Installing a Domain Controller

This is the second document in a series of 3. First use the document Lab Setup, then this Domain Controller document, and finally the WEP Enterprise document.

In order to setup Windows based RADIUS, the following steps have to be done:

- 1. Install a Domain Controller and DNS
- 2. Install IIS and CA as the Enterprise Root CA
- 3. Install IAS and setup user accounts.

Each of these steps will be broken down in finer detail. The system will be configured to use WPA Enterprise V1 + AES

1. Install a Domain Controller and DNS.

1.1. Setup the NetBIOS name

To avoid any assumptions, we begin with setting the Computer Name (NetBIOS).

- 1. Right click on My Computer
- 2. Choose Properties,
- 3. On System Properties, click on the Computer Name tab. (See below figure)



4. Click Change

Computer Name Changes	5				? X
You can change the name computer. Changes may aff	and the ect acc	members ess to nel	hip ol work	this resour	ces.
Computer name:					
radius					
Full computer name:					
radius.					
					- 1
				More	a
Member of					
C Domain:					_
• Workgroup:					
WORKGROUP			_		_
J					
		ОК	1	Can	sel

- 5. Type in the NetBIOS name (this will become part of the fully qualified domain name)
- 6. Click OK, then OK, then OK, then Yes and allow for a restart.

- 1.2. Installing a Domain Controller.
 - 1. Click the Start Button
 - 2. Click Programs
 - 3. Click Administrative Tools
 - 4. Click Configure Your Server Wizard

The Configure Your Server Wizard displays.



5. Click the Next button



- 6. Choose Domain Controller
- 7. Click Next, then Next

The Active Directory Installation Wizard displays.



8. Click Next

The Domain Controller Type window displays.



9. Click Next

The Create New Domain window displays.



10. Click Next

The New Domain Name window displays.

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:	
bringsjoy.com	
< <u>B</u> ack <u>N</u> ext >	Cancel

- 11. Enter the domain name as shown above (bringsjoy.com)
- 12. Click Next, then Next, then Next

The DNS Registration Diagnostics window displays.

Active Directory Installation Wizard
DNS Registration Diagnostics Verify DNS support, or install DNS on this computer.
Diagnostic Failed Image: Comparison of the problem later by configuring DNS manually. (Advanced) Image: Diagnostic Failed Image: Comparison of the problem later by configuring DNS manually. (Advanced)
< <u>B</u> ack <u>N</u> ext > Cancel

- 13. Choose the second radio button
- 14. Click Next

The Permissions window displays.

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. Anonymous users can read information on this domain.				
 Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems 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 > Cancel				

- 15. Choose the second radio button and click Next.
- 16. Either enter PASSWORDx2, or leave it blank
- 17. Click Next, then Next, and wait 4 hours.
- 1.3. DNS Setup follows.



1. Click Ok

上 Local Area Connection Properties	<u>?</u> ×
General Authentication Advanced	
Connect using:	
Wware Accelerated AMD PCNet Ad Configure	
, This connection uses the following items:	
Client for Microsoft Networks Genetic Content of Microsoft Networks Genetic Content of Microsoft Networks File and Printer Sharing for Microsoft Networks File Content Protocol (TCP/IP)	
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
Sho <u>w</u> icon in notification area when connected Notify <u>m</u> e when this connection has limited or no connectivity	y
OK Can	cel

The Local Area Connection Properties window displays.

- 2. Choose Internet Protocol (TCP/IP)
- 3. Place a check mark on [Show icon in...]
- 4. Click on the Properties button

The Local Area Connection Properties window displays.

Internet Protocol (TCP/IP) Propertie	5	<u>? ×</u>
General		
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network support ask your network administrator	:s ,
O Obtain an IP address automatical	ly	
• Use the following IP address:		
IP address:	172 . 16 . 1 . 10	
S <u>u</u> bnet mask:	255.255.0.0	
Default gateway:	172 . 16 . 1 . 1	
C Obtain DNS server address autor	natically	
Use the following DNS server add	resses:	
Preferred DNS server:		
<u>A</u> lternate DNS server:		
	Ad <u>v</u> anced.	
	OK Can	cel

- 5. Fill the information as shown above [
 - IP address:172.16.1.10/16
 - Subnet mask 255.255.0.0
 - Default Gateway: 172.16.1.1
- 6. Click OK and OK Remember that we are setting up also a DNS server
- 7. Click the Close button
 - DNS registration will start as part of the DC setup
 - DO NOT CLICK on skip DNS installation
- 8. Choose Finish, then Restart Now
- 9. Once restarted click on the Finish button.

2. CA and IIS

Although it is possible to add the CA server and IIS services at the same time, the steps that follow will do it separately. I have noticed that when installed at the same time, a small popup error message comes up in regards to the CA.

