Microsoft Solutions for Security

Securing Wireless LANs with Certificate Services

Appendixes

Release 1.6

Microsoft®

Appendixes Overview

The following appendixes are included with the solution guidance for *Securing Wireless LANs with Certificate Services*:

- Appendix A: Windows Version Support Matrix
- Appendix B: Solution Scripts and Support Files
- Appendix C: Delivery Guide
- Appendix D: WPA Support

Table of Contents

Appendix A: Windows Version Support Matrix

Introduction

The table in this appendix displays the status of different client and server Microsoft® Windows® operating system versions. The table lists the role of the system within the solution guidance for *Securing Wireless LANS with Certificate Services*, the different operating system versions that might be used in that role, and the support status for each operating system. The final column in the table includes additional explanatory notes or cautions.

The support status for each of the server roles is classified as one of the following:

- **Supported and Tested**—The operating system version has been used in the Microsoft Solutions for Security (MSS) test lab to build the solution, and it has been tested to work as part of the solution.
- **Supported**—The operating system version has not been tested as part of this solution, but Microsoft supports its use in this role. You may need to perform additional configuration or customization beyond the guidance included with this solution.
- **Not Supported**—The operating system version will not work within the solution as described. It may be possible to configure the unsupported system to work correctly, but doing this is likely to involve a significant amount of effort.
- **Unknown**—The operating system version may work in this role—there is no technical reason for it not to work—but ensuring that it will work is subject to your own verification and testing.

Where an operating system version is not displayed against a role, it will either not work (**Not Supported**), or it is unknown whether it will work (**Unknown**).

Table A.1: Support Status of Operating System Versions in the Solution

Role	Operating system version	Status	Notes
Wireless client	-Windows XP Professional -Windows XP Professional Tablet Edition	Supported and Tested	
	Microsoft Windows 2000	Supported	Need to obtain 802.1X client from Microsoft.com. The user certificates are deployed manually or scripted.
	-Microsoft Windows NT® version 4.0 -Windows 9*x*	Supported	Need to obtain 802.1X client via Premier Support. Certificates are deployed manually or scripted.
	Other platforms	Unknown	Clients need to support 802.1X and the Extensible Authentication Protocol-Transport Layer Security (EAP−TLS) protocol. Certificates are deployed manually or scripted.
Root Certification Authority (CA)	Microsoft Windows Server™ 2003, Standard Edition	Supported and Tested	
	-Windows Server 2003, Enterprise Edition -Windows 2000 Server	Supported	
	Third-party CA	Unknown	Must support revocation.
Issuing CA	Windows Server 2003, Enterprise Edition	Supported and Tested	

(continued)

	-Other Windows Server versions -Third-party CAs	Not Supported	Usable certificates can be generated.
RADIUS Server	Windows Server 2003, Standard Edition or Enterprise Edition	Supported and Tested	Standard Edition only supports up to 50 wireless access points (APs).
	Windows 2000 Server	Supported	Windows 2000 Internet Authentication Service (IAS) may be used for wireless 802.1X with some lost functionality.
	Other platforms	Not Supported	
Domain controllers	Windows Server 2003, Standard Edition or Enterprise Edition	Supported and Tested	The Active Directory® directory service must have Windows 2003 schema and a domain in Windows 2000 native mode or higher.
	Windows 2000 Server	Supported	Active Directory must have Windows 2003 schema and a domain in Windows 2000 native mode or higher.
Web server	Internet Information Service (IIS): Windows Server 2003	Supported and Tested	
	IIS: Windows 2000	Supported	
	Other platforms	Not Supported	Most Web servers will work for certificate revocation list (CRL) and CA certificate publication. Active Serve Pages (ASP) support is required for CA enrollment pages.

(continued)

Infrastructure servers, such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)	Windows Server 2003, Standard Edition or Enterprise Edition	Supported and Tested	
	Windows 2000 Server	Supported	
	Other platforms	Unknown	Third-party DHCP, DNS, and management solutions should work equally well with this solution as long as they fulfill the basic requirements for Windows client and Active Directory.

Appendix B: Solution Scripts and Support Files

Introduction

This appendix contains a brief description of the scripts and other support files supplied with the solution for *Securing Wireless LANS with Certificate Services*. Although functional and tested, the scripts and support files are supplied as aids for producing your own administrative scripts. They are not intended to server as production quality code.

