# **Configuring a Windows 2003 Server for IAS**

When setting up a Windows 2003 server to function as an IAS server for our demo environment we will need the server to serve several functions. First of all we will configure the server to be a Domain Controller so that we can use Active Directory to define users and/or machines. Next we will configure the server to act as a Certificate Authority for providing certificate services for our demo environment. In order for the certificate services to operate fully, we will also need to enable IIS to all web access for certificate requests. Finally we need to enable IAS to allow the server to function as a Radius server.

The following tasks should be done in the order shown.

- 1. Configure the Server as a Domain Controller
- 2. Enable IIS on the Server
- 3. Configure the Server as a Certificate Authority
- 4. Download the CA Certificate
- 5. Enable and configure IAS

The remainder of this document will show the step by step process required to complete each of these tasks. It is assumed that we will be starting from a freshly installed Windows 2003 Server.

### Configure the Server as a Domain Controller

When a newly installed 2003 server is first logged into, the following window will be opened. This Manage Your Server window will allow you to change the role that your server plays on the network. In order to configure the server to be a Domain Controller we need to start the process by selecting the Add or remove a role option in this window.



The configuration wizard will now start and ask you to verify that preliminary steps have been completed. Hit "Next" to continue.

Configure Your Server Wizard	×
<b>Preliminary Steps</b> You can ensure that you successfully configure your server by completing the following steps before continuing.	No.
Before continuing, verify that the following steps have been completed.	
<ul> <li>Install all modems and network cards.</li> </ul>	
Attach all necessary cables.	
<ul> <li>If you plan to use this server for Internet connectivity, connect to the Internet now.</li> </ul>	
<ul> <li>Turn on all peripherals, such as printers and external drives.</li> </ul>	
Have your Windows Server 2003 Setup CD available, or know your network installation path.	
When you click Next, the wizard will search for network connections.	
< <u>B</u> ack. Cancel	Help

The wizard will then provide a list of server roles that can be configured. As shown below, select "Domain Controller" from the list and hit the "Next" Button.

Server Role You can set up this server to perform one role to this server, you can run this wizard Select a role. If the role has not been adde	or more specific role I again. ed, vou can add it, I	s. If you want to add more than one
remove it. If the role you want to add or n Server Role File server Print server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DNS server	emove is not listed, o <u>Configured</u> No No No No No No No No No No	Domain Controller (Active Directory) Domain controllers store directory data and manage user logon processes and directory searches. Read about domain controllers
Streaming media server WINS server	NU No No < Back	Next > Cancel Help

The Wizard will ask you to confirm your selection. Press "Next" to confirm and continue.

igure Your Server Wizard	×
Summary of Selections View and confirm the options you have selected.	<b>N</b>
<u>S</u> ummary:	
Run the Active Directory Installation Wizard to set up this server as a domain controller	
To change your selections, click Back. To continue setting up this role, click Next.	
< Back Next > Cancel	Help

The Active Directory Installation Wizard will now start. Select "Next" to continue.



A warning window will now be displayed. Press "Next" to continue.

Active Directory Installation Wizard	×
Operating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.	Ş
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.	
<ul> <li>The following older versions of Windows cannot meet the new requirements:</li> <li>Windows 95</li> <li>Windows NT 4.0 SP3 or earlier</li> </ul>	
By default, computers running those versions of Windows will not be able to log on with a domain controller running Windows Server 2003 or access domain resources.	
For more information, see <u>Compatibility Help</u> .	
< <u>B</u> ack <u>Next</u> > Cancel	

You will now be asked to specify a Domain Controller Type. Here we will want to select the Domain controller for a new domain radio button, and select "Next" to continue.

Active Directory Installation Wizard
Domain Controller Type Specify the role you want this server to have.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?
Domain controller for a new domain
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.
C Additional domain controller for an existing domain
Proceeding with this option will delete all local accounts on this server.
All cryptographic keys will be deleted and should be exported before continuing.
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
< <u>B</u> ack <u>N</u> ext > Cancel

Next select the "Domain in new forest" radio button, and select "Next" to continue.

Active Directory Installation Wizard
Create New Domain Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
C Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
O Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< <u>B</u> ack <u>N</u> ext > Cancel

At this point you will be asked for the DNS name of the new domain to be created. Enter the desired domain name and select "Next" to continue.

Active Directory Installation Wizard	×
New Domain Name Specify a name for the new domain.	
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).	
Eull DNS name for new domain:	
arubawest.com	
,	
< <u>B</u> ack <u>N</u> ext>	Cancel

Next you will be shown the NetBIOS name that will be used for this domain. Select "Next" to continue.

