tera, DNS	
J. J. J.	

- Select the specific Web site (Secure), right-click the site and click **Properties**.
 Click the **Directory Security** tab. In the **Secure Communications** section, click **Server Certificate**.

Secure Properties		? ×
Web Site Operator Directory Security	s Performance ISAPI Filters HTTP Headers Custom Er	Home Directory Documents rors Server Extensions
Anonymous acces	s and authentication control le anonymous access and edit the entication methods for this resource.	Edit
IP address and do	main name restrictions : or deny access to this resource using dresses or internet domain names]
		Edit
Secure communica	ations	
enabl resou	ire secure communications and le client certificates when this rce is accessed.	Server Certificate View Certificate
		Edit
	OK Cancel	Apply Help

4. The Web Server Certificate Wizard will start. Click Next.



5. Select Create a New Certificate and click Next.

IIS Certificate Wizard		×
Server Certificate There are three methods for assigning a certificate to a Web site.		
Select the method you want to use for this web site:		
 Create a new certificate. 		
Assign an existing certificate		
Import a certificate from a Key Manager backup file.		
< Back	Next >	Cancel

6. Select Prepare the request now, but send it later and click Next.

IIS C	ertificate Wizard
De	layed or Immediate Request You can prepare a request to be sent later, or you can send one immediately.
	Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?
	Prepare the request now, but send it later
	C Send the request immediately to an online certification authority
	< Back Next > Cancel

7. In the **Name** field, enter a name that you can remember. It will default to the name of the Web site for which you are generating the CSR.

NOTE: When you generate the CSR, you need to specify a bit length. The bit length of the encryption key determines the strength of the encrypted certificate which you send to the third-party CA. The higher the bit length, the stronger the encryption. Most third-party CAs prefer a minimum of 1024 bits.

IIS Certificate Wizard 🔀 🔀
Name and Security Settings Your new certificate must have a name and a specific bit length.
Type a name for the new certificate. The name should be easy for you to refer to and remember.
Secure
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.
Bit length:
Server Gated Cryptography (SGC) certificate (for export versions only)
< Back Next > Cancel

8. In the **Organization Information** section, enter your organization and organizational unit information. This must be accurate, because you are presenting these credentials to a third-party CA and you must comply with their licensing of the certificate.

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:	
CertsBraindumps.com	
Organizational unit:	
Article Department	
< Back Next > Cance	el

9. Click Next to access the Your Site's Common Name section.

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 D name. If the server is on the intranet, you may prefer to use the computer's NetBIC name. If the common name changes, you will need to obtain a new certificate.	NS IS
Common name:	
SERVER	
< Back Next >	Cancel

Note: The **Your Site's Common Name** section is responsible for binding the certificate to your Web site. For SSL certificates, enter the host computer name with the domain name. For Intranet servers, you may use the NetBIOS name of the computer that is hosting the site. Click **Next** to access geographical information.

 Enter your country, state or province, and country or region information. Completely spell out your state or province and country or region; do not use abbreviations. Click Next.

IIS Certificate Wizard 🛛 🛛 🗡
Geographical Information The certification authority requires the following geographical information.
Country/Region: GB (United Kingdom) 💌 State/province:
London
City/locality:
London
State/province and City/locality must be complete, official names and may not contain abbreviations.
< Back Next > Cancel

11. Save the file as a .txt file.

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:\certreq.txt	Browse
< Back	t> Cancel

Note: When you actually send the request to the CA, you must paste the contents of this file into the request. This file will be encrypted and contain a header and footer for the contents. You must include both the header and footer when you request the certificate. A CSR should resemble the following:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDATCCAmoCAQAwbDEOMAwGA1UEAxMFcGxhbjgxDDAKBgNVBAsTA1BTUzE SMBAGA1UEChMJTWljcm9zb2Z0MRIwEAYDVQQHEwIDaGFybG90dGUxFzAVBg NVBAgTDk5vcnRoIENhcm9saW5hMQswCQYDVQQGEwJVUzCBnzANBgkghkiG9w 0BAQEFAAOBjQAwgYkCgYEAtW1koGfdt+EoJbKdxUZ+5vE7TF1ZuT+xaK9jEWHE Sfw11zoRKrHzHN0fASnwg3vZ0ACteQy5SiWmFaJeJ4k7YaKUb6chZXG3GqL4YiSK FaLpJX+YRiKMtmIJzFzict5GVVGHsa1IY0BDYDO2XOAlstGIHCtENHOKpzdYdANR g0CAwEAAaCCAVMwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUGCis GAQQBgjcCAQ4xJzAIMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgE FBQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8 AZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBIAGwAIABDAHIAeQBwAHQAbw BnAHIAYQBwAGqAaQBjACAAUAByAG8AdqBpAGQAZQByA4GJAGKa0jzBn8fkxSc rWsdnU2eUJOMUK5Ms87Q+fjP1/pWN3PJnH7x8MBc5isFCjww6YnIjD8c3OfYfjkmW c048ZuGoH7ZoD6YNfv/SfAvQmr90eGmKOFFiTD+hl1hM08gu2oxFU7mCvfTQ/2lbX P7KYFGEqaJ6wn0Z5yLOByPqblQZAAAAAAAAAAAWDQYJKoZlhvcNAQEFBQADg YEAhpzNy+aMNHAmGUXQT6PKxWpaxDSjf4nBmo7oMhfC7ClvR0McCQ+CBwuLz D+UJxI+kjgb+gwcOUkGX2PCZ7tOWzcXWNmn/4YHQI0MGEXu0w67sVc2R9DIsHD NzeXLIOmjUl935qy1uoIR4V5C48YNsF4ejlgjeCFsbCojJb9/2RM= -----END NEW CERTIFICATE REQUEST-----

