

INSTALLARE E CONFIGURARE WINDOWS 2003 SERVER COME STAND-ALONE CERTIFICATION AUTHORITY

Certification Authorities (CAs) issue certificates for a number of different purposes. In the context of your ISA Server firewall/VPN server, a CA can provide a certificate that allows:

- L2TP/IPSec VPN connections from VPN clients VPN clients can establish L2TP/IPSec connections to the ISA Server firewall/VPN server. A machine certificate is required to create the IPSec encrypted tunnel.
- L2TP/IPSec VPN connections from VPN gateways (VPN routers) Remote VPN gateways can call the ISA Server firewall/VPN server and establish a gateway to gateway link. These VPN gateways act as VPN routers and allow packets to be routed between networks through a the VPN tunnel established between the VPN gateways.
- L2TP/IPSec VPN connections to VPN servers The ISA Server firewall/VPN server may need to establish a VPN client connection to a VPN server. For example, some Internet Service Providers require that machines establish a VPN connection with their VPN server in order to obtain a public address to connect to the Internet. In this case the ISA Server firewall/VPN server is a VPN client to the ISP's VPN server.
- L2TP/IPSec VPN connections to VPN gateways
 The ISA Server firewall/VPN server may need to call a VPN gateway to establish a VPN gateway to gateway
 link. Packets from networks behind each VPN gateway and be routed to a remote network behind the
 opposite gateway. The ISA Server firewall/VPN server is a VPN router using the Internet as its transit
 internetwork.
- Certificate-based user authentication using a certificate stored on the user machine Users can obtain certificates and use those certificates to authenticate with the VPN server. The user certificate is stored on the user's computer and a VPN connectoid can be configured to present this certificate during the PPP user authentication process.
- Certificate-based user authentication using a certificate stored on a Smart Card Users can obtain certificates and use the certificate to authenticate with the VPN server. The user certificate is stored on a Smart Card and the VPN connectoid can be configured to present this certificate during the PPP user authentication process.

A Microsoft Certificate Server can take on one of four roles:

- Enterprise Root CA
- Enterprise Subordinate CA
- Stand-alone Root CA
- Stand-alone Subordinate CA

A Microsoft Stand-alone CA has the following characteristics:

- The stand-alone CA does not require Active Directory. This makes the stand-alone CA the Certificate Authority of choice in environments where there is no Active Directory infrastructure
- The stand-alone CA knows nothing about the user or computer account requesting the certificate. You must
 manually and explicitly include all details required to obtain the type of certificate you require.
- The stand-alone CA isn't aware of the accounts in the Active Directory. If a user certificate is required, the user account must be in the local SAM of the stand-alone CA machine.
- The stand-alone CA does not immediately issue a certificate after the certificate request is made. By default, an administrator must approve the certificate request and then the client must retrieve the certificate after an administrator approves the request. The reason is the stand-alone CA does not check the validity of the user account.
- You cannot add or remove certificate templates to the stand-alone CA.
- The stand-alone CA can not issue user certificates that are stored on Smart Cards that allow the user to log on to a Windows Server 2003 domain
- The stand-alone CA's self-signed certificate is not automatically added to the requester's Trust Root Certification Authorities certificate store. You must add the CA certificate to the Root Store manually.
- The stand-alone CA can receive limited support from the Active Directory when it is installed by a domain administrator in an Active Directory domain. When the stand-alone CA is installed by a domain administrator, the CA certificate of the stand-alone CA will be added to the Trusted Root Certification Authorities certificate store for all domain users and computers.



We recommend that you install a stand-alone CA only when:

- You do not have an Active Directory domain, and/or
- You do not require automatic deployment of certificates to users and computers

If you have users who require certificates and those users are not members of your Active Directory domain, then use a stand-alone Certificate Server. These users can obtain certificates from the stand-alone CA's Web enrollment site. The Web enrollment site runs on Internet Information Server 6.0. You need to install IIS on the stand-alone CA computer before installing Certificate Services.

