Microsoft Windows Server 2003

Deploying Wireless Provisioning Services (WPS) Technology

James McIllece
Microsoft Corporation

Version: March 2005

Abstract

This whitepaper describes a Wireless Internet Service Provider (WISP) network that allows you to provide pay-per-use, monthly service, and long-term Internet access to new and existing customers through wireless access points deployed in public areas, such as airports and shopping malls. With Wireless Provisioning Services (WPS) technology, new and existing customers with computers running Windows XP with Service Pack 2 (SP2) can connect to your Wi-Fi network without manual configuration of the computer or network connection.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.
The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.
This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Contents

Introduction

By using Wireless Provisioning Services (WPS) technology, your organization can offer wireless access in any location where you provide connectivity with Wi-Fi hotspots to new and existing customers that have computers running Windows XP with Service Pack 2 (SP2).

Wi-Fi means "wireless fidelity" and is the IEEE 802.11 technical standard for short range wireless data transmissions. Wi-Fi hotspots are areas where you deploy one or more wireless access points. WPS technology allows new customers without a previously established account to securely connect to your network at the Wi-Fi hotspot location, create and pay for an account, and access the Internet.

One of the key challenges of deploying wireless technologies in public places is providing customers with the correct network configuration for their computers. Many customers are unaccustomed to manually configuring network settings, and might forego use of public wireless networks due to the difficulty of these configurations. In addition, erroneous configurations can prevent customers from connecting successfully.

With WPS technology, your customers do not need any knowledge of network technology, and they do not need to manually configure their computers or join a domain to connect to your network. During the account-creation process, customers' computers are automatically and transparently supplied — or provisioned — with all configuration necessary for them to successfully access your network and services.

WPS technology allows you to provide your customers with the following account-creation and computer configuration options:

- Customers can create their account and automatically provision their computer over the Internet in advance of arrival at your Wi-Fi hotspot locations.
- Customers who arrive at your Wi-Fi hotspots without previously creating an account and provisioning their computers can spontaneously connect, provision their computer, create an account, and access the Internet through your Wi-Fi hotspot.

WPS technology is deployed by using the following:

- One or more computers running Windows Server 2003 with Service Pack 1 (SP1) and later, and Internet Authentication Service (IAS). If you use a RADIUS server other than IAS in Windows Server 2003 with SP1, you need to verify with your RADIUS server vendor whether their servers support WPS. A royalty-free license that covers WPS protocol implementation is available for RADIUS and other server vendors through the Published Protocols and Royalty-Free License site on MSDN at http://go.microsoft.com/fwlink/?LinkId=33674
- One or more computers running Windows XP Home Edition with SP2; Windows XP Professional with SP2; or Windows XP Tablet PC Edition with SP2.
- Additional servers on your network. For example, these servers include a provisioning server, a DHCP server, and a domain controller with a user accounts database. Depending on the deployment method you choose, you might need additional servers as described in this paper.
- Network access servers and other network hardware. This hardware includes wireless access points, routers, and other devices.
- One or more custom applications or databases that you design. For example, a Web application running on an HTTPS-enabled Web server that passes customer data from the customer to the provisioning server.

These hardware and software components of WPS technology are deployable by three types of organizations with two different methods used to provide customers with the ability to create and pay for an account before obtaining access to the Internet. The following introductory sections describe these organizations and methods, and further introduce the key components of WPS technology.

Who can use WPS technology

WPS technology is designed for use by three types of organizations:

- **Hotspot service providers (HSPs)**. HSPs deploy wireless access points in public places, such as shopping malls and airports, but HSPs are not Internet service providers (ISPs). Instead, the HSP contracts with one or more ISPs, and offers customers one or more service plans to choose from when they want to establish an account for Internet access.
- **Wireless Internet service provider** (**WISPs**). WISPs are ISPs that either deploy Wi-Fi hotspots in public places or outsource Wi-Fi hotspot services to an HSP.
- **Enterprises**. Enterprises can use WPS technology to provide managed guest access on their networks. The WISP scenarios in this paper apply to enterprises as well as WISPs.

Key WPS components

The following section introduces key WPS client and server components.

WPS technology in Windows XP with SP2

Wireless Provisioning Services technology is included in Service Pack 2 for Windows XP. WPS enables a wireless client computer running Windows XP Home

Edition with SP2, Windows XP Tablet PC Edition with SP2, or Windows XP Professional with SP2, to connect to and download network configuration information from a provisioning server. After the Windows XP with SP2 client has obtained network configuration information, it automatically configures the connection to your network.

Windows XP with SP2 WPS technology consists of the following two components:

- **Network Provisioning Service.** The Network Provisioning Service automatically downloads XML configuration files from provisioning servers. Users and administrators do not need to configure the Network Provisioning Service because the service automatically configures itself.
- **Wireless Zero Configuration service.** The Wireless Zero Configuration service in Windows XP with SP2 has new WPS technology capabilities. Wireless Zero Configuration, also called Wireless Auto Configuration in this paper, interacts with the Network Provisioning Service and IEEE 802.1X authentication on the client computer to provide WPS functionality. Users and administrators do not need to configure the Wireless Auto Configuration service because the service automatically configures itself.

In all uses of WPS technology, computer configuration is performed in the background and is transparent to users, with no client computer configuration needed by administrators.

WPS technology on Windows XP with SP2 also supplies your customers with a sign-up wizard that allows them to create an Internet access account. The wizard passes the customer’s personal data, such as credit card information, over a secure connection to a custom application that processes the information and creates the user account on your network.

The provisioning server

A provisioning server is a computer running Internet Information Services (IIS) or a third-party Web server that maintains a collection of information files that are used to configure client computers during the connection and account sign-up process. These information files are created using Extensible Markup Language (XML) and WPS XML schemas, and are stored on the provisioning server. The provisioning server supplies the XML files to clients when client computers request provisioning information from the provisioning server.

There are multiple XML schemas for WPS that allow you to create XML data files to define network configuration and other parameters for client computers connecting to your network. Using WPS XML data files, you can customize and define the sign-up experience users will have when connecting to your network by using the sign-up wizard included in Windows XP with SP2. In addition to the network and security settings, this includes branding information (such as your company logo), location information (where your Wi-Fi hotspots are located), plan offering (types of accounts your customers can purchase), and Help content to assist your customers when they need additional information.

There are two methods you can use to create and configure your XML master file and subfiles:

- Use the WPS Authoring Tool to create a WPS project and publish your XML master file and subfiles to the provisioning server. The WPS Authoring Tool has a graphical user interface and is designed to assist you in accurately producing and managing a collection of XML files for your WPS solution. Using the WPS Authoring Tool to create your XML data files is recommended, as it is based on the XML schema and allows you to validate your XML files against the XML schema before using the XML files in a production environment. Download the WPS Authoring Tool at http://go.microsoft.com/fwlink/?LinkId=40535.
- Use the XML schema to manually create your XML master file and subfiles. After you have created these files, you can enter information specific to your network and deployment parameters. For example, where the location of the provisioning server is required, you can provide an HTTPS URL. In another example, you might need to enter your domain name in several places; you can examine the schemas and example files and determine where to insert your domain name.

For more information, see “XML Schemas” later in this document.

In some scenarios depicted in this paper, the provisioning server maintains an account processing application in addition to storing and providing clients with XML configuration files. Other scenarios place the account processing application on a dedicated server. The account processing application is a Web application that you create based on your business model and the requirements of WPS technology.

The account processing application, whether installed on the provisioning server or a dedicated server, processes XML documents sent from client computers when customers create an Internet access account. The XML documents passed from client to server contain data provided by the customer, such as the customer name, address, and credit card information. When promotion codes are used, these codes are also passed to the account processing application from the client in an XML document.

The account processing application processes all of the data provided by the client, and performs the appropriate action. For example, the account processing application can verify promotion codes against a Microsoft® SQL Server™ 2000 database, create a user account in an Active Directory® directory service user accounts database, and perform financial functions such as verify credit card information and charge the customer’s credit card.

The IAS server

Internet Authentication Service (IAS) is the Microsoft implementation of Remote Authentication Dial-In User Service (RADIUS) server and proxy. IAS in Windows Server 2003 with SP1 is a component of all WPS scenarios depicted in this paper. In some scenarios, an IAS proxy is also required.

Key WPS processes

The following section introduces key processes that occur during the provisioning of clients and the network connection process that allows your customers to create an account.

Pre-provisioning the client computer

Pre-provisioning occurs when client computers are provisioned before arriving at a Wi-Fi hotspot. There are three possible methods for pre-provisioning a client computer:

- Computer original equipment manufacturers (OEMs) pre-provision clients. OEMs can include promotional offers for WISP connectivity with the sale of their computers. This allows purchasers of the OEM's products to arrive at the Wi-Fi hotspot for the advertised WISP with their computer already configured.
- The Information Technology (IT) department at an organization pre-provisions clients. Before supplying employees with new computers, the IT department can pre-provision the client for employees.
- Customers connect to the WISP and pre-provision their computer. WISP customers have the option of creating their account and downloading network configuration information before arriving at the location where they will wirelessly access the Internet through your network. For example, a customer preparing for a business trip might establish an account online and download network configuration files before leaving their office or home.

Provisioning the client computer

Client computers are provisioned with your network configuration at a Wi-Fi hotspot. When new customers connect at a Wi-Fi hotspot, IAS sends a packet containing the location of the provisioning server to Windows XP on the client computer. Windows XP then downloads network configuration information from your provisioning server, and the client computer is automatically configured to access your network.

Phased network access

Phased network access occurs when a new customer arrives at your Wi-Fi hotspot with a computer running Windows XP with SP2. Phased network access consists of the following two stages:

1. Customers are allowed to connect to your network and authenticate as guest to establish an account. While the customer is connected as guest, they do not have access to the Internet. During this first connection phase, customers can create and pay for a new account. When the account is established, guest access is terminated by WPS.
2. Customers are automatically reauthenticated with the newly established account credentials. When the customer is authenticated and authorized with new account credentials, they are provided with access to both your network and to the Internet.

Phased network access is accomplished by temporarily isolating the client computer from the rest of your network using either a virtual local area network (VLAN)-aware gateway device (for example, an access controller or a VLAN-aware router or switch) or IP filters applied to the connection by IAS and wireless access points that provide this capability.

Client isolation is necessary to provide security and to prevent users from accessing the Internet through your network without first establishing a paid account.

When new customers first connect to your network, they are allowed access to your provisioning server and any other necessary network resources (such as your DHCP server), but their access to the Internet is blocked. After they create and pay for an account and reauthenticate with the new account credentials, they are allowed access to the Internet.

If you have deployed IP filters to isolate client computers from the Internet during the first connection phase, customers are granted Internet access upon reauthentication because the IP filters are not applied to the connection. If you have deployed VLANs to isolate client computers from the Internet during the first connection phase, customers are granted Internet access upon reauthentication because they are placed on a VLAN that provides access to the Internet.

Scenarios overview

The method that you use to isolate client computers affects the hardware and software configuration of your network. In the first section of this paper, the following scenarios are depicted:

- **WPS technology for a WISP with VLANs**. This scenario depicts a WISP network using VLANs for client isolation, and is recommended for WISPs and HSPs deploying WPS technology.
- **WPS technology for the Enterprise**. This scenario depicts a secure WISP network using VLANs for client isolation, and is recommended for enterprises deploying WPS technology. This scenario is similar to the first scenario, however it includes a perimeter network between the Wi-Fi hotspots and the enterprise local area network (LAN).

In the last two sections of this paper, two untested beta scenarios using IP filters for client computer isolation are presented in overview:

- A WISP using IP filters for client isolation
- An HSP using IP filters for client isolation

Configuring IAS for WPS technology

For all scenarios in this paper, whether you are deploying IAS as a RADIUS proxy or IAS as a RADIUS server, you must configure IAS to be compatible with WPS technology by creating the **EnableWPSCompatibility** registry entry. When you configure and enable this registry entry, and then open a connection request policy profile in the IAS console, connection request policy user interface elements that allow you to configure Protected Extensible Authentication Protocol (PEAP) become visible.

To configure EnableWPSCompatibility

1. Open **Registry Editor**.
2. Browse to the following registry path: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Policy**
3. Right-click the **Policy** key, click **New**, and then click **DWORD value**.

4. A new value is added to the details pane, with the default name of the value highlighted for editing. Replace the default name by typing **EnableWPSCompatibility**, then press Enter.
5. Right-click on **EnableWPSCompatibility**, and then click **Modify**.
6. In **Edit DWORD value**, in **Value data**, change the integer to **1**. The default value is **0** (disabled). All values other than **1** (enabled) are treated as **0** (disabled).

To verify that EnableWPSCompatibility is enabled

1. Open the IAS console.
2. Double-click on **Connection Request Processing**, and then click **Connection Request Policies**.
3. In the right pane, double-click the default connection request policy, named **Use Windows authentication for all users**, and then click **Edit Profile**. The **Edit Profile** dialog box opens.
4. On the **Authentication** tab, below Authenticate requests on this server, you can see the Protected EAP check box.

To verify that EnableWPSCompatibility is disabled

1. Open the IAS console.
2. Double-click on **Connection Request Processing**, and then click **Connection Request Policies**.
3. In the right pane, double-click the default connection request policy, named **Use Windows authentication for all users**, and then click **Edit Profile**. The **Edit Profile** dialog box opens.
4. On the Authentication tab, below Authenticate requests on this server, you cannot see the Protected EAP check box.

For additional IAS configuration steps, see the deployment scenarios in this paper.

WPS technology for a WISP with VLANs

If your organization is a WISP, you can deploy WPS technology using a VLAN-aware gateway device, such as an access controller, a VLAN-aware router, or a VLAN-aware switch. In this circumstance, network resources such as the provisioning server and the IAS server reside on a Network Resource VLAN, while access to the Internet is provided to customers who have established an account by switching them to an Internet VLAN.

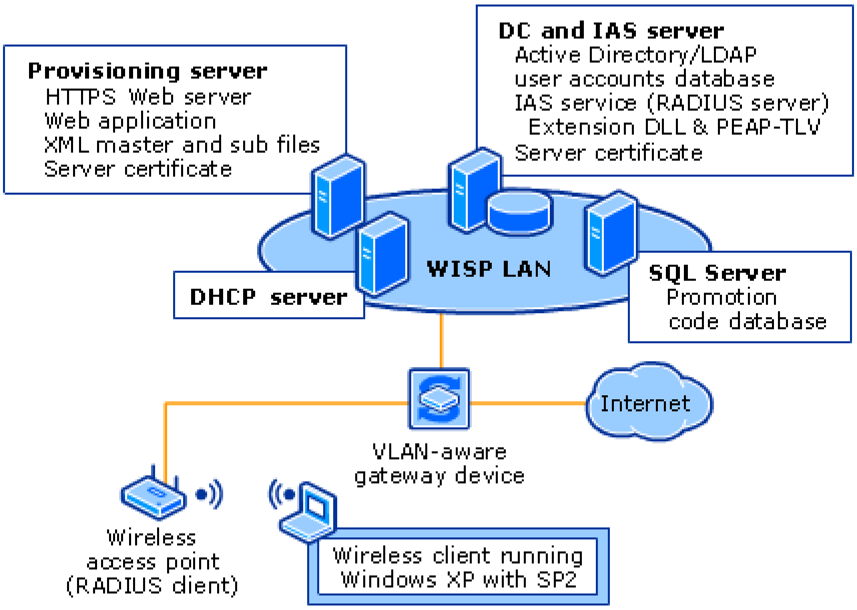
In the sections that follow, the components of a WISP network using a VLAN-aware gateway device are described, how the components work together during a new customer sign-on are detailed, and how to deploy a WISP network with VLANs is explained.

Components of WPS technology with VLANs

This deployment scenario, designed for an ISP that deploys Wi-Fi hotspots as a WISP, has the following features:

- A VLAN-aware gateway device is used for client computer isolation during the account sign-up process.
- Customers sign up using a promotion code. Many organizations introduce new services through the use of promotional campaigns in which customers are provided with a special or discounted offer when they sign up for an account using a promotion or pre-paid code. This implementation of WPS technology depicts a WISP that uses promotion or pre-paid codes for a spontaneous customer sign-up at a Wi-Fi hotspot. The codes are stored in a database on a server running SQL Server 2000 or a third-party database application.

The following illustration depicts the components of a WISP network using a VLAN-aware gateway device for client computer isolation.



Components of a WISP network using VLANs

Wi-Fi hotspot components

Following are the components that comprise the wireless local area network (WLAN):

Wireless client

A computer running Windows XP Home Edition with SP2, Windows XP Professional with SP2, or Windows XP Tablet PC Edition with SP2. The computer must be equipped with a wireless network adapter that provides support for IEEE standard 802.11, IEEE standard 802.1X authentication, and Wired Equivalent Privacy (WEP). Support for Wi-Fi Protected Access (WPA) is preferred, but not required.

Wireless access point (RADIUS client)

One or more wireless access points deployed on the WISP LAN with a wired connection to the access controller, VLAN-aware switch or router, or other gateway device.

The wireless access point is configured as a RADIUS client to the Internet Authentication Service (IAS) server deployed on the WISP LAN. The wireless access points used for WPS technology must meet the following requirements:

- Support for the use of VLANs.

- Support for the IEEE standard 802.1X authentication.
- Support for Wi-Fi Protected Access (WPA) is preferred. WPA is supported by Windows XP with SP2. To deploy WPA, use wireless network adapters and wireless access points that also support WPA.
- Support for RADIUS authentication and RADIUS accounting, including:
    - Support for the Class attribute as defined in RFC 2865, "Remote Authentication Dial-in User Service (RADIUS)," to allow session correlation for RADIUS authentication and accounting records. For session correlation, when you configure RADIUS accounting at your IAS server or proxy, you must log all accounting data that allow applications (such as billing applications) to query the database, correlate related fields, and return a cohesive view of each session in the query results. At a minimum, to provide session correlation, you must log the following IAS accounting data: NAS-IP-Address; NAS-Identifier (you need both NAS-IP-Address and NAS-Identifier because the access server can send either attribute); Class; Acct-Session-Id; Acct-Multi-Session-Id; Packet-Type; Acct-Status-Type; Acct-Interim-Interval; NAS-Port; and Event-Timestamp.
    - Support for accounting interim requests, which are sent periodically by some access servers during a user session, that can be logged. This type of request can be used when the Acct-Interim-Interval RADIUS attribute is configured to support periodic requests in the remote access profile on the IAS server. The access server, in this case a wireless access point, must support the use of accounting interim requests if you want the interim requests to be logged on the IAS server.
    - Support for IP address range filtering.
    - Support for dynamic retransmit timeout (RTO) estimation or exponential backoff to handle congestion and delays in a wide area network (WAN) environment.

In addition, there are some filtering features that the access points must support to provide enhanced security for the network. These filtering options include:

- **DHCP filtering.** The access point must filter on IP ports to prevent the transmission of DHCP broadcast messages in the instance that the client is a DHCP server. The access point must block the client from sending IP packets from port 68 to the network.
- **DNS filtering.** The access point must filter on IP ports to prevent a client from performing as a DNS server. The access point must block the client from sending IP packets from port 53 to the network.

WISP LAN components

Following are the components that comprise the WISP LAN.

VLAN-aware gateway device

The VLAN-aware gateway device can be an access controller, a VLAN-aware router, a VLAN-aware switch, or any other device that can be configured to apply IAS-provided parameters to client connections. The VLAN-aware gateway device is configured with two VLANs: a Network Resource VLAN and an Internet VLAN.

The Network Resource VLAN allows all users access to the provisioning server and DHCP server. This VLAN grants access to network resources that allow customers to connect to your network as guest, create an account, receive provisioning information from the provisioning server, and pay for the account.

The Internet VLAN provides access to the Internet. Only customers who have created and paid for accounts are switched to this VLAN and granted Internet access. This process occurs when Windows XP reauthenticates the user with the newly created account information. When the user is authenticated and authorized by your IAS server, the IAS server returns attributes to the VLAN-aware wireless access point; the access point instructs the VLAN-aware gateway device to route client traffic to the Internet VLAN.

Provisioning server

The WISP provisioning server is configured with the following components.

HTTPS Web server

The Internet Information Services (IIS) or third-party Web server must be deployed with Secure Hypertext Transfer Protocol (HTTPS).

Web application

The WISP Web server is configured with an account processing Web application that processes data provided during customer sign-up or account renewal. When a customer uses the sign-up wizard on a client computer to create and pay for a WISP account, the customer enters data, such as name, address, and credit card information that is converted to an XML document on the client. Windows XP sends this XML document to the WISP provisioning server.

The account processing application on the provisioning server must be capable of accepting and processing the XML documents containing the user data. For example, the account processing application must compare the promotion code entered by the user to a promotion code in the SQL Server database, and then dynamically create an account in the Active Directory user accounts database with the properties (domain and security group membership) described in the database. The account processing application must also contain a credit card verification component to process customers' payment information. The account processing Web application must permit new customers to sign up and to permit existing customers to renew their subscriptions for service.

XML master file and subfiles

The WISP provisioning server stores the XML master file and subfiles that provide the client with all configuration information needed to access the network, create an account, pay for the account, and ultimately access the Internet. For more information about the XML master file and subfiles, see "XML schemas" in this paper.

Server certificate

For server authentication to client computers, the WISP provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust. For more information, see "Server Certificate Requirements" in this paper.

In test lab deployments of WPS technology, you can deploy your own certification authority in lieu of using a public trusted root CA. In this circumstance you must install the private trusted root CA certificate on all clients used for testing so that the clients will trust the CA and so that your servers, such as your provisioning server and your IAS server, can be successfully authenticated by the clients.