Active Directory Installation Wizard	×
NetBIOS Domain Name Specify a NetBIOS name for the new domain.	<b>X</b>
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.	
Domain NetBIOS name: ARUBAWEST	
< <u>B</u> ack <u>N</u> ext > Ca	ancel

Now you will be given the option to change the location of the Active Directory database and directory. Just keep the defaults and select "Next" to continue.

Active Directory Installation Wizard
Database and Log Folders Specify the folders to contain the Active Directory database and log files.
For best performance and recoverability, store the database and the log on separate hard disks.
Where do you want to store the Active Directory database?
Database folder:
C:\WINDOWS\NTDS Browse
Where do you want to store the Active Directory log?
Log folder:
C:\WINDOWS\NTDS Browse
< <u>B</u> ack <u>N</u> ext > Cancel

Now you can change the location of the Shared System Volume. Select "Next" to continue.

Active Directory Installation Wizard
Shared System Volume Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse
< <u>B</u> ack <u>N</u> ext > Cancel

At this point the wizard will give you the option of installing DNS on this server. If you ever want to add a computer to this domain, it will be necessary for that computer to have access to the DNS for this domain. Since this is a fictious domain, it works best if this server also acts as the DNS server. Select "Install and configure the DNS server" as show below and select "Next" to continue.

2
Ì

You will be asked if you need to support any pre-Windows 2000 operating systems will need to be supported. Select "Next" to continue.

Active Directory Installation Wizard	×
Permissions Select default permissions for user and group objects.	×
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.	
Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.	
<ul> <li>Anonymous users can read information on this domain.</li> <li>Permissions compatible only with Windows 2000 or Windows Server 2003</li> </ul>	
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.	
< <u>B</u> ack <u>N</u> ext > Can	cel

You will now be prompted for a Restore Mode Password. Enter and confirm the password and select "Next" to continue.

Active Directory Installation Wizard					
Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.					
Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.					
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.					
Restore Mode Password:					
Confirm password:					
For more information about Directory Services Restore Mode, see <u>Active Directory Help</u> .					
< <u>B</u> ack <u>N</u> ext > Cancel					

You will now be given an opportunity to review your config options before they are applied. Press "Next" to continue or "Back" if something needs to be changed.

Active Directory Installation Wizard	×
Summary Review and confirm the options you selected.	<b>X</b>
You chose to: Configure this server as the first domain controller in a new forest of domain trees. The new domain name is arubawest.com. This is also the name of the new forest. The NetBIOS name of the domain is ARUBAWEST Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.	•
To change an option, click Back. To begin the operation, click Next.	
< <u>B</u> ack <u>N</u> ext >	Cancel

At this point the Active Directory Installation Wizard will install and configure AD based on all of your previous selections. This could take several minutes to complete.

Active Directory Installation Wizard		
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.		
Starting		
Cancel		

When the Wizard finished the following window will be displayed. Select "Finish" to continue.



You are now finished with the Active Directory configuration, and your server is now a Domain Controller. Select "Finish" to continue.

Configure Your Server Wizard					
	This Server is Now a Domain Controller				
	You have successfully set up this server as a domain controller. To add or remove another role, run the Configure Your Server Wizard again. <u>View the next steps for this role</u>				
	For a record of your changes, see the <u>Configure Your Server log</u> . To close this wizard, click Finish.				
	< Back Finish Cancel Help				

At this point you must restart the system. Select "Restart Now" and the server will reboot.



#### **Enable IIS on the Server**

As Discussed before you will need to enable IIS so that Certificate Services are available via the web once we configure the server to be a Certificate Authority. This should be done before Configuring the CA so that all CA components are installed properly. This install will start by adding another role for your server using the window below. Select "Add or remove role" to start adding the IIS features.



Now select "Application server(IIS, ASP.NET)" and select "Next" to continue.

Configure Your Server Wizard		×
Server Role You can set up this server to perform one role to this server, you can run this wizar Select a role. If the role has not been add remove it. If the role you want to add or r	or more specific rol d again. ed, you can add it.	es. If you want to add more than one
Server Role File server Print server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DHCP server Streaming media server WINS server	Configured No No No No No No Yes Yes No No No No	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 <u>Configure Your Server log</u> .
p	< <u>B</u> ack	Next > Cancel Help

You will then be asked if you want to install any other tools on the server. You don't need any of these, so just select "Next" to continue.

Configure Your Server Wizard
Application Server Options IIS, COM+, ASP.NET, and Microsoft .NET Framework are installed automatically for this role.
Select the additional tools that you want to install on this server.
FrontPage Server Extensions are a set of Web server extensions that you can use to publish content with FrontPage, Visual Studio, and Web Folders.
Enable ASP.NET
ASP.NET is a powerful programming framework for building Web-based applications and services that can target any browser or device.
< <u>B</u> ack <u>N</u> ext > Cancel Help

You will now have an opportunity to review your selections. Select "Next" to continue.

