

CONFIGURARE OWA CON SSL

Outlook Web Access costituisce uno degli aspetti più intriganti di Exchange Server permettendo un servizio di webmail efficiente e ricco di features, quasi al pari di Microsoft Outlook.

La messa in sicurezza tramite SSL (Secure Socket Layer) è pressoché indispensabile dato che altrimenti i dati viaggerebbero su http, e quindi in chiaro su internet.

Gli step per conseguire questo risultato sono piuttosto semplici e probabilmente li avrete già eseguiti svariate volte per l'attivazione di SSL sui vostri siti.

Il certificato digitale per il sito può essere ottenuto da un ente ufficiale di certificazione, in alternativa è possibile produrre un certificato self-signed.

Per configurare IIS con SSL:

 Aprire la mmc di IIS, fare clic con il tasto destro sul sito di OWA e selezionare "Directory Security". Fare clic su "Server Certificate" e generare la richiesta di nuovo certificato:

IS Certificate Wizard	×
Server Certificate These are the 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.	
C Import a certificate from a .pfx file	
C Copy or Move a certificate from a remote server site to this site.	
< Back Next >	Cancel
Fig.1	

• Se non si possiede una CA di tipo Enterprise selezionare l'opzione Prepare the request now, but send it later":

IIS Certificate Wizard	×	
Delayed or Immediate Request You can prepare a request to be sent later, or you can send one	1	
immediately.		
Do you want to prepare a certificate request to be sent later, or do you want to immediately to an online certification authority?	send it	
Prepare the request now, but send it later		
Send the request immediately to an online certification authority		
	4	b
	Connel	
< <u>B</u> ack <u>N</u> ext >		
Fig.2		

2

Nella richiesta è fondamentale specificare correttamente il nome FQDN dell'indirizzo cui la posta web dovrà essere raggiungibile: •

IIS Ce	tificate Wizard
Nam	and Security Settings our new certificate must have a name and a specific bit length.
ך ז 1	ype a name for the new certificate. The name should be easy for you to refer to and member. ame:
	nail.tuodominio.it
1 1 0	he bit length of the encryption key determines the certificate's encryption strength. he greater the bit length, the stronger the security. However, a greater bit length may ecrease performance.
E	it lengt <u>h</u> : 1024
Γ	Select cryptographic service provider (CSP) for this certificate
	< <u>B</u> ack <u>N</u> ext > Cancel
	Fig.3

- -2)
 - Inserire i valori corretti per la vostra azienda: •

certificate Wizard Image: Certificate Mizard ganization 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: aa	
< <u>B</u> ack <u>N</u> ext > Cancel Fig.4	

Anche qui è indispensabile inserire il nome FQDN: •

IIS Cert	ificate Wizard					
Your S You	Site's Common N ur Web site's comm	lame non name is its fu	lly qualified doma	in name.	ŧ	
Typ nar nar	pe the common name. If the server is me.	me for your site. I on the intranet, y	f the server is on ou may prefer to r	the Internet, use use the compute	e a valid DNS er's NetBIOS	
lf tł	he common name (changes, you will	need to obtain a	new certificate.		
<u>C</u> or	mmon name:					
ma	ail.tuodominio.it					
					_	
				1 N 1		

Fig.5

Inserite i dati geografici: •

0

IIS Certificate Wizard	1
Geographical Information The certification authority requires the following geographical information.	
<u>C</u> ountry/Region: <mark>IT (Italy)</mark>	
<u>S</u> tate/province:	
ge 💌	\sim
City/Jocality:	\sim
ge 🔽	
State/province and City/locality must be complete, official names and may not contain abbreviations.	
< <u>B</u> ack <u>N</u> ext > Cancel	
Fig.6	

Infine salvate il file di richiesta certificato: •

Infine salva	ate il file di richiesta certificato:	
115	Certificate Wizard	×
Ce	ertificate 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.	
	<u>F</u> ile name:	
	c:\certreq.txt	B <u>r</u> owse
	< <u>B</u> ack <u>N</u> ext >	Cancel
	Fig.7	



- Terminata la fase di creazione della richiesta di certificato passatela alla vostra CA o ad un ente di certificazione ufficiale. Quindi tornate su IIS per completare il lavoro
- Si avvia il processo e si fa clic su 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 Delete the pending request 		K
		•
< <u>B</u> ack <u>N</u> ext >	Cancel	
Fig.8		

Selezionate il vostro certificato:

_		
	IIS Certificate Wizard	x
	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.	
	ratn and nie name:	
	< <u>B</u> ack <u>N</u> ext > Cancel	
	Fig.9	



La porta 443 dovrebbe andare bene anche per voi!