Domain controller and IAS server

The WISP domain controller and IAS server is running Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1, and is configured with the following components.

Active Directory

In this scenario, Active Directory is deployed. The user accounts database on the domain controller must be an Active Directory user accounts database or a database that uses Lightweight Directory Access Protocol (LDAP) and supports dynamic creation of user accounts.

When a customer signs up for an account, the account processing Web application on the provisioning server creates a new account in the user accounts database, and adds the user to a group that has clearly defined access privileges that match the type of account the customer purchased when signing up.

If you use an accounts database other than Active Directory, IAS authentication and authorization extensions must be written and installed for this process to function correctly.

Internet Authentication Service (IAS)

IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy, and is used to authenticate and authorize users connecting to your network. IAS is configured with remote access policies that allow guest authentication for non-domain member computers and users. It is also configured to provide attributes to RADIUS clients (access points) that instruct the gateway device to apply the attributes to client connections. Protected Extensible Authentication Protocol (PEAP) with MS-CHAP v2 is configured on remote access policies as the authentication method used by wireless clients.

Extension DLL and URL PEAP-TLV

An IAS extension DLL defining a URL PEAP-TLV provides IAS with the ability to send the location of the provisioning server to client computers.

PEAP-Type-Length-Value (PEAP-TLV) is an Extensible Authentication Protocol (EAP) authentication type that allows the IAS server to pass information to client computers attempting to connect to your network.

In this circumstance, the value contained in the PEAP-TLV is an HTTPS Uniform Resource Locator (URL) that provides client computers running Windows XP with SP2 with the location of the WISP provisioning server. With this URL, Windows XP can download the WISP XML files to the client computer.

In addition to the URL of the provisioning server, the URL PEAP-TLV includes an action parameter. The action parameter directs Windows XP to perform a specific task. The action parameter included in the URL PEAP-TLV defines tasks such as new customer sign-up, existing account renewal, and password change.

For more information, see “How to create an IAS extension DLL and a URL PEAP-TLV” in this paper.

Server certificate

To authenticate the IAS server to the wireless client computers using PEAP, the WISP IAS server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public CA, such as Verisign or Thawte, that is trusted by client computers. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust. If you install IAS and Active Directory on the same computer, the computer must have a certificate. If you install IAS and Active Directory on different computers, only the IAS server needs a certificate.

SQL server

A computer running SQL Server 2000 or another SQL-compatible relational database application.

The promotion code database running on the SQL server is configured with the following fields: promotion code, user name, domain name, security group, and expiration date. With the exception of the user name field, each field for each record is preconfigured with a value. The value for the user name field is assigned by the Web application when a customer creates a user account with a promotion code that matches a value in the promotion code field in the database. By predefining the domain in which the user account is created by the Web application and the Active Directory security group to which the user account is joined as a member, you can assign network access and other permissions for your customers.

DHCP server

The DHCP server must be able to assign valid public IP addresses to computers accessing the network through the wireless access points.

How a WISP works with VLANs

The Internet connection process using WPS technology with a VLAN-aware gateway device differs depending on whether the customer attempting to connect is a new customer or an existing customer. The following example describes the process for a new customer using a promotion code at a Wi-Fi hotspot location. In addition, the manner in which IAS handles an expired account is explained.

New customer connection example

When a new customer connects to a WISP and establishes an account, the following stages occur:

1. The customer discovers the WISP network at a Wi-Fi hotspot
2. The customer authenticates as guest
3. The client is provisioned and the customer establishes an account
4. The customer is authenticated with the new account credentials
5. The user is switched to a VLAN that provides Internet access

In the next section we will look at these stages in more detail.

1. The customer discovers the WISP network at a Wi-Fi hotspot

When a customer arrives at the WISP Wi-Fi hotspot with a portable computer running Windows XP Home Edition with SP2, Windows XP Tablet PC Edition with SP2, or

Windows XP Professional with SP2, the computer comes within range of the WISP access point beacon.

Wireless auto configuration on the client computer detects the beacon information from the access point, which is configured to broadcast the Secure Set Identifier (SSID) of the WISP's network. The SSID is equivalent to the network name.

The customer is informed by Windows XP that a wireless network is available. In this example, the customer possesses a promotion code to use for account establishment, and proceeds by clicking **Connect**.

2. The customer authenticates as guest

Wireless auto configuration uses 802.1X and PEAP guest authentication to connect to the WISP network through the access point, automatically passing a null user name and a blank password to the WISP IAS server. The access point is connected to a VLAN-aware gateway device that allows traffic from the client to pass through the Network Resource VLAN, but blocks the client from access to the Internet VLAN.

The IAS server is the PEAP authenticator and TLS endpoint for customers who connect as guest. The TLS tunnel is created between the wireless client and the IAS server. All subsequent messages between wireless client and IAS server pass through this tunnel, which traverses the access point and the gateway device.

Server authentication is performed when the IAS server verifies its identity to the client computer using a certificate that contains the Server Authentication purpose in Enhanced Key Usage (EKU) extensions. This certificate is issued by a public CA that the client computer trusts.

The IAS server authenticates and authorizes the customer as guest. In the Access-Challenge message that the IAS server sends to the client is a URL PEAP-TLV attribute. The URL PEAP-TLV message contains the URL of the provisioning server. This URL provides the client with the location of the XML master file.

The wireless client computer receives an IP address lease from the DHCP server. The address is from an IP address range configured in a scope on the DHCP server. In addition to the IP address, the client receives DHCP options, such as a default gateway and a DNS server IP address.

3. The client is provisioned and the customer creates an account

The XML master file on the provisioning server contains pointers to the XML subfiles. The wireless client creates an HTTPS connection with the provisioning server and downloads the XML master file and subfiles. When the XML sign-up file is downloaded, the sign-up wizard is started on the wireless client to allow the customer to create and pay for an account with the WISP.

Using the sign-up wizard on the wireless client computer, the customer steps through the process of signing up for an account. The customer enters the promotion code as well as personal data such as name, address, and credit card number. The data entered by the customer is converted into an XML document.

The XML document containing the customer’s sign-up data is sent to the Web application on the WISP provisioning server.

The Web application checks the promotion code entered by the user against the promotion code database on the SQL server. If the promotion code is valid, the Web application continues processing the customer’s data.

The Web application processes the customer payment information. After payment is verified and sign-up information is completed successfully, the Web application reads the domain and security group information from the promotion code database on the SQL server and creates a user account in Active Directory and adds the account to the security group. The Web application also enters the new user name in the promotion code database.

An XML document containing the new account credentials is sent from the WISP provisioning server to the client computer. The client computer uses the credentials to configure wireless auto configuration and 802.1X under the name of the WISP.

4. The customer is authenticated with the new account credentials

Wireless auto configuration restarts the association to the SSID for the WISP.

Wireless auto configuration finds the correct 802.11 profile, which was downloaded with the other WISP information. Wireless auto configuration re-associates with the access point using the correct profile.

802.1X restarts the authentication process using PEAP-MS-CHAP v2 and the new account credentials.

As the client starts the authentication process with PEAP-MS-CHAP v2 authentication, a TLS channel is created between the customer's client computer and the WISP IAS server.

In the second stage of PEAP-MS-CHAP v2 authentication, the WISP IAS server authenticates and authorizes the connection request against the new account in the Active Directory user accounts database. The IAS server sends an Access-Accept message to the access point. Included in the Access-Accept message are attributes that specify which VLAN the customer can access.

5. The customer is switched to a VLAN that provides Internet access

The access point instructs the gateway device to assign the client to the Internet VLAN rather than the Network Resource VLAN. In addition, 802.1X on the access point opens the virtual port to provide Internet access to the client.

The wireless client computer receives an IP address lease from the DHCP server. The address is from an IP address range configured in a scope on the DHCP server. In addition to the IP address, the client receives DHCP options, such as a default gateway and a DNS server IP address.

The wireless client computer can now access the Internet.

How IAS handles an expired account

You can determine the types of account plans that you want to offer your customers. These plans can range from fees based on hourly use to accounts with life spans as long as a day, a month, or longer.

It is important for IAS to determine whether a connecting or connected client computer has a valid account, and to take the appropriate action if the customer's account is expired. The following example illustrates how IAS determines that a 24-hour account is current and how WPS technology behaves when the account expires.

Twenty-four hour connect option example

When the customer arrives at the WISP, the customer chooses an access account that has a one-day (24-hour) lifespan. The customer and client computer proceed through the account creation process described above, and then connect to the Internet. The following process occurs:

1. In the Access-Accept message sent by the IAS server, the IAS server sets a session timeout of 60 minutes for the client computer connection to the access point.
2. After 60 minutes, the access point requests that the client reauthenticate. The

client reauthenticates successfully and the customer's session is not interrupted.

3. Each 60 minutes thereafter, the access point requests that the client reauthenticate. During each authentication the IAS server checks the current time against the expiry time for the user account to discover whether the customer is authorized to access the network.
4. On the last re-authentication, at hour 23 in the account lifespan and before 24 hours have passed, the IAS authorization check fails and the IAS server sends a URL PEAP-TLV message to the client that contains the account renewal action parameter and an HTTPS URL for an XML master file. The URL PEAP-TLV supplies the customer with the location of the provisioning server where the customer can renew the account.
5. Upon receiving the URL in the URL PEAP-TLV message, 802.1X requests that Windows XP display the account renewal application to the customer.
6. The customer renews the account and 802.1X initiates authentication using the new account credentials.
7. During authentication with the IAS server, the IAS server authenticates and authorizes the customer against the user accounts database, and sends an Access-Accept message containing a session timeout of 60 minutes to the access point.
8. During this process, because the account has not expired, the customer maintains connection to the Internet.

If the customer does not complete the renewal process before the 24-hour account lifespan is reached, authentication fails and customer access to the Internet is terminated. When authentication fails, Windows XP attempts authentication as guest. The VLAN-aware gateway device is configured to allow the connection to the Network Resource VLAN, and the customer is provided with the option of renewing the account for continued access.

How to deploy WPS technology with VLANs

In the set of instructions that follow, these assumptions are made:

1. The computer functioning as your IAS/RADIUS server has Windows Server 2003 with SP1 installed, and the **EnableWPSCompatibility** registry key is enabled according to the instructions in ”Configuring IAS for WPS technology” in this paper.
2. Client computers are running Windows XP Home Edition with SP2; Windows XP Professional with SP2; or Windows XP Tablet PC Edition with SP2.
3. All of your hardware, including the VLAN-aware gateway device and VLAN-aware wireless access points, meet all of the technical requirements stated in “Components of WPS technology with VLANs” in this paper.
4. You have already deployed a computer running SQL Server 2000 or a third-party database program on your network. For information about SQL Server 2000, see SQL Server at http://go.microsoft.com/fwlink/?LinkId=20014.
5. You have SQL Server 2000 or third-party relational database development experience and you understand how to use SQL Server 2000 or a third-party database program to create, modify, administer, and manage your databases.
6. You have experience deploying an Internet Information Services (IIS) or third-

party Web server with HTTPS. If you are deploying IIS, you understand how to use Active Server Pages (ASP), and you can develop applications using Microsoft .NET Framework 1.1.

7. You have software development experience that allows you to create your custom Web application that will be installed and run on the provisioning server.
8. You have software development experience that allows you to create an IAS extension DLL.

> **Note**
>
> The instructions that follow use four servers upon which various programs and services are installed. If you deploy WPS technology in a test lab, you can reduce or increase the number of servers in a manner appropriate to your available hardware resources. For example, in a test lab environment you might want to deploy Active Directory, IAS, IIS, and DHCP on the same server.

To deploy WPS technology with VLANs, the basic steps are as follows:

1. Configure the domain controller and IAS server
2. Configure the DHCP server
3. Install and configure your VLAN-aware gateway device
4. Install and configure your wireless access points
5. Configure RADIUS clients in IAS
6. Create your Web application
7. Configure the provisioning server
8. Configure XML master and subfiles
9. Configure the database on the SQL server
10. Configure the Windows XP–based client computer
11. Configure certificates in a test lab environment (optional)

Configure the domain controller and IAS server

Install Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1 on a computer that meets or exceeds the minimum hardware requirements for the respective operating system. After the operating system is installed, you can perform General configuration, Active Directory configuration, IAS configuration, and IAS extension DLL & URL PEAP-TLV configuration.

General configuration

1. Assign the server a static IP address. Determine the IP address range for the WISP LAN, and determine how many devices need static IP addresses from that range. For example, the domain controller and IAS server must have a static IP address, and it is generally a good idea to provide static IP addresses to other key servers, such as the DHCP server and WISP provisioning server. IP addresses that are statically assigned are excluded from distribution by a DHCP server through definition of an exclusion range on the DHCP server. The exclusion range falls at the beginning of the IP address range, so choose one of the addresses from the beginning of the range that you plan on excluding when you configure DHCP, and assign it to the domain controller by using Network Connections. For more information, see “To configure TCP/IP for static addressing.” At http://go.microsoft.com/fwlink/?LinkId=20015.

2. Install a server certificate obtained from a public trusted root certification authority, such as a certificate from Verisign.
   For more information, see "Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication" at http://go.microsoft.com/fwlink/?LinkId=33675.
   When you obtain the certificate, it must conform to the minimum server certificate requirements described earlier in this paper.
   For more information, see "Network access authentication and certificates" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20016.

> **Note**
>
> If you are deploying WPS technology in a test lab environment, you can install a private CA rather than obtain certificates from a public CA. For more information, see "Configure certificates in a test lab environment (optional)" in this paper.

Active Directory configuration

1. Install Active Directory and DNS. To install Active Directory, open Command Prompt, type **dcpromo**, and then follow the instructions provided in the wizard, entering your network configuration information in the wizard as you progress.
2. Design and create your security groups. When users sign up and create an account, your Web application adds the new user account as the member of a security group that you create in this step. The Web application chooses group membership based on the value of the security group field in the promotion code database on your SQL Server, so you need to match the security group you create to the security group field in the SQL server database. If you have the need for multiple security groups, you can assign permissions to each group individually. For more information, see "To create a new group" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20018 and "Assign user rights to a group in Active Directory" at http://go.microsoft.com/fwlink/?LinkId=20019.

> **Important**
>
> The security groups you create in Active Directory are named and used in the SQL Server database and in IAS remote access policy.

3. Enable the Guest account in Active Directory. If guest access is not enabled in Active Directory, new customers cannot access your provisioning server by authenticating as guest. To enable the Guest account, open the Active Directory Users and Computers snap-in, and then double-click **Users**. Right-click the account named **Guest**, and then click **Enable Account**.

To perform the next procedure, you must be a member of either the Domain Admins group in the domain for which you want to raise functionality or the Enterprise Admins group in Active Directory; or you must have been delegated the appropriate authority.

Raise the domain functional level to either Windows 2000 native or Windows Server 2003 by doing the following:

1. Open the Active Directory Domains and Trusts snap-in. Click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.

2. In the console tree, right-click the domain for which you want to raise functionality, and then click **Raise Domain Functional Level**.
3. In Select an available domain functional level, do one of the following:
   a. To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
   b. To raise domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.

> **Important**
>
> If you have or will have any domain controllers running Windows NT 4.0 and earlier, then do not raise the domain functional level to Windows 2000 native. After the domain functional level is set to Windows 2000 native, it cannot be changed back to Windows 2000 mixed.
>
> Likewise, if you have or will have any domain controllers running Windows NT 4.0 and earlier or Windows 2000, then do not raise the domain functional level to Windows Server 2003. After the domain functional level is set to Windows Server 2003, it cannot be changed back to Windows 2000 mixed or Windows 2000 native.

The current domain functional level is displayed under **Current domain functional level** in the **Raise Domain Functional Level** dialog box.

For more information, see "Domain and forest functionality" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?linkid=30600.

For information about configuring Active Directory replication, see "Active Directory replication" in this paper.

IAS configuration

For IAS, the three configuration stages are General configuration, Remote access policy configuration, and Connection request policy configuration. (RADIUS client configuration occurs later in the overall WISP deployment process.)

General configuration

1. Install Internet Authentication Service.
   For more information, see "To install IAS" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20028.
2. Register IAS in Active Directory. In order for IAS to have permission to read user accounts in Active Directory, IAS must be registered in Active Directory. For more information, see "To enable the IAS server to read user accounts in Active Directory" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20030.
3. Delete the default remote access policies. To delete the policies, open the IAS console, and then click **Remote Access Policies**. Select each existing policy, right-click the policy, and then click **Delete**.
4. Create your IAS extension DLL. For more information, see "How to create an IAS extension DLL and a URL PEAP-TLV" in this paper.
5. Install the DLL on your IAS server and configure DLL registry keys according to your needs.
   To install your DLL, do the following:
   - Open Command Prompt and change directories to the folder that contains your DLL.

- Type the following: **regsvr32** *DLL_name.dll*, where *DLL_name.dll* is the name of your DLL file.

Remote access policy configuration

There are two remote access policies configured for WPS technology. The Guest access policy provides network parameters and rules for users connecting as guest. The Valid Users access policy provides network parameters and rules for users who have valid WISP accounts.

> **Note**
>
> If you have a variety of account types that you offer to customers and these accounts have different properties (such as membership to different security groups), you might find it necessary to create more than two remote access policies on your IAS server. If this is the case, you can use the remote access policies described below to extrapolate how to create additional policies.

To configure the Guest access policy

1. Open the Internet Authentication Service console and, if necessary, double-click Internet Authentication Service.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Use the **New Remote Access Policy Wizard** to create a policy. For the WISP guest access policy, you can choose the following:
   a. For **How do you want to set up this policy?** select **Use the wizard to set up a typical policy for a common scenario**.
   b. For **Policy name**, type **Guest access** (or type another name for your policy that you prefer).
   c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
   d. For **Grant access based on the following,** click **User**.
   e. In **Select the EAP type for this policy**, select **Protected EAP (PEAP)**, and then click **Configure**.
   f. In **Certificate issued**, select the certificate that you want the IAS server to use to verify its identity to client computers. Also select the **Enable Fast Reconnect** check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration.

1. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created. Make the following configuration changes to the policy:
2. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
3. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
4. In the policy Properties dialog box, click **Grant remote access permission**.
5. Click **Edit Profile**. On the **Authentication** tab, in **Unauthenticated access**, click **Allow clients to connect without negotiating an authentication method**.

To configure the Valid Users access policy

1. Open the Internet Authentication Service snap-in and, if necessary,

double-click **Internet Authentication Service**.

2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Use the **New Remote Access Policy Wizard** to create a policy. For the WISP Valid users access policy, you can choose the following:
   a. For **How do you want to set up this policy?** verify that **Use the wizard to set up a typical policy for a common scenario** is selected.
   b. For **Policy name**, type **Valid Users** (or type another name for your policy that you prefer).
   c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
   d. For **Grant access based on the following,** click **Group,** and then click **Add**. In **Enter the object name to select**, type the name of a security group that you defined when configuring Active Directory. For example, if you created a group named Valid Users, type **Valid Users**, and then click **OK**.

| | Impor | The following three items must match: the name of the security group in Active Directory, the value of the **security group** field in the SQL Server database, and the name of the security group configured in the Valid Users access policy in IAS. The Web application uses the value of the SQL Server database **security group** field to determine group membership for new accounts.

   e. In **Select the EAP type for this policy**, select **Protected EAP (PEAP)**, and then click **Configure**.
   f. In **Certificate issued**, select the certificate that you want the IAS server to use to verify its identity to client computers. Also check the **Enable Fast Reconnect** check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration.

1. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created. Make the following configuration changes to the policy:
2. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
3. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
4. In the policy Properties dialog box, click Grant remote access permission.
5. Click **Edit Profile**, and then click the **Advanced** tab. By default, the **Service-Type** attribute appears in **Attributes** with a value of **Framed**. To specify additional connection attributes required for WPS technology with VLANs, click **Add**, and then add the following attributes:
   - **Framed-Protocol**. Value: **PPP**
   - **Tunnel-Medium-Type**. Value: **802 (Includes all 802 media plus Ethernet canonical format)**
   - **Tunnel-Pvt-Group-ID**. Value: Enter the integer that represents the VLAN number for the Internet VLAN. For example, if your access controller's Internet VLAN is VLAN 4, type **4**.
   - **Tunnel-Type**. Value: **Virtual LANs (VLAN)**

- **Tunnel-Tag**. Value: Obtain this value from your hardware documentation

> **Important**
>
> IAS evaluates remote access policies in the order in which they appear in the IAS console under **Remote Access Policies**. The Valid Users access policy must be the first policy in the list of remote access policies or valid user authentication will fail. Because IAS places newly created policies in the first position and the Valid Users access policy was the last policy created, the Valid Users access policy should now appear first in the IAS console, with the Guest access policy appearing second. If this is not the case, move the Valid Users access policy into first position.

Connection request policy configuration

By default, there is one connection request policy predefined in the IAS console, called **Use Windows authentication for all users**. This policy can be used for WPS technology.

1. In the IAS console, double-click **Connection Request Processing**, click Connection Request Policies, and then double-click the policy **Use Windows authentication for all users**.
2. Click **Edit Profile**. The **Edit Profile** dialog box opens.
3. On the **Authentication** tab, click **Authenticate requests on this server**, and then check the **Protected EAP** check box.
4. Click **Configure Certificate**. Select the certificate you want IAS to use to authenticate to clients, and then click **OK** three times to close all dialog boxes and return to the IAS console.

> **Note**
>
> If you access the profile of a connection request policy in the IAS console and you cannot see the **Protected EAP** check box or the **Configure Certificate** button, you must first configure IAS for compatibility with WPS technology as described in "Configuring IAS for WPS technology" in this paper.