Terms of Use

The scripts and support files provided with this solution are subject to the Microsoft standard TERMS OF USE. The terms are located on the Microsoft–Information on Terms of Use page at www.microsoft.com/info/cpyright.htm.

Note: Ensure that you thoroughly test these scripts and tools in a test environment before deploying them in any production environment.

List of Solution Guidance Files

Common Scripts

- constants.vbs
- helper.vbs

Certificate Services Scripts

- pkiparams.vbs
- ca_monitor.vbs
- ca_monitor.wsf
- ca_operations.vbs
- ca_operations.wsf
- ca_setup.vbs
- ca_setup.wsf

IAS and WLAN Scripts

- ias_tools.vbs
- ias_tools.wsf
- wl_tools.vbs
- wl_tools.wsf
- IASClientExport.bat
- IASClientImport.bat
- IASExport.bat
- IASImport.bat
- IAS_Data.bat

IAS and WLAN Support File

- IASAccessPrep.txt

Optional Component Unattended Files

- OC_AddIAS.txt
- OC_AddIIS.txt
- OC_RemoveRootUpdate.txt

Structure of the Scripts

The batch files are relatively simple to follow, but the Microsoft® Visual Basic® Scripting Edition (VBScript) files require some explanation to understand how they work together. Unlike many VBScript examples, these scripts are multifunctional. To provide access to the different functions, the scripts take advantage of the "job" functionality of Microsoft Windows® Scripting Host (WSH). This allows several independent program functions by specifying a job name as a parameter to the script.

The scripts mostly occur in pairs—a .wsf file and a .vbs file. The WSF file contains the "user interface" to different script operations. The VBS file contains all of the code that does the work of the program.

All of the WSF script files use the syntax where *JobName* is the name of the operation required and *WScriptFile* is the name of the XML interface file for the script as in the following example:

cscript //job:*JobName WScriptFile*.wsf

An excerpt from one of the WSF files includes the following information:

```
<?xml version="1.0" encoding="utf-8" ?>
<package xmlns="Windows Script Host
        <job id="GetCaCerts ">
                <comment></comment>
                <script language="VBScript" src="constants.vbs" />
                <script language="VBScript" src="pkiparams.vbs" />
                <script language="VBScript" src="helper.vbs" />
                <script language="VBScript" src="ca_operations.vbs" />
                <script language="VBScript
                <![CDATA[
                        GetCaCerts
                ]]>
                </script>
        </job>
        <job id="PublishRootCertstoIIS ">
                <comment></comment>
                <script language="VBScript" src="constants.vbs" />
                <script language="VBScript" src="pkiparams.vbs" />
                <script language="VBScript" src="helper.vbs" />
                <script language="VBScript" src="ca_operations.vbs" />
                <script>
                <![CDATA[
                        PublishCertstoIIS ROOT_CERT_SOURCE, WWW_LOCAL_PUB_PATH
                ]]>
                </script>
        </job>
```

The first job is GetCACerts. The job definition for this specifies that the following VBS files: constants.vbs, pkiparams.vbs, helper.vbs, and ca_operations.vbs will be loaded and contain functions or subroutines that the job requires. The final section of the code sample specifies the top-level function that will be executed to start the job; in this case, GetCACerts. (This example has the same name as the job but this does not need to be the case.) Notice that the second job—PublishRootCertstoIIS—supplies parameters to the called function.

The VBS files do the real work, and there are three main types:

- Operation-specific script files that contain functions related only to that one type of operation. (For example, ca_operations.vbs contains functions related to Certification Authority, or CA, operations.)
- Generic function script files that contain more general functions that all of the operation-specific scripts use. Helper.vbs is the only one of these scripts and it contains functions such as creating user accounts and error checking functions.
- Parameter script files that contain VBScript constants that define how the operational scripts run. These have been collected so that they are easier to change in one place rather than embedding them in the script functions. In this category are the constants.vbs file, which contains global parameters, and the pkiparams.vbs file, which contains parameters specific to the Public Key Infrastructure (PKI) setup and operations.

Description of Scripts and Support Files

This section describes each of the script and support files listed earlier.

Common Scripts

There are two common script files.

Constants.vbs

This script contains common values users can set that the other VBS and WSF files use. (For example, the settings for SMTP and Event log alerts are set in this script.)