12. Confirm your request details. Click **Next** to finish, and exit the Web Server Certificate Wizard.

IIS Certificate Wizard Request File Summary You have chosen to genera	te a request file.			×
To generate the following re	quest, click Next.			
File name:c:\certreq.txt				
Your request contains the fo	llowing information	n:		
Issued To Friendly Name Country / Region State / Province City Organization Organizational Unit	SERVER Secure GB London London CertsBraindump Article Departme	s.com ent		
		< Back	Next >	Cancel

The CSR generating steps has been completed.

Requesting a Trial Certificate:

Certificates are obtained from the CA (Certificate Authorities). Different Third-Party CA(s) offer a trial certificate free of cost. Here we will request a server certificate to Verisign (a popular CA) on Internet.

1. Launch your browser, Open <u>www.verisign.com</u> website and find the link for Free Trial SSL Id as shown below.

🚈 YeriSign Inc www.verisign.com - Microsoft Internet Explorer 📃 📃 🗙					
File Edit View Favorites Tools Help					
] ← Back → → • 🤅	🗿 😰 🚮 🔯 Search 📷	Favorites 🎯History 🛛 🖏 🗸	🖨 🖸 • 🗐 🏷		
Address 🙋 http://ww	ww.verisign.com/		▼ 🔗 Go		
🛛 Links 🛭 🙋 Customize Lii	nks 🙋 Free Hotmail 🔌 Wir	ndows			
THE REPORT	THE REAL		WWWW.		
erprise 🤌	Small / Medium Business >>	Personal / Home Office »	I .com □ .net □ .us □ .org □info		
plete solutions for ing a secure digital prise	Everything to create, secure, and grow your online business	Get started with your own online identity and Web site	RENEW A DOM		
ge Your Brand Online » or Enterprise Servers » Aanagement and PKI » Iting Services »	Business Domain Names » Build a Web Site » Accept Online Payments » Get SSL Site Security »	Find a Domain Name » Build Your Web Site » Buy Personalized E-Mail » Secure Java/Authenticode »	DIGITAL CERTIFICATES & SSL Buy Guide FREE SSL Trial ID Product Renewals Free Guides and Trials		
	More	<u>More</u>	Events		
Done Some Some					

- 2. Fill out your Registration Information with a valid E-mail address to receive the digital certificate.
- 3. Follow the different steps (Normally five on Verisign) of online application to obtain the certificate.
 - Note: The CA can change the whole enrollment procedure according to its own policy.
- 4. Verisign will mail you with your digital certificate and instruction about using it.

Obtaining the Trial Certificate:

You will receive an e-mail from Verisign containing the same CSR text as you have sent it to but with a digitally signed signature. Just copy that text, paste it in a notepad and save the file with .Cer extension. Its your digital certificate.

Save As					<u>?×</u>
Save in:	🔁 Verisign Certifi	cate	•	🗢 🗈 💣 🛙	
History Desktop My Documents My Computer	File manage	11			Save 2
My Network P	Cause as human				Cancel
	Save as type:				
	Encoding:	ANSI		•	//

Installing the Trial Certificate:

To install the certificate, follow these steps:

- Open the IIS MMC as described in the "Generating the CSR" section.
 Access the **Properties** dialog box for the Web site on which you are installing the certificate.
- 3. Click the Directory Security tab and click Server Certificate. This starts the Web Server Certificate Wizard. Click Next.
- 4. Select Process the Pending Request and install the certificate and click Next.

IIS Certificate Wizard		×
Pending Certificate Request A pending certificate request is a request to which the certification authority has not yet responded.		
A certificate request is pending. What would you like to do?		
Process the pending request and install the certificate		
O Delete the pending request		
< Back	Next >	Cancel

- Browse to the file that you saved in previous step with .cer extension. Verify the certificate summary, click **Next** twice, then click **Finish**.
 After Finishing the wizard, you can view the installed certificate with the private key by clicking on the View Certificate Tab as shown below.