Configure the DHCP server

On a computer running Windows Server 2003:

1. Install DHCP.
   For more information, see "To install a DHCP server" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20034.
2. In the DHCP console, run **New Scope Wizard** twice. Create two VLAN scopes from which IP addresses will be leased to wireless clients connected to the VLANs. Each scope must define a different IP address range using either a private address range or a public IP address range. If you are using network address translation (NAT), you can use a private IP address range; otherwise, the IP addresses leased to wireless clients must be from a public IP address range.
   For more information, see "To create a new scope" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20123.
3. While running New Scope Wizard, create an exclusion range for the IP addresses you will be assigning statically. For example, if you need to statically assign 10 IP addresses from the address range 10.1.1.1 through

10.1.1.254, your exclusion range is defined as 10.1.1.1 through 10.1.1.10.

4. While running New Scope Wizard, assign scope options. On the **Configure DHCP Options** page, select **Yes, I want to configure these options now**. Scope options are applied only to leases of addresses from within the IP address range that the scope defines, which provides flexibility as your network grows. Define the **DNS server** and **Domain name** options, as well as any other options that are appropriate for your network configuration.
5. While running New Scope Wizard, activate the scope. The option to activate the scope while running the wizard is available only if you have chosen to configure DHCP scope options in the previous steps.
   For more information, see "To activate a scope" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20124.
6. Authorize the DHCP server in Active Directory.
   For more information, see "To authorize a DHCP server in Active Directory" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20125.

The DHCP server is now online and able to provide IP address leases to client computers. In some cases you might want to examine the types and durations of accounts you offer your customers and adjust the DHCP lease duration accordingly. In most cases when deploying WPS technology, the default lease duration of eight days is too long and should be shortened considerably.

DHCP example

In this example, you are creating two VLANs and two scopes, one scope for each VLAN.

VLAN 2

VLAN 2 is the Network Resource VLAN that provides access to network resources (such as the IAS server and DHCP server) for wireless computers connecting as guest. VLAN 2 blocks access to the Internet, however. The DHCP scope for VLAN 2 is defined with the following example parameters:

- **Address range:** 192.168.1.1 through 192.168.1.254. This is a private IP address range. If you are using NAT, you can use this range on your network. If you are not using NAT, use a public IP address range. In addition, if your wireless deployment is large, select an IP address range that provides more IP addresses for lease to clients.
- **Exclusion range:** 192.168.1.1 through 192.168.1.10. By using this exclusion range, the available address pool for clients is 192.168.1.11 through 192.168.1.254. Ten IP addresses are excluded so that you can statically assign these addresses to computers and devices on your network. For example, the router IP address must be statically assigned on the router.
- **DHCP scope option 003, Router:** 192.168.1.1. The router IP address must be an address that falls within the exclusion range so that the DHCP server does not lease the router IP address to a wireless client computer, thereby creating an address conflict.
- **DHCP scope option 006, DNS server:** the IP address of the Active Directory and DNS server on the WISP LAN.

Note that DHCP scope option 003, Router, provides client computers with the IP address of their default gateway IP address. In this case, the default gateway for wireless clients is the VLAN-aware gateway device, whether it is an access controller, a VLAN-aware router, a VLAN-aware switch, or another compatible device. When you configure your VLAN-aware gateway device, you can specify the IP address that the device uses for each VLAN.

In this example, you must configure the VLAN-aware gateway device so that it uses the IP address 192.168.1.1 on VLAN 2.

For your WPS deployment you can configure additional DHCP options as needed. For example, if you are using a WINS server, you can configure your VLAN scopes with DHCP option 044, WINS/NBNS Servers.

VLAN 4

VLAN 4 is the Internet VLAN that provides access to the Internet. Users who have successfully created an account are switched to this VLAN after completing the provisioning and sign-up process. The DHCP scope for VLAN 4 is defined with the following example parameters:

- **Address range:** 192.168.2.1 through 192.168.2.254
- **Exclusion range:** 192.168.2.1 through 192.168.2.10
- **DHCP scope option 003, Router:** 192.168.2.1. The router IP address must be an address that falls within the exclusion range so that the DHCP server does not lease the router IP address to a wireless client computer, thereby creating an address conflict.
- **DHCP scope option 006, DNS server:** the IP address of the Active Directory and DNS server on the WISP LAN.

For VLAN 4 in this example, you must configure the VLAN-aware gateway device so that it uses the IP address 192.168.2.1 on VLAN 4.

Install and configure your VLAN-aware gateway device

Configure two VLANs on the gateway device: a Network Resource VLAN that provides access to the WISP LAN, and an Internet VLAN that provides access to the Internet.

The remote access policies you create in IAS determine which VLAN your customers can access:

- The Guest access policy places users on the Network Resource VLAN so that they can create and pay for a valid user account.
- The Valid Users access policy in IAS places customers on the Internet VLAN.

Each VLAN has a different IP address range. When configuring your DHCP server, you created a scope for each VLAN, and you defined DHCP scope option 003, Router. This is the IP address commonly referred to as the “default gateway.” You must configure the VLAN-aware gateway device as the default gateway for each VLAN, using an IP address from the IP address range that you defined on your DHCP server.

Choosing the IP address for the default gateway for each VLAN

Your VLAN-aware gateway device is the default gateway for both VLANs and is configured with a different IP address for each VLAN.

After you define an IP address range for a VLAN on your DHCP server, you can use any IP address from that range as the IP address for the default gateway. To prevent an IP address conflict, however, exclude some IP addresses from the range for use by devices that you want to configure with a static IP address. When you create an exclusion range for an IP address range, the DHCP server does not lease IP addresses from the exclusion range to DHCP clients.

> **Note**
>
> IP address conflicts occur when two devices or computers on the same subnet have the same IP address. This situation can occur if you configure a device or computer with a static IP address that is also an address that the DHCP server can lease to DHCP clients.

Thus ensure that you assign an IP address from the exclusion range as the IP address for the default gateway. The address you use does not need to be the first address in the exclusion range, but it must be an address contained within the exclusion range.

In accordance with the example provided in the DHCP configuration section of this paper, configure the VLAN-aware gateway device so that it uses an IP address from the exclusion range 192.168.1.1 through 192.168.1.10 for VLAN 2. For example, you can configure the VLAN-aware gateway device so that it uses the IP address 192.168.1.1 on VLAN 2.

> **Important**
>
> In each scope you configure on the DHCP server, the value you enter for DHCP scope option 003, Router, must match the IP address you assign to the VLAN-aware gateway device for use on each VLAN. For example, if you configure a scope on the DHCP server for VLAN 2 with the IP address range 192.168.1.1 through 192.168.1.254, and you assign the DHCP scope option 003, Router, with the value 192.168.1.1, you must configure the VLAN-aware gateway device to use the IP address 192.168.1.1 on VLAN 2.

Similarly, as described in “Configure the DHCP server” in this paper, configure the VLAN-aware gateway device so that it uses an IP address from the exclusion range 192.168.2.1 through 192.168.2.10 for VLAN 4. For example, you can configure the VLAN-aware gateway device so that it uses the IP address 192.168.2.1 on VLAN 4.

In some circumstances you might prefer to use your VLAN-aware gateway device as the DHCP server for each VLAN. If this is the case, you must define IP address ranges and exclusion ranges on the VLAN-aware gateway device rather than on a DHCP server.

See the product documentation for your VLAN-aware gateway device for information about configuring your hardware.

> **Important**
>
> The Internet VLAN integer must match the value you configure for the Tunnel-Pvt-Group-ID attribute in the Valid Users access policy on your IAS server. For example, if VLAN 4 leads to the Internet, the value of the Tunnel-Pvt-Group-ID attribute in the profile of the Valid Users access policy must be 4.

Install and configure your wireless access points

Following is an example of how to configure your wireless access points for use with WPS technology. This example depicts configuration of a Cisco 802.1X–compatible access point. If you use a different 802.1X–compatible access point, follow the directions in your product documentation and in “Using other access points” in this paper.

The Cisco access point used in this example provides a Web-based interface for access point configuration. To use this interface for access point configuration, you must physically connect the access point to the network, log on to a computer that has

network connectivity to the access point, and then open a Web browser, such as Microsoft® Internet Explorer.
Type the IP address for your 802.1X–compatible access point in the Web browser address bar, and then press ENTER. The access point configuration page appears in the Web browser.

To configure your wireless access point

1. On the configuration page, click the **Setup** tab, and then click **Express Setup**.
2. In the **Radio Service Set ID (SSID)** field, type an SSID for the access point, and then click **OK**.
3. Under **Services**, click **Security**, and then click **Radio Data Encryption (WEP)**.
4. On the **AP Radio Data Encryption** page, select the **Open** check boxes for the **Accept Authentication Type** and the **Require EAP** options, and then clear all other check boxes.
5. In the **Encryption Key** box, type a 32-digit WEP key. In the **Key Size** list, select **128 bit**, and then, to update the page, click **Apply**.
6. In the **Use of Data Encryption by Station is** list, select **Full Encryption**, and then click **OK**.
7. On the **Security Setup** page, click **Authentication Server**. The following table shows the values to set on the **Authenticator Configuration** page.

Item	Value
802.1X Protocol Version (for EAP Authentication)	Draft 10
Server Name/IP	IAS server IP address
Server Type	RADIUS
Port	1812
Shared Secret	Type the shared secret you want to use for RADIUS clients
Timeout (in seconds)	20
User server for	EAP Authentication

8. When you have completed the configuration of the authentication server, click **OK**.

Using other access points

If you are using an access point (AP) other than Cisco, follow the directions in your access point documentation using the following guidelines:

- **Authentication or RADIUS server**: Specify your IAS server by IP address or FQDN, depending on the requirements of the AP.
- **SSID**: Specify a Secure Set Identifier (SSID), which is an alphanumeric string that serves as the network name. This name is broadcast by APs to wireless clients and is visible to users at your Wi-Fi hotspots.
- **RADIUS settings**: Use RADIUS authentication on User Datagram Protocol (UDP) port 1812 and use RADIUS accounting on UDP port 1813.
- **Secret or shared secret**: Use a strong shared secret and configure the IAS server with the same shared secret.
- **EAP**: Configure the AP to require EAP from wireless clients.
- **802.1X and WEP**: Enable IEEE 802.1X authentication and WEP.

Note

Make sure that you use a strong shared secret. For more information about how to create a strong shared secret, see "Shared secrets" in Windows Server 2003 Help and Support Center or on the Web at http://go.microsoft.com/fwlink/?LinkId=41035.

Configure RADIUS clients in IAS

In the IAS console, add each access point on your network as a RADIUS client. In addition, configure the shared secret used between the access points and the IAS server. For more information, see "To add RADIUS clients" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20031 and "To configure the Message Authenticator attribute and shared secret" at http://go.microsoft.com/fwlink/?LinkId=20032.

Configuring RADIUS clients by IP address range

If your IAS server is running Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, you can configure RADIUS clients by IP address range. This is a useful feature when you have a large number of access points to deploy; if you deploy your access points on the same subnet or VLAN within the same IP address range, configuration of RADIUS clients in IAS is simplified. Instead of individually configuring each access point as a RADIUS client in IAS, you can configure all access points at once using the IP address range of the subnet or VLAN upon which the APs reside. In this circumstance, use the same shared secret for all access points, and make sure that the shared secret is strong.

By contrast, you can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. With Windows Server 2003, Standard Edition, if the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query. With IAS in Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients.

Create your Web application

Your Web application must be capable of performing the following functions:

- Communicating with Wireless Provisioning Services using HTTPS.
- Uploading XML master file and subfiles that are stored on the provisioning server to client computers that request the files.
- Accepting and processing XML documents from client computers that contain customer data, such as promotion code, customer name, customer address, and other information.
- Accepting and processing XML documents from client computers that contain credit card information. This includes verifying the credit card and charging the customer account.
- Reading the promotion code database records to validate promotion codes.
- Reading the promotion code database records to determine the domain in which to create a new user account.

- Reading the promotion code database records to determine the security group membership for a new user account.
- Writing a user name to the user name field in the promotion code database.
- Dynamically creating new accounts in Active Directory (or a third-party LDAP-compliant database) using data provided by customers as well as parameters from the promotion code database.

It is recommended that the design of your Web application provides customers with knowledge of their user name and password. Customers can either be allowed to designate their own user name and password or this information can be provided to them upon completion of the sign-up wizard. Following are some circumstances where customers need to know their password-based credentials:

- For a variety of reasons, user authentication might fail. For example, cached credentials might get corrupted or network connectivity issues might prevent wireless client computers from successfully authenticating.
- The user account expires and the customer wants to renew their account. In this circumstance, IAS sends a URL PEAP-TLV to the wireless client that contains the renewal action parameter and the URL of the provisioning server. After the wireless client is directed to your account renewal application, the customer must have their password-based credentials to renew their account.

If your customers know their user name and password, they can attempt to connect to your network until they are successful. If they do not have this information, they cannot fix the problem without calling your help desk.

You can create your Web application with the Microsoft .NET Framework 1.1 or with other application development software. If you want to create your Web application with the .NET Framework 1.1, you need the Microsoft .NET Framework 1.1 Software Development Kit.

Microsoft .NET Framework 1.1 Software Development Kit

Microsoft .NET Framework 1.1 Software Development Kit (SDK) includes .NET Framework 1.1, as well as everything you need to write, build, test, and deploy applications using .NET Framework 1.1. This includes documentation, samples, command-line tools, and compilers.

If you have already installed Microsoft® Visual Studio® .NET, you do not need to install .NET Framework 1.1 SDK separately; Visual Studio .NET includes the SDK.

If you want to distribute .NET Framework 1.1 with your application, download .NET Framework 1.1 Redistributable in addition to the SDK.

You can get .NET Framework 1.1 SDK from the Download Center at http://go.microsoft.com/fwlink/?LinkId=17161. You can run .NET Framework 1.1 SDK on the following platforms:

- Windows Server 2003
- Microsoft Windows 2000 (Service Pack 2 is recommended)
- Windows XP Professional or Windows XP Home Edition (Windows XP Professional is required to run ASP.NET)

Configure the provisioning server

For the provisioning server, if you are using Internet Information Services (IIS), do the following:

1. Install Internet Information Services and ASP.NET.
   For more information, see “To install Internet Information Services (IIS) 6.0” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20033.
2. Verify that you have .NET Framework 1.1 installed by clicking **Start** on your Windows desktop, selecting **Control Panel**, and then double-clicking the **Add or Remove Programs** icon. When that window appears, scroll through the list of applications. If you see Microsoft .NET Framework 1.1 listed, the latest version is already installed and you do not need to install it again.
   a. If Microsoft .NET Framework 1.1 is already installed: register ASP.NET with Microsoft .NET Framework 1.1 by running the following command at Command Prompt:
   %WINDIR%\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe –I
   b. If Microsoft .NET Framework 1.1 is not installed: Install .NET Framework 1.1. You can install .NET Framework 1.1 through Microsoft Windows Update at http://go.microsoft.com/fwlink/?LinkId=284 or you can see the MSDN topic “How to Get the .NET Framework 1.1” at http://go.microsoft.com/fwlink/?LinkId=30841.
3. Create two folders in the Web server root location %systemroot%\Inetpub\wwwroot. You can use one folder to hold your custom Web application and one folder to hold the XML master and subfiles that you will be creating in later steps. For example, you can create a folder named **wpsdeploy** (%systemroot%\Inetpub\wwwroot\wpsdeploy) to contain your Web application, and you can create a folder named **wpsfiles** (%systemroot%\Inetpub\wwwroot\wpsfiles) to contain your XML files.
4. Install your Web application into the folder you created for the Web application files.
5. Set user permissions for the Web application. Open Windows Explorer and browse to the location where you installed your Web application. For example, if you named your folder wpsdeploy, browse to %systemroot%\Inetpub\wwwroot\wpsdeploy. Right-click the wpsdeploy folder, and then click **Sharing and Security**. On the **Security** tab, click **Add**. In **Enter the object names to select**, type **Everyone**, and then click **OK**. In **Permissions for Everyone**, enable **Write** permissions by checking the **Allow** check box.
6. Enable HTTPS. You must configure IIS to use a certificate for secure Web communications between the provisioning server and clients. To enable HTTPS you must install a server certificate obtained from a public trusted root certification authority, such as a certificate from Verisign or Thawte. When you obtain the certificate, it must conform to the minimum server certificate requirements described in this paper.
   For more information, see “Network access authentication and certificates” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20016.
   To enable Secure Sockets Layer (SSL) and HTTPS, complete the following procedures.

Note

If you are deploying a certification authority in a test lab environment, you must install and configure the CA before completing the following procedures.

To obtain a new server certificate using Web Server Certificate Wizard

1. In **IIS Manager**, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In **Web Server Certificate Wizard**, click **Create a new certificate**.
5. Complete **Web Server Certificate Wizard**, which will guide you through the process of requesting a new server certificate.

To install a server certificate using Web Server Certificate Wizard

1. In **IIS Manager**, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In **Web Server Certificate Wizard**, click **Assign an existing certificate**.
5. Complete **Web Server Certificate Wizard**, which will guide you through the process of installing a server certificate.

Note

The Web Server Certificate Wizard always denotes this step as "assigning" a certificate to a resource (such as a file, directory, or site), not as "installing."

Configure XML master and subfiles

There are two methods you can use to create and configure your XML master and subfiles:

- Use the WPS Authoring Tool to create a WPS project and publish your XML files. The WPS Authoring Tool has a graphical user interface and is designed to assist you in accurately producing and managing a collection of XML files for your WPS solution. For more information, see "Using the WPS Authoring Tool" at http://go.microsoft.com/fwlink/?LinkId=41067. Using the WPS Authoring Tool to create your XML data files is recommended. You can download the WPS Authoring Tool at http://go.microsoft.com/fwlink/?LinkId=40535.
- Use the XML schemas provided in this paper to create your files. After you have created these files, you can enter information specific to your network and deployment parameters. For example, where the location of the provisioning server is required, you can provide an HTTPS URL. In another example, you may need to enter your domain name in several places; you can examine the schemas and example files and determine where to insert your domain name.

When your XML files are configured with the information for your organization, you can store them on your provisioning server and configure your Web application so that it can find the files when necessary. If you are using Internet Information Services as your Web server, you can install the files at the location *%systemroot%* \inetpub\wwwroot.

Configure the database on the SQL server

On the computer running SQL Server 2000 or a third-party product with similar functionality, create a promotion code database with the following fields, using the appropriate data type for each field:

- **Promotion code.** This field contains promotion codes that you distribute publicly to potential customers. When customers sign up for an account, they provide the promotion code that is matched by the Web application to a value in this field in the database.
- **User name.** This field has no value assigned until a customer creates an account. At this time, the Web application assigns a value to this field.
- **Domain name.** This field contains the domain name where you want the Web application to create the user account when a customer signs up using the promotion code.
- **Security group.** The Web application joins the new user account to the security group defined in this field.
- **Expiration date.** If your promotion lasts for a specific period of time, you can enter the expiration date related to the promotion code in this field. If a user with a promotion code attempts to create an account after the expiration date for the promotion, they cannot do so.

Populate the database with records, providing values for all fields except user name, and enable the data link between your Web application and the SQL server. Also configure security and authentication on the SQL server so that your Web application has permission to access and write to the database. For more information, see SQL Server at http://go.microsoft.com/fwlink/?LinkId=20014.

Important

When you configure values for records in the SQL Server database, the following three items must match: the name of the security group in Active Directory, the value of the **security group** field in the SQL Server database, and the name of the security group configured in the Valid user remote access policy in IAS. The Web application uses the value of the SQL Server database **security group** field to determine group membership for new accounts.

Configure the Windows XP-based client computer

On the computer running Windows XP Professional, Windows XP Tablet PC Edition, or Windows XP Home Edition, install SP2. The computer must have a wireless network adapter compatible with IEEE 802.11 and 802.1X.

Note

If you are deploying WPS technology in a test lab environment where you have deployed your own enterprise root CA, you must import the CA certificate into the Trusted Root Certification Authorities certificate store on the client computer. If this certificate is not imported into the client certificate store, the client computer will not trust the enterprise root CA and server authentication to the client will fail. For more information, see “Configure certificates in a test lab environment (optional)” in this paper.

Configure certificates in a test lab environment (optional)

If you are deploying WPS technology in a test lab, you can obtain server certificates from a public trusted root CA or you can deploy Certificate Services for Windows Server 2003 on your test network. To deploy Certificate Services and enroll certificates to domain member computers (such as the servers on your networks), do the following:

1. On a computer running Windows Server 2003, install Certificate Services.
   For more information, see "To install an enterprise root certification authority" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20035.
2. Add a server certificate template to the certification authority and configure the certification authority to allow computers to request a certificate that is based on the template you create.
   For WPS technology in a test lab environment, you must create a server certificate that will be trusted by client computers. The server certificate must meet the requirements stated in "Server certificate requirements" in this paper. In addition, you must base your certificate on the correct certificate template for the operating system you are running. If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Standard Edition, and your IAS server is a domain member, base your certificate on the Computer certificate template. If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Enterprise Edition, and your IAS server is a domain member, base your certificate on the **RAS and IAS Server** certificate template.
   For more information, see "To create a certificate template" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20036.
3. Autoenroll certificates to domain member computers. Autoenrollment allows domain member computers to automatically obtain, or enroll, certificates. For WPS technology, autoenroll certificates to servers using the certificate template you created in the previous step.
   For more information, see "Planning for autoenrollment deployment" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20037 and "Checklist: Configuring certificate autoenrollment" at http://go.microsoft.com/fwlink/?LinkId=20038.
4. Install the enterprise CA certificate in the Trusted Root Certification Authority certificate store on client computers being used for testing purposes. You can request the enterprise root CA certificate by using Web enrollment services, which is installed with Certificate Services, or you can export the server certificate to a floppy disk, and then import the certificate into the Trusted Root Certification Authority certificate store on the client.
   For more information, see "To export a certificate" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20039 and "To import a certificate" at http://go.microsoft.com/fwlink/?LinkId=20040.