Helper.vbs

This script contains common support routines that many of the other VBS scripts use (for example, user and group creation, alerting routines, and miscellaneous utility functions).

Certificate Services Scripts

This section describes the Certificate Services scripts.

pkiparams.vbs

This script contains PKI- and CA-specific values that the user can change. Some of these values *must* be changed before you can use them (to reflect the correct setting for your environment); others you do not have to change unless you want the scripts to behave differently. The main chapters of the guide (Chapter 7, "Implementing the Public Key Infrastructure," and Chapter 11, "Managing the Public Key Infrastructure") provide guidance for where you must or may need to change a value, in these procedures.

PKIParams.vbs is referenced by all other scripts with a "CA_" prefix.

ca_setup.vbs and ca_setup.wsf

These scripts contain functions to configure the baseline settings of the CAs that are used to create security groups and users. There are setup routines for the root and issuing CAs. Most of the values actually set are controlled from the pkiparams.vbs file. See Chapter 7, "Implementing the Public Key Infrastructure," for more information on this file.

The jobs contained in these scripts include the following:

- CertLocalGroups—This job creates local security groups (used on the root CA) for CA administration. The group creation function is called multiple times as part of the job, each time with a different group name.
- CertDomainGroups—This job creates domain security groups for CA and PKI administration. It contains multiple calls to create different groups. The group type (Local, Global, or Universal) is specified as a parameter within the job definition.
- CertLocalTestAccts—This job creates test user accounts for root CA administration.
- CertDomainTestAccts—This job creates test domain accounts for online CA administration.
- RootCAConfig—This job configures root CA parameters using calls to certutil.
- IssCAConfig—This job configures issuing CA parameters using calls to certutil.

ca_monitor.vbs and ca_monitor.wsf

These scripts contain functions to check the status of the CA and the PKI. The scripts specifically check to verify that the CA is responsive and that the CA certificates and certificate revocation lists (CRLs) are up to date. The scripts generate either Event Log entries or Simple Mail Transfer Protocol (SMTP) alerts or both. They are designed to be run by a Microsoft Operations Manager (MOM) agent (or similar management agent running on the server), or by the Windows task scheduler on an online CA. This scripting procedure is used only in Chapter 11, "Managing the Public Key Infrastructure."

The jobs contained in these scripts include the following:

- IsCAAlive—This job checks to see if the Certificate Services remote procedure calls (RPC) interfaces are responding.
- CheckCRLs—This job checks the CRLs of the CA on which the script is run and the CRLs for all parent CAs up to the root. Alerts are issued if a CRL has expired, a CRL is near expiration, and when a new CRL should have been issued.
- CheckCACerts—This job checks the CA certificate of the CA on which the script is run and the certificates for all parent CAs up to the root. Alerts are issued if a certificate has expired, when a certificate is one month from expiration, and if a certificate is due for renewal (normally at half of its lifetime).
- SetupSMTPAlerts—This job sets up the CA to produce e-mail alerts when a pending certificate request (waiting for Certificate Manager approval) has been queued at the CA.

ca_operations.vbs and ca_operations.wsf

These scripts contain functions relevant to the ongoing operations on the CA, such as publishing certificates and CRLs, and CA key and database backup. These scripts are mainly used in Chapter 11, "Managing the Public Key Infrastructure," but they are also used in some of the procedures in Chapter 7, "Implementing the Public Key Infrastructure."

The jobs contained in these scripts include the following:

- GetCaCerts—This job retrieves the CA certificate(s) from the root CA and stores them to a floppy disk.
- GetCRLs—This job retrieves the CRL(s) from the root CA and stores them to a floppy disk.
- PublishCertstoAD—This job publishes the Root CA Certificate (retrieved with GetCaCerts) to the Microsoft Active Directory® directory service.
- PublishCRLstoAD—This job publishes the Root CA CRL(s) (retrieved with GetCRLs) to Active Directory.
- PublishRootCertstoIIS—This job publishes the Root CA Certificate (retrieved with GetCaCerts) to the Internet Information Services (IIS) Web server.
- PublishRootCRLstoIIS—This job publishes the Root CA CRL(s) (retrieved with GetCRLs) to the IIS Web server.
- PublishIssCertstoIIS—This job publishes the Issuing CA Certificate (retrieved with GetCaCerts) to the IIS Web server.
- PublishIssCRLstoIIS—This job publishes the Issuing CA CRL(s) (retrieved with GetCRLs) to the IIS Web server.
- BackupCaKeys—This job backs up the CA certificates and keys to a floppy disk.
- BackupCaDatabase—This job runs NTBackup.exe to perform a system state backup (including CA database and logs) of the CA.