2.1. Installing IIS

IIS is used as one channel to send a certificate to the wireless client.

- 1. Click the Start Button
- 2. Click Control Panel
- 3. Click Add or Remove Programs

The Local Area Connection Properties window displays.



- 4. Choose Add/Remove Windows Components in the Quick Task bar
- 5. Choose Application Server
- 6. Choose Internet Information Services
- 7. Choose World Wide Web Service See the screen capture on the next page.

🐞 Add or Remove Programs		
Windows Components Wizard		x
Application Server	×	
Internet Information Services (IIS)	x	(\mathbf{a})
World Wide Web Service	×	
To add or remove a component, click the check box. A shaded box mear of the component will be installed. To see what's included in a component Subcomponents of World Wide Web Service:	ns that only part t, click Details.	
🔲 🕒 Internet Data Connector	0.0 MB	
Remote Administration (HTML)	5.7 MB	
🗌 🔤 Remote Desktop Web Connection	0.4 MB	
🔲 🔊 Server Side Includes	0.0 MB	
🔲 🔊 WebDAV Publishing	0.0 MB	
🗹 🔮 World Wide Web Service	1.9 MB	
	•	
Description: A core component of IIS that uses HTTP to exchange info Web clients on a TCP/IP network.	rmation with	
Total disk space required: 15.1 MB	Details	
Space available on disk: 6547.1 MB	2-7-1	L
. ОК	Cancel	P

8. Click OK, then OK, then OK then Next, then Finish.

2.2. Certificate of Authority setup

- 1. Click the Start Button
- 2. Click Control Panel
- 3. Go to Add or Remove Programs
- 4. Choose Add/Remove Windows Components in the Quick Task bar
- 5. Choose Certificate Services and click Yes in response to the popup window.

The CA Identifying Information window displays.

Windows Components Wizard	×
CA Identifying Information Enter information to identify this (CA.
Common name for this CA:	
paquetin	
<u>D</u> istinguished name suffix:	
DC=bringsjoy,DC=com	
Preview of distinguished name:	
CN=paquetin,DC=bringsjoy,DC=corr	1
⊻alidity period: 5 Years ▼	Expiration date: 6/17/2011 10:27 PM
<	Back Next > Cancel Help

- 6. Enter "paquetin" in the Common name for this CA box, as shown above.
- 7. Click Next, then Next, then Yes, then Yes to the ASP popup window then click Finish.

To see if the CA issued a certificate, there are two choices:

- 8. Quick Way
 - Click Start
 - Click Control Panel
 - Click Administrative tools
 - Choose Certificate Authority Jump to the last picture in this section.
- 9. Long Way
 - Opening the Certificates (local computer) snap-in.
 This is the long way of doing it, but this procedure paves the way for other maintenance options if needed later on

To a open a Console window

- 10. Click Start
- 11. Click Run

The Run window displays



- 12. Enter mmc in the Open: box as shown above
- 13. Click OK

The Console window displays

🚡 Console1		- 🗆 ×
File Action View Fav	orites <u>W</u> indow <u>H</u> elp	
Console Root		
Console Root	Name There are no items to show in this view.	

14. From the File menu click Add/Remove Snap-in ...

The Add/Remove Snap-in window displays/

Add/Remove Snap-in	<u>?</u> ×
Standalone Extensions	
Use this page to add or remove a standalone Snap-in from the console.	
Snap-ins added to:	
	- 1
Description	
Add <u>R</u> emove <u>About</u>	
ОК Са	ancel

15. Click Add

16. From the list choose Certification Authority then click Add.

The Certification Authority window displays/

Certification Authority	×
Select the computer you want this snap-in to manage. This snap-in will always manage: • Local computer: (the computer this console is running on) • Another computer: • Another computer: • Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.]
< <u>B</u> ack Finish Cance	el

17. Click Finish, then Close, then OK

🚡 Console1 - [Console Root\Certificatio	n Authority (Lo	ocal)\paquetin\Issu	ed Certificates]	
📸 Eile Action View Favorites Windo	ow <u>H</u> elp			_ & ×
📄 Console Root	Request ID	Requester Name	Binary Certificate	Certificate Template
🖻 🚋 Certification Authority (Local)	2	BRINGSJOY\RAD	BEGIN CERTI	Domain Controller (
🖻 😨 paquetin				
Revoked Certificates				
Issued Certificates				
Pending Requests				
Failed Requests				
Certificate Templates				
	1			F
1				
				J

If for some reason, you do not see a certificate, please reboot the machine before continuing

3. Setup IAS to configure RADIUS

- 1. Click Start
- 2. Click Control Panel
- 3. Click Add or Remove Programs
- 4. Choose Add/Remove Windows Components in the Quick Task bar
- 5. Open details for Networking Services

The Networking Services window displays.