WPS technology for the enterprise

Enterprises can deploy WPS technology to simplify the process of providing Internet access to organization visitors. You can provide business partners and other visitors with promotion codes, which visitors use to gain Internet access through your Wi-Fi hotspots.

In the sections that follow, the components of WPS technology for the enterprise are described, how the components work together during a user sign-up is detailed, and how to deploy WPS technology for the enterprise is explained.

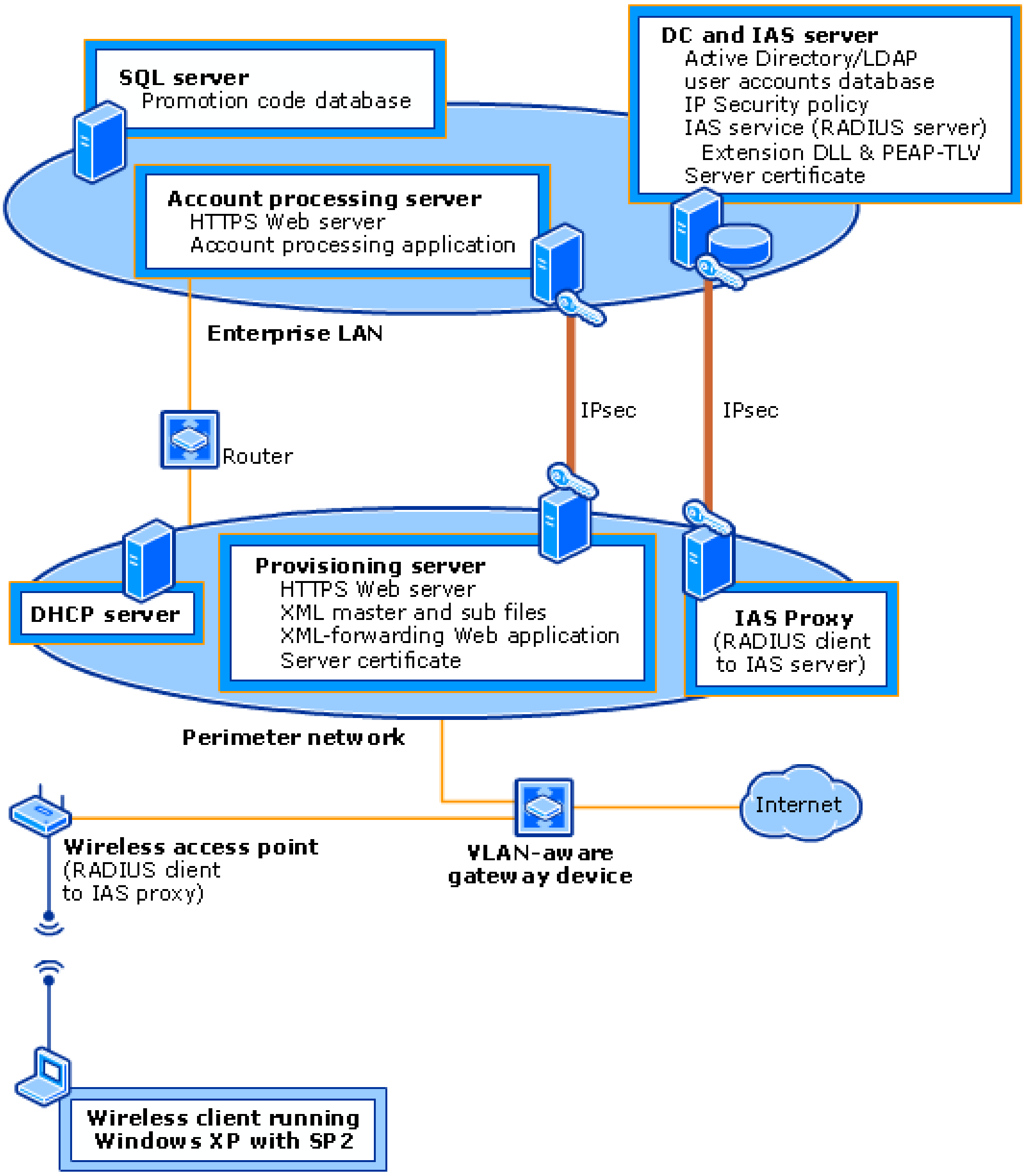
Components of WPS technology for the enterprise

This deployment scenario, designed for the enterprise that deploys Wi-Fi hotspots, has the following features:

- A VLAN-aware gateway device is used for client computer isolation during the account sign-up process.
- Users gain network access by using a promotion code. The codes are stored in a database on a server running SQL Server 2000 or a third-party database application.
- A perimeter network stands between wireless access points and the Enterprise LAN.
- On the perimeter network, an IAS proxy server forwards RADIUS messages between RADIUS clients (access points) and the IAS server on the Enterprise LAN. In addition, IPsec is deployed between the IAS proxy and IAS server to provide security for RADIUS traffic.
- The provisioning server on the perimeter network does not process user information or create accounts in the user account database. The provisioning server on the perimeter network maintains a custom XML-forwarding application that forwards XML files containing customer sign-up information to the account processing application on the account processing server. In addition, IPsec is deployed between the provisioning server and the account processing server on the enterprise LAN to provide security for traffic between the XML-forwarding application and the account processing application.

The account processing server is located on the enterprise LAN. The account processing server verifies promotion codes against the SQL Server database and creates accounts in the user accounts database for business partners or other visitors that have valid promotion codes and access to your Wi-Fi hotspots.

The following illustration depicts the components of an enterprise WISP network using a perimeter network and a VLAN-aware gateway device for client computer isolation.



Components of WPS technology for the enterprise

In the following sections are descriptions of the components of an enterprise WISP network, including components of the WLAN, the perimeter network, and the enterprise LAN.

Wi-Fi hotspot components

Following are the components that comprise the wireless local area network (WLAN), or Wi-Fi hotspot:

Wireless client

A computer running Windows XP Home Edition with SP2, Windows XP Professional with SP2, or Windows XP Tablet PC Edition with SP2. The computer must be equipped with a wireless network adapter that provides support for IEEE standard 802.11, IEEE standard 802.1X authentication, and Wired Equivalent Privacy (WEP). Support for Wi-Fi Protected Access (WPA) is preferred, but not required.

Wireless access point (RADIUS client)

One or more wireless access points deployed with a wired connection to the access controller, VLAN-aware switch or router, or other gateway device.

The wireless access point is configured as a RADIUS client to the Internet Authentication Service (IAS) proxy deployed on the perimeter network. The wireless access points used for WPS technology must have the following required features:

- Support for the use of VLANs.
- Support for the IEEE standard 802.1X authentication.
- Support for Wi-Fi Protected Access (WPA) is preferred.
- Support for RADIUS authentication and RADIUS accounting, including:
  - Support for the Class attribute as defined in RFC 2865, "Remote Authentication Dial-in User Service (RADIUS)," to allow session correlation for RADIUS authentication and accounting records. For session correlation, when you configure RADIUS accounting at your IAS server or proxy, you must log all accounting data that allow applications (such as billing applications) to query the database, correlate related fields, and return a cohesive view of each session in the query results. At a minimum, to provide session correlation, you must log the following IAS accounting data: NAS-IP-Address; NAS-Identifier (you need both NAS-IP-Address and NAS-Identifier because the access server can send either attribute); Class; Acct-Session-Id; Acct-Multi-Session-Id; Packet-Type; Acct-Status-Type; Acct-Interim-Interval; NAS-Port; and Event-Timestamp.
  - Support for accounting interim requests, which are sent periodically by some access servers during a user session, that can be logged. This type of request can be used when the Acct-Interim-Interval RADIUS attribute is configured to support periodic requests in the remote access profile on the IAS server. The access server, in this case a wireless access point, must support the use of accounting interim requests if you want the interim requests to be logged on the IAS server.
  - Support for IP address range filtering.

- Support for dynamic RTO estimation or exponential backoff to handle congestion and delays in a wide area network (WAN) environment.

In addition, there are some filtering features that the access points must support to provide enhanced security for the network. These filtering options include:

- **DHCP filtering**. The access point must filter on IP ports to prevent the transmission of DHCP broadcast messages in the instance that the client is a DHCP server. The access point must block the client from sending IP packets from port 68 to the network.
- **DNS filtering**. The access point must filter on IP ports to prevent a client from performing as a DNS server. The access point must block the client from sending IP packets from port 53 to the network.

Perimeter network components

- Following are the components that comprise the perimeter network.

VLAN-aware gateway device

The VLAN-aware gateway device can be an access controller, a VLAN-aware router, a VLAN-aware switch, or any other device that can be configured to apply IAS-provided parameters to client connections. The VLAN-aware gateway device is configured with two VLANs: a Network Resource VLAN and an Internet VLAN.

The Network Resource VLAN allows all users access to the provisioning server and DHCP server. This VLAN grants access to network resources that allow users to connect to your network as guest, create an account, and receive provisioning information from the provisioning server.

The Internet VLAN provides access to the Internet. Only users who have promotion codes and have created accounts using the sign-up wizard are switched to this VLAN and granted Internet access. This process occurs when Windows XP reauthenticates the user with the newly created account information. When the user is authenticated and authorized by your IAS server, the IAS server returns attributes to the VLAN-aware wireless access point; the access point instructs the VLAN-aware gateway device to route traffic from the client to the Internet VLAN.

IAS proxy

The IAS proxy is running Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1, and is configured with the following components.

Internet Authentication Service

IAS is configured as a proxy to forward RADIUS messages between RADIUS clients, such as access points that are located on the wireless LAN, and the IAS server that is located on the Enterprise LAN.

IPsec

An Active Directory-based IPsec policy provides private, secure communications for RADIUS traffic between the IAS proxy and the IAS server.

Provisioning server

The enterprise provisioning server is configured with the following components.

HTTPS Web server

The Internet Information Services (IIS) or third-party Web server must be deployed with HTTPS.

XML master and subfiles

The enterprise provisioning server stores the XML master and subfiles that provide the client with all configuration information needed to access the network, create an account, and ultimately access the Internet. For more information about the XML master file and subfiles, see "XML schemas" in this paper.

XML-forwarding Web application

The XML-forwarding Web application is a custom program, application, or service that you create and install on your provisioning server. The XML-forwarding application is used to forward XML documents from client computers to the account processing server on the Enterprise LAN. The XML documents are created on client computers when users run the sign-up wizard and enter all required information, such as their name and promotion code. Windows XP packages the information as an XML document, and then sends the document to the provisioning server. The XML-forwarding application then forwards the document to the account processing server.

Server certificate

For server authentication to client computers, the provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, which is trusted by client computers. The trusted root certification authority certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust.

In test lab deployments of WPS technology, you can deploy your own certification authority in lieu of using a public trusted root CA. In this circumstance you must install the private trusted root CA certificate in the Trusted Root Certification Authorities certificate store on all clients. In addition, you must enroll certificates to your provisioning server and IAS server that meet the minimum server certificate requirements. For more information, see "Server Certificate Requirements" in this paper.

IPsec

An Active Directory-based IPsec policy provides private, secure communications for all traffic between the account processing server on the Enterprise LAN and the provisioning server on the perimeter network.

DHCP server

If you do not deploy network address translation (NAT), the DHCP server must be able to assign valid public IP addresses to computers accessing the network through the wireless access points. However, if you deploy NAT, you can assign IP addresses from a private IP address range to wireless client computers.

Router

A router connects the perimeter network and the Enterprise LAN.

Enterprise LAN components

Following are the components that comprise the Enterprise LAN.

Domain controller and IAS server

The enterprise domain controller and IAS server is running Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1, and is configured with the following components.

Active Directory

In this scenario, Active Directory is deployed. The user accounts database on the domain controller must be an Active Directory user accounts database or a database that uses Lightweight Directory Access Protocol (LDAP) and supports dynamic creation of user accounts.

When a user signs up for an account, the account processing Web application on the account processing server creates a new account in the user accounts database, and adds the user to a group that has clearly defined access privileges.

If you use an accounts database other than Active Directory, IAS extensions must be written and installed for this process to function correctly.

IP Security (IPsec) policy

In Active Directory, an IPsec policy for the domain includes the following:

- **IPsec rule for IAS proxy and server**. This rule protects RADIUS traffic between the IAS proxy on the perimeter network and the IAS server on the Enterprise LAN.
- **IPsec rule for HTTPS Web servers**. This rule protects all traffic between the provisioning server on the perimeter network and the account processing server on the Enterprise LAN.

Internet Authentication Service (IAS)

IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server, and is used to authenticate and authorize users connecting to your network. IAS is configured with remote access policies that allow guest authentication for non-domain member computers and users. It is also configured to provide attributes to RADIUS clients (access points) that instruct the gateway device to apply the attributes to client connections.

Protected Extensible Authentication Protocol (PEAP) with MS-CHAP v2 is configured in remote access policies as the authentication method used by clients and server.

Extension DLL and URL PEAP-TLV

AN IAS extension DLL defining a URL PEAP-TLV provides IAS with the ability to send the location of the provisioning server to client computers.

PEAP-Type-Length-Value (PEAP-TLV) is an Extensible Authentication Protocol (EAP) authentication type that allows the IAS server to pass information to client computers attempting to connect to your network.

In this circumstance, the value contained in the PEAP-TLV is an HTTPS Uniform Resource Locator (URL) that provides client computers with the location of the WISP provisioning server. With this URL, Windows XP can download the WISP XML files to the client computer.

In addition to the URL of the provisioning server, the URL PEAP-TLV includes an action parameter. The action parameter directs the client to perform a specific task. The action parameter included in the URL PEAP-TLV defines tasks such as new customer sign-up, existing account renewal, and password change.

For more information, see “How to create an IAS extension DLL and a URL

PEAP-TLV" in this paper.

Server certificate

For server authentication to client computers, the enterprise IAS server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust. If you install IAS and Active Directory on the same computer, the computer must have a certificate. If you install IAS and Active Directory on different computers, only the IAS server needs a certificate.

Account processing server

The account processing server is configured with the following components:

HTTPS Web server

The Internet Information Services (IIS) or third-party Web server must be deployed with HTTPS.

Account processing Web application

The account processing Web server is configured with an account processing Web application that processes data provided during user sign-up or account renewal. The Web application accepts and processes XML documents forwarded from the provisioning server on the perimeter network.

When a user completes the sign-up wizard on a client computer, the user enters data, such as name, organization affiliation, and promotion code, that is converted to an XML document on the client. Windows XP sends this XML document to the provisioning server on the perimeter network, which in turn forwards the XML document to the account processing application.

The account processing application must be capable of accepting and processing the XML documents containing the user data. For example, the account processing application must compare the promotion code entered by the user to a promotion code in the SQL Server database, and then dynamically create an account in the Active Directory user accounts database with the properties (domain and security group membership) described in the database.

IPsec

An Active Directory-based IPsec policy provides private, secure communications for all traffic between the account processing server on the Enterprise LAN and the provisioning server on the perimeter network.

SQL server

A computer running SQL Server 2000 or another SQL-compatible relational database application.

The promotion code database on the SQL server is configured with the following fields: promotion code, user name, domain name, security group, and expiration date. With the exception of the user name field, each field for each record is preconfigured with a value. The value for the user name field is assigned by the Web application when a user creates an account with a promotion code that matches a value in the promotion code field in the database. By predefining the domain in which the user account is created by the Web application and the Active Directory security group to which the user account is joined as a member, you can assign network access and other permissions for your users.

How WPS technology works for the enterprise

The following example describes how the components of a WPS network for the enterprise interact during the connection and account creation process for a new user.

New user connection example

When a new user connects and establishes an account, the following four basic stages occur:

1. The user discovers the network at a Wi-Fi hotspot
2. The user authenticates as guest
3. The client is provisioned and the user establishes an account
4. The user is authenticated using the new account credentials

In the next section we will look at these stages in more detail.

1. The user discovers the network at a Wi-Fi hotspot

When a user arrives at the Wi-Fi hotspot with a portable computer running Windows XP Home Edition with SP2, Windows XP Tablet PC Edition with SP2, or Windows XP Professional with SP2, the computer comes within range of the access point beacon.

Wireless auto configuration on the client computer detects the beacon information from the access point, which is enabled with broadcast Secure Set Identifier (SSID). The SSID is equivalent to the network name.

The user is informed by Windows XP that a wireless network is available. In this example, the user is employed by a business partner of the enterprise, and is provided by the enterprise with a promotion code to use for account establishment. The user proceeds by clicking **Connect**.

2. The user authenticates as guest

Wireless Auto Configuration uses 802.1X and PEAP guest authentication to connect to the enterprise perimeter network through the access point, automatically passing a null user name and a blank password to the IAS proxy, which forwards the message to the IAS server. The access point is connected to a VLAN-aware gateway device that allows traffic from the client to pass through the Network Resource VLAN, but blocks the client from access to the Internet VLAN.

The IAS server is the PEAP authenticator and TLS endpoint for users who connect as guest. The TLS tunnel is created between the client and the IAS server. All subsequent messages between client and server pass through this tunnel, which traverses the access point, the gateway device, and the IAS proxy.

Server authentication is performed when the IAS server verifies its identity to the client computer using a certificate that contains the Server Authentication purpose in Enhanced Key Usage (EKU) extensions. This certificate is issued by a public trusted root CA that the client computer trusts.

The IAS server authenticates and authorizes the customer as guest. In the Access-Challenge message that the IAS server sends to the client is a URL PEAP-TLV message. The URL PEAP-TLV contains the URL of the provisioning server. This

URL provides the client with the location of the XML master file.
The client computer receives an IP address lease from the DHCP server. The address is from a public IP address range configured in a scope on the DHCP server. In addition to the IP address, the client receives DHCP options, such as DNS server IP address.

3. The client is provisioned and the user creates an account

The XML master file on the provisioning server contains pointers to the XML subfiles. The client downloads the XML master file and subfiles. When the XML sign-up schema is downloaded, the sign-up wizard is started on the client to allow the user to create an account.
Using the sign-up wizard on the client computer, the user steps through the process of signing up for an account. The customer enters the promotion code as well as personal data such as name, employer, and job title. The data entered by the user is converted into an XML document.
The XML document containing the user's sign-up data is sent to the XML-forwarder Web application on the provisioning server.
The XML-forwarder Web application on the provisioning server sends the XML document to the account processing application on the account processing server.
The account processing application checks the promotion code entered by the user against the promotion code database on the SQL server. If the promotion code is valid, the account processing Web application continues processing the user's data.
The account processing Web application reads the domain and security group information from the promotion code database on the SQL server. The account processing application creates a user account in Active Directory and adds the account to the security group. The application also enters the new user name in the promotion code database.
An XML document containing the new account credentials is sent from the account processing server to the XML-forwarder application on the provisioning server; the XML-forwarder application passes the XML document to the client computer. The client computer uses the credentials to configure wireless auto configuration and 802.1X under the name of the enterprise.

4. The user is authenticated using the new account credentials

Wireless auto configuration restarts the association to the SSID for the enterprise WLAN.
Wireless auto configuration finds the correct 802.11 profile which was downloaded with the other network information. Wireless auto configuration re-associates with the access point using the correct profile.
802.1X restarts the authentication process using PEAP-MS-CHAP v2 and the new account credentials.
As the client starts the authentication process with PEAP-MS-CHAP v2 authentication, a TLS channel is created between the customer's client computer and the enterprise IAS server.
In the second stage of PEAP-MS-CHAP v2 authentication, the IAS server authenticates and authorizes the connection request against the new account in the Active Directory user accounts database. The IAS server sends an Access-Accept message to the access point. Included in the Access-Accept message are attributes that specify which VLAN the customer can access.
The access point instructs the gateway device to assign the client to the Internet VLAN rather than the Network Resource VLAN.

The gateway device switches the client to the Internet VLAN, and the customer is provided with access to the Internet.

How to deploy WPS technology for the enterprise

In the set of instructions that follow, these assumptions are made:

1. The computer functioning as your IAS server has Windows Server 2003 with SP1 installed, and the **EnableWPSCompatibility** registry key is enabled according to the instructions in “Configuring IAS for WPS technology” in this paper.
2. Client computers are running Windows XP Home Edition with SP2; Windows XP Tablet PC Edition with SP2; or Windows XP Professional with SP2.
3. All of your hardware, including the VLAN-aware gateway device and VLAN-aware wireless access points, meet all of the technical requirements stated in “Components of WPS technology for the enterprise” in this paper**.**
4. You have already deployed a computer running SQL Server 2000 or a third-party database program on your network. For information about SQL Server 2000, see SQL Server at http://go.microsoft.com/fwlink/?LinkId=20014.
5. You have SQL Server 2000 or third-party relational database development experience and you understand how to use SQL Server 2000 or a third-party database program to create, modify, administer, and manage your databases.
6. You have experience deploying an Internet Information Services (IIS) or third-party Web server with HTTPS.
7. You have software development experience that allows you to create two custom Web applications. One Web application runs on the provisioning server and forwards XML documents between the account processing application and client computers. Another Web application runs on the account processing server and processes user data and creates user accounts in Active Directory or an LDAP-compliant third-party user accounts database.
8. You have software development experience that allows you to create an IAS extension DLL.

To deploy WPS technology for the Enterprise, the basic steps are as follows:

> **Note**
>
> The instructions that follow use four servers upon which various programs and services are installed. If you deploy WPS technology in a test lab, you can reduce or increase the number of servers in a manner appropriate to your available hardware resources. For example, in a test lab environment you might want to deploy Active Directory, IAS, IIS, and DHCP on the same server.