Configure Your Server Wizard	×
Summary of Selections View and confirm the options you have selected.	<b>K</b>
Summary:	
Install Internet Information Services (IIS) Enable COM+ for remote transactions Enable Microsoft Distributed Transaction Coordinator (DTC) for remote access Install FrontPage Server Extensions	
To change your selections, click Back. To continue setting up this role, click Next.	
< <u>B</u> ack <u>Next</u> > Cancel	Help

IIS will now be installed.

Configure Your Server Wizard				×
Applying Selections The Configure Your Server Wizard is adding	the selected role	e to this server.		No.
Installing and configuring IIS				
	< <u>B</u> ack	<u>N</u> ext >	Cancel	Help

The wizard will change as IIS continues to be installed.

Windows Components Wizard	×
<b>Configuring Components</b> Setup is making the configuration changes you requested.	đ
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.	
Status: Configuring WMI	
< <u>B</u> ack <u>N</u> ext >	

When IIS is finished installing you will see the window below.



## Configure the Server as a Certificate Authority

You can now configure the server to be a Certificate Authority. Start the process by selecting Start> Control Panel> Add or Remove Programs as shown below.



Select "Windows Components" and a list of windows components will be displayed. Now check the box next to "Certificate Services" and select "Next".

Windows Components Wizard	×
Windows Components You can add or remove components of Windows.	t
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included in Details.	box means that only in a component, click
<u>C</u> omponents:	
Accessories and Utilities	4.5 MB 🔺
🗹 🦪 Application Server	24.6 MB 💻
🗹 🙀 Certificate Services	1.4 MB
🔲 🛄 E-mail Services	1.1 MB
	22.0 MB 🗾
Description: Installs a certification authority (CA) to issue certific public key security programs.	cates for use with
Total disk space required: 4.6 MB	Details
Space available on disk: 2775.4 MB	
< <u>B</u> ack <u>N</u> ext >	Cancel Help

You will see the following message. Press "Yes" to continue.

Microsof	t Certificate Services	×
1	After installing Certificate Services, the machine name and domain membership may not be changed binding of the machine name to CA information stored in the Active Directory. Changing the machin membership would invalidate the certificates issued from the CA. Please ensure the proper machin domain membership are configured before installing Certificate Services. Do you want to continue?	d due to the ne name or domain e name and ,
	<u>[ Yes</u> ] <u>N</u> o	

Now select the "Enterprise root CA" radio button, and select "Next" to continue.

Windows Components Wizard	×
<b>CA Type</b> Select the type of CA you want to set up.	đ
<ul> <li>Enterprise root CA</li> <li>Enterprise subordinate CA</li> <li>Stand-alone root CA</li> <li>Stand-alone subordinate CA</li> <li>Stand-alone subordinate CA</li> <li>Description of CA type</li> <li>The most trusted CA in an enterprise. Should be installed before any other CA.</li> </ul>	
□ Use custom settings to generate the key pair and CA certificate < Back Next > Cancel H	

At this point you will ask for the Common Name for the CA. The CN "ArubawestCSVR" was used in the example below. Select "Next" to continue.

Windows Components Wizard		×
CA Identifying Information Enter information to identify	this CA.	B
Common name for this CA: ArubawestCSVR		_
Distinguished name suffix:		
Preview of distinguished name:		
CN=ArubawestCSVR,DC=arub	awest,DC=com	-
Validity period: 5 Years ▼	Expiration date: 4/6/2010 10:39 AM	
	< Back Next > Cancel	Help

You will now be given an opportunity to change the location of the database and log files. Just select "Next" to continue.

Windows Components Wizard	×		
Certificate Database Settings Enter locations for the certificate database, database log, and configuration information.			
<u>C</u> ertificate database:			
C:\WINDOWS\system32\CertLog	Br <u>o</u> wse		
Certificate <u>d</u> atabase log:			
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se		
Store configuration information in a shared folder Shared folder:			
	Browse		
Preserve <u>e</u> xisting certificate database			
<u> &lt; B</u> ack <u>N</u> ext > Cance	I Help		

You will get a warning that IIS will need to be stopped. Select "Yes" to continue.

Microsoft	rosoft Certificate Services 🔀			
1	To complete the installation, Certificate Services must temporarily stop the Internet Information Services. Do you want to stop the service now?			
	<u>Y</u> es <u>N</u> o			

You will get a message stating that Active Server Pages needs to be enabled. Select "Yes" to continue.

Microsoft	t Certificate Services	1
1	Active Server Pages (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?	

At this point the wizard is finished, and the server will now function as a CA.



### **Download the CA Certificate**

At this point you will need to Download the CA Certificate to make this server a trusted CA on this local machine. To do this you need to open a web browser and browse to the IP of this server and to the /certsrv page. In my case I needed to browse to <u>http://192.168.1.206/certsrv/</u>. Internet explorer may show the following warning. Select "OK" to continue.