IAS and WLAN Scripts

This section describes the IAS and WLAN scripts.

ias_tools.vbs and ias_tools.wsf

These scripts contain jobs to assist with user setup for Microsoft Internet Authentication Service (IAS). The scripts are used in Chapter 8, "Implementing the RADIUS Infrastructure," and Chapter 9, "Implementing the Wireless LAN Security Infrastructure."

The jobs contained in these scripts include the following:

- CreateIasGroups—This job creates the domain security groups required by the solution to administer IAS.
- UpdateUsersRAP—This job edits the user dial-in properties to enable remote access. (This was not used in the solution but has been included in case you want to use it.) Using this script updates user objects in the USERS container *only*; if you want to update objects elsewhere, use the script as a template and modify it for your own purposes.

wl_tools.vbs and wl_tools.wsf

These scripts create security groups that are used to manage wireless local area network (WLAN) users and contain a routine for generating RADIUS/WirelessAP secrets. These scripts are used in Chapter 9, "Implementing the Wireless LAN Security Infrastructure."

The jobs contained in these scripts include the following:

- CreateWirelessGroups—This job creates security groups that are used to manage user and computer authorization, certificate enrolment, and the application of wireless policies.
- GenPWD—This job generates cryptographically random passwords for the wireless access points (APs) and IAS servers. The job uses CAPICOM to generate the random strings.

IAS Management Scripts

This section describes the IAS management scripts.

- IASClientExport.bat and IASClientImport.bat—These batch files allow export of the IAS server RADIUS client information to a floppy disk for safe storage. The import script imports the IAS server RADIUS client information from a floppy disk and loads it back into IAS server. These scripts are used in Chapter 12, "Managing the RADIUS and Wireless LAN Security Infrastructure."
- IASExport.bat and IASImport.bat—The IASExport script exports common IAS configuration state (minus RADIUS client information) to configuration text files located in D:\IASConfig. This script is run as a nightly event via Task Scheduler and it is used to export the primary IAS RADIUS server settings.

  The IASImport batch file imports previously-exported IAS configuration state from configuration text files located in D:\IASConfig. This file is used for disaster recovery and to build the secondary and tertiary IAS servers detailed in Chapter 8, "Implementing the RADIUS Infrastructure” in the Build Guide. These batch files also are used in Chapter 12, "Managing the RADIUS and Wireless LAN Security Infrastructure."

- IAS_Data.bat—This batch file creates, sets permissions, and shares IAS folders. This file is configured to run from the same domain as the groups used to apply permissions to the folders. If this is not the case, edit the script to use the explicit domain name. This file is used in Chapter 8, "Implementing the RADIUS Infrastructure.”

IAS Supplementary file

This section describes the IAS supplementary file.

- IASAccessPrep.txt—This text file contains the header line and data types for RADIUS request log data, which is imported into Microsoft Access by IAS Security Auditors. You will find instructions for using this file in Chapter 12, "Managing the RADIUS and Wireless LAN Security Infrastructure."

Optional Component Installation Files

- OC_AddIIS.txt and OC_RemoveRootUpdate.txt—You can use these text files with the Windows Optional Components Manager (OC Manager) to specify which components to install and remove. These files allow the automated installation of IIS and removal of the Root Update Service. These text files are used in Chapter 7, "Implementing the PKI."
- OC_AddIAS.txt—You can use this text file with the OC Manager to specify which components to install to allow automated installation of IAS. This text file is used in Chapter 8, "Implementing the RADIUS Infrastructure.”

Appendix C: Delivery Guide

Introduction

This guide provides general information intended for business planners, IT architects, or project managers regarding Microsoft best practices for coordinating and implementing the *Securing Wireless LANS with Certificate Services* solution. This guide also includes pointers to the following resources:

- Microsoft Solution Framework (MSF).
- Microsoft Operations Framework (MOF).
- Microsoft Security Risk Management Guide (SRMG).
- Sources for prerequisite knowledge and training on the topics essential to this solution.
- Descriptions of the tools and resources provided with and specific to this solution to assist you in planning, scheduling, and managing your implementation.