IIS Certificate Wizard SSL Port Specify the SSL port for this web site.			×	
SSL port this web site should use:				
	< <u>B</u> ack	<u>N</u> ext >	Cancel	

Breve riassunto, fate clic su Next e avete finito:

IIS Cer <mark>tificate</mark> Wizard		x
Certificate Summary You have chosen to in	nstall a certificate from a response file.	
To install the following	certificate, click Next.	
File name:	c:\revolutioncert.cer	
Certificate details: Issued To Issued By Expiration Date Friendly Name Country/Region State / Province City Organization Organizational Unit	mail.tuodominio.it frosinix.datasiel.net 09/08/2007 mail.tuodominio.it IT ge ge aa aa aa	
	< <u>B</u> ack <u>Next</u> ≻	Cancel

Fig.11



A questo punto il vostro sito è già abilitato all'uso di SSL.

Potete verificarlo con l'utilizzo di un browser: https://mail.tuodominio.it

E' possibile forzare l'utilizzo di SSL in questo modo: Web Site ->Directory Security -> Secure Communications -> Edit e selezionare il flag "Require secure channel (SSL)"

Web Site Performance ISAPI Filters Home Directory Documents Directory Security HTTP Headers Custom Errors Authentication and access control Enable anonymous access and edit the authentication methods for this resource. Edit IP address and domain name restrictions Edit Edit IP addresses or Internet domain names. Edit Secure communications Edit Image: Provide the secure communications and enable client certificates when this resource is accessed. Server Certificate Image: Provide the secure is accessed. View Certificate Image: Provide the secure is accessed. Edit Image: Provide the secure is accessed. Fig.12	Web Site Performance ISAPI Filters Home Directory Documents Directory Security HTTP Headers Custom Errors Authentication and access control Enable anonymous access and edit the authentication methods for this resource. Edit IP address and domain name restrictions Edit Edit IP address and domain name restrictions Edit IP address or Internet domain names. Edit Secure communications Edit Image: Secure communications and enable client certificates when this resource is accessed. Server Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. Yiew Certificate Image: Secure client certificates when this resource is accessed. <th>efault Web Site</th> <th>Properties</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>?×</th>	efault Web Site	Properties						?×
Documents Directory Security HTTP Headers Custom Errors Authentication and access control Enable anonymous access and edit the authentication methods for this resource. Edit IP address and domain name restrictions Edit Edit IP address and domain name restrictions Edit IP address and domain name restrictions Edit IP address and domain name restrictions Edit Secure communications Edit Image: Provide the secure communications and enable client certificates when this resource is accessed. Server Certificate Image: Provide the secure communications and enable client certificates when this resource is accessed. Server Certificate Image: Provide the secure communications and enable client certificates when this resource is accessed. Server Certificate Image: Provide the secure communications and enable client certificate secure certificate secure is accessed. Server Certificate Image: Provide the secure communications and enable client certificate secure cer	Documents Directory Security HTTP Headers Custom Errors Authentication and access control Enable anonymous access and edit the authentication methods for this resource. Edit IP address and domain name restrictions Edit Edit IP address and domain name restrictions Edit IP address and domain name restrictions Edit IP addresses or Internet domain names. Edit Secure communications Edit Image: Provide the enable client certificates when this resource is accessed. Server Certificate Image: Provide the enable client certificates when this resource is accessed. Yiew Certificate Image: Provide the enable of the enable client certificate when this resource is accessed. Edit Image: Provide the enable client certificates when this resource is accessed. Yiew Certificate Image: Provide the enable client certificates when this resource is accessed. Fig.12 Image: Provide the enable client certificates when this resource is accessed. Fig.12	Web Site	Performance		SAPI Filters	1	Home	Directory	