Internet	Explorer	×
⚠	Microsoft Internet Explorer's Enhanced Security Configuration is currently enabled on your server. This enhanced level of security reduces the risk of attack from Web-based content that is not secure, but it may also prevent Web sites from displaying correctly and restrict access to network resources.	
	In the future, do not show this message	
<u>Learn m</u>	ore about Internet Explorer's Enhanced Security Configuration OK	ן

At this point you may prompted with a login screen. You can use the administrator account and password.

Connect to 192.168	.1.206
	G A
Connecting to 192.16	68.1.206
<u>U</u> ser name:	🕵 RUBAWEST\administrator 💌 🗾
Password:	•••••
	Remember my password
	OK Cancel

At this point you should see the web page as shown below. Select the link "Download a CA certificate, certificate chain, or CRL.



Now you will see the following page. Select the link "Install this CA certificate chain".

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	<u>_</u>	
<u>File Edit View Favorites Tools Help</u>		2
🕓 Back 👻 🕥 👻 😰 🐔 🔎 Search 👷 Favorites 🔌 Media  🖉	) • 🚴 🖻	
Address 🗃 http://192.168.1.206/certsrv/certcarc.asp	🔽 🔁 Go 🛛 Lin	ks »
<i>Microsoft</i> Certificate Services ArubawestCSVR	Home	
Download a CA Certificate, Certificate Chain, or CRL		-
To trust certificates issued from this certification authority, in	stall this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, sele	ect the certificate and encoding method.	
CA certificate:		
Encoding method:		
© DER © Base 64		
Download CA certificate		
Download CA certificate chain		
Download latest base CRL Download latest delta CRL		
		-
😂 Install this CA certificate chain	🖉 Trusted sites	1

You will be prompted asking if you want to add the certificate. Select "Yes" to continue.

Potentia	Scripting Violation
♪	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	Yes []

You may also see the following message. Select "Yes" to continue.

Internet Explorer	×
When you send information to the Trusted sites, it might be possible for others to see that information. Do you want to continue?	
In the future, do not show this message.	
<u>Y</u> es <u>N</u> o	

Windows Components Wizard	×
Windows Components You can add or remove components of Windows.	<b>E</b>
To add or remove a component, click the checkbox. A shaded by part of the component will be installed. To see what's included in Details. Components:	ox means that only a component, click
Internet Explorer Enhanced Security Configuration	0.0 MB
Management and Monitoring Tools	61 MB
An anagement and mentioning reas	2.6 MB
Band Print Services	0.0 MB
Bemote Installation Services	20MB
Description: Contains a variety of specialized, network-related se	rvices and protocols.
Total disk space required: 2.9 MB Space available on disk: 2748.7 MB	<u>D</u> etails
< <u>B</u> ack <u>N</u> ext> C	Cancel Help
< <u>B</u> ack <u>N</u> ext > C letworking Services	Cancel Help
< Back       Next >       C         Intervention       C       C       C	Cancel Help X Ins that only part nt, click Details.
<u>A Back</u> <u>Next</u> C           Itetworking Services           To add or remove a component, click the check box. A shaded box mea of the component will be installed. To see what's included in a componer           Subcomponents of Networking Services:	Cancel Help
< Back       Next >       C         Networking Services       C         To add or remove a component, click the check box. A shaded box mea of the component will be installed. To see what's included in a componer       Subgomponents of Networking Services:         Subgomponents of Networking Services:       Image: Component System (DNS)         Image: Domain Name System (DNS)       Image: Component System (DNS)	Cancel Help
< Back Next > C Active remove a component, click the check box. A shaded box mea of the component will be installed. To see what's included in a component Subgomponents of Networking Services: Subgomponents of Networking Services: ✓ Domain Name System (DNS) Dynamic Host Configuration Protocol (DHCP)	Cancel Help
< Back Next > C Actworking Services To add or remove a component, click the check box. A shaded box mea of the component will be installed. To see what's included in a componer Subcomponents of Networking Services: Subcomponents of Networking Services: ✓ Domain Name System (DNS) Dynamic Host Configuration Protocol (DHCP) ✓ Internet Authentication Service PDC aver HILLE Representation	Cancel Help  The second
< Back Next > C Actworking Services To add or remove a component, click the check box. A shaded box mea of the component will be installed. To see what's included in a componer Subgomponents of Networking Services: Subgomponents of Networking Services: Image: Subgomponent of Networking Services: Image: State of Networking Services: Image: State of Networking Services: Image: State of Networking Services Image:	Cancel Help Ins that only part Int, click Details. I.6 MB O.0 MB O.0 MB O.0 MB O.0 MB
< Back       Next >       C         Networking Services       C         To add or remove a component, click the check box. A shaded box mean of the component will be installed. To see what's included in a component Subcomponents of Networking Services:       Subcomponents of Networking Services:         Subcomponents of Networking Services:       Image: Domain Name System (DNS)       Image: Domain Host Configuration Protocol (DHCP)         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service       Image: Dynamic Host Configuration Service         Image: Dynamic Host Configuration Service       Image: Dynamic Host Confi	Cancel Help Help Ins that only part ht, click Details. 1.6 MB ▲ 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.0 MB
< Back	Cancel Help Help Ins that only part ht, click Details. 1.6 MB ▲ 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.0 MB 0.9 MB
< Back       Next >       C         detworking Services         To add or remove a component, click the check box. A shaded box mean of the component will be installed. To see what's included in a component Subcomponents of Networking Services:         Subcomponents of Networking Services:         Image: Domain Name System (DNS)         Dynamic Host Configuration Protocol (DHCP)         Image: Description:         Enables authentication, authorization and accounting of dusers. IAS supports the RADIUS protocol.	Ancel Help
< Back       Next >       C         Retworking Services         To add or remove a component, click the check box. A shaded box means of the component will be installed. To see what's included in a component Subgomponents of Networking Services:         Subgomponents of Networking Services:         Image: Domain Name System (DNS)         Domain Name System (DNS)         Dynamic Host Configuration Protocol (DHCP)         Image: Internet Authentication Service         Image: RPC over HTTP Proxy         Image: Simple TCP/IP Services         Image: TAS supports the RADIUS protocol.         Total disk space required:       2.9 MB	Ancel Help