This ISA Server 2000 VPN Deployment Kit document describes the following procedures:

- Installing the Microsoft Internet Information Services World Wide Web service
- Install a Windows Server 2003 standalone Certification Authority

Installing Microsoft Internet Information Services World Wide Web Service

Perform the following steps to install IIS 6.0 on the Windows Server 2003 computer. The machine can be a standalone server, a member server in an Active Directory domain, or even a domain controller:

- 1. Click Start, point to Control Panel and click Add or Remove Programs.
- 2. Click the Add/Remove Windows Components button in the Add or Remove Programs window (figure 1).

🐻 Add or Rem	ove Programs		
5	Currently installed programs:	<u>S</u> ort by:	Name 🗾
C <u>h</u> ange or Remove Programs	⊕ ¥Mware Tools		Size <u>1.06MB</u> Used <u>rarely</u>
Add <u>N</u> ew Programs	To change this program or remove it from	Las n your computer, click Change/Remove.	t Used On 5/28/2003 Change/Remove
Add/Remove			
<u>w</u> indows Components			
🦺 Start 🛛 🕑	🥑 🔢 Add or Remove Programs		🍓 🗊 11:45 AM
		Fig.1	

3. On the Windows Components window, click on the Application Server entry and click the Details button (figure 2).



🔂 Add or Rem	ove Programs Windows Components Wizard	
Change or Remove Programs	Windows Components You can add or remove components of Windows.	
Add <u>N</u> ew Programs	To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components:	2003 ove
~	Accessories and Utilities 4.5 MB	
Add/Remove	✓ Catificate Services	
<u>_W</u> indows	E-mail Services	
Components	Eax Services 22.0 MB	
	Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.	
	Total disk space required: 3.6 MB Space available on disk: 1943.5 MB	
	< <u>B</u> ack <u>N</u> ext> Cancel Help	
🥑 Start 🛛 🕑	🥭 🔢 📆 Add or Remove Programs 🛛 📆 Windows Component 🦓	5:18 PM

4. On the Application Server page, click on the Internet Information Services (IIS) entry and click the Details button (figure 3).



😿 Add or Rem	ove Programs Windows Components Wizard	- <u>D×</u>
	Application Server	
Change or Remove Programs	To add or remove a component, click the check box. A shaded box means that only of the component will be installed. To see what's included in a component, click Det.	part <u>6MB</u> ails. 2003
	Application Server Console 0.0 MB	- hve
Add New	ASP.NET 0.0 MB	
Programs	🗹 🙆 Enable network COM+ access 0.0 MB	
-	🗆 🗇 🗊 Enable network DTC access 0.0 MB	
	🔲 🎇 Internet Information Services (IIS)	
Add/Remove <u>W</u> indows Components	 Message Queuing 6.5 MB Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP). 	rt I
	Total disk space required: 3.6 MB <u>D</u> etails.	
	OK Cance	
	< <u>Back</u> <u>N</u> ext> Cancel	Help
🦺 Start 🛛 🕑	Add or Remove Programs Windows Component Fig.3	🌯 🗊 5:18 РМ

5. In the Internet Information Service (IIS) dialog box, put a checkmark in the World Wide Web Service checkbox and click OK (figure 4).





🐻 Add or Remo	yve Programs	هل-	×
	Windows Components Wizard	×	
101	Application Server	l l l l l l l l l l l l l l l l l l l	
Change or Remove	Internet Information Services (IIS)	БМЕ	3
Programs Add New	To add or remove a component, click the check box. A shade of the component will be installed. To see what's included in a Sub <u>c</u> omponents of Internet Information Services (IIS):	ed box means that only part a component, click Details. 5.1 MB	
Programs	Internet Information Services Manager	1.3 MB	
	🗌 🎬 Internet Printing	0.0 MB	
	NNTP Service	1.2 MB	
Add/Remove	SMTP Service	1.3 MB	
<u>W</u> indows	🗹 🥥 World Wide Web Service	8.0 MB	
Components			
	Description: A core component of IIS that uses HTTP to ex Web clients on a TCP/IP network.	xchange information with	
	Total disk space required: 14.1 MB	Details	
	Space available on disk: 1943.5 MB		
	-	OK Cancel	
		IP I	
🛃 Start	🤿 🔰 🚮 Add or Remove Programs 🛛 🚮 Windows Co	omponent 😵 🔂 5:20 F	РМ
Start S	Fig.4	omponent	-