1. Create your enterprise Web applications
2. Configure the enterprise domain controller and IAS server
3. Configure the enterprise account processing server
4. Configure the database on the enterprise SQL server
5. Install and configure the enterprise router
6. Configure the enterprise XML master file and subfiles
7. Configure the enterprise provisioning server
8. Configure the enterprise DHCP server

9. Install and configure your enterprise VLAN-aware gateway device
10. Install and configure your enterprise wireless access points
11. Install and configure the enterprise IAS proxy
12. Configure RADIUS clients at the enterprise IAS server
13. Configure the enterprise Windows XP-based client computer
14. Configure certificates in an enterprise test lab environment (optional)

Create your enterprise Web applications

The XML forwarding Web application to be installed on the provisioning server must be capable of performing the following functions:

- Communicating with client computers using HTTPS.
- Uploading the XML master file and subfiles that are stored on the provisioning server to client computers that request the files.
- Accepting XML documents from client computers that contain user data.
- Forwarding XML documents that contain user data to the account processing server.

The account processing Web application to be installed on the account processing server must be capable of performing the following functions:

- Accepting and processing XML documents from the provisioning server that contain user data, such as promotion code, user name, and other information.
- Reading the promotion code database records to validate promotion codes.
- Reading the promotion code database records to determine the domain in which to create a new user account.
- Reading the promotion code database records to determine the security group membership for a new user account.
- Writing a user name to the user name field in the promotion code database.
- Dynamically creating new accounts in Active Directory (or a third-party LDAP-compliant database) using data provided by users and parameters derived from the promotion code database.

It is recommended that the design of your Web application provides users with knowledge of their password-based credentials (user name and password). Users should either be allowed to designate user name and password or this information should be provided to them upon completion of the sign-up wizard. Following are some circumstances where users will need to know their password-based credentials:

- For a variety of reasons, user authentication might fail. For example, cached credentials might get corrupted or network connectivity issues might prevent wireless client computers from successfully authenticating.
- The user account expires and the user wants to renew their account. In this circumstance, IAS sends a URL PEAP-TLV to the wireless client that contains the renewal action parameter (**#renewal**) and the URL of the provisioning server. After the wireless client is directed to your account renewal application, the user must have their password-based credentials to renew their account.

If your users know their user name and password, they can attempt to connect to your network until they are successful. If they do not have this information, they cannot fix the problem without calling your help desk.

You can create your Web application with the Microsoft .NET Framework 1.1 or with other application development software. If you want to create your Web application with the .NET Framework 1.1, you need the Microsoft .NET Framework 1.1 Software Development Kit.

Microsoft .NET Framework 1.1 Software Development Kit

Microsoft .NET Framework 1.1 Software Development Kit (SDK) includes .NET Framework 1.1, as well as everything you need to write, build, test, and deploy applications using .NET Framework 1.1. This includes documentation, samples, command-line tools, and compilers.

If you have already installed Microsoft® Visual Studio® .NET, you do not need to install .NET Framework 1.1 SDK separately; Visual Studio .NET includes the SDK.

If you want to distribute .NET Framework 1.1 with your application, download .NET Framework 1.1 Redistributable in addition to the SDK.

You can get .NET Framework 1.1 SDK from the Download Center at http://go.microsoft.com/fwlink/?LinkId=17161. You can run .NET Framework 1.1 SDK on the following platforms:

- Windows Server 2003
- Microsoft Windows 2000 (Service Pack 2 is recommended)
- Windows XP Professional or Windows XP Home Edition (Windows XP Professional is required to run ASP.NET)

Configure the enterprise domain controller and IAS server

Install Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1 on a computer that meets or exceeds the minimum hardware requirements for the respective operating system. After the operating system is installed, you can perform general configuration, Active Directory configuration, IPsec policy configuration, IAS configuration, and IAS extension DLL & URL PEAP-TLV configuration.

General configuration

1. Assign the server a static IP address.
   For more information, see "To configure TCP/IP for static addressing" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20015
2. Install a server certificate obtained from a public trusted root certification authority, such as a certificate from Verisign.
   For more information, see "Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication" at http://go.microsoft.com/fwlink/?LinkId=33675.

When you obtain the certificate, it must conform to the minimum server certificate requirements described in this paper.

For more information, see "Network access authentication and certificates" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20016.

> **Note**
>
> If you are deploying WPS technology in a test lab environment, you can install a private CA rather than obtain certificates from a public CA. For more information, see "Configure certificates in an enterprise test lab environment (optional)" in this paper.

Active Directory configuration

1. Install Active Directory and DNS. To install Active Directory, open Command Prompt, type **dcpromo**, and then follow the instructions provided in the wizard, entering your network configuration information in the wizard as you progress.
2. Design and create your security group or groups. When users sign up and create an account, your Web application adds the new user account as the member of a security group that you create in this step. The Web application chooses group membership based on the value of the security group field in the promotion code database on your SQL server, so you need to match the security group you create to the security group field in the SQL Server database. If you have the need for multiple security groups, you can assign permissions to each group individually. For more information, see "To create a new group" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20018 and "Assign user rights to a group in Active Directory" at http://go.microsoft.com/fwlink/?LinkId=20019.

> **Important**
>
> The security groups you create in Active Directory are named and used in the SQL Server database and in IAS remote access policy.

3. Enable the Guest account in Active Directory. If guest access is not enabled in Active Directory, new customers cannot access your provisioning server by authenticating as guest. To enable the Guest account, open the Active Directory Users and Computers snap-in, and then double-click **Users**. Right-click the account named **Guest**, and then click **Enable Account**.

To perform this procedure, you must be a member of the Domain Admins group in the domain for which you want to raise functionality or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority.

Raise the domain functional level to Windows 2000 native or Windows Server 2003 by doing the following:

1. Open the Active Directory Domains and Trusts snap-in. Click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain for which you want to raise functionality, and then click Raise Domain Functional Level.
3. In Select an available domain functional level, do one of the following:
   a. To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
   b. To raise domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.

The current domain functional level is displayed under **Current domain functional level** in the **Raise Domain Functional Level** dialog box.

> **Important**
>
> If you have or will have any domain controllers running Windows NT 4.0 and earlier, then do not raise the domain functional level to Windows 2000 native. After the domain functional level is set to Windows 2000 native, it cannot be changed back to Windows 2000 mixed.
>
> Likewise, if you have or will have any domain controllers running Windows NT 4.0 and earlier or Windows 2000, then do not raise the domain functional level to Windows Server 2003. After the domain functional level is set to Windows Server 2003, it cannot be changed back to Windows 2000 mixed or Windows 2000 native.

For more information, see "Domain and forest functionality" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30600.
For information about configuring Active Directory replication, see "Active Directory replication" in this paper.

IPsec policy configuration

One IP Security policy can contain rules that accomplish the following:

- Protect RADIUS traffic between the IAS proxy and the IAS server
- Protect all traffic between the provisioning server and the account processing server

> **Note**
>
> To successfully complete IP Security policy configuration, you must know the IP addresses of the following servers: the IAS proxy, the provisioning server, and the account processing server.

To create an IP Security policy in Active Directory using the IP Security Policy Management snap-in, do the following:

1. Click **Start**, click **Run**, type **MMC**, and then click **OK**.
2. Click **File**, click **Add/Remove Snap-in**, and then click **Add**.
3. Click **IP Security Policy Management**, and then click **Add**.
4. Click the Active Directory domain of which this computer is a member. Click **Finish**, click **Close**, and then click **OK**.
5. To add a new policy, in the console tree, click **IP Security Policies on Active Directory**. On the **Action** menu, click **Create IP Security Policy**. The IP Security Policy Wizard is started. Click **Next**.
6. In **IP Security Policy Name**, type a name for your IPsec policy. Optionally, type a description for the policy. Click **Next**.
7. In **Requests for Secure Communication**, verify that **Activate the default response rule** is selected. Click **Next**.
8. In **Default Response Rule Authentication Method**, verify that **Active Directory default (Kerberos V5 protocol)** is selected. Click **Next**, and then click **Finish**.
   The ***PolicyName* Properties** dialog box opens, where ***PolicyName*** is the name you typed for your policy. For example, if you named your policy "WPS policy," the dialog box that opens is named **WPS policy Properties**.

To create a rule with RADIUS traffic filters

1. In ***PolicyName* Properties**, click **Add**. The Create IP Security Rule Wizard is started. Click **Next**.
2. In **Tunnel Endpoint**, verify that **This rule does not specify a tunnel** is

> **Note**
>
> The Create IP Security Rule Wizard is also referred to as the Security Rule Wizard.

selected. Click **Next**.

3. In **Network Type**, verify that **All network connections** is selected.
4. In **IP Filter List**, click **Add**. In **Name**, type **RADIUS filters**, and then click **Add**. The **IP Filter Wizard** is started. Click **Next**.
5. In **IP Filter Description and Mirrored property**, type **RADIUS port 1812**. Verify that **Mirrored. Match packets with the exact opposite source and destination addresses** is selected. Click **Next**.
6. In **IP Traffic Source**, verify that **My IP Address is selected** in Source address. Click **Next**.
7. In **IP Traffic Destination**, click **Destination address**, and then select **A specific IP Address**. In **IP address**, type the IP address of the IAS proxy server that is located on the perimeter network. Click **Next**.
8. In **IP Protocol Type**, click **Select a protocol type**, and then select **UDP**. Click **Next**.
9. In **IP Protocol Port**, for **Set the IP protocol port**, verify that **From any port** is selected. Select **To this port**, type **1812**, click **Next**, and then click **Finish**. The **IP Filter List** dialog box is now visible.
10. In **IP filter list**, click **Add**. The **IP Filter Wizard** is started. Click **Next**.
11. In **IP Filter Description and Mirrored property**, type **RADIUS port 1813**. Verify that **Mirrored. Match packets with the exact opposite source and destination addresses** is selected. Click **Next**.
12. In **IP Traffic Source**, verify that **My IP Address** is selected in Source address. Click **Next**.
13. In **IP Traffic Destination**, click **Destination address**, and then select **A specific IP Address**. In **IP address**, type the IP address of the IAS proxy server that is located on the perimeter network. Click **Next**.
14. In **IP Protocol Type**, click **Select a protocol type**, and then select **UDP**. Click **Next**.
15. In **IP Protocol Port**, for **Set the IP protocol port**, verify that **From any port** is selected. Select **To this port**, type **1813**, click **Next**, and then click **Finish**. To close the RADIUS filters **IP Filter List**, click **OK**. The **Security Rule Wizard** is still running and should now be visible. In **IP Filter Lists**, select **RADIUS filters**, and then click **Next**.
16. In **Filter Action**, click **Require Security**. Click **Next**.
17. In **Authentication Method**, verify that **Active Directory default (Kerberos V5 protocol)** is checked, and then click **Next**.
18. In **Completing the IP Filter Wizard**, verify that the **Edit properties** check box is cleared, and then click **Finish**. This returns you to the ***PolicyName*** **Properties** dialog box.

To create an IPsec rule for all traffic between the provisioning server and the account processing server

1. In ***PolicyName*** **Properties**, click **Add**. The Create IP Security Rule Wizard is started. Click **Next**.
2. In **Tunnel Endpoint**, verify that **This rule does not specify a tunnel** is selected. Click **Next**.
3. In **Network Type**, verify that **All network connections** is selected. Click

Next.

4. In **IP Filter List**, click **Add**. In **Name**, type **Provisioning server filters**, and then click **Add**. The IP Filter Wizard is started. Click **Next**.
5. In **IP Filter Description and Mirrored property**, type a description for the filter. Verify that **Mirrored. Match packets with the exact opposite source and destination addresses** is selected. Click **Next**.
6. In **IP Traffic Source**, click **Source address**, and then select **A specific IP Address**. In **IP Address**, type the IP address of the provisioning server that is located on the perimeter network. Click **Next**.
7. In **IP Traffic Destination**, click **Destination address**, and then select **A specific IP Address**. In **IP address**, type the IP address of the account processing server that is located on the enterprise LAN. Click **Next**.
8. In **IP Protocol Type**, verify that the value of Select a protocol type is Any. Click **Next**.
9. In **Completing the IP Filter Wizard**, verify that the **Edit properties** check box is cleared, and then click **Finish**. This returns you to the **IP Filter List** dialog box. Click **OK**.
10. The **Security Rule Wizard** is still running and should now be visible. In **IP Filter List**, select **Provisioning server filters**, and then click **Next**.
11. In **Filter Action**, click **Require Security**. Click **Next**.
12. In **Authentication Method**, verify that **Active Directory default (Kerberos V5 protocol)** is selected, and then click **Next**.
13. In **Completing the Security Rule Wizard**, verify that the **Edit properties** dialog box is cleared, and then click **Finish**.
14. This returns you to the ***PolicyName*** **Properties** dialog box. Displayed in **IP Security rules** are two rules, **RADIUS filters** and **Provisioning server filters**. To close the ***PolicyName*** **Properties** dialog box, click **OK**.

IAS configuration

For IAS, the three configuration stages are general configuration, remote access policy configuration, and connection request policy configuration. RADIUS client configuration occurs later in the overall WPS deployment process.

General configuration

1. Install Internet Authentication Service.
   For more information, see "To install IAS" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20028.
2. Register IAS in Active Directory. In order for IAS to have permission to read user accounts in Active Directory, IAS must be registered in Active Directory. For more information, see "To enable the IAS server to read user accounts in Active Directory" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20030.
3. Delete the default remote access policies. To delete the policies, open the IAS console and click **Remote Access Policies**. Select each existing policy, right-click the policy, and then click **Delete**.
4. Install your RADIUS extension DLL on your IAS server:
   a. Open Command Prompt and change directories to the folder that contains your DLL.
   b. Type the following: **regsvr32** *DLL_name.dll*, where *DLL_name.dll*

is the name of your DLL file.

Make sure that you configure DLL registry keys according to your needs. For more information, see "How to create an IAS extension DLL and a URL PEAP-TLV" in this paper.

Remote access policy configuration

There are two remote access policies configured for WPS technology. The Guest access policy provides network parameters and rules for users connecting as a guest. The Valid Users access policy provides network parameters and rules for users who have valid enterprise accounts.

> **Note**
>
> If you have a variety of account types that you offer to users and these accounts have different properties (such as membership to different security groups), you might find it necessary to create more than two remote access policies on your IAS server. If this is the case, you can use the remote access policies described below to extrapolate how to create additional policies.

To configure the Guest access policy

1. Open the Internet Authentication Service console and, if necessary, double-click **Internet Authentication Service**.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. The **New Remote Access Policy Wizard** starts. For the Guest access policy, specify the following:
   a. For **How do you want to set up this policy?** verify that **Use the wizard to set up a typical policy for a common scenario** is selected.
   b. For **Policy name**, type **Guest access** (or type another name for your policy that you prefer).
   c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
   d. For **Grant access based on the following,** click **User**.
   e. In **Select the EAP type for this policy**, select **Protected EAP (PEAP)**, and then click **Configure**.
   f. In **Certificate issued**, select the certificate that you want the IAS server to use to verify its identity to client computers. Also select the **Enable Fast Reconnect** check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration.

1. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created.
2. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
3. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
4. In the policy **Properties** dialog box, click **Grant remote access permission**.
5. Click **Edit Profile**. On the **Authentication** tab, in **Unauthenticated access**, click **Allow clients to connect without negotiating an authentication method.**

To configure the Valid Users access policy

1. Open the Internet Authentication Service console and, if necessary, double-click **Internet Authentication Service**.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Use **New Remote Access Policy Wizard** to create a policy. For the Valid Users access policy, you can choose the following:
    a. For **How do you want to set up this policy?** verify that **Use the wizard to set up a typical policy for a common scenario** is selected.
    b. For **Policy name**, type **Valid Users** (or type another name for your policy that you prefer).
    c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
    d. For **Grant access based on the following,** click **Group,** and then click **Add**. In **Enter the object name to select**, type the name of a security group that you defined when configuring Active Directory.

> Impor
>
> The following three items must match: the name of the security group in Active Directory, the value of the security group field in the SQL server database, and the name of the security group configured in the Valid User access policy in IAS. The Web application uses the value of the SQL server database security group field to determine group membership for new accounts.

    e. In Select the EAP type for this policy, select Protected EAP (PEAP), and then click Configure.
    f. In Certificate issued, select the certificate that you want the IAS server to use to verify its identity to client computers. Also select the Enable Fast Reconnect check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration.

1. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created.
2. In the policy Properties dialog box, for **Policy conditions**, click **Add**.
3. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
4. In the policy Properties dialog box, click **Grant remote access permission**.
5. Click **Edit Profile**, and then click the **Advanced** tab. By default, the **Service-Type** attribute appears in **Attributes** with a value of **Framed**. To specify additional connection attributes required for WPS technology with VLANs, click **Add**, and then add the following attributes:
    a. **Framed-Protocol**. Value: **PPP**
    b. **Tunnel-Medium-Type**. Value: **802 (Includes all 802 media plus Ethernet canonical format)**
    c. **Tunnel-Pvt-Group-ID**. Value: Enter the integer that represents the VLAN number for the Internet VLAN. For example, if your access controller's Internet VLAN is VLAN 4, type **4**.
    d. **Tunnel-Type**. Value: **Virtual LANs (VLAN)**
    e. **Tunnel-Tag**. Value: Obtain this value from your hardware

documentation

> **Important**
>
> IAS evaluates remote access policies in the order in which they appear in the IAS console under **Remote Access Policies**. The Valid Users access policy must be the first policy in the list of remote access policies or else valid user authentication will fail. Because IAS places newly created policies in the first position and the Valid Users access policy was the last policy created, the Valid Users access policy should now appear first in the IAS console, with the Guest access policy appearing second. If this is not the case, move the Valid Users access policy into first position.

Connection request policy configuration

By default, there is one connection request policy predefined in the IAS console, called **Use Windows authentication for all users**. This policy can be used for WPS technology.

To configure connection request policy

1. In the IAS console, double-click **Connection Request Processing**, click Connection Request Policies, and then double-click the policy **Use Windows authentication for all users**.
2. Click **Edit Profile**. The **Edit Profile** dialog box opens.
3. On the **Authentication** tab, click Authenticate requests on this server, and then select the Protected EAP check box.
4. Click **Configure Certificate**, select the certificate you want IAS to use to verify its identity to client computers, and then click **OK** three times to close all dialog boxes and return to the IAS console.

> **Note**
>
> If you access the profile of a connection request policy in the IAS console and you cannot see the **Protected EAP** check box or the **Configure Certificate** button, you must first configure IAS for compatibility with WPS technology as described in “Configuring IAS for WPS technology” in this paper.

Configure the enterprise account processing server

For the account processing server, if you are using Internet Information Services (IIS), do the following:

1. Install Internet Information Services and ASP.NET.
2. For more information, see “To install Internet Information Services (IIS) 6.0” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20033.
3. Verify that you have .NET Framework 1.1 installed by clicking **Start** on your Windows desktop, selecting **Control Panel**, and then double-clicking the **Add or Remove Programs** icon. When that window appears, scroll through the list of programs. If you see Microsoft .NET Framework 1.1 listed, the latest version is already installed and you do not need to install it again.
    a. If Microsoft .NET Framework 1.1 is already installed, register ASP.NET with Microsoft .NET Framework 1.1 by running the following command at Command Prompt:
    %WINDIR%\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe –I
    b. If Microsoft .NET Framework 1.1 is not installed, install it by using

Microsoft Windows Update at http://go.microsoft.com/fwlink/?LinkId=284.

For more information, see "How to Get the .NET Framework 1.1" at http://go.microsoft.com/fwlink/?LinkId=30841.

4. Create two folders in the Web server root location %systemroot%\Inetpub\wwwroot. You can use one folder to hold your custom Web application and one folder to hold the XML master and subfiles that you will be creating in later steps. For example, you can create a folder named **wpsdeploy** (%systemroot%\Inetpub\wwwroot\wpsdeploy) to contain your Web application, and you can create a folder named **wpsfiles** (%systemroot%\Inetpub\wwwroot\wpsfiles) to contain your XML files.
5. Install your Web application into the folder you created for the Web application files.
6. Set user permissions for the Web application. Open Windows Explorer and browse to the location where you installed your Web application. For example, if you named your folder wpsdeploy, browse to %systemroot%\Inetpub\wwwroot\wpsdeploy. Right-click on the wpsdeploy folder, and then click **Sharing and Security**. On the **Security** tab, click **Add**. In **Enter the object names to select**, type **Everyone**, and then click **OK**. In **Permissions for Everyone**, enable **Write** permissions by selecting the **Allow** check box.
7. Enable HTTPS. You must configure IIS to use a certificate for secure Web communications between the account processing server and the provisioning server. To enable HTTPS you must install a server certificate obtained from a public trusted root certification authority, such as a certificate from Verisign or Thawte. When you obtain the certificate, it must conform to the minimum server certificate requirements described in this paper.

For more information, see "Network access authentication and certificates" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20016.

To enable Secure Sockets Layer (SSL) and HTTPS, complete the following procedures.

> **Note**
>
> If you are deploying a certification authority in a test lab environment, you must install and configure the CA before completing the following procedures.

To obtain a new server certificate using the Web Server Certificate Wizard

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In the Web Server Certificate Wizard, click **Create a new certificate**.
5. Complete the **Web Server Certificate Wizard**, which will guide you through the process of requesting a new server certificate.

To install a server certificate using the Web Server Certificate Wizard

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure**

communications, click **Server Certificate**.

4. In the Web Server Certificate Wizard, click **Assign an existing certificate**.
5. Complete the **Web Server Certificate Wizard**, which will guide you through the process of installing a server certificate.