ΟK

I

Cancel

### **Enable and configure IAS**

Now we are ready to install and configure IAS. Start the process by bring us the windows component wizard just as we did earlier for installing Certificate Services. Here you need to click on the "Networking Services" line to view all of the available services. Check the box next to "Internet Authentication Service" and select "Next" to continue.

dows components wizard	
Windows Components	
rou can add or remove components or windows.	Ľ
To add or remove a component, click the checkbox. A shaded part of the component will be installed. To see what's included Details.	I box means that only in a component, click
Components:	
🗹 🥶 Internet Explorer Enhanced Security Configuration	0.0 MB 🔺
🗆 🗄 Management and Monitoring Tools	6.1 MB
🗹 🚉 Networking Services	2.6 MB 💛
🔲 불 Other Network File and Print Services	0.0 MB
🗖 💻 Bernote Installation Services	2 0 MB 🔟
Description: Contains a variety of specialized, network-related	services and protocols.
Total disk space required: 2.9 MB	Detaile
Space available on disk: 2769.6 MB	
	end la ma

The wizard will complete and you should see the following message.

Windows Components Wizard		X
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
-0	To close this wizard, click Finish.	
	< Back	Help

You can now configure IAS by going to Start>Administrative Tools>Internet Authentication Service> .

		_			
	🙀 upgrade.rtf - WordPad	ø	Active Directory Domains and Trusts		<u>–</u>
	Hie Edit View Insert Format He	5	Active Directory Sites and Services		_
		1	Active Directory Users and Computers		
			Certification Authority		
Administrator		5	Cluster Administrator		-
$\sim$	-	<b>9</b>	Computer Management		
Manage Your Server	😏 My Computer		Configure Your Server Wizard		-
Ě	The Control Devel	, a	Data Sources (ODBC)		
CAL Command Prompt		Ŀ	Distributed File System		
<u> </u>	🍿 Administrative Tools 🔹 🕨	2	DNS		
		6	Domain Controller Security Policy		
[ <b>????</b> ]		6	Domain Security Policy		
Notepad	Help and Support	4	Event Viewer		
		2	Internet Authentication Service		
🧾 wordPad	→ Search		Manages authentication, authorization, auditing	g, and	
Metwork Load Balancing	777 <u>R</u> un		<sup>L1</sup> accounting for VPN, dial-up, 802.1× wireless or m switch connection attempts that are compatible	ethernet with the IETF	
Manager			RADIUS protocol.		
			Microsoft .NET Framework 1.1 Wizards	I - In I	
		6	Microsoft SharePoint Administrator	.ep	
		1	Network Load Balancing Manager		
		阂	Performance		
		Ø	Remote Desktops		
All Duramana A		<u>_</u>	Routing and Remote Access		
All Programs 🕨		- 10-	Services		🔏 Recycle Bin
	🔎 Log Off 🛛 O Shut Down	1 🔂	Terminal Services Configuration		
🕂 Start 🛛 🚱 🛋 🖉 🗐 📖	porade.rtf - WordPad	- 72. 142	Terminal Services Manager		🦥 🧞 11:01 AM
1 - State 1 - State 1 - State -	pgraasina morarda	-		J	S THOT MIN

Here you will be presented with the IAS setup GUI.