6. Click OK on the Application Server dialog box (figure 5).

Add or Rem	ve Programs	-, 🗆
	Windows Components Wizard	×
- 1	Application Server	
Change or Remove Programs	To add or remove a component, click the check box. A of the component will be installed. To see what's includ Subcomponents of Application Server:	A shaded box means that only part ded in a component, click Details.
	Application Server Console	0.0 MB
Add New	ASP.NET	0.0 MB
Programs	🗹 🙆 Enable network COM+ access	0.0 MB
-	🗆 💦 Enable network DTC access	0.0 MB
	Internet Information Services (IIS)	18.1 MB
d/Remove	🗌 🚅 Message Queuing	6.5 MB
mponents	Description: IIS Includes Web, FTP, SMTP, and NN for FrontPage Server Extensions and Ac	TP support, along with support ctive Server Pages (ASP).
	Total disk space required: 14.1 MB	Details
	Space available on disk: 1943.5 MB	
		OK Cancel
	< Back N	ext > Cancel Help

7. Click Next on the Windows Components dialog box (figure 6).



Add or Rem <u>ove</u>	Programs	-1012
🧠 I 💆	indows Components Wizard	×
Change or Remove Programs	Windows Components You can add or remove components of Windows.	
Add New	To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.	2003 pve
Frograms	Components:	-
~	Accessories and Utilities 4.5 MB	
	Application Server 24.6 MB	
.dd/Hemove Windows	L B Centificate Services 1.4 MB	
Components	E-mail Services 1.1 MB	1
	Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console. Total disk space required: 14.1 MB Space available on disk: 1943.5 MB	
	<u>K</u> ack <u>N</u> ext > Cancel H	elp
Start 🛛 🕑 🥭	Add or Remove Programs	🌯 🗐 🛛 5:22 PM

8. Click Finish on the Completing the Windows Components Wizard page (figure 7).

~



👸 Add or Rem	ove Programs	-lov
Change or Remove Programs	Windows Components Wizard Image: Completing the Windows Components Wizard Completing the Windows Components Wizard Ou have successfully completed the Windows Components Wizard. To close this wizard, click Finish.	6MB arely 2003 ove
	K Back Finish Help	
🏄 Start 🛛 🚱	Add or Remove Programs Windows Component Fig.7	5:26 PM

Installing Microsoft Certificate Services

Perform the following steps to install and configure a stand-alone CA on a Windows Server 2003 computer:

Note: We recommend that you install the stand-alone CA on a member server or domain controller on your internal network. This will allow the stand-alone CA's certificate to be placed automatically into the Trusted Root Certification Authorities certificate store for all users and computers.

- 1. At a member server or domain controller in your internal network, log on as a domain administrator. Click Start, point to Control Panel and click Add/Remove Programs.
- 2. In the Add or Remove Programs window (figure 8), click the Add/Remove Windows Components button.



🐻 Add or Ren	nove Programs		- 🗆 ×
5	Currently installed programs:	Sort by: Name	
C <u>h</u> ange or Remove Programs	働 VMware Tools	Size Used	<u>1.06MB</u> rarely
Add <u>N</u> ew	To change this program or remove it from your computer, click Change/R	Last Used On 57 lemove. Change/R	28/2003 lemove
Add/Remove <u>W</u> indows Components			
💋 Start 🛛 🕑	Add or Remove Programs Fig.8	*	11:00 AM

 In the Windows Components dialog box (figure 9), click on the Certificate Services entry and click the Details button.