Microsoft Solution Framework

MSF provides proven practices for planning, building, and deploying a variety of technology solutions. MSF combines best practices of software design and development together with building and deploying infrastructure into a single project lifecycle for guiding technology solutions of all kinds. MSF helps organizations to achieve a delicate balance of flexibility while meeting commitments and minimizing risk. MSF provides a wealth of resources to Microsoft customers for download from MSDN on the Microsoft Solutions Framework (MSF) Web page at www.Microsoft.com/MSF/.

The fundamental approaches of MSF include:

- Readiness Management
- Project Management
- Risk Management
- The Team Model
- The Process Model

Readiness Management

At the start of a solution project, before the vision/scope phase, the organization needs to have a clear understanding of:

- Its specific security scenario and requirements:
  - To address the needs of organizations initiating security solution implementations, Microsoft Solutions for Security (MSS) has created the SRMG. The SRMG is a detailed process used to determine which threats and vulnerabilities have the greatest potential impact on a particular organization. Because every organization has different business requirements, it is impossible to create one list of vulnerabilities that will have the same impact on every environment. So the SRMG enables an organization to incrementally build its security and identify potential areas requiring remediation in the future.
- Its internal competencies:
  - This solution is intended to be easily understood and readily implemented by a Microsoft Certified Systems Engineer (MCSE) with two years of experience, with at least basic familiarity with the following Microsoft Official Curriculum (MOC) materials:
    - Course 2810: Fundamentals of Network Security
    - Course 2821: Designing and Managing a Public Key Infrastructure
    - Course 2830: Designing Security for Microsoft Networks
    - Course 2150: Designing a Secure Microsoft Windows 2000 Network
    - Course 2153: Implementing a Microsoft Windows 2000 Network Infrastructure

Project Management

MSF provides a large and diverse body of materials to assist organizations with application development and infrastructure deployment project management. This solution uses a subset of these MSF tools and methodologies to derive a number of project management tools intended to assist business planners or IT architects implement this solution, including:

- A sample Microsoft® Project schedule detailing the tasks, time required, and resources for a reference implementation of the solution that is included in the Tools and Resources download kit provided with this solution. (Securing_Wireless_LANs_Master_Project_Sched.mpp)
- A sample project cost analysis derived directly from the sample project schedule and reference implementation details from Microsoft also are included. This provides an approximation of the hardware, software, and labor costs to implement the solution. This spreadsheet is intended to be a template that the end user can modify to reflect the number of servers necessary and organization labor costs to quickly approximate an estimate of the implementation cost. (Secure Wireless LAN Cost Analysis.xls)

Risk Management

An essential element of project management is controlling the inherent risks of a project. Most individuals associate the concept of risk with the potential for loss, including value, control, functionality, quality, or time. However, risks also arise from the uncertainty surrounding project decisions and their outcomes, which can result in a failure to maximize opportunity gain.

MSF advocates the aggressive management of risks by planning mitigation strategies and contingency plans well before these risks can become actual issues or blocking factors to success.

To enable IT professionals to more thoroughly understand the risks that they may face in considering the implementation of this solution, a sample risk assessment derived from this MSF approach and based on an actual implementation of this solution is provided in the accompanying Tools and Resources download. (Secure Wireless LAN Risk Analysis.xls)

The Team Model

MSF provides both a framework for separating the roles and responsibilities of application development and infrastructure deployment initiatives, and the tools for defining the roles and their interactions. The roles include:

- **Program Management**—The resource in this role manages the project specification and serves as the primary architect; maintains the project schedule and reports project status; drives assessment and risk management; facilitates negotiation within the team; and coordinates the feature versus schedule versus resources tradeoff decision-making.
- **Product Management**—The resource in this role acts as the customer advocate and manages customer requirements; drives the shared vision/scope of the project; develops and maintains the business case; and drives feature versus schedule versus resource tradeoff decisions.
- **Development**—The resource in this role specifies the features of the solution design; estimates the time and effort required to complete each feature; and builds or supervises the building of the solution.

- **Test**—The resource in this role verifies the solution functionality and ensures that all known issues are documented.
- **User Experience**—The resource in this role acts as a user advocate; manages user requirements; drives usability and performance enhancement tradeoff decisions; and develops and provides user training.
- **Release Management**—The resource in this role acts as advocate for operations, support, and delivery channels; manages procurement; coordinates solution deployment; and drives manageability and supportability tradeoff decisions.

