Configuring Wireless Internet Security Remote Access

This Appendix describes how to configure and add wireless remote access points (APs) as RADIUS clients of the Microsoft 2003 and Vista Internet Authentication Service (IAS) servers.

ADDING THE ACCESS POINTS AS RADIUS CLIENTS TO IAS

You must add wireless remote APs as RADIUS clients to IAS before they are allowed to use RADIUS authentication and accounting services. The wireless remote APs at a given location will typically be configured to use an IAS server at the same location for their primary RADIUS server and another IAS server at the same or a different location as the secondary RADIUS server. The terms "primary" and "secondary" here do not refer to any hierarchical relationship, or difference in configuration, between the IAS servers themselves. The terms are relevant only to the wireless remote APs, each of which has a designated primary and secondary (or backup) RADIUS server. Before you configure your wireless remote APs, you must decide which IAS server will be the primary and which will be the secondary RADIUS server for each wireless remote AP[1].

The following procedures describe adding RADIUS clients to two IAS servers. During the first procedure, a RADIUS secret is generated for the wireless remote AP; this secret, or key, will be used by IAS and the AP to authenticate each other. The details of this client along with its secret are logged to a file. This file is used in the second procedure to import the client into the second IAS[1].

Tip: You must not use this first procedure to add the same client to two IAS servers. If you do this, the client entries on each server will have a different RADIUS secret configured and the wireless remote AP will not be able to authenticate to both servers.

1. "Securing Wireless LANs with PEAP and Passwords, Chapter 5: Building the Wireless LAN Security Infrastructure," © 2008 Microsoft Corporation. All rights reserved. Microsoft Corporation, One Mcrosoft Way, Redmond, WA 98052-6399, 2007.

ADDING ACCESS POINTS TO THE FIRST IAS SERVER

This part of the appendix describes the adding of wireless remote APs to the first IAS server. A script is supplied to automate the generation of a strong, random RADIUS secret (password) and add the client to IAS. The script also creates a file (defaults to Clients.txt) that logs the details of each wireless remote AP added. This file records the name, IP address, and RADIUS secret generated for each wireless remote AP. These will be required when configuring the second IAS server and wireless remote APs[1].

Tip: The RADIUS clients are added to IAS as "RADIUS Standard" clients. Although this is appropriate for most wireless remote APs, some APs may require that you configure vendor–specific attributes (VSA) on the IAS server. You can configure VSAs either by selecting a specific vendor device in the properties of the RADIUS clients in the Internet Authentication Service MMC or (if the device is not listed) by specifying the VSAs in the IAS remote access policy.

SCRIPTING THE ADDITION OF ACCESS POINTS TO IAS SERVER (ALTERNATIVE PROCEDURE)

If you do not want to add the wireless remote APs to the IAS server interactively using the previous procedure, you can just generate the RADIUS client entries output files for each wireless remote AP without adding them to IAS. You can then import the RADIUS client entries into both the first IAS server and the second IAS server. Because you can script this whole operation, you may prefer to add your RADIUS clients this way if you have to add a large number of wireless remote APs[1].

Tip: This procedure is an alternative method for adding RADIUS clients in a scripted rather than an interactive fashion.

CONFIGURING THE WIRELESS ACCESS POINTS

Having added RADIUS clients entries for the wireless remote APs to IAS, you now need to configure the wireless remote APs themselves. You must add the IP addresses of the IAS servers and the RADIUS client secrets that each AP will use to communicate securely with the IAS servers. Every wireless remote AP will be configured with a primary and secondary (or backup) IAS server. You should perform the procedures for the wireless remote APs at every site in your enterprise[1].

The procedure for configuring wireless remote APs varies depending on the make and model of the device. However, wireless remote AP vendors normally provide detailed instructions for configuring their devices. Depending on the vendor, these instructions may also be available online[1].

Prior to configuring the security settings for your wireless remote APs, you must configure the basic wireless network settings. These will include but are not limited to:

- IP Address and subnet mask of the wireless remote AP
- Default gateway
- Friendly name of the wireless remote AP
- Wireless Network Name (SSID)[1]

The preceding list will include a number of other parameters that affect the deployment of multiple wireless remote APs: settings that control the correct radio coverage across your site, for example, 802.11 Radio Channel, Transmission Rate, and Transmission Power, and so forth. Discussion of these parameters is outside the scope of this appendix. Use the vendor documentation as a reference when configuring these settings or consult a wireless network services supplier[1].

The guidance in this appendix assumes that you have set these items correctly and are able to connect to the wireless remote AP from a WLAN client using an unauthenticated connection. You should test this before configuring the authentication and security parameters listed later in this appendix[1].

TABLE eH.1 Wireless Access Point Configuration

Item	Setting
Authentication Parameters	
Authentication Mode	802.1 X Authentication
Re-authentication	Enable
Rapid/Dynamic Re-keying	Enable
Key Refresh Time-out	60 minutes
Encryption Parameters (these settings usually relate to static WEP encryption)	(Encryption parameters may be disabled or be overridden when rapid re-keying is enabled)
Enable Encryption	Enable
Deny Unencrypted	Enable
RADIUS Authentication	
Enable RADIUS Authentication	Enable
Primary RADIUS Authentication Server	Primary IAS IP Address
Primary RADIUS Server Port	1812 (default)
Secondary RADIUS Authentication Server	Secondary IAS IP Address
Secondary RADIUS Server Port	1812 (default)
RADIUS Authentication Shared Secret	XXXXXX (replace with generated secret)
Retry Limit	5
Retry Timeout	5 seconds
RADIUS Accounting	
Enable RADIUS Accounting	Enable
Primary RADIUS Accounting Server	Primary IAS IP Address
Primary RADIUS Server Port	1813 (default)
Secondary RADIUS Accounting Server	Secondary IAS IP Address
Secondary RADIUS Server Port	1813 (default)
RADIUS Accounting Shared Secret	XXXXXX (replace with generated secret)
Retry Limit	5
Retry Timeout	5 seconds