We will need to setup a Radius Client (The Aruba Controller) and a Remote Access Policy to be applied when users are authenticating.

🎾 Internet Authentication Service	
<u>File Action View H</u> elp	
<ul> <li>Internet Authentication Service (Local)</li> <li>RADIUS Clients</li> <li>Remote Access Logging</li> <li>Remote Access Policies</li> <li>Connection Request Processing</li> </ul>	Welcome to Internet Authentication           Service           Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).           To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.           For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

To add a radius client right click on the "Radius Client" folder and select New>Radius client.



You will now see a menu allowing you to assign a Friendly Name, and IP address for the client. Select "Next" to continue.

New RADIUS Client	×
Name and Address	
Type a friendly name and either an IP Address	or DNS name for the client.
Eriendly name: ArubaCon	troller
Client address (IP or DNS):	
192.168.1.235	⊻erify
	< <u>B</u> ack <u>N</u> ext > Cancel

Next you will be asked to select a Client-Vendor, and to define a shared secret. Use RADIUS Standard, and any shared secret you wish. Select "Finish" and the client is now created.

New RADIUS Client	×
Additional Information	
If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.	
<u>C</u> lient-Vendor:	
RADIUS Standard	
Shared secret:	
Confirm shared secret:	
Request must contain the Message Authenticator attribute	
< <u>B</u> ack Finish Cance	

Next we need to create a Remote Access Policy. Again, right click on the Remote Access Policy line, and select New>Remote Access Policy.

Pinternet Authentication Service		_O×
Eile Action View Help		
Internet Authentication Service (Local)	Name	Order
Remote Access Logging	Connections to Microsoft Routing and Remote	1 2
Remote Access Policy	<b>[</b>	
<u>N</u> ew ▶ Re	emote Access <u>P</u> olicy	
⊻iew ►		
Refresh		
Export List		
Help		· ·
New Pamote Access Policy	]	
IN A RELIDUE ALLESS POILY	J	

Now the Remote Access Policy Wizard will start, Select "Next" to continue.

New Remote Access Policy Wizard		
	Welcome to the New Remote Access Policy Wizard This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server. To continue, click Next.	
	< <u>₿</u> ack [ <u>N</u> ext>] Canc	el

First you need to give the policy a name, and select "Next" to continue

New Remote Acces	ss Policy Wizard	×
<b>Policy Configu</b> The wizard c	ration Method an create a typical policy, or you can create a custom policy.	Ø
How do you w	vant to set up this policy?	
co <u>o</u> se me	e wizard to set up a typical policy for a common scenario	
© <u>S</u> et up a	a custom policy	
Type a name tł	hat describes this policy.	
Policy name:	Aruba Users	
	Example: Authenticate all VPN connections.	
	< <u>B</u> ack <u>N</u> ext> Can	cel

Next select "Wireless" as the access method, and select "Next" to continue.

New Remote Access Policy Wizard
Access Method Policy conditions are based on the method used to gain access to the network.
Calest the method of second for which you want to grapte a policy
Select the method of access for which you want to create a policy.
O VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
O <u>D</u> ial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
Wireless
Use for wireless LAN connections only.
C Ethernet
Use for Ethernet connections, such as connections that use a switch.
< <u>B</u> ack <u>N</u> ext > Cancel

Now you will be asked if you want to grant access by individual user or by groups. In the example below, User is chosen. Select "Next" to continue.

New Remote Access Policy Wizard	×
User or Group Access You can grant access to individual users, or you can grant access to select groups.	ed 💡
Grant access based on the following:	A <u>d</u> d <u>R</u> emove
< <u>B</u> ack <u>N</u> ext >	Cancel

Now you will be asked what EAP type to use. IAS only supports PEAP and EAP-TLS. In this example PEAP is selected. Select "Next" to continue.

New Remote Access Policy Wizard
Authentication Methods EAP uses different types of security devices to authenticate users.
Select the EAP type for this policy.
Protected EAP (PEAP)
< <u>B</u> ack <u>N</u> ext > Cancel

The following window will be displayed. Select "Finish".