🔂 Add or Remove Programs	- D ×
Windows Components Wizard	
Windows Components Change or You can add or remove components of Windows	
Programs	rarely
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Be Details.	8/2003 emove
Programs Components:	
Accessories and Utilities 4.5 MB	
Application Server 24.6 MB —	
Add/Removi 1.4 MB	
Components L E-mail Services 1.1 MB	
ILL @AFax Services 2211MB	
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.	
Total disk space required: 2.9 MB Details	
Space available on disk: 1942.7 MB	
A Back Newth Carroel Hele	
	11.02.444
Vindows Component	T1:03 AM

4. In the Certificate Services dialog box, put a checkmark in the Certificate Services CA checkbox (figure 3). A Microsoft Certificate Services dialog box appears and informs you that you can not change the machine name or the domain membership of the machine while it acts as a certificate server. Read the information in the dialog box and click Yes.



🐻 Add or Remove Progr	ams	
Windows Co	imponents Wizard	×
W W	a	
Remove		¹) <u>1.06МВ</u>
Programs To a	dd or remove a component, click the check box. A shaded box means that only part e component will be installed. To see what's included in a component, click Details	rarely
	e component nambo anticale. Po coo ministro monados an a component, enert porane.	28/2003
	Components of Certificate Services	Remove
Programs	Certificate Services Web Enrollment Support 1.2 MB	
A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
	crosoft Certificate Services	
Add/Removi	After installing Certificate Services, the machine name and domain	
	name to CA information stored in the Active Directory. Changing the	
r	machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine	
	name and domain membership are configured before installing Certificate Services . Do you want to continue?	
1		
5	<u>Yes</u> <u>N</u> o	
	UK Cancel	
	Kext Next Lancel Help	
A Chart 1	Add or Remove Programs	11-02 AM
- statt	Fig.10	9 🕑 11.03 AM

5. Both the Certificate Services CA and Certificate Services Web Enrollment Support checkboxes are checked (figure 11). Click OK in the Certificate Services dialog box.



🔂 Add or Remov	ve Programs	- O ×
Win 🔬	idows Components Wizard	
Change or	Certificate Services	▼ 1.06MB
Programs	To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Certificate Services:	<u>rarely</u> 28/2003
Add Now	Certificate Services CA 0.2 MB	Remove
Programs	Certificate Services Web Enrollment Support	
Add/Remov <u>W</u> indows Components	Description: Allows you to publish web pages on your server to submit requests and retrieve certificates from a CA. Total disk space required: 4.6 MB Space available on disk: 1942.7 MB	
	CAncel	
🎒 Start 🛛 🕑 🧃	Add or Remove Programs 🔂 Windows Component) 11:05 AM

6. Click Next in the Windows Components dialog box (figure 12).



👸 Add or Rei	move Programs	
× 1	Vindows Components Wizard	×
Change or Remove Programs	Windows Components You can add or remove components of Windows.	<u>1.06MB</u> rarely
Add <u>N</u> ew Programs	To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.	'28/2003 Remove
<i>i</i>	Components: 4.5 MB	
	Application Server 24.6 MB	
Add/Remov	🗹 🥵 Certificate Services	
Components	🗆 🛄 E-mail Services 1.1 MB	
	I @4Eax Services 22.0 MB	
	Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.	
	Total disk space required: 4.6 MB Details	
	Space available on disk: 1942.7 MB	
	< <u>B</u> ack <u>N</u> ext > Cancel Help	1
🛃 Start 🛛 📴	😥 🔢 🔂 Add or Remove Programs 🛛 🔂 Windows Component 🥞	🔁 11:07 AM
	Fig.12	

7. Select the Stand-alone root CA option on the CA Type page (figure 13). Click Next. -



🐻 Add or R	emove Programs	, LON
	Windows Components Wizard	
Change or Remove Programs	CA Type Select the type of CA you want to set up.	1.06MB
Add <u>N</u> ew Programs	 Enterprise root CA Enterprise subordinate CA Stand-alone root CA Stand-alone subordinate CA Description of CA type The most trusted CA in a CA hierarchy. 	'28/2003 Remove
Lomponents	Use custom settings to generate the key pair and CA certificate < Back Next> Cancel Help	
A Charl	🗿 🚳 🔰 🔂 Add ar Barrana Reagana 🖉 Miradawa Camanana 🖉 🕅	30 11-09 AM
Jatan J	Fig.13	J 11.00 AM

8. On the CA Identifying Information page (figure 14), type in a Common name for this CA. The common name of the CA is typically the DNS host name or NetBIOS name (computer name) of the machine running Certificate Services. In this example, the name of the machine is WIN2003DC, so we will enter WIN2003DC in the Common name for this CA text box. The default Validity Period of the CA's self-signed certificate is 5 years. Accept this default value unless you have a reason to change it. Click Next.