Authentication and access control Image: Secure communications	Authentication and access control Image: Second control in the second control is resource. IP address and domain name restrictions IP address and domain name restrictions Image: Second control in the second control is resource using in the second control is resource using in the second control is resource using in the second control is resource is accessed. Secure communications Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when the resource is accessed. Image: Secure communications and enable client certificates when the resource is accessed. Image: Secure communications and enable client certificates when the resource is accessed. Image: Secure communications and enable client certificates when the resource is accessed. Image: Secure communications and enable client	Documents	Directory Securit	:у	HTTP Heade	ers	Cus	stom Errors	- 1,
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 IP addresses or Internet domain names. Secure communications Edit Secure communications Edit enable client certificates when this resource is accessed. Server Certificate View Certificate View Certificate Edit Edit OK Cancel Apply Fig.12 Fig.12	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 IP addresses or Internet domain names. Edit Secure communications Require secure communications and enable client certificates when this resource is accessed. Kelter and the secure communications OK Cancel Apply Help Fig.12	Authenticatio	n and access control –						٦
IP address and domain name restrictions IP address and domain name restrictions IP addresses or Internet domain names. Edit Secure communications Image: Secure communications and enable client certificates when this resource is accessed. View Certificate View Certificate Image: Secure communications and enable client certificates when this resource is accessed. View Certificate Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure certificate certificates when this resource is accessed. Image: Secure certificate certificate certificates certificates Image: Secure certificate certificate certificates certificates certificates certificates Image: Secure certificate certificates certifi	IP address and domain name restrictions Image: Secure communications Image: Secure communications Image: Secure communications Image: Secure communications Image: Secure communications and enable client certificates when this resource is accessed. Image: Secure certificate certificates when this resource is accessed. Image: Secure certificate certificate certificate Image: Secure certificate certificate Image: Secure certificate	\$	Enable anonymous acc authentication method	ess and Is for this	edit the resource.		<u>E</u> dit		
Grant or deny access to this resource using IP addresses or Internet domain names. Edit Secure communications enable client certificates when this resource is accessed. Yew Certificate Yew Certificate Edit OK Cancel Apply Help Fig.12	Grant or deny access to this resource using IP addresses or Internet domain names. Edit Secure communications mable client certificates when this resource is accessed. View Certificate Edit OK Cancel Apply Help Fig.12	⊢IP address ar	nd domain name restric	tions —					
Edit Secure communications Require secure communications and enable client certificates when this resource is accessed. Yiew Certificate Edit OK Cancel Apply Help Fig.12	Edit Secure communications Require secure communications and enable client certificates when this resource is accessed. Yew Certificate Edit Edit Fig.12		Grant or deny access t IP addresses or Intern	o this re iet domai	source using n names.				
Secure communications Require secure communications and enable client certificates when this resource is accessed.	Secure communications Require secure communications and enable client certificates when this resource is accessed. View Certificate Edit OK Cancel Apply Help Fig.12				[Edįt		
Require secure communications and enable client certificates when this resource is accessed. Server Certificate View Certificate Edit Edit Edit	Require secure communications and enable client certificates when this resource is accessed. View Certificate Edit OK Cancel Apply Help Fig.12	- Secure comm	unications						
enable client certificates when this resource is accessed. Server Certificate View Certificate Edit Edit Edit OK Cancel Apply Help Fig.12	enable client certificates when this resource is accessed. Server Certificate View Certificate Edit Edit Edit OK Cancel Apply Help Fig.12 Help		Require secure commu	nications	and	c	C - 1161		
View Certificate Edit OK Cancel Apply Help Fig.12	OK Cancel Apply Help Fig.12		enable client certificate resource is accessed.	es when	this _	Server	Certifi	cate	
OK Cancel Apply Help Fig.12	OK Cancel Apply Help Fig.12				_	<u>V</u> iew ∙	Certific	ate	
OK Cancel Apply Help Fig.12	OK Cancel Apply Help Fig.12						E <u>d</u> it		
OK Cancel Apply Help Fig.12	OK Cancel Apply Help Fig.12								-
OK Cancel Apply Help Fig.12	OK Cancel Apply Help Fig.12								
Fig.12	Fig.12		ОК		ancel	Apply	/	Help	
			<u> </u>	Fig.12	2				
		P_{D}							
		VV							
		Va,							