New Remote Access Policy Wizard		
8	Completing the New Remote Access Policy Wizard	
	You have successfully completed the New Remote Access Policy Wizard. You created the following policy:	
	Aruba Users	
	Conditions: NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"	
	Authentication: EAP(Protected EAP (PEAP))	
	Encryption: Basic, Strong, Strongest, No encryption	
	To close this wizard, click Finish.	
	< <u>B</u> ack [Finish] Cancel	

### The new policy will be added

Aruba Users Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"
A <u>d</u> d <u>E</u> dit <u>R</u> emove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit <u>P</u> rofile
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions: De <u>n</u> y remote access permission
O Grant remote access permission
OK Cancel Apply

Edit Dial-in Profile	<u>?</u> ×	
Dial-in Constraints IP Multilink		
Authentication Encryption Advanced		
Select the authentication methods you want to allow for this connection		
EAP Methods		
Microsoft Encrypted Authentication version 2 (MS-CHAP v2)		
User can <u>c</u> hange password after it has expired		
Microsoft Encrypted Authentication (MS-CHAP)		
Uger can change password after it has expired		
Encrypted authentication (CHAP)		
Unencrypted authentication (PAP, SPAP)		
Unauthenticated access	7	
Allow clients to connect without negotiating an authentication method.		
	-	
	]	
	NY	
Select EAP Providers		<u>? ×</u>
EAP types are negotiated in the order in which they are listed.		
EA <u>P</u> types:		
Protected EAP (PEAP)	M	ove <u>U</u> p
	Mo	ve <u>D</u> own
Add <u>E</u> dit <u>R</u> emove OK		Cancel
	_	

Dial-in Se	ttings	×
♪	You selected one or more authentication methods. To ensure that each protocol is correctly configured for th remote access, policy, and domain levels, follow the step-by-step procedures in Help. View the corresponding Help topic?	ie
	<u>Y</u> es <u>N</u> o	

🤣 Internet Authentical	tion Service				ſ	_ []]
Eile <u>A</u> ction <u>V</u> iew <u>H</u> e	elp					
⇐ ⇒ 🗈 🖬 🗙	🗗 🖳 🔮 🔺 🤊	+				
Internet Authentication	Service (Local)	Nam	e		0	
RADIUS Clients		S AI	ruba	Users	1	
E Remote Access Log	ging	S.C.	onne	ections to Microsoft Routing and Remote	2	
	cies t Processing	<b>_</b> \$0	onne	ections to other access servers	3	
	c i rocossing		ana.			
			≈Ę. ~3.	Active Directory Domains and Trusts		
			Active Directory Sites and Services			
			<u> </u>	Active Directory Users and Computers		
			i 🔛	Certification Authority		w abiast
Administrator			in l	the Active Directory.		
	Mu Commenter		ē.	Computer Management		
Manage Your Server	S My Computer		3	Configure Your Server Wizard		
-	Control Dapal		<b>B</b>	Data Sources (ODBC)		
C:\ Command Prompt			Ŀ.	Distributed File System		
<b>6</b>	🏹 Administrative To	ools 🔸	2	DNS		
Windows Explorer			6	Domain Controller Security Policy		
	Printers and Fax	es	6	Domain Security Policy		
Notepad	<u></u>		9	Event Viewer		
	Help and Suppor	t	٠	Internet Authentication Service		
📝 WordPad	Search		6	Internet Information Services (IIS) Manage	er	
	<i>~</i>		۲.	Licensing		
Network Load Balancing Manager	7 <u>R</u> un			Manage Your Server		
			<u>a</u>	Microsoft .NET Framework 1.1 Configuratio	n	
			<u>7</u> 2	Microsoft .NET Framework 1.1 Wizards		
			<b>e</b>	Microsoft SharePoint Administrator		
			1	Network Load Balancing Manager		
			1	Performance		
			С	Remote Desktops		
			ġ	Routing and Remote Access		
All <u>P</u> rograms			Ф.	Services		
		S church	Þ	Terminal Server Licensing		
		Shut Down	Ā	Terminal Services Configuration		
🍠 Start 🛛 🞯 🥭 🔢 🕎 upgr	ade.rtf - WordPad (	🤣 Internet	ł	Terminal Services Manager		

<i> </i> Active Directory Users and Comp	uters			
G Eile Action View Window Help				
Active Directory Users and Computers	Active Directory Use	ers and Computers [g	greg-lvn7gvvuxw.arubawest.	.com] 2 objects
E Saved Queries	Name	Туре	Description	
Property arubawest.com     Prove Builtin     Computers     Onders     Prove Domain Controllers     Prove Domain Controllers     Prove Domain Controllers     DescurityPrincipals     Users	Saved Queries	Domain	Folder to store your favor.	
	<u> </u>			