🐻 Add or Re	move Programs	
	Windows Components Wizard	×
Change or Remove Programs	CA Identifying Information Enter information to identify this CA.	1.06MB rarely
1	Common name for this CA:	28/2003
	WIN2003DC	Remove
Add <u>N</u> ew Programs	Distinguished name suffix:	
1	DC=internal,DC=net	
<u> </u>		
Add/Removi Windows	Preview of distinguished name:	
Components	CN=WIN2003DC,DC=internal,DC=net	
	Validity period: Expiration date:	
	5 Years - 6/13/2008 11:10 AM	
	< <u>B</u> ack <u>Next</u> > Cancel H	elp
🏄 Start 🛛 🕝	👌 🥶 🛛 📆 Add or Remove Programs 🛛 📆 Windows Component	🍓 🗊 11:10 AM
	Fig.14	

9. On the Certificate Database Settings page (figure 15), use the default locations for the Certificate Database and Certificate Database Log. You do not need to specify a shared folder to store configuration information because this information will be stored in the Active Directory. Click Next.

Ð



🐻 Add or Ren	nove Programs	, LOX			
· · · · ·	/indows Components Wizard	×			
Change or Remove Programs	Certificate Database Settings Enter locations for the certificate database, database log, and configuration information.				
1	<u>C</u> ertificate database:	28/2003			
Add New	C:\WINDOWS\system32\CertLog Browse	Remove			
Programs	Certificate database log:				
F	C:\WINDOWS\system32\CertLog Browse				
Add/Removi Windows Components	Store configuration information in a shared folder Shared folder: Browse Preserve existing certificate database				
_	<u> < B</u> ack <u>N</u> ext > Cancel <u>Help</u>				
🎒 Start 🛛 🚱	Add or Remove Pr Windows Comp Windows Comp Fig.15	🍓 🗐 11:15 АМ			

10. Click Yes on the Microsoft Certificate Services dialog box (figure 16) informing you that Internet Information Services must be stopped temporarily.





👸 Add or Rei	nove Programs	
×	/indows Components Wizard	×
Change or Remove Programs	Certificate Database Settings Enter locations for the certificate database, database log, and configuration information.	I.06MB rarely
	<u>C</u> ertificate database:	28/2003
A del Naur	C:\WINDOWS\system32\CertLog Browse	Remove
Programs	Certificate database log:	
1	C: Microsoft Certificate Services	
Add/Removi Windows Components	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now? Yes Yes	
-	Cancel Help	_
		-
💋 Start 🛛 🎯	Add or Remove Pr Windows Comp W Help and Support) 🗐 11:17 AM

11. Click Yes on the Microsoft Certificate Services dialog box (figure 17) informing you that Active Server Pages must be enabled on IIS if you wish to use the Certificate Services Web enrollment site.





🐻 Add or Re	move Programs	
Change or Remove Programs	Configuring Components Setup is making the configuration changes you requested.	<u>I.06MB</u> rarely
Add <u>N</u> ew	Please wait while Setup configures the components. This may take several minutes, depending on the components selected.	'28/2003 Remove
Add/Remove <u>W</u> indows Components	Microsoft Certificate Services Image: Services (ASPs) must be enabled in Internet Information Services (IIS) in order to allow Certificate Services to provide web enrollment services. Enabling ASPs is a potential security risk and must be carefully evaluated. You can enable ASPs later if you choose not to do it now. IIS must be manually reconfigured later to enable this functionality. Do you want to enable Active Server Pages now? Yes No	
	< <u>B</u> ack <u>N</u> ext > Help	
🎒 Start 🛛 🕝	Add or Remove Pr 🔂 Windows Comp 🎯 Help and Support 🗞	11:27 AM