ENABLING SECURE WLAN AUTHENTICATION ON ACCESS POINTS

You must configure each wireless remote AP with a primary and a secondary RADIUS server. The wireless remote AP will normally use the primary server for all authentication requests, and switch over to the secondary server if the primary server is unavailable. It is important that you plan the allocation of wireless remote APs and carefully decide which server should be made primary and which should be made secondary. To summarize:

In a site with two (or more) IAS servers, balance your wireless remote APs across the available servers so that approximately half of the wireless remote APs use server

TABLE eH.2 Wireless Access Point Security Configuration

Item	Recommended Setting	Notes
General		
Administrator Password	xxxxxx	Set to complex password.
Other Management Passwords	xxxxxx	Some devices use multiple management passwords to help protect access using different management protocols; ensure that all are changed from the defaults to secure values.
Management Protocols		
Serial Console	Enable	If no encrypted protocols are available, this is the most secure method of configuring wireless remote APs although this requires physical serial cable connections between the wireless remote APs and terminal and hence cannot be used remotely.
Telnet	Disable	All Telnet transmissions are in plaintext, so passwords and RADIUS client secrets will be visible on the network. If the Telnet traffic can be secured using Internet Protocol security (IPsec) or SSH, you can safely enable and use it.
HTTP	Disable	HTTP management is usually in plaintext and suffers from the same weaknesses as unencrypted telnet. HTTPS, if available, is recommended.
HTTPS(SSL or TLS)	Enable	Follow the vendor's instructions for configuring keys/certificates for this.
SNMP Communities		SNMP is the default protocol for network management. Use SNMP v3 with password protection for highest security. It is often the protocol used by GUI configuration tools and network management systems. However, you can disable it if you do not use it.
Community 1 Name	XXXXXX	The default is usually "public." Change this to a complex value.
Community 2 Name	Disabled	Any unnecessary community names should be disabled or set to complex values.

1 as primary and server 2 as secondary, and the remaining use server 2 as primary and server 1 as secondary[1].

In sites where you have only one IAS server, this should always be the primary server. You should configure a remote server (in the site with most reliable connectivity to this site) as the secondary server[1].

In sites where there is no IAS server, balance the wireless remote APs between remote servers using the server with most resilient and lowest latency connectivity. Ideally, these servers should be at different sites unless you have resilient wide area network (WAN) connectivity[1].

Table eH.1[1] lists the settings that you need to configure on your wireless remote APs. Although the names and descriptions of these settings may vary from one vendor to another, your wireless remote AP documentation helps you determine those that correspond to the items in Table H.1[1].

Tip: The Key Refresh Time-out is set to 60 minutes for use with dynamic WEP. The Session Timeout value set in the IAS remote access policy is the same or shorter than this. Whichever of these has the lower setting will take precedence, so you only need to modify the setting in IAS. If you are using WPA, you should increase this setting in the AP to eight hours. Consult your vendor's documentation for more information.

Use the same RADIUS secrets procedure to add wireless remote APs to IAS. Although you may have not yet configured a secondary IAS server as a backup to the primary server, you can still add the server's IP address to the wireless remote AP now (to avoid having to reconfigure it later)[1].

Depending on the wireless remote AP hardware model, you may not have separate configurable entries for Authentication and Accounting RADIUS servers. If you have separate configurable entries, set them both to the same server unless you have a specific reason for doing otherwise. The RADIUS retry limit and timeout values given in Table H.1 are common defaults but these values are not mandatory[1].

Note: If you are currently using wireless remote APs with no security enabled or only static WEP, you need to plan your migration to an 802.1 X–based WLAN.

ADDITIONAL SETTINGS TO SECURE WIRELESS ACCESS POINTS

In addition to enabling 802. 1X parameters, you should also configure the wireless remote APs for highest security. Most wireless network hardware is supplied with insecure management protocols enabled and administrator passwords set to well-known defaults, which poses a security risk. You should configure the settings listed in Table eH.2[1]; however, this is not an exhaustive list. You should consult your vendor's documentation for authoritative guidance on this topic. When choosing passwords and community names for Simple Network Management Protocol (SNMP), use complex values that include upper and lowercase letters, numbers, and punctuation characters. Avoid choosing anything that can be guessed easily from information such as your domain name, company name, and site address[1].

You should not disable SSID (WLAN network name) broadcast since this can interfere with the ability of Windows XP to connect to the right network. Although disabling the SSID broadcast is often recommended as a security measure, it gives little practical security benefit if a secure 802.1X authentication method is being used. Even with SSID broadcast from the AP disabled, it is relatively easy for an attacker to determine the SSID by capturing client connection packets. If you are concerned about broadcasting the existence of your WLAN, you can use a generic name for your SSID, which will not be attributable to your enterprise[1].

REPLICATING RADIUS CLIENT CONFIGURATION TO OTHER IAS SERVERS

Typically, the wireless remote APs in a given site are serviced by an IAS server at that site. For example, the site A IAS server services wireless remote APs in site A, while the site B server services wireless remote APs in site B and so on. However, other server settings such as the remote access policies will often be common to many IAS servers. For this reason the export and import of RADIUS client information is handled separately by the procedures described in this appendix. Although you will find relatively few scenarios where replicating RADIUS client information is relevant, it is useful in certain circumstances (for example, where you have two IAS servers on the same site acting as primary and secondary RADIUS servers for all wireless remote APs on that site)[1].