> **Note**
>
> The Web Server Certificate Wizard always denotes this step as "assigning" a certificate to a resource (such as a file, directory, or site), not as "installing."

Configure the database on the enterprise SQL server

On the computer running SQL Server 2000 or a third-party product with similar functionality, create a promotion code database with the following fields, using the appropriate data type for each field:

- **Promotion code.** This field contains promotion codes that you distribute publicly to potential customers. When customers sign up for an account, they provide the promotion code that is matched by the Web application to a value in this field in the database.
- **User name.** This field has no value assigned until a customer creates an account. At this time, the Web application assigns a value to this field.
- **Domain name.** This field contains the domain name where you want the Web application to create the user account when a customer signs up using the promotion code.
- **Security group.** The Web application joins the new user account to the security group defined in this field.
- **Expiration date.** If your promotion lasts for a specific period of time, you can enter the expiration date related to the promotion code in this field. If a user with a promotion code attempts to create an account after the expiration date for the promotion, they cannot do so.

Populate the database with records, providing values for all fields except user name, and enable the data link between your Web application and the SQL server. Also configure security and authentication on the SQL server so that your Web application has permission to access and write to the database. For more information, see SQL Server at http://go.microsoft.com/fwlink/?LinkId=20014.

> **Important**
>
> When you configure values for records in the SQL Server database, the following three items must match: the name of the security group in Active Directory, the value of the **security group** field in the SQL Server database, and the name of the security group configured in the Valid User access policy in IAS. The Web application uses the value of the SQL Server database **security group** field to determine group membership for new accounts.

Install and configure the enterprise router

The router must be capable of forwarding traffic between the enterprise LAN and the perimeter network.

Configure the enterprise XML master file and subfiles

There are two methods you can use to create and configure your XML master and subfiles:

- Use the WPS Authoring Tool to create a WPS project and publish your XML files. The WPS Authoring Tool has a graphical user interface and is designed to assist you in accurately producing and managing a collection of XML files for your WPS solution. For more information, see "Using the WPS Authoring Tool" at http://go.microsoft.com/fwlink/?LinkId=41067. Using the WPS Authoring Tool to create your XML data files is recommended.
- Use the XML schemas provided in this paper to create your files. Once you have created these files, you can enter information specific to your network and deployment parameters. For example, where the location of the provisioning server is required, you can provide an HTTPS URL. In another example, you might need to enter your domain name in several places; you can examine the schemas and example files and determine where to insert your domain name.

When your XML files are configured with the information for your organization, you can store them on your provisioning server and configure your Web application so that it can find the files when necessary. If you are using Internet Information Services as your Web server, you can install the files at the location *%systemroot%* \inetpub\wwwroot.

Configure the enterprise provisioning server

For the provisioning server, do the following:

1. Install Internet Information Services and ASP.NET.
2. For more information, see "To install Internet Information Services (IIS) 6.0" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20033.
3. Verify that you have .NET Framework 1.1 installed by clicking **Start** on your Windows desktop, selecting **Control Panel**, and then double-clicking the **Add or Remove Programs** icon. When that window appears, scroll through the list of programs. If you see Microsoft .NET Framework 1.1 listed, the latest version is already installed and you do not need to install it again.
   a. If Microsoft .NET Framework 1.1 is already installed, register ASP.NET with Microsoft .NET Framework 1.1 by running the following command at Command Prompt:
   %WINDIR%\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe –I
   b. If Microsoft .NET Framework 1.1 is not installed, install it by using Microsoft Windows Update at http://go.microsoft.com/fwlink/?LinkId=284.
   For more information, see "How to Get the .NET Framework 1.1" at http://go.microsoft.com/fwlink/?LinkId=30841.
4. Create two folders in the Web server root location %systemroot% \Inetpub\wwwroot. You can use one folder to hold your custom Web application and one folder to hold the XML master file and subfiles that you will be creating in later steps. For example, you can create a folder named

wpsdeploy (%systemroot%\Inetpub\wwwroot\wpsdeploy) to contain your Web application, and you can create a folder named **wpsfiles** (%systemroot%\Inetpub\wwwroot\wpsfiles) to contain your XML files.

5. Install your Web application into the folder you created for the Web application files.
6. Set user permissions for the Web application. Open Windows Explorer and browse to the location where you installed your Web application. For example, if you named your folder wpsdeploy, browse to %systemroot%\Inetpub\wwwroot\wpsdeploy. Right-click on the wpsdeploy folder, and then click **Sharing and Security**. On the **Security** tab, click **Add**. In **Enter the object names to select**, type **Everyone**, and then click **OK**. In **Permissions for Everyone**, enable **Write** permissions by selecting the **Allow** check box.
7. Enable HTTPS. You must configure IIS to use a certificate for secure Web communications between the provisioning server and clients. To enable HTTPS you must install a server certificate obtained from a public trusted root certification authority, such as a certificate from Verisign or Thawte. When you obtain the certificate, it must conform to the minimum server certificate requirements described in this paper.

For more information, see "Network access authentication and certificates" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20016.

To enable Secure Sockets Layer (SSL) and HTTPS, complete the following procedures.

> **Note**
>
> If you are deploying a certification authority in a test lab environment, you must install and configure the CA before completing the following procedures.

To obtain a new server certificate using the Web Server Certificate Wizard

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In the Web Server Certificate Wizard, click **Create a new certificate**.
5. Complete the **Web Server Certificate Wizard**, which will guide you through the process of creating a new server certificate.

To install a server certificate using the Web Server Certificate Wizard

1. In IIS Manager, expand the local computer, and then expand the **Web Sites** folder.
2. Right-click the Web site or file that you want, and then click **Properties**.
3. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
4. In Web Server Certificate Wizard, click **Assign an existing certificate**.
5. Complete the **Web Server Certificate Wizard**, which will guide you through the process of installing a server certificate.

> **Note**
>
> Web Server Certificate Wizard always denotes this step as "assigning" a certificate to a resource (such as a file, directory, or site), not as "installing."

Configure the enterprise DHCP server

On a computer running Windows Server 2003:

1. Install DHCP.
   For more information, see “To install a DHCP server” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20034.
2. In the DHCP console, run New Scope Wizard twice. Create two VLAN scopes from which IP addresses will be leased to wireless clients connected to the VLANs. Each scope must define a different IP address range using either a private address range or a public IP address range. If you are using network address translation (NAT), you can use a private IP address range; otherwise, the IP addresses leased to wireless clients must be from a public IP address range.
   For more information, see “To create a new scope” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20123.
3. While running the New Scope Wizard, create an exclusion range for the IP addresses you will be assigning statically. For example, if you need to statically assign ten IP addresses from the address range 10.1.1.1 through 10.1.1.254, your exclusion range is defined as 10.1.1.1 through 10.1.1.10.
4. While running the New Scope Wizard, choose to assign scope options. On the **Configure DHCP Options** page, select **Yes, I want to configure these options now**. Scope options are applied only to leases of addresses from within the IP address range that the scope defines, which provides flexibility as your network grows. Define DNS server and Domain name options, as well as any other options that are appropriate for your network configuration.
5. While running the New Scope Wizard, activate the scope. The option to activate the scope while running the wizard is available only if you have chosen to configure DHCP options in the previous steps.
   For more information, see “To activate a scope” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20124.
6. Authorize the DHCP server in Active Directory.
   For more information, see “To authorize a DHCP server in Active Directory” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20125.

The DHCP server is now online and able to provide IP address leases to client computers. In some cases you might want to examine the types and durations of accounts you offer your users and adjust the DHCP lease duration accordingly. In most cases, when deploying WPS technology the default lease duration of eight days is too long and should be shortened considerably.

DHCP example

In this example, you are creating two VLANs and two scopes, one scope for each VLAN.

VLAN 2

VLAN 2 is the Network Resource VLAN that provides access to network resources (such as the IAS server and DHCP server) for wireless computers connecting as guest. VLAN 2 blocks access to the Internet, however. The DHCP scope for VLAN 2 is defined with the following example parameters:

- **Address range:** 192.168.1.1 through 192.168.1.254. This is a private IP address range. If you are using NAT, you can use this range on your network. If you are not using NAT, use a public IP address range. In addition, if your wireless deployment is large, select an IP address range that provides more IP addresses for lease to clients.
- **Exclusion range:** 192.168.1.1 through 192.168.1.10. By using this exclusion range, the available address pool for clients is 192.168.1.11 through 192.168.1.254. Ten IP addresses are excluded so that you can statically assign these addresses to computers and devices on your network. For example, the router IP address must be statically assigned on the router.
- **DHCP scope option 003, Router:** 192.168.1.1. The router IP address must be an address that falls within the exclusion range so that the DHCP server does not lease the router IP address to a wireless client computer, thereby creating an address conflict.
- **DHCP scope option 006, DNS server:** the IP address of the Active Directory and DNS server on the enterprise LAN

Note that DHCP scope option 003, Router, provides client computers with the IP address of their default gateway IP address. In this case, the default gateway for wireless clients is the VLAN-aware gateway device, whether it is an access controller, a VLAN-aware router, a VLAN-aware switch, or another compatible device. When you configure your VLAN-aware gateway device, you can specify the IP address that the device uses for each VLAN.

In this example, you must configure the VLAN-aware gateway device so that it uses the IP address 192.168.1.1 on VLAN 2.

For your WPS deployment you can configure additional DHCP options as needed. For example, if you are using a WINS server, you can configure your VLAN scopes with DHCP option 044, WINS/NBNS servers.

VLAN 4

VLAN 4 is the Internet VLAN that provides access to the Internet. Users who have successfully created an account are switched to this VLAN after completing the provisioning and sign-up process. The DHCP scope for VLAN 4 is defined with the following example parameters:

- **Address range:** 192.168.2.1 through 192.168.2.254
- **Exclusion range:** 192.168.2.1 through 192.168.2.10
- **DHCP scope option 003, Router:** 192.168.2.1. The router IP address must be an address that falls within the exclusion range so that the DHCP server does not lease the router IP address to a wireless client computer, thereby creating an address conflict.
- **DHCP scope option 006, DNS server:** the IP address of the Active Directory and DNS server on the Enterprise LAN

For VLAN 4 in this example, you must configure the VLAN-aware gateway device so that it uses the IP address 192.168.2.1 on VLAN 4.

Install and configure your enterprise VLAN-aware gateway device

Configure two VLANs on the gateway device: a Network Resource VLAN that provides access to the WISP LAN, and an Internet VLAN that provides access to the Internet.

The remote access policies you created in IAS determine which VLAN your customers can access:

- The Guest access policy places users on the Network Resource VLAN so that they can create and pay for a valid user account.
- The Valid Users access policy in IAS places customers on the Internet VLAN.

Each VLAN has a different IP address range. When configuring your DHCP server, you created a scope for each VLAN, and you defined DHCP scope option 003, Router. This is the IP address commonly referred to as the “default gateway.”

You must configure the VLAN-aware gateway device as the default gateway for each VLAN, using an IP address from the IP address range that you defined on your DHCP server.

Choosing the IP address for the default gateway for each VLAN

Your VLAN-aware gateway device is the default gateway for both VLANs and is configured with a different IP address for each VLAN.

Important

In each scope you configure on the DHCP server, the value you enter for DHCP scope option 003, Router, must match the IP address you assign to the VLAN-aware gateway device for use on each VLAN. For example, if you configure a scope on the DHCP server for VLAN 2 with the IP address range 192.168.1.1 through 192.168.1.254, and you assign the DHCP scope option 003, Router, with the value 192.168.1.1, you must configure the VLAN-aware gateway device to use the IP address 192.168.1.1 on VLAN 2.

Similarly, as described in “Configure the DHCP server” in this paper, configure the VLAN-aware gateway device so that it uses an IP address from the exclusion range 192.168.2.1 through 192.168.2.10 for VLAN 4. For example, you can configure the VLAN-aware gateway device so that it uses the IP address 192.168.2.1 on VLAN 4.

In some circumstances you might prefer to use your VLAN-aware gateway device as the DHCP server for each VLAN. If this is the case, you can define IP address ranges and exclusion ranges on the VLAN-aware gateway device rather than on a DHCP server.

See the product documentation for your VLAN-aware gateway device for information about configuring your hardware.

Important

The Internet VLAN integer must match the value you configure for the Tunnel-Pvt-Group-ID attribute in the Valid Users access policy on your IAS server. For example, if VLAN 4 provides access to the Internet, the value of the Tunnel-Pvt-Group-ID attribute in the profile of the Valid Users access policy must be 4.

Install and configure your enterprise wireless access points

Configure the access points to use your RADIUS server, including configuration of the server IP address and the shared secret. Follow the directions in your access point documentation for other configuration settings, using the following guidelines:

- **Authentication or RADIUS server**: Specify your IAS server by IP address or FQDN, depending on the requirements of the AP.
- **SSID**: Specify a Secure Set Identifier (SSID), which is an alphanumeric string that serves as the network name. This name is broadcast by APs to wireless clients and is visible to users at your Wi-Fi hotspots.
- **RADIUS settings**: Use RADIUS authentication on User Datagram Protocol (UDP) port 1812 and use RADIUS accounting on UDP port 1813.
- **Secret or shared secret**: Use a strong shared secret and configure the IAS server with the same shared secret.
- **EAP**: Configure the AP to require EAP from wireless clients.
- **802.1X and WEP**: Enable IEEE 802.1X authentication and WEP.

If your IAS server is running Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition, you can configure RADIUS clients by IP address range. This is a useful feature when you have a large number of access points to deploy; if you deploy your access points on the same subnet or VLAN within the same IP address range, configuration of RADIUS clients in IAS is simplified. Instead of individually configuring each access point as a RADIUS client in IAS, you can configure all access points at once using the IP address range of the subnet or VLAN upon which the APs reside. In this circumstance, use the same shared secret for all access points, and make sure that the shared secret is strong.

Install and configure the enterprise IAS proxy

For IAS proxy, the three configuration stages are general configuration, RADIUS client configuration, and connection request policy configuration.

General configuration

1. Install Internet Authentication Service.
   For more information, see "To install IAS" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20028.
2. Delete the default remote access policies. To delete the policies, open the IAS console, and then click **Remote Access Policies**. Select each existing policy, right-click the policy, and then click **Delete**.

RADIUS client configuration

In the IAS console, add the wireless access points as RADIUS clients. In addition, configure the shared secret used between the IAS proxy and the access points. For more information, see "To add RADIUS clients" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20031 and "To configure the Message Authenticator attribute and shared secret" at http://go.microsoft.com/fwlink/?LinkId=20032.

If your IAS server is a computer running Windows Server 2003, Enterprise Edition with SP1, or Windows Server 2003, Datacenter Edition with SP1, and if you have configured your wireless access points with IP addresses from the same IP address range, you can configure the access points as RADIUS clients using the IP address range rather than individually configuring each access point.

> **Note**
>
> You can configure IAS in Windows Server 2003, Standard Edition with SP1, with a maximum of 50 RADIUS clients. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. With Windows Server 2003, Standard Edition with SP1, if the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query. With IAS in Windows Server 2003, Enterprise Edition with SP1, and Windows Server 2003, Datacenter Edition with SP1, you can configure an unlimited number of RADIUS clients. In addition, you can configure RADIUS clients by specifying an IP address range.

Connection request policy configuration

When you configure a remote RADIUS server group in the IAS console of the proxy server, you instruct the proxy server to forward messages to the IAS servers included in the remote RADIUS server group. To configure the IAS server on the Enterprise LAN as a member of a remote RADIUS server group, do the following:

1. In the IAS console, double-click **Connection Request Processing**. The folder expands to display Connection Request Policies and Remote RADIUS Server Groups. Right-click on **Remote RADIUS Server Groups**, and then select **New Remote RADIUS Server Group**. New Remote RADIUS Server Group Wizard is started. Click **Next**.
2. In **Group Configuration Method**, click **Custom**. Type a value for Group Name. Click **Next**.
3. In **Add Servers**, click **Add**. In **Add RADIUS Server**, type the IP address of the IAS server on the enterprise LAN. To verify connectivity, click **Verify**.
4. Click the **Authentication/Accounting** tab. In **Shared secret** and **Confirm shared secret**, type the shared secret that you will also use on the IAS server. Click **OK**.
5. In **Add Servers**, click **Next**, and then click **Finish**.
6. The **New Connection Request Policy Wizard** is started. Click **Next**. In **Policy Configuration Method**, verify that the type of policy is set to **A typical policy for a common scenario**. In **Policy Name**, type the name for your connection request policy. Click **Next**.
7. In **Request Authentication**, select **Forward connection requests to a remote RADIUS server for authentication**. Click **Next**.
8. In **Realm Name**, type the realm name of the connection requests that will be forwarded. Also verify that the name of the remote RADIUS server group that you created is selected in **Server group**. Click **Next**, and then click **Finish**. For more information, see “Realm Names” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=34426.
9. In the IAS console, under **Connection Request Processing**, click **Connection Request Policies**. In the right pane of the IAS console, there are two connection request policies: the policy you just created, and the default connection request policy. The default connection request policy is named **Use Windows authentication for all users**. To delete the default policy, right-click **Use Windows authentication for all users**, and then click **Delete**. To confirm the deletion, click **Yes**.

Note

If you access the profile of a connection request policy in the IAS console and you cannot see the **Protected EAP** check box or the **Configure Certificate** button, you must first configure IAS for compatibility with WPS technology as described in "Configuring IAS for WPS technology" in this paper.

Configure RADIUS clients at the enterprise IAS server

In the IAS console, add the IAS proxy server as a RADIUS client. In addition, configure the shared secret used between the IAS proxy and the IAS server.

Important

Because you are using an IAS proxy between the IAS server and the access points, do not configure the access points as RADIUS clients to the IAS server. Access points are configured as RADIUS clients at the IAS proxy only.

For more information, see "To add RADIUS clients" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20031 and "To configure the Message Authenticator attribute and shared secret" at http://go.microsoft.com/fwlink/?LinkId=20032.

Configure the enterprise Windows XP-based client computer

On the computer running Windows XP Professional, Windows XP Tablet PC Edition, or Windows XP Home Edition, install SP2. The computer must have a wireless network adapter compatible with IEEE 802.11 and 802.1X.

Note

If you are deploying WPS technology in a test lab environment where you have deployed your own enterprise root CA, you must import the CA certificate into the Trusted Root Certification Authorities certificate store on the client computer. If this certificate is not imported into the client certificate store, the client computer will not trust the enterprise root CA and server authentication to the client will fail. For more information, see "Configure certificates in an enterprise test lab environment (optional)" in this paper.

Configure certificates in an enterprise test lab environment (optional)

If you are deploying WPS technology in a test lab, you can obtain server certificates from a public trusted root CA or you can deploy Certificate Services for Windows Server 2003 on your test network. To deploy Certificate Services and enroll certificates to domain member computers (such as the servers on your networks), do the following:

1. On a computer running Windows Server 2003, install Certificate Services.
   For more information, see "To install an enterprise root certification authority" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20035.
2. Add a server certificate template to the certification authority and configure the certification authority to allow computers to request a certificate that is based on the template you create.

For WPS technology in a test lab environment, you must create a server certificate that will be trusted by client computers. The server certificate must meet the requirements stated in this paper. In addition, you must base your certificate on the correct certificate template for the operating system you are running. If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Standard Edition, and your IAS server is a domain member, base your certificate on the **Computer** certificate template. If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Enterprise Edition, and your IAS server is a domain member, base your certificate on the **RAS and IAS Server** certificate template.
For more information, see "To create a certificate template" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20036.

3. Autoenroll certificates to domain member computers. Autoenrollment allows domain member computers to automatically obtain, or enroll, certificates. For WPS technology, autoenroll certificates to servers using the certificate template you created in the previous step.
For more information, see "Planning for autoenrollment deployment" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20037 and "Checklist: Configuring certificate autoenrollment" at http://go.microsoft.com/fwlink/?LinkId=20038.
4. Install the enterprise CA certificate in the Trusted Root Certification Authority certificate store on client computers being used for testing purposes. You can request the enterprise root CA certificate by using Web enrollment services, which is installed with Certificate Services, or you can export the server certificate to a floppy disk, and then import the certificate into the Trusted Root Certification Authority certificate store on the client.
For more information, see "To export a certificate" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20039 and "To import a certificate" at http://go.microsoft.com/fwlink/?LinkId=20040.

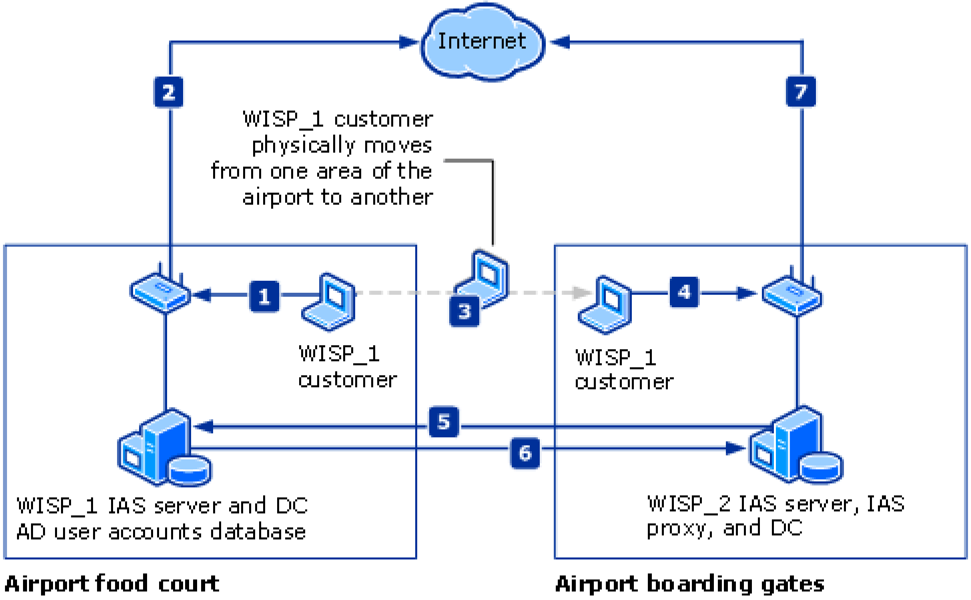
WISP Roaming Agreement Deployments

In some circumstances, two or more wireless ISPs might find it beneficial to create a roaming agreement that allows customers from one WISP to connect to the Internet through the Wi-Fi hotspots owned and operated by the other WISP or WISPs.