Networking Services	X
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	ns that only part nt, click Details.
Sub <u>c</u> omponents of Networking Services:	
🗹 畏 Domain Name System (DNS)	1.7 MB 🔺
Dynamic Host Configuration Protocol (DHCP)	0.0 MB
🗹 畏 Internet Authentication Service	0.0 MB
🗆 🚐 Remote Access Quarantine Service	0.1 MB
BPC over HTTP Proxy	0.0 MB
Element Simple TCP/IP Services	0.0 MB 🚽
🗆 🚐 Windows Internet Name Service (WINS)	0.9 MB 💌
Description: Enables authentication, authorization and accounting of d users. IAS supports the RADIUS protocol.	ial-up and VPN
Total disk space required: 5.1 MB	Details
Space available on disk: 5908.3 MB	E south the
ОК	Cancel

- 6. Choose Internet Authentication Service
- 7. Click OK, then Next, t hen Next]
- 3.1. Setup the RADIUS client

This is accomplished in the IAS MMC, which can be opened on a default installation by

- 1. Clicking Start
- 2. Clicking Programs
- 3. Clicking Administrative Tools
- 4. Clicking Internet Authentication Service.

The Internet Authentication Service window displays



5. Right click on RADIUS Clients and select 'New RADIUS Client'

The New RADIUS Client window displays

New RADIUS Client		X
Name and Address		
Type a friendly name and either a	n IP Address or DNS name for the client.	
Eriendly name:	WIFI AP	_
Client address (IP or DNS):		
172.16.1.0/24	⊻erify	
,		_
	< <u>B</u> ack <u>N</u> ext ≻ C	ancel

6. Enter Friendly name and IP address (or range) of access point and click Next This is where you can allow for a group of AP's to be managed under 1 RADIUS server. With the above configuration of 172.16.1.0/24, we can add several AP's as needed and they will connect to the RADIUS server as long the AP's are on the same network/subnet. The Additional Information window displays

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

- 7. Select 'RADIUS Standard'(Default) from the Client-Vendor: drop-down list
- 8. Enter your pre-shared key in both the Shared secret: box and Confirm shared secret: boxes.

In our scenario it is "qaz123". This key should be as long as possible for production purposes, a random character generator is recommended.

9. Check Request must contain the Message Authenticator attribute.

3.2. Configure logging

- 1. Highlight Remote Access Logging on the IAS tree in the left pane.
- 2. Double click Local File in the right pane



The Local File Properties window displays.

Local File Properties	×
Settings Log File	_
Log the following information:	
Accounting requests (for example, accounting start or stop)	
Authentication requests (for example, access-accept or access-reject)	
Periodic status (for example, interim accounting requests)	
OK Cancel Apply	

 Select all 3 check boxes: Accounting requests, Authentication requests, and Periodic status for full logging to log files. To find these logs, you can use the Windows Search utility specifying for "IN*.LOG". These logs are very useful in the process of troubleshooting.

3.3. Setup a Remote Access Policy

- 1. Right click on Remote Access Policies
- 2. Select 'New Remote Access Policy'

The New Remote Access Policy Wizard displays.

New Remote Access Policy Wizard		
	Welcome to the New Remote Access Policy Wizard	
	< <u>B</u> ack <u>Next</u> > Cance	

3. Click Next

The Policy Configuration Method window displays.

New Remote Access	Policy Wizard 🔀
Policy Configural The wizard can	tion Method In create a typical policy, or you can create a custom policy.
How do you war	nt to set up this policy?
	vizard to set up a typical policy for a common scenario
◯ <u>S</u> et up a c	custom policy
Type a name tha	t describes this policy.
Policy name:	Wireless
E	Example: Authenticate all VPN connections.
	Z Back Next Cancel

- 4. Select Use the wizard to set up a typical policy for a common scenario
- 5. Enter a Policy name In our scenario it is Wireless
- 6. Click Next

The Access Method window displays.

New Remote Access Policy Wizard	×
Access Method Policy conditions are based on the method used to gain access to the network.	Ŷ
Select the method of access for which you want to create a policy.	
○ 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.	
Use for dial-up connections that use a traditional phone line or an Integrated Serv Digital Network (ISDN) line.	rices
 Wireless Use for wireless LAN connections only. 	
○ <u>E</u> thernet	
Use for Ethernet connections, such as connections that use a switch.	
< <u>B</u> ack <u>N</u> ext > Ca	ncel

- 7. Select Wireless
- 8. Click Next

The User or Group Access Method window displays.

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

- 9. Select User to gran level access For simplicity sake, we are using the user option, but for management, it is best to create group policies
- 10. Click Next.

The User or Group Access Method window displays.