12. Click Finish on the Completing the Windows Components Wizard page (figure 18).

(O)
$\langle \rho \rangle$



🐻 Add or Remove Programs		, <u>-</u> □×
Windows Components Wizard Change or Remove Programs Add New Programs Add New Add/Remove	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	▼ <u>1.06MB</u> <u>rarely</u> '28/2003 Remove
Windows Components	To close this wizard, click Finish.	
	K Back Finish Help	
🛃 Start 🛛 🞯 🥔 👘 🔂 Add or Remov	e Pr 🚮 Windows Comp 🕐 Help and Support 🛛 🌺 🗄 Fig.18) 11:30 AM

13. Close the Add or Remove Programs window.

The standalone Certificate Server is now ready to accept certificate requests.

Approving Certificate Requests to a Standalone Certificate Authority

The stand-alone CA does not automatically issue a certificate when a certificate request is made. The reason is the standalone CA is not able to confirm the validity of the request. It does not check the information provided by the requestor against a directory, such as the enterprise CA does when validating credentials against the Active Directory.

You should keep this default behavior for your published standalone CA in order to prevent users on the Internet from obtaining certificates without your review. Perform the following steps to approve a certificate request:

1. Click Start and point to Administrative Tools. Click on the Certification Authority link (figure 19).



		Active Directory Domains and Trusts
Administrator		📓 Active Directory Sites and Services
Manage Your Server	My Computer	 Active Directory Users and Computers Certification Authority Cluster Administrator Component Services
Windows Explorer	Administrative Tools	Computer Management Configure Your Server Wizard Data Server (ODDC)
Notepad	Printers and Faxes O	Data Sources (UDBC) Distributed File System A DNS
Certification Authority	Search	 Domain Controller Security Policy Domain Security Policy Event Viewer
	(/ <u>H</u> un	Internet Information Services (IIS) Manager
		Manage Your Server Microsoft .NET Framework 1.1 Configuration Microsoft .NET Framework 1.1 Wizards
All <u>P</u> rograms 🕨	-	 Network Load Balancing Manager Network Monitor
Start 🛛 🕑 🥭 🚽 🔤 Co	💋 Log Off 🔟 Shut Down	 Performance Remote Desktops

2. In the Certification Authority console (figure 20), expand the server name and then click on the Pending Certificates node. You see a list of pending certificate requests in the right pane of the console. You can see who requested the certificate by scrolling to the right and looking under the Requester Name column (not shown). Right click on the certificate request in the right pane of the console, point to All Tasks and click Issue. The certificate request is removed from the Pending Requests node.



Eile Action View Help ← → € ●				
Certification Authority (Local)	Request ID 2 3 4	Binary Request	Request Status The operation of The operation of The operation of Tasks Image: status efresh elp Den	Code Request Disposition Me omple Taken Under Submissic omple Taken Under Submissic omple Taken Under Submissic v Attributes/Extensions ort Bigary Data e y
Contains operations that can be performe	d on the object. and Prompt	Certifica	tion Authority	💌 🕹 🗐 3:19 PM

3. Click on the Issued Certificates node in the left pane of the Certification Authority console. The certificate request you approved appears in the right pane of the console. This indicates the certificate request was approved. It does not indicate the machine issuing the request has returned to the Web enrollment site to retrieve the certificate (figure 21).



📴 Certification Authority				_ _ _ ×
<u>File Action ⊻iew H</u> elp				
← → 🗈 🖬 😰 🛱 😤				
Ertification Authority (Local)	Request ID	Requester Name	Binary Certificate	Certificate Ter
E Cert	8 4	INTERNAL\IUSR_WIN2003DC	BEGIN CERTI.	
Revoked Certificates				
	•			F
	1998 - 19)		
💆 Start 🗍 🞯 🥪 🔤 🔤 Comman	d Prompt	Certification Authorit	y 📑	🍐 🗐 3:21 PM
		Fig.21		