The Process Model

The Process Model is the major element of MSF, representing best practices that have been identified, used, and refined by Microsoft from its own experiences coordinating large-scale application development and infrastructure deployment projects. The primary concepts of the MSF Process Model include:

- **Managing tradeoffs**—A balance must exist between resources (people and money), schedule (time), and features (scope). Should one of these elements require change, the other items also must change in some manner.
- **Milestone driven approach**—Milestones are a key theme in MSF. They are used to plan and monitor project progress, and they serve as intermediary points in the project. They are used to gauge progress, ensure synchronization with customer expectations, coordinate with other team members on deliverables, and check in with stakeholders or sponsors regarding the progress and direction of the project.
- **Iterative approach**—MSF recommends that solutions are developed by building, testing, and deploying core functionality first, then regularly adding sets of features. This approach relies on “living” documents that are regularly refreshed as new feature sets are added. It relies on using daily builds of the solution, frequently gauging progress, and ongoing tracking and control of project artifacts.
- **Regular phases and milestones**—A wide variety of valuable project tools and templates are available online from MSF for each of the following project phases:
  - **Envisioning Phase**
    - Vision/scope template
    - Project structure template
    - Risk assessment tool and management tools
  - **Planning Phase**
    - Business, User, System, and other requirements templates
    - Functional Specification templates
    - Development, Risk Management, Test, Training, Quality, and other Planning templates
  - **Building Phase**
    - Templates for content and code deliverables
    - Test plan and test case templates (a detailed solution test plan and test cases are included in Chapter 13, “Testing the Solution”).
  - **Deploying Phase**
    - Deployment and Communication plan templates

MSF is closely related to MOF, which is the Microsoft approach to achieving mission-critical production system reliability, availability, and manageability. MOF is based on an internationally accepted set of best practices in IT service management called the IT Infrastructure Library (ITIL). MSF and MOF have been designed to work effectively either together or independently.

Microsoft Operations Framework

The Microsoft Operations Framework (MOF) provides technical guidance that enables organizations to achieve mission-critical system reliability, availability, supportability, and manageability of Microsoft products and technologies. The Operations Guide for this solution is based on MOF, and it outlines the appropriate tasks necessary for operating, supporting, optimizing, and changing the solution.

MOF provides valuable operational guidance in the form of white papers, operations guides, assessment tools, best practices, case studies, templates, support tools, and services. This guidance may help you address the people, process, technology, and management issues pertaining to operations within complex, distributed, heterogeneous IT environments.

MOF and MSM are discussed in more detail in Chapter 10, “Introduction to the Operations Guide.”

Summary

This Delivery Guide provides general information about Microsoft best practices for coordinating and implementing the solution for *Securing Wireless LANs with Certificate Services.*

Appendix D: WPA Support

Introduction

The *Securing Wireless LANS with Certificate Services* solution is by design compatible with Wi‒Fi Protected Access (WPA) security for wireless LANs (WLANs). WPA compatibility has been successfully tested in a lab that was configured according to the steps in this guidance. This document describes several items that you should consider when evaluating how you can use WPA with this solution.

WEP and WPA Overview

Wired Equivalent Privacy (WEP) was defined as part of the Institute for Electrical Engineers (IEEE) 1999 802.11 wireless networking standard to provide a level of protection equivalent to a wired system. Basic (or static) WEP provides encryption and access control for wireless traffic based on a pre-shared key. WEP has been shown to have several vulnerabilities that can allow a determined attacker to eventually overcome this native 802.11 security control.

The WLAN industry has responded to the vulnerabilities WEP by offering a stronger security solution called WPA. WPA increases the level of data protection and access control for WLAN systems through a standards-based, interoperable security specification. The first release of WPA is an early subset of the 802.11i standard and is expected to maintain compatibility in the future. 802.11i is currently expected to be released as WPA 2.0.

At the time of publication, many organizations still had a lot of WLAN hardware deployed that did not support WPA. It is important that this solution supports both this hardware and the newer WPA-compliant equipment. Although WPA provides a higher level of security than dynamic WEP, the latter is still a viable solution until all hardware can be updated to support WPA.