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

- 11. Select Protected EAP (PEAP) from the drop-down list. It should appear as the default value.
- 12. Click Configure ...

The User or Group Access Method window displays.

Protected EAP Properties	5	? ×
This server identifies itself (Select the certificate that y	to callers before the connection is comple ou want it to use as proof of identity.	ted.
Certificate issued	radius.bringsjoy.com	•
Friendly name:		
Issuer:	paquetin	
Expiration date:	6/17/2007 10:26:40 PM	
🔽 Enable Fast Reconnect		
E <u>a</u> p Types		
Secured password (EAP-M	SCHAP v2)	Move <u>U</u> p
		Move <u>D</u> own
<u>A</u> dd <u>E</u> dit	<u>R</u> emove OK	Cancel

- 13. Ensure the correct Certificate issue option is selected.
- 14. Select the Enable Fast Reconnect check box
- 15. Optionally, you may
 - Select the EAP Type "Secured password (EAP-MSCHAPv2)"
 - Click Edit, and
 - Adjust options as desired.
- 16. When done, click OK, then Finish

Later on, if needed you can configure scheduled hours or days of the week in which connections are allowed or denied.

3.4. Configure user accounts

The final step required on the server is to configure a user account to be used with the RADIUS account. This can be an existing AD account, or you can add a group to be used exclusively for wireless access authentication.

- 1. Click Start
- 2. Click Programs
- 3. Click Administrative Tools
- 4. Click Active Directory Users and Computers

The Active Directory Users and Computers window displays.

🐗 Active Directory Users an	nd Computers			
🎻 Eile <u>A</u> ction <u>V</u> iew <u>W</u> ind	dow <u>H</u> elp			_ 8 ×
← → 🗈 💽 🐰 🛍	X 🗗 🛃 🗟	😫 🦉 💯 🕍	7 🍕 🙍	
Active Directory Users and •	Users 21 objects			
E Gaved Queries	Name	Туре	Description	
🖻 🎒 bringsjoy.com	🙎 Administrator	User	Built-in account for admini	
	🕵 Cert Publishers	Security Group	Members of this group are	
	GERTSVC_D	Security Group		
	💯 DnsAdmins	Security Group	DNS Administrators Group	
	🕵 DnsUpdatePr	Security Group	DNS clients who are permi	
	💯 Domain Admins	Security Group	Designated administrators	
	🕵 Domain Com	Security Group	All workstations and serve	
	🕵 Domain Cont	Security Group	All domain controllers in th	-

- 5. Select the domain to be used for the wireless users.
- 6. Right click on the User folder
- 7. Select New
- 8. Select User.

The New Object – User window displays.

New Object - User		x
Create in:	bringsjoy.com/Users	
<u>F</u> irst name:	laptop <u>I</u> nitials:	
Last name:		
Full n <u>a</u> me:	laptop	
<u>U</u> ser logon name:		
laptop	@bringsjoy.com	
User logon name (pre	- <u>W</u> indows 2000):	
BRINGSJOY	laptop	
	< <u>B</u> ack <u>N</u> ext > Cancel	

- 9. Enter the user information as shown above.
- 10. Click Next.

- 11. Enter "!qwerty1" in both the Password: and Confirm password: boxes It has to be VERY secure so we are using text and number
- 12. Deselect the checkbox User must change password at next logon
- 13. Select the checkboxes User cannot change password and Password never expires
- 14. Click Next.

New Object - User	×
Create in: bringsjoy.com/Users	
Password:	
 User must change password at next logon User cannot change password Reserved pever expires 	
Account is disabled	
< <u>B</u> ac	k <u>N</u> ext > Cancel

The confirmation window displays.

New Object - User	×
Create in: bringsjoy.com/Users	
When you click Finish, the following object will be created:	
Full name: laptop	
User logon name: laptop@bringsjoy.com	
The user cannot change the password. The password never expires.	
	T
,	
< <u>B</u> ack [Finish]	Cancel

15. Click Finish.

- 16. Right click on the new user
- 17. Select Properties

The laptop Properties window displays

aptop Properties	<u>?</u> ×	
Account Profile Telephones Organizat	ion Member Of Dial-in E	
Remote Access Permission (Dial-in or VPN)		
Allow access		
C Deny access		
C Control access through Remote Access Policy		
Callback Options	<u> </u>	
• No <u>C</u> allback		
C Set by Caller (Routing and Remote Access Service only)		
C Always Callback to:		
Assign a Static IP Address		
Apply Static Boutes		
Define routes to enable for this Dial-in connection.	Static Roytes	
Start 📗 🞯 🥶 📗 🥫 Domain Contr	roller 🧹 Active Director	

- 18. Select the Dial-in tab
- 19. Select Allow access.

We are done with the server side configuration.