For example, one WISP might operate Wi-Fi hotspots in the food court at an airport, while another WISP operates Wi-Fi hotspots at the boarding gates of the same airport. By entering into a roaming agreement, the WISPs provide their customers with the ability to sign up at the food court WISP, roam to the boarding gate WISP, and remain connected to the Internet.

The following two graphics illustrate how a roaming agreement works when two WISPs offer services to customers at the same physical location.

In the illustration below, a new customer connects to WISP_1 at a Wi-Fi hotspot located in the food court of an airport, then roams to the airport boarding gates and connects to an AP at a Wi-Fi hotspot owned and operated by WISP_2.


Internet
2
7
WISP_1 customer physically moves from one area of the airport to another
1
WISP_1 customer
3
4
WISP_1 customer
5
6
WISP_1 IAS server and DC AD user accounts database
WISP_2 IAS server, IAS proxy, and DC
Airport food court
Airport boarding gates

The following text describes the numbered process in the illustration above:

1. A new customer arrives at the airport food court and connects to WISP_1. The customer runs the sign-up wizard, and creates and pays for an account with WISP_1.
2. The customer is authenticated and authorized by the WISP_1 IAS server and is granted access to the Internet.
3. The WISP_1 customer walks from the airport food court to the airport boarding gates.
4. The WISP_2 AP SSID exists in the WISP_1 SSID XML subfile, and the WISP_1 customer's computer associates with the WISP_2 AP. WPS technology on the client computer automatically begins the authentication process using credentials from the WISP_1 account created at the food court.
5. The WISP_2 IAS proxy is configured to forward access requests containing the WISP_1 realm name to the WISP_1 IAS server. The WISP_1 customer Access-Request message is therefore forwarded to the WISP_1 IAS server.
6. The WISP_1 IAS server authenticates and authorizes the user, and sends an Access-Accept message to the WISP_2 IAS proxy. The WISP_2 IAS proxy forwards the Access-Accept to the AP.
7. The WISP_1 customer is granted access to the Internet through the AP owned and operated by WISP_2.

If you have a WISP that you want to configure for use with WPS technology, you can use the scenarios depicted in this paper to deploy the technology. If you want to establish a roaming agreement with another WISP, you can perform the additional steps that follow.

Key roaming agreement configuration steps

If your WISP (WISP_1) has a roaming agreement with another WISP (WISP_2) that allows your customers to connect to the Internet through WISP_2 APs, perform the following steps:

1. Add SSIDs that are advertised by WISP_2 APs to your SSID XML subfile. For more information, see “Using the WPS Authoring Tool” at http://go.microsoft.com/fwlink/?LinkId=41067.
2. Configure the WISP_2 IAS proxy as a RADIUS client on your IAS server. When your customers connect to WISP_2 APs, the WISP_2 IAS proxy forwards authentication requests to your IAS server for authentication and authorization. For more information, see “To add RADIUS clients” at http://go.microsoft.com/fwlink/?LinkId=20031 and “To configure the Message Authenticator attribute and shared secret” at http://go.microsoft.com/fwlink/?LinkId=20032.
3. Configure IAS logging to provide session correlation so that you can effectively use the IAS logs for billing purposes. For more information, see “Remote Access Logging” at http://go.microsoft.com/fwlink/?LinkId=41038 and "Deploying SQL Server Logging with Windows Server 2003 Internet Authentication Service (IAS)" at http://go.microsoft.com/fwlink/?LinkId=41039.

WISP_2 allows customers of WISP_1 to connect to WISP_2 APs. WISP_2 uses IAS as a RADIUS proxy, including the use of connection request policy and a remote RADIUS server group, to identify WISP_1 customers and forward their access requests to the IAS server at WISP_1 for authentication and authorization.

If your WISP functions as WISP_2 in the roaming agreement scenario, perform the following steps:

1. Create a remote RADIUS server group that contains the IAS servers for WISP_1. In the IAS console, run the New Remote RADIUS Server Group wizard: in **Connection Request Processing**, right-click **Remote RADIUS Server Groups**, and then click **New Remote RADIUS Server Group**. After you have run the New Remote RADIUS Server Group wizard, the New Connection Request Policy wizard is automatically launched.
2. Create a connection request policy that forwards WISP_1 customer connection requests to the WISP_1 IAS server. In the IAS console, run the New Connection Request Policy wizard and create a new connection request policy that is configured to **Forward connection requests to a remote RADIUS server for authentication**. In **Realm name**, type the realm name of WISP_1. For example, if the realm name for WISP_1 is example.com, type **example.com**.

Server certificate requirements

Certificates installed on your servers must be obtained from a public trusted root certification authority (such as Verisign or Thawte) and must meet the minimum server certificate requirements. WPS technology uses the PEAP-MS-CHAP v2 authentication method; with PEAP-MS-CHAP v2, the client accepts the server's authentication attempt when the server certificate meets the following requirements:

- The Subject name contains a value. If you issue a certificate to your IAS server that has a blank Subject, the certificate is not available to authenticate your IAS server.

- The computer certificate on the server chains to a public trusted root CA and does not fail any of the checks that are performed by CryptoAPI and specified in the remote access policy.
- The IAS server computer certificate is configured with the Server Authentication purpose in Enhanced Key Usage (EKU) extensions. (The object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1.)
- The server certificate is configured with a required cryptographic service provider (CSP) value of Microsoft RSA SChannel Cryptographic Provider.
- The Subject Alternative Name (SubjectAltName) extension, if used, must contain the DNS name of the server.

With PEAP and EAP-TLS, servers display a list of all installed certificates in the computer certificate store, with the following exceptions:

- Certificates that do not contain the Server Authentication purpose in EKU extensions are not displayed.
- Certificates that do not contain a Subject name are not displayed.
- Registry-based and smart card-logon certificates.

Note

When you deploy PEAP-MS-CHAP v2 on a private network, client computers are configured to validate server certificates by using the **Validate server certificate** option. With WPS technology, however, Wireless Provisioning Services automatically configures this option on client computers running Windows XP.

Active Directory replication

If you are deploying WPS technology in multiple physical locations, calculate your customers' travel times between these locations and adjust Active Directory replication so that user accounts replicate quickly enough for users to log on at different locations. Latency in Active Directory replication might temporarily affect the ability of a customer or user to log on to the network at a different location.

For example, if you deploy Wi-Fi hotspots at a shopping mall in Helsinki, Finland, and at an airport in Florence, Italy, imagine a customer creating an account at one location and then traveling to the other location. Calculate the minimum amount of time it will take your customer to travel from Helsinki to Florence (or from Florence to Helsinki), and then verify that Active Directory replication between these two locations occurs in a shorter amount of time. Thus if it takes a customer eight hours to travel from Helsinki to Florence, configure Active Directory replication between Helsinki and Florence to occur within seven hours of the creation of the account.

If a user account created at one location has not replicated to another location by the time your customer arrives there, authentication will fail and the customer will not be able to log on to your network using their new account credentials.

For more information, see the “Active Directory Replication Topology Technical Reference” on the Web at http://go.microsoft.com/fwlink/?LinkId=41041.

XML Schemas

The following XML schemas are supported for WPS technology:

- **Master file schema.** The master file schema is used to provide the locations of XML subfiles to client computers.
- **Wizard schema.** The wizard schema is used by the sign-up and renewal wizards for account creation or renewal.
- **Register schema.** The register schema contains a node with 3 subnodes: one for sign-up, one for renewal, and one for password expired. The text for each sub-node is a URL that points to the corresponding xml file. The signup sub-node is required, however the renewal and password expired sub-nodes are optional.
- **SSID schema.** The SSID schema is used to provide clients with network Secure Set Identifier information.
- **Locations schema.** The Locations schema is used to provide customers with a list of locations from which they can access your network.
- **Branding schema.** The Branding schema is used to identify your company to your customers with artwork, such as your company logo, that is downloaded and displayed in the client computer user interface.
- **Help schema.** The Help schema is used to provide customers with technical information and assistance.
- **EAP schemas.** The EAP schemas are used to configure connection and user properties on client computers.

The next section describes the XML for each schema.

Master file schema

The following XML describes the XML master file schema for use by HSPs, WISPs, and enterprises to provide client computers with the locations of the XML subfiles and network information.

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.microsoft.com/provisioning/Master"
xmlns="http://www.microsoft.com/provisioning/Master"
elementFormDefault="qualified">
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
schemaLocation="http://www.w3.org/2001/xml.xsd" />
    <xs:element name="Master">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="TTL" type="xs:positiveInteger" />
                <xs:element name="DomainName" type="xs:string" />
                <xs:element name="UpdateFrom" type="anyHttps" />
                <xs:element name="LangSet" minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Subfile" maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element name="URL" type="anyHttps" />
                                        <xs:element name="Version"
type="xs:positiveInteger" />
                                    </xs:sequence>
                                    <xs:attribute name="Name" type="xs:string"
use="required" />
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                        <xs:attribute ref="xml:lang" use="required" />
                    </xs:complexType>
                </xs:element>
                <xs:element name="OtherMasters" minOccurs="0">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="MasterURL" type="anyHttps"
maxOccurs="unbounded" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:simpleType name="anyHttps">
        <xs:restriction base="xs:string">
            <xs:pattern value="https://(.)+" />
        </xs:restriction>
    </xs:simpleType>
</xs:schema>
```

Wizard schema

The following XML describes the Wizard XML schema used by the sign-up and renewal wizards while customers create or renew an account.

```
<?xml version="1.0"?>
<xs:schema targetNamespace="http://www.microsoft.com/provisioning/Wizard"
xmlns:mstns="http://www.microsoft.com/provisioning/Wizard"
       xmlns="http://www.microsoft.com/provisioning/Wizard"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
       xmlns:msdata="urn:schemas-microsoft-com:xml-msdata"
attributeFormDefault="qualified" elementFormDefault="qualified">
       <xs:element name="wizard">
              <xs:complexType>
                      <xs:sequence>
                             <xs:element name="purpose" minOccurs="1"
maxOccurs="1">
                                    <xs:simpleType>
                                           <xs:restriction base="xs:string">
                                                  <xs:enumeration value="signup"
/>
                                                  <xs:enumeration
value="renewal" />
                                                  <xs:enumeration
value="password" />
                                           </xs:restriction>
                                    </xs:simpleType>
                             </xs:element>
                             <xs:element name="postToUrl" type="xs:string"
minOccurs="1" maxOccurs="1" />
                             <xs:element name="panel-welcome" minOccurs="1"
maxOccurs="1">
                                    <xs:complexType>
                                           <xs:sequence>
                                                  <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
```

```
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="icon"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="branding"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                            </xs:sequence>
                                     </xs:complexType>
                              </xs:element>
                              <xs:element name="panel-plan" minOccurs="1"
maxOccurs="1">
                                     <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" msdata:Ordinal="0" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" msdata:Ordinal="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" msdata:Ordinal="2" />
                                                   <xs:element name="plan"
minOccurs="1" maxOccurs="unbounded">
                                                          <xs:complexType>
                                                                 <xs:sequence>

<xs:element name="title" type="xs:string" minOccurs="0" maxOccurs="1"
msdata:Ordinal="0" />

<xs:element name="description" type="xs:string" minOccurs="0" maxOccurs="1"
msdata:Ordinal="1" />
                                        <xs:element name="fulldescription"
minOccurs="0" maxOccurs="1" msdata:Ordinal="2" >
                                            <xs:complexType>
                                                <xs:sequence>
                                                    <xs:element name="MHTML"
type="xs:string" minOccurs="1" maxOccurs="1"/>
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:element>

<xs:element name="includePanels" minOccurs="1" maxOccurs="1">

<xs:complexType>

       <xs:sequence>

              <xs:element name="includePanel" minOccurs="0"
maxOccurs="unbounded">

                     <xs:complexType>

                            <xs:attribute name="name" form="unqualified"
type="xs:string" />

                            <xs:attribute name="id" use="required"
form="unqualified" type="xs:string" />

                     </xs:complexType>

              </xs:element>

       </xs:sequence>
```

```
</xs:complexType>

</xs:element>
                                                                  </xs:sequence>
                                                                  <xs:attribute
name="category" form="unqualified" type="xs:string" />
                                                                  <xs:attribute
name="selected" form="unqualified" type="xs:boolean" />
                                                           </xs:complexType>
                                                   </xs:element>
                                            </xs:sequence>
                                            <xs:attribute name="hint"
use="optional" form="unqualified" type="xs:string" />
                                            <xs:attribute name="error"
use="optional" form="unqualified" type="xs:string" />
                                     </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-promotion" minOccurs="0"
maxOccurs="unbounded">
                                     <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element
name="promotionalcode" type="editField" minOccurs="0" maxOccurs="1"
nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                     </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-personal" minOccurs="0"
maxOccurs="unbounded">
                                     <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="salutation"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="first-name"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="middle-
initial" type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="last-name"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="suffix"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="company"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="jobtitle"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="language-
preference" type="comboBox" minOccurs="0" maxOccurs="1" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-contact" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="address1"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="address2"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="city"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="state"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="country"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="zipcode"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="telephone1"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="telephone2"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="email"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-privacy" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="check1"
type="check box" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="check2"
type="check box" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="check3"
type="check box" minOccurs="0" maxOccurs="1" nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-creditcard" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
```

```
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="card-name"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="card-number"
type="nonReadOnlyEditField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="card-
expdate" type="nonReadOnlyEditField" minOccurs="0" maxOccurs="1"
nillable="true" />
                                                   <xs:element name="card-
securitycode" type="nonReadOnlyEditField" minOccurs="0" maxOccurs="1"
                                                           nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-billing" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="first-name"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="middle-
initial" type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="last-name"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="suffix"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="address1"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="address2"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="city"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="state"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="country"
type="comboBox" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="zipcode"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="telephone1"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="telephone2"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-coupon" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
```

```
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="coupon"
type="editField" minOccurs="1" maxOccurs="1" nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-credentials" minOccurs="0"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="username"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                                   <xs:element name="password"
type="editField" minOccurs="0" maxOccurs="1" nillable="true" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-terms" minOccurs="1"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="terms"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                    </xs:complexType>
                             </xs:element>
                             <xs:element name="panel-post" minOccurs="1"
maxOccurs="unbounded">
                                    <xs:complexType>
                                            <xs:sequence>
                                                   <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                   <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                            </xs:sequence>
                                            <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
```

```
                                        </xs:complexType>
                                </xs:element>
                                <xs:element name="panel-finish" minOccurs="1"
maxOccurs="unbounded">
                                        <xs:complexType>
                                                <xs:sequence>
                                                        <xs:element name="title"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                        <xs:element name="subtitle"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                        <xs:element name="body"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                        <xs:element name="info"
type="xs:string" minOccurs="0" maxOccurs="1" />
                                                </xs:sequence>
                                                <xs:attribute name="id"
use="required" form="unqualified" type="xs:string" />
                                        </xs:complexType>
                                </xs:element>
                        </xs:sequence>
                        <xs:attribute name="error" use="optional"
form="unqualified" type="xs:string" />
                        <xs:attribute name="hint" use="optional" form="unqualified"
type="xs:string" />
                </xs:complexType>
        </xs:element>
        <xs:complexType name="editField">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute name="required" use="optional"
form="unqualified" type="xs:boolean" />
                                <xs:attribute name="maxlen" use="optional"
form="unqualified" type="xs:positiveInteger" />
                                <xs:attribute name="hint" use="optional"
form="unqualified" type="xs:string" />
                                <xs:attribute name="error" use="optional"
form="unqualified" type="xs:string" />
                                <xs:attribute name="readonly" use="optional"
form="unqualified" type="xs:boolean" />
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="nonReadOnlyEditField">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute name="required" use="optional"
form="unqualified" type="xs:boolean" />
                                <xs:attribute name="maxlen" use="optional"
form="unqualified" type="xs:positiveInteger" />
                                <xs:attribute name="hint" use="optional"
form="unqualified" type="xs:string" />
                                <xs:attribute name="error" use="optional"
form="unqualified" type="xs:string" />
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
        <xs:complexType name="comboBox">
                <xs:sequence>
                        <xs:element name="entry" minOccurs="1"
maxOccurs="unbounded" nillable="true">
                                <xs:complexType>
                                        <xs:simpleContent>
                                                <xs:extension base="xs:string">
```

```
                                                        <xs:attribute name="selected"
form="unqualified" type="xs:boolean" />
                                                </xs:extension>
                                        </xs:simpleContent>
                                </xs:complexType>
                        </xs:element>
                </xs:sequence>
                <xs:attribute name="required" use="optional" form="unqualified"
type="xs:boolean" />
                <xs:attribute name="hint" use="optional" form="unqualified"
type="xs:string" />
                <xs:attribute name="error" use="optional" form="unqualified"
type="xs:string" />
                <xs:attribute name="readonly" use="optional" form="unqualified"
type="xs:boolean" />
        </xs:complexType>
        <xs:complexType name="check box">
                <xs:simpleContent>
                        <xs:extension base="xs:string">
                                <xs:attribute name="check" form="unqualified"
type="xs:boolean" />
                        </xs:extension>
                </xs:simpleContent>
        </xs:complexType>
</xs:schema>
```

Register schema

The following XML describes the Register schema.

```
<?xml version="1.0"?>

<xs:schema id="registerFile"
targetNamespace="http://www.microsoft.com/provisioning/Register"
xmlns="http://www.microsoft.com/provisioning/Register"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:msdata="urn:schemas-microsoft-
com:xml-msdata" attributeFormDefault="qualified" elementFormDefault="qualified">
  <xs:element name="register">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="signup"          type="anyHttps" minOccurs="1"
maxOccurs="1" />
        <xs:element name="renewal"         type="anyHttps" minOccurs="0"
maxOccurs="1" />
        <xs:element name="passwordExpired" type="anyHttps" minOccurs="0"
maxOccurs="1" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="registerFile" msdata:IsDataSet="true"
msdata:EnforceConstraints="False">
    <xs:complexType>
      <xs:choice maxOccurs="1">
        <xs:element ref="register" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
  <xs:simpleType name="anyHttps">
    <xs:restriction base="xs:string">
      <xs:pattern value="https://(.)+"/>
    </xs:restriction>
  </xs:simpleType>
```

```
</xs:schema>
```

SSID schema

The following XML describes the Secure Set Identifier (SSID) schema.

```
<?xml version="1.0" encoding="utf-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           targetNamespace="http://www.microsoft.com/provisioning/SSID"
           xmlns="http://www.microsoft.com/provisioning/SSID"
           elementFormDefault="qualified">
  <xs:element name="SSIDs">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" name="ssid">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Priority" type="xs:positiveInteger" minOccurs="0"
/>
              <xs:element name="Connection" minOccurs="0" >
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="IBSS" />
                    <xs:enumeration value="ESS" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="Authentication" minOccurs="0" >
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Open" />
                    <xs:enumeration value="Shared" />
                    <xs:enumeration value="WPA" />
                    <xs:enumeration value="WPAPSK" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="Encryption" minOccurs="0" >
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="None" />
                    <xs:enumeration value="WEP" />
                    <xs:enumeration value="TKIP" />
                    <xs:enumeration value="CCMP" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="KeyIndex" type="xs:positiveInteger" minOccurs="0"
/>
              <xs:element name="IEEE802.1X" type="xs:string" minOccurs="0" />
              <xs:element name="Non802.1XURL" type="xs:anyURI" minOccurs="0" />
            </xs:sequence>
            <xs:attribute name="Name" type="xs:string" use="required" />
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Locations schema

The following XML describes the Locations schema, which provides your customers with the locations of your Wi-Fi hotspots.

```
<?xml version="1.0" ?>
<xs:schema id="hotspotfinder"
targetNamespace="http://www.microsoft.com/provisioning/HotSpotLocation"
xmlns="http://www.microsoft.com/provisioning/HotSpotLocation"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:msdata="urn:schemas-microsoft-
com:xml-msdata" attributeFormDefault="qualified" elementFormDefault="qualified">
    <xs:element name="hotspotfinder" msdata:IsDataSet="true"
msdata:EnforceConstraints="False">
        <xs:complexType>
            <xs:choice maxOccurs="unbounded">
                <xs:element name="entry">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="city" type="xs:string"
minOccurs="0" />
                            <xs:element name="state" type="xs:string"
minOccurs="0" />
                            <xs:element name="country" type="xs:string"
minOccurs="0" />
                            <xs:element name="zipcode" type="xs:string"
minOccurs="0" />
                            <xs:element name="operator" type="xs:string"
minOccurs="0" />
                            <xs:element name="location" type="xs:string"
minOccurs="0" />
                            <xs:element name="address" type="xs:string"
minOccurs="0" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:choice>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Branding schema

The following XML describes the branding schema, which you can use to identify your company to your customers.