The Impact of WPA on This Solution

You can think of WPA as a replacement for WEP in this *Securing Wireless LANs with Certificate Services* solution. The majority of the solution components are unaffected by the introduction of WPA. The solution was successfully tested for compatibility with WPA by configuring WPA-enabled networking equipment in a similar fashion to WEP-based equipment and making changes to client computers.

Because WPA uses the 802.1X protocol for network authentication, the Remote Authentication Dial-In User Service (RADIUS), Microsoft® Certificate Services, and most of the Microsoft Active Directory® directory service settings work as configured. One significant consideration is that you can only configure the WPA-specific settings using Group Policy if you have at least one domain controller running Windows Server 2003 Service Pack 1 (alternatively, you may be able to configure the Group Policy settings on a domain member running Windows Server 2003 that is not a domain controller). You will find more information on this topic later in this appendix. The following table lists items to consider when using WPA with this solution.

Table D.1: Solution Components Requiring Consideration

Solution item	Consideration	Comments
Microsoft Windows® XP hardware drivers	You should contact your network interface card (NIC) vendor to assess which cards you can upgrade for WPA support and the availability of Windows XP client drivers.	Look for drivers that have passed testing by the Windows Hardware Quality Labs (WHQL). Driver support for the Windows Wireless Zero Configuration service enables card firmware to be dynamically updated to support WPA. Confirm driver support for the WZC service with your vendor.
Windows XP client configuration	The client configuration settings will need to change. This solution has been tested by selecting WPA as the authentication method and Temporal Key Integrity Protocol (TKIP) as the encryption protocol.	TKIP replaces WEP as the encryption method, and WPA mandates 802.1X as the authentication method.
Timed client re-authentication	This solution utilizes RADIUS settings to ensure that clients perform a reauthentication every 10 minutes so that WEP keys are regenerated.	TKIP rekeys each packet; therefore, it makes the requirement for client reauthentication for WEP key purposes obsolete. Leaving this setting at 10 minutes places an unnecessary load on your Microsoft Internet Authentication Service (IAS) servers. You can change the session timeout to 10 hours when using WPA.
Wireless Network Group Policy	The existing Wireless Network Group Policy that ships with Windows Server 2003 prior to SP1 was developed prior to WPA availability and therefore cannot configure client WPA settings.	You must use Windows Server 2003 SP1 to configure Group Policy WPA settings. Otherwise you must manually configure the wireless client settings.

Configuring the Secure Wireless LAN Solution with WPA

You can perform the following high-level steps to configure the solution to use WPA:

1. Upgrade the firmware on the existing wireless access points (AP) to support WPA, or deploy new wireless APs that support WPA. Be sure to add any new wireless APs as RADIUS clients to the IAS server according to the instructions in this guidance. Configure the WPA settings on the wireless APs according to the vendor specifications.
2. Upgrade the WLAN network interface card (NIC) driver to a version that supports WPA. Microsoft is working with many WLAN card vendors to support upgrading firmware through the adapter card driver.
3. Remove the wireless computer from the security group that applies the Wireless Network Group Policy. Create a new Group Policy Object (GPO) using Windows Server 2003 SP1 and configure the wireless client settings for WPA. Specify WPA as the authentication type and TKIP as the encryption type. Create an additional security group and grant it Apply Policy permissions on the WPA GPO. Use this group to control which clients receive WPA settings. If you have not deployed SP1 of Windows Server 2003, you must manually configure wireless client settings for WPA.
4. Test authentication to the WLAN using WPA. IAS should log a System Event Log message with a source of **IAS** and an event ID of **1**. This indicates a successful authentication.

More Information

Use the following resources to find more information on the topics detailed in this appendix:

- The Cable Guy—March 2003, Wi–Fi Protected Access (WPA) Overview on Microsoft TechNet at www.microsoft.com/technet/community/columns/cableguy/cg0303.mspx.
- Microsoft Knowledge Base Article 815485, “Overview of the WPA Wireless Security Update in Windows XP” at http://support.microsoft.com/?kbid=815485.
- The Microsoft Press Pass Announcement about WPA availability at www.microsoft.com/presspass/press/2003/mar03/03-31WiFiProtectedAccessPR.asp.
- IEEE 802.11 Wireless LAN Security with Microsoft Windows XP at www.microsoft.com/downloads/details.aspx?FamilyID=67fdeb48-74ec-4ee8-a650-334bb8ec38a9&displaylang=en.