ecure Communicatio	ns			×	
Require secure ch	annel (SSL)				
Require <u>1</u> 28-bit	encryption				
Client certificates					
Ignore client certif	icates				
O Accept client certil	icates				
C Require client cert	ificates				
Enable client certif	icate manning				
Client cortificator can	he manned to V	Windows usor			$\sim \times$
accounts. This allows	access control	to resources using	- n		
client certificates.			E <u>d</u> it		
Enable certificate	trust list				
⊆urrent CTL;				~	
	Ne <u>w</u>	Edjt			
	ОК	Cancel	<u>H</u> el	lp	
	Fiç	g.13			

L'ultimo step è quello di ridirezionare automaticamente tutto il traffico HTTP su HTTPS. C'è un articolo sulla Knowledge base di Microsoft http://support.microsoft.com/?kbid=839357

In sintesi:

Creare dentro la root del vostro sito una directory chiamata CustomErrors

Creare dentro alla directory CustomErrors un file chiamato Owahttps.asp contenente il seguente codice: <%

If Request.ServerVariables("HTTPS") = "off" Then Response.Redirect "https://" & Request.ServerVariables("HTTP_HOST") & "/Exchange" End If

%>

In IIS selezionare la directory CustomError e fare clic su Create Application e assicuratevi che l'applicazione faccia parte del pool ExchangeApplicationPool:

ustomErrors Properties			? ×
Directory Documents D	Pirectory Security HTTP Headers	Custom Errors	
The content for this re	source should come from:		
•	The <u>d</u> esignated directory		
0.	A share located on another compu	ter	
0.	A redirection to a <u>U</u> RL		
Local path:	CustomErrors		
Scrip <u>t</u> source accest	s Iog ⊻isits Index this re	esource	
Directory browsing			
Application settings			
Application name:	CustomErrors	Remove	
Starting point:	<default site="" web="">\Cust</default>	Configuration	n]
Execute permissions:	Scripts only	▼	
Application pool:	DefaultAppPool	▼ Unload	
	OK Cancel	Apply H	Help
	Fig.14		

•

0

Aggiungere *Owahttps.asp* nella lista dei *Default Documents* In *Directory Security* permettere l'accesso anonimo e disabilitare il flag *Require SSL* •

			or anonym	ous access:	-1
<u>U</u> ser name:	TIOSK_RE	VOLUTION		Browse	
Password:	•••••	••••			
Authenticated	access				
For the following	ig authentica	ation methods,	user name	e and passwor	d d
are required wi - anon	ien: ymous acces	s is disabled, or	r		
- acces	s is restricte	d using NTFS a	ccess con	trol lists	
🔲 Integrated	Wi <u>n</u> dows au	thentication			
🔲 Digest auth	entication fo	r Windows dom	nain serve	rs	
🔲 Ba <u>s</u> ic authe	ntication (pa	assword is sent	in clear te	ext)	
.NET Passp	ort au <u>t</u> hentio	tation			
Defeult dom	ainy			Soloct	
Deradic gom				Selection	
				S <u>e</u> lect	
<u>R</u> ealm;					
<u>R</u> ealm:	ок	Cancel	1	Help	

52

Secure Communications		×
Require secure channel (SSL)		
Require <u>1</u> 28-bit encryption		
Client certificates		
 Ignore client certificates 		
Accept client certificates		
C 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.	E <u>d</u> it]
OK Cancel	Help	

Fig.16



- Passiamo alla virtual directory di Exchange:
 - Exchange -> Custom Errors fare doppio clic sul 403.4 e immettere questi valori:
 - O Message Type: URL
 - URL: /CustomErrors/Owahttps.asp

Edit Custom Erro	or Properties 📃 🗡	1
Error code:	403 Sub Error Code: 4	
Dennicion:	Forbidden - SSL required	• X
Message type:		
<u>U</u> RL:	/CustomErrors/Owahttps.asp	
		2 ,•`
	OK Cancel <u>H</u> elp	
	Fig.17	_

In Directory Security verificare che il flag Require SSL sia selezionato (l'avevamo già fatto in precedenza).