Secure Properties	<u>? ×</u>				
Web Site Operators Performance ISAPI Filters H Directory Security HTTP Headers Custom Err	Home Directory Documents fors Server Extensions				
Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource.	Edit				
IP address and domain name restrictions Grant or deny access to this resource using					
	Edit				
Secure communications					
Require secure communications and enable client certificates when this resource is accessed.	Server Certificate				
	Edit				
OK Cancel	Apply Help				

Certifi	icate			? ×
Gen	eral Details Cer	tification Path		
L E				
	Eertifical	e Information		
	This certificate i	is intended to:		
	•Ensures the •Proves you	identity of a remote computer r identity to a remote computer		
	* Refer to the cert	ification authority's statement fo	or details.	
	Issued to:	SERVER		
	Issued by:	For VeriSign authorized testing assurances (C)VS1997	only. No	
	¥alid from	3/4/2003 to 3/19/2003		
	🌮 You have a p	rivate key that corresponds to t	his certifi	cate.
			Issuer	Statement
				ОК

Note: This trial certificate is valid for only fifteen days

Enforcing SSL and testing secure site:

Now that the server certificate is installed, you can enforce SSL secure channel communications with clients of the Web server. First, you need to enable port 443 for secure communications with the Web site. To do this, follow these steps:

- 1. Right-click the secure Web site on and click **Properties**.
- 2. Click the **Web Site** tab. In the **Web Site Identification** section, verify that the **SSL Port** field is populated with the numeric value **443**.

Secure Properties	<u>?</u> ×			
Directory Security Web Site Operators	HTTP Headers Custom Errors Server Extensions Performance ISAPI Filters Home Directory Documents			
Web Site Identification				
Description:	Secure			
IP Address:	(All Unassigned) Advanced			
TCP Port:	85 SSL Port:			
Connections C Unlimited Limited To: Connection Timeout: HTTP Keep-Alives	1,000 connections 900 seconds s Enabled			
Enable Logging -				
Active log format:				
W3C Extended Log File Format				
	OK Cancel Apply Help			

If SSL port is not populated with 443 port number, follow the next step.

3. Click **Advanced**. You should see two fields. The IP address and port of the Web site should already be listed in the **Multiple identities for this web site** field. Under the **Multiple SSL Identities for this web site** field, click **Add** if port 443 is not already listed. Select the server's IP address, and type the numeric value **443** in the **SSL Port** field. Click **OK**.

A	Advanced Web Site SSL Identification					
	Identification					
	IP Address:	(All Unassigned)		•		
	SSL Port:	443				
	(OK)	Cancel	Help			

4. Click **Ok** to close the Advanced Website configuration Windows.

dvanced Multiple Web Site Configuration					
IP Address	TCP Port	Host Head	ler Name		
🍹 (All Unassigned)	85				
Add	F	emove	Edit		
IP Address			SSL	Port	
Y (All Unassigned)			443		
Add	R	emove	Edit		
		Cancel	Help		

Now that port 443 is enabled, you can enforce SSL connections. To do this, follow these steps:

1. Click the **Directory Security** tab. In the **Secure Communications** section, note that **Edit** is now available. Click **Edit**.

Secure Properties	? ×	
Web Site Operators Performance ISAPI Filters Directory Security HTTP Headers Custom E	Home Directory Documents rrors Server Extensions	
Anonymous access and authentication control Enable anonymous access and edit the authentication methods for this resource.	Edit	
IP address and domain name restrictions Grant or deny access to this resource usin IP addresses or internet domain names.	g Edit	
Secure communications Require secure communications and enable client certificates when this resource is accessed.	Server Certificate View Certificate Edit	
OK Cancel	Apply Help	

1. Select Require Secure Channel (SSL).

NOTE: If you specify 128-bit encryption, clients who use 40-bit or 56-bit strength browser will not be able to communicate with your site unless they upgrade their encryption strength.

Secure Communications		×
Require secure channel (SSL)	 	
Require 128-bit encryption		
Client certificates		
Ignore client certificates		
C Accept client certificates		
C Require client certificates		
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	Edit	
Current CTL:		-
New Edit		
OK Cancel	Help	

 Open your browser and try to connect to your Web server by using the standard http:// protocol. If SSL is being enforced, you receive the following error message:



3. Now access your server with the <u>https://Server</u> URL. Your secure site with SSL enabled will be shown.



SSL Secured (128 Bit)

Important Note:

Before using your Trial SSL Server ID, install the Test CA Root in each browser you plan to use as part of your test of SSL. To download the Test CA Root, Click on the link (Like this <u>http://www.verisign.com/support/install/index.html#trial</u>) provided you in your e-mail and follow the instructions there.

If you like this article, then please give your comments in the forum and cast your vote for this topic.