Image: Second Secon	live Directory Users and Comp	uters			
← →       ▲	G Eile Action View Window Help				
Active Directory Users and Computer:       Users 21 objects         Saved Queries       Name       Type         Description       Image: Computer Structure         Administrator       User       Built-in account for admini	⇔ → 🗈 🖬 🐰 💼 🗙 😭	1 🗟 🗟 👔	1 📅 👛 🖓 🍕	1	
Saved Queries     Name     Type     Description       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved Queries       Image: Saved Queries     Image: Saved Queries     Image: Saved Queries     Image: Saved	Active Directory Users and Computers	Users 21 objects			
Administrator User Built-in account for admini	E → E Saved Queries	Name	Туре	Description	
		2 Administrator	User	Built-in account for admini	
Computers Security Group Members of this group are		Cert Publishers	Security Group	Members of this group are	
Domain Controllers	🕀 🧭 Domain Controllers		Security Group	DNS Administrators Group	
Emergen Security Principals	⊕ □ ForeignSecurityPrincipals	Domain Admins	Security Group	Designated administrators	
Domain Comp Security Group All workstations and serve		Domain Comp	Security Group	All workstations and serve	
Domain Contr Security Group All domain controllers in th		Domain Contr	Security Group	All domain controllers in th	
Domain Guests Security Group All domain guests		💯 Domain Guests	Security Group	All domain guests	
Domain Users Security Group All domain users		Domain Users	Security Group	All domain users	
Enterprise Ad Security Group Designated administrators		Enterprise Ad	Security Group	Designated administrators	
Group Policy Security Group Members in this group can			Security Group	Puilt in account for quart	
Weinser Oser Builden account for guest			Security Group	Group for the Help and Su	
IIS WPG Security Group IIS Worker Process Group		TIS WPG	Security Group	IIS Worker Process Group	
IUSR_GREG-L User Built-in account for anony		IUSR_GREG-L	User	Built-in account for anony	
😰 IWAM_GREG User Built-in account for Intern		🖸 IWAM_GREG	User	Built-in account for Intern	
OWS_171398 Security Group Microsoft SharePoint role '		20W5_171398	Security Group	Microsoft SharePoint role '	
RAS and IAS Security Group Servers in this group can		STRAS and IAS	Security Group	Servers in this group can	
Schema Admins Security Group Designated administrators		Schema Admins	Security Group	Designated administrators	
SUPPORT_38 User This is a vendor's account		SUPPORT_38	User Security Crown	This is a vendor's account	
Martenecclience Security Group Members or this group ha			security Group	members or this group ha	
		1			

New Object - User			×
Create in: arubawest	.com/Users		
Password:	••••		
User must change password at	t next logon		
<ul> <li>User cannot change password</li> <li>Password never expires</li> </ul>			
Account is disabled			
	< <u>B</u> ack	<u>N</u> ext >	Cancel
New Object - User			×
Create in: arubawest	.com/Users		
When you click Finish, the followin	g object will be c	reated:	
Full name: Greg Pifer			<u> </u>
User logon name: gpifer@arubawa	est.com		

< <u>B</u>ack

Finish

-

Cancel

The password never expires.

🍜 Active Directory Users and Comp	outers			
🎻 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> e	elp			
⇔ →   🗈 💽   🐰 💼   🗙 🖆	' 🕅 🖪   😰   🦉	? 😼 🛍 💎 🍕	6	
ntive Directory Users and Computers	Users 22 objects			
🗄 🧰 Saved Queries	Name	Туре	Description	
🖃 📵 arubawest.com	🖸 Administrator	User	Built-in account for admini	
E Computers	🕵 Cert Publishers	Security Group	Members of this group are	
	DnsAdmins	Security Group	DNS Administrators Group	
	🕵 DnsUpdatePr	Security Group	DNS clients who are permi	
	💯 Domain Admins	Security Group	Designated administrators	
	Domain Comp	Security Group	All workstations and serve	
	Domain Contr	Security Group	All domain controllers in th	
	💯 Domain Guests	Security Group	All domain guests	
	💯 Domain Users	Security Group	All domain users	
	Enterprise Ad	Security Group	Designated administrators	
	🕵 Greg Pifer	User		
	Group Policy	Security Group	Members in this group can	
	Guest	User	Built-in account for guest	
	HelpServices	Security Group	Group for the Help and Su	
	WPG	Security Group	IIS Worker Process Group	
	IUSR_GREG-L	User	Built-in account for anony	
	IWAM_GREG	User	Built-in account for Intern	
	WS_171398	Security Group	Microsoft SharePoint role '	
	RAS and IAS	Security Group	Servers in this group can	
	Schema Admins	Security Group	Designated administrators	
	SUPPORT_38	User	This is a vendor's account	
	TelnetClients	Security Group	Members of this group ha	

Greg Pifer Properties
Remote control         Terminal Services Profile         COM+           General         Address         Account         Profile         Telephones         Organization           Member Of         Dial-in         Environment         Sessions
Remote Access Permission (Dial-in or VPN)   Allow access  Deny access
C Control access through Remote Access <u>Policy</u> ☐ ⊻erify Caller-ID:
Callback Options  No Callback  Set by Caller (Routing and Remote Access Service only)  Always Callback to:
Assign a Static IP Address
Define routes to enable for this Dial-in Static Routes
OK Cancel Apply