```
<?xml version="1.0" ?>
<xs:schema id="BrandingFile"
targetNamespace="http://www.microsoft.com/provisioning/Branding"
xmlns="http://www.microsoft.com/provisioning/Branding"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:msdata="urn:schemas-microsoft-
com:xml-msdata" attributeFormDefault="qualified" elementFormDefault="qualified">
    <xs:element name="Branding">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="FriendlyName" type="xs:string" minOccurs="1"
maxOccurs="1" />
                <xs:element name="PostConnectedAction" type="xs:string"
minOccurs="0" maxOccurs="1"/>
                <xs:element name="ServiceDescription" type="xs:string"
minOccurs="1" maxOccurs="1"/>
```

```
                <xs:element name="Logo" type="xs:string" minOccurs="1"
maxOccurs="1" />
                <xs:element name="Header" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="BrandingFile" msdata:IsDataSet="true"
msdata:EnforceConstraints="False">
        <xs:complexType>
            <xs:choice maxOccurs="1">
                <xs:element ref="Branding" />
            </xs:choice>
        </xs:complexType>
    </xs:element>

</xs:schema>
```

Help schema

The following XML is the Help schema that allows HSPs and WISPs to provide customers with user assistance.

```
<?xml version="1.0" ?>
<xs:schema id="HelpFile"
targetNamespace="http://www.microsoft.com/provisioning/Help"
xmlns="http://www.microsoft.com/provisioning/Help"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:msdata="urn:schemas-microsoft-
com:xml-msdata" attributeFormDefault="qualified" elementFormDefault="qualified">
    <xs:element name="Help">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="MHTML" type="xs:string" minOccurs="1"
maxOccurs="1"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="HelpFile" msdata:IsDataSet="true"
msdata:EnforceConstraints="False">
        <xs:complexType>
            <xs:choice maxOccurs="1">
                <xs:element ref="Help" />
            </xs:choice>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

EAP schemas

There are eight EAP schemas, including the following:

Connection properties schemas:

- Base EAP Connection Properties schema
- EAP Connection Properties schema
- MS-CHAP v2 Connection Properties schema
- Microsoft PEAP Connection Properties schema

User properties schemas:

- Base EAP User Properties schema
- EAP User Properties schema
- MS-CHAP v2 User Properties schema
- Microsoft PEAP User Properties schema

Each of these schemas is described below.

Connection properties schemas

Following are the four connection properties schemas.

Base EAP Connection Properties schema

The following XML describes the Base EAP Connection Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/BaseEapConnectionPro
pertiesV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      version="1.0"
   >
   <xs:complexType name="BaseEapTypeParameters" abstract="true" />
   <xs:complexType name="BaseEapParameters">
      <xs:sequence>
         <xs:element name="Type" type="xs:integer"/>
         <xs:any
               processContents="lax"
               minOccurs="0"
               maxOccurs="unbounded"
               namespace="##any"
         />
         <!-- One or more elements of the kind as follows should go in here. -->
         <!--
         <xs:element ref="EapType" maxOccurs="unbounded" />
         -->
      </xs:sequence>
   </xs:complexType>
   <xs:element name="EapType" type="BaseEapTypeParameters" abstract="true"/>
   <xs:element name="Eap" type="BaseEapParameters"/>
</xs:schema>
```

EAP Connection Properties schema

The following XML describes the EAP Connection Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/EapConnectionPropert
iesV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/EapConnectionPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapConnectionPrope
rtiesV1"
      version="1.0"
   >
   <xs:import
         namespace="http://www.microsoft.com/provisioning/BaseEapConnectionProper
tiesV1"
         schemaLocation="BaseEapConnectionPropertiesV1.xsd"
   />
   <xs:element name="Connections">
      <xs:complexType>
         <xs:sequence>
            <xs:element name="Connection" minOccurs="0" maxOccurs="unbounded">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="Name" type="xs:string" />
                     <xs:element ref="baseEap:Eap" maxOccurs="unbounded" />
                  </xs:sequence>
               </xs:complexType>
            </xs:element>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

MS-CHAP v2 Connection Properties schema

The following XML describes the MS-CHAP v2 Connection Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/MsChapV2ConnectionPr
opertiesV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/MsChapV2ConnectionPropertiesV1
"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapConnectionPrope
rtiesV1"
      version="1.0"
   >
   <xs:import
      namespace="http://www.microsoft.com/provisioning/BaseEapConnectionPropertie
sV1"
      schemaLocation="BaseEapConnectionPropertiesV1.xsd"
   />
   <xs:element name="EapType" substitutionGroup="baseEap:EapType">
      <xs:complexType>
         <xs:complexContent>
            <xs:extension base="baseEap:BaseEapTypeParameters"/>
         </xs:complexContent>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

Microsoft PEAP Connection Properties schema

When you configure the PEAP Connection Properties XML file, change the value of **DisableUserPromptForServerValidation** from zero (0, or false) to one (1, or true). Also add the Secure Hash Algorithm (SHA-1) hash of your trusted root CA certificate to **TrustedRootCA**. In the following example, the SHA-1 hash of the trusted root CA certificate is the hexadecimal string: **a4 34 89 15 9a 52 0f 0d 93 d0 32 cc af 37 e7 fe 20 a8 b4 19**. When you use a SHA-1 hash in the XML file, you can keep the spaces between the pairs of numbers in the hash - you do not need to delete the spaces.

```
<msPeap:DisableUserPromptForServerValidation>1</msPeap:DisableUserPromptForServer
Validation>
<msPeap:TrustedRootCA>a4 34 89 15 9a 52 0f 0d 93 d0 32 cc af 37 e7 fe 20 a8 b4
19</msPeap:TrustedRootCA>
```

You can specify more than one trusted root CA certificate by inserting additional lines that contain **TrustedRootCA** and the SHA-1 hashes of the additional certificates. The following example depicts an XML file that designates three trusted root CA certificates:

```
<msPeap:DisableUserPromptForServerValidation>1</msPeap:DisableUserPromptForServer
Validation>
<msPeap:TrustedRootCA>SHA-1 hash of the CA 1 certificate</msPeap:TrustedRootCA>
<msPeap:TrustedRootCA>SHA-1 hash of the CA 2 certificate</msPeap:TrustedRootCA>
<msPeap:TrustedRootCA>SHA-1 hash of the CA 3 certificate</msPeap:TrustedRootCA>
```

To obtain the SHA-1 hash of a trusted root CA certificate

1. Open the Certificates snap-in for the Local Computer certificate store.
2. In the left pane, double-click **Certificates (Local Computer)**, and then double-click the **Trusted Root Certification Authorities** subfolder.
3. The Certificates folder is a subfolder of the Trusted Root Certification Authorities folder. Click the **Certificates** folder.
4. In the details pane, browse to the certificate for your trusted root CA. Double-click the certificate. The **Certificate** dialog box opens.
5. In the **Certificate** dialog box, click the **Details** tab.
6. In the list of fields, select **Thumbprint**.
7. In the lower pane, the hexadecimal string that is the SHA-1 hash of your certificate is displayed. Select the SHA-1 hash and press the Windows keyboard shortcut for the Copy command (CTRL+C) to copy the hash to the Windows clipboard.

For more information about using the Certificates snap-in, see "To manage certificates for a computer" in Windows XP Help and Support Center or on the Web at http://go.microsoft.com/fwlink/?LinkId=41042.

For more information about Windows keyboard shortcuts, see "Windows keyboard shortcuts overview" in Windows XP Help and Support Center or on the Web at http://go.microsoft.com/fwlink/?LinkId=36303.

The following XML describes the Microsoft PEAP Connection Properties schema.

```
<?xml version="1.0"?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/MsPeapConnectionProp
ertiesV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapConnectionPrope
rtiesV1"
      version="1.0"
   >
   <xs:import
         namespace="http://www.microsoft.com/provisioning/BaseEapConnectionProper
tiesV1"
         schemaLocation="BaseEapConnectionPropertiesV1.xsd"
   />

   <xs:element name="EapType" substitutionGroup="baseEap:EapType">
      <xs:complexType>
         <xs:complexContent>
            <xs:extension base="baseEap:BaseEapTypeParameters">
               <xs:sequence>
                  <xs:element
                        name="ServerValidation"
                        type="ServerValidationParameters"
                        minOccurs="0"
                  />
                  <xs:element name="FastReconnect" type="xs:boolean"
minOccurs="0"/>
                  <xs:element name="InnerEapOptional" type="xs:boolean"
minOccurs="0"/>
                  <xs:element ref="baseEap:Eap" minOccurs="0"
maxOccurs="unbounded" />
               </xs:sequence>
            </xs:extension>
         </xs:complexContent>
      </xs:complexType>
   </xs:element>

   <xs:complexType name="ServerValidationParameters">
      <xs:sequence>
         <xs:element
               name="DisableUserPromptForServerValidation"
               type="xs:boolean"
               minOccurs="0"
         />
         <!-- A set of server names delimited by semicolons -->
         <!-- each server name can be represented by regular -->
         <!-- expressions -->
         <xs:element name="ServerNames" type="xs:string" minOccurs="0" />
         <!-- The thumbprint of a trusted root CA is -->
         <!-- a hexadecimal string that contains -->
         <!-- the SHA-1 hash of the certificate. -->
         <xs:element
               name="TrustedRootCA"
               type="xs:hexBinary"
               minOccurs="0"
               maxOccurs="unbounded"
         />
      </xs:sequence>
   </xs:complexType>
</xs:schema>
```

User properties schemas

Following are the four user properties schemas.

Base EAP User Properties schema

The following XML describes the Base EAP User Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/BaseEapUserPropertie
sV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      version="1.0"
   >
   <xs:complexType name="BaseEapTypeParameters" abstract="true" />
   <xs:complexType name="BaseEapParameters" >
      <xs:sequence>
         <xs:element name="Type" type="xs:integer"/>
         <xs:any
               minOccurs="0"
               processContents="lax"
               maxOccurs="unbounded"
               namespace="##any"
         />
         <!-- One or more elements of the kind as follows should go in here. -->
         <!--
         <xs:element ref="EapType" maxOccurs="unbounded" />
         -->
      </xs:sequence>
   </xs:complexType>
   <xs:element name="EapType" type="BaseEapTypeParameters" abstract="true"/>
   <xs:element name="Identity" type="xs:string" abstract="true" />
   <xs:element name="Eap" type="BaseEapParameters"/>
</xs:schema>
```

EAP User Properties schema

The following XML describes the EAP User Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/EapUserPropertiesV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/EapUserPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV
1"
      version="1.0"
   >
   <xs:import
         namespace="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV1
"
         schemaLocation="BaseEapUserPropertiesV1.xsd"
   />
   <xs:element name="User">
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="baseEap:Eap" maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

MS-CHAP v2 User Properties schema

The following XML describes the MS-CHAP v2 User Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/MsChapV2UserProperti
esV1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/MsChapV2UserPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV
1"
      version="1.0"
   >
   <xs:import
         namespace="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV1
"
         schemaLocation="BaseEapUserPropertiesV1.xsd"
   />
   <xs:element name="Username" substitutionGroup="baseEap:Identity"/>
   <xs:element name="EapType" substitutionGroup="baseEap:EapType">
      <xs:complexType>
         <xs:complexContent>
```

```
            <xs:extension base="baseEap:BaseEapTypeParameters">
               <xs:sequence>
                  <xs:element ref="Username" minOccurs="0" />
                  <xs:element name="Password" type="xs:string" minOccurs="0" />
                  <xs:element name="LogonDomain" type="xs:string" minOccurs="0"/>
               </xs:sequence>
            </xs:extension>
         </xs:complexContent>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

Microsoft PEAP User Properties schema

The following XML describes the Microsoft PEAP User Properties schema.

```
<?xml version="1.0" ?>
<xs:schema
      targetNamespace="http://www.microsoft.com/provisioning/MsPeapUserProperties
V1"
      elementFormDefault="qualified"
      xmlns="http://www.microsoft.com/provisioning/MsPeapUserPropertiesV1"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:baseEap="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV
1"
      version="1.0"
   >
   <xs:import
         namespace="http://www.microsoft.com/provisioning/BaseEapUserPropertiesV1
"
         schemaLocation="BaseEapUserPropertiesV1.xsd"
   />
   <xs:element name="RoutingIdentity" substitutionGroup="baseEap:Identity"/>
   <xs:element name="EapType" substitutionGroup="baseEap:EapType">
      <xs:complexType>
         <xs:complexContent>
            <xs:extension base="baseEap:BaseEapTypeParameters">
               <xs:sequence>
                  <xs:element ref="RoutingIdentity" minOccurs="0"/>
                  <xs:element ref="baseEap:Eap" minOccurs="0"
maxOccurs="unbounded" />
               </xs:sequence>
            </xs:extension>
         </xs:complexContent>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

How to use IAS with a third-party user accounts database

If you deploy a third-party user accounts database for use with WPS technology, you must create and install two IAS extension DLLs:

- An authorization extension DLL that provides the URL PEAP-TLV if the customer or user account does not exist, is expired, or is disabled.
- An authentication extension DLL that retrieves the customer's or user's plaintext password from the third-party user accounts database and returns the password to IAS.

You can configure IAS for use with a third-party user accounts database by:

- Creating and installing an EAP authentication extension DLL. Because PEAP-MS-CHAP v2 is required for WPS technology, you must write an EAP authentication extension DLL to retrieve the password from the third-party user account database.
- Creating a new user account on your IAS server.
- Configuring a connection request policy on your IAS server that maps all user accounts to one account on the IAS server.
- Configuring a remote access policy in IAS that authorizes accounts mapped to the new account.

Create an IAS authentication extension DLL

Your IAS authentication extension DLL can use the following attributes:

- **ratProviderName**. This attribute indicates the remote RADIUS server group to which to forward the authentication request. The **ratProviderType** attribute is read-only. If **ratProviderType** is a RADIUS proxy, the extension DLL can change the value of **ratProviderName** to indicate the remote RADIUS server group to which the request should be forwarded.
- **ratClearTextPassword**. To support third-party user database use with PEAP-MS-CHAP v2, the IAS extension authentication DLL, this attribute retrieves the user password from the third-party user accounts database and sends this information back to IAS.

The IAS authentication extension DLL must also keep track of **ratUniqueId**. After the password is retrieved for the **ratUniqueId**, you do not need to retrieve the password again. If the account does not exist, is disabled, or is expired, the reason code **ratRejectReasonCode** must be sent back to IAS.

For more information, see “How to create an IAS extension DLL and a URL PEAP-TLV” in this paper.

Install the IAS authentication extension DLL on the IAS server

After you have created your IAS extension DLL, you must install the DLL on your IAS server and configure DLL registry keys according to your needs.

To install your DLL

1. Open Command Prompt and change directories to the folder that contains your DLL.
2. Type the following: **regsvr32** *DLL_name.dll*, where *DLL_name.dll* is the name of your DLL file.

Create a user account on the IAS server

You can create user accounts and group accounts in Active Directory to manage domain users. When you are not using Active Directory as your user accounts database, you can create user accounts and group accounts on a local computer to manage users specific to that computer.

To deploy IAS with a third-party user accounts database, you must create one user account on your IAS server to which you can map all user accounts in the third-party database. Your extension DLL performs authentication against the third-party database, while IAS performs authorization with the user account you create on the IAS server.

To create a user account on the IAS server

1. Open **Computer Management**. To open Computer Management, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. In **Computer Management**, under **System Tools**, click **Local Users and Groups**. In the details pane, double-click **Users**.
3. On the **Action** menu, click **New User**. The **New User** dialog box opens.
4. In **User Name**, type a name for the account. In **Password** and **Confirm Password**, type a strong password. Clear the **User must change password at next logon** check box, and then select the **User cannot change password** and **Password never expires** check boxes.
5. Click **Create**, and then click **Close**.

> **Note**
>
> By default, user accounts created on the local computer in Windows Server 2003 have dial-in properties set to **Control access through Remote Access Policy**. This is the correct setting for the user account you have created and the setting should not be changed.

For more information, see "Strong passwords" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=34427.

Configure IAS connection request policy

To configure IAS connection request policy

1. Open **Internet Authentication Service**.
2. In the console tree, double-click **Connection Request Processing**, and then click **Connection Request Policies**.
3. In the details pane, double-click the policy that you want to configure. For example, double-click the default policy, named **Use Windows authentication for all users**.
4. In the **Properties** dialog box, click **Edit Profile**.
5. On the **Authentication** tab, click Authenticate requests on this server.
6. On the **Attribute** tab, confirm that the User-Name attribute is selected in **Attribute**. If it is not selected, click **Attribute**, select **User-Name**, and then click **Add**.
7. The **Attribute Manipulation Rule** dialog box opens. In **Find**, type pattern matching syntax that matches all values for User-Name that are passed to IAS by your access servers. For example, if values for the User-Name attribute match the syntax *user@example.com*, type **(.*)@.***.
8. In **Replace with**, type the name of the local computer and the name of the user account you created on the IAS server in the following syntax: *computer-name\user*.
9. Click **OK** twice.

> **Note**
>
> If you copy the IAS connection request policy described above to another IAS server, change the attribute manipulation rule by changing the computer name and user name in the rule to the computer name of the new server and the user name of an account on the new server. If you do not change the computer name and user name specified in the rule, attribute manipulation on the new server will not work.

For more information, see "Pattern Matching Syntax" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=41049.

Configure IAS remote access policy

There are two remote access policies configured for WPS technology. The Guest access policy provides network parameters and rules for users connecting as guest. The Valid users access policy provides network parameters and rules for users who have valid WISP accounts.

To configure the Guest access policy

1. Open the Internet Authentication Service snap-in and, if necessary, double-click **Internet Authentication Service**.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Use the **New Remote Access Policy Wizard** to create a policy. For the WISP guest access policy, you can choose the following:
   a. For **How do you want to set up this policy?** verify that **Use the wizard to set up a typical policy for a common scenario** is selected.
   b. For **Policy name**, type **Guest access** (or type another name for your policy that you prefer).
   c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
   d. For **Grant access based on the following,** click **User**.
   e. In **Select the EAP type for this policy**, select **Protected EAP (PEAP)**, and then click **Configure**.
   f. In **Certificate issued**, select the certificate that you want the IAS server to use to verify its identity to client computers. Also select the **Enable Fast Reconnect** check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created.

To complete configuration of the Guest access policy

1. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
2. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
3. In the policy Properties dialog box, click Grant remote access permission.
4. Click Edit Profile. On the Authentication tab, in Unauthenticated access, click Allow clients to connect without negotiating an authentication method.

Configure the Valid users policy

To configure the Valid users remote access policy

1. Open **Internet Authentication Service**.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.
3. Use the **New Remote Access Policy Wizard** to create a policy. For the remote access policy, you can choose the following:

a. For **How do you want to set up this policy?** verify that **Use the wizard to set up a typical policy for a common scenario** is selected.
b. For **Policy name**, type **Valid Users** (or type another name for your policy that you prefer).
c. For **Select the method of access for which you want to create a policy**, click **Wireless**.
d. For **Grant access based on the following,** click **User**.
e. In **Select the EAP type for this policy**, select **Protected EAP (PEAP)**, and then click **Configure**.
f. In **Certificate issued**, select the certificate that you want the IAS server to use to verify its identity to client computers. Also check the **Enable Fast Reconnect** check box.

After you have completed creating the policy and have closed the wizard by clicking **Finish**, you need to perform additional policy configuration.

To complete configuration of the Valid users remote access policy

1. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created.
2. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
3. In the policy Properties dialog box, click **Grant remote access permission**.
4. Click **Edit Profile**. On the **Authentication** tab, clear all check boxes except Strongest encryption (MPEE 128 bit).

> **Note**
>
> If you are isolating client computers by using VLANs, you must also add VLAN attributes to the Valid Users access policy. If you are isolating client computers by using IP filters, you must add IP filters to the access policy.

PEAP-MS-CHAP v2

Protected Extensible Authentication Protocol (PEAP) is a member of the family of Extensible Authentication Protocol (EAP) protocols. PEAP uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as an Internet Authentication Service (IAS) or Remote Authentication Dial-In User Service (RADIUS) server. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-MS-CHAP v2, that can operate through the TLS encrypted channel provided by PEAP. PEAP is used as an authentication method for 802.1X wireless client computers, but is not supported for virtual private network (VPN) or other remote access clients.

PEAP authentication process

There are two stages in the PEAP authentication process between PEAP client and authenticator. The first stage sets up a secure channel between the PEAP client and the authenticating server. The second stage provides EAP authentication between the

EAP client and authenticator.

PEAP stage one: TLS encrypted channel

The wireless client associates with a wireless access point. An IEEE 802.11-based association provides an Open System or Shared Key authentication before a secure association is created between the client and access point. After the IEEE 802.11-based association is successfully established between the client and access point, the TLS session is negotiated with the access point. After authentication is successfully completed between the wireless client and the server (for example, an IAS server), the TLS session is negotiated between them. The key that is derived during this negotiation is used to encrypt all subsequent communication.

PEAP stage two: EAP-authenticated communication

Complete EAP communication, including EAP negotiation, occurs inside the TLS channel created by PEAP during the first stage of the PEAP authentication process. The IAS server authenticates the user or the client computer with the method that is determined by the EAP type and selected for use within PEAP. For deployments of WPS technology, EAP-MS-CHAP v2 is the authentication type used within PEAP. The access point only forwards messages between wireless client and RADIUS server —the access point (or a person monitoring it) cannot decrypt these messages because it is not the TLS end point.

Packet sequence for a successful authentication attempt with valid credentials

After PEAP stage one occurs and the TLS channel is created between the IAS server and the 802.1X wireless client, for a successful authentication attempt where the user has supplied valid password-based credentials using WPS technology with PEAP-MS-CHAP v2, the RADIUS message sequence is:

1. The IAS server sends an identity request message to the client: EAP-Request/Identity.
2. The client responds with an identity response message: EAP-Response/Identity.
3. The IAS server sends an MS-CHAP v2 challenge message: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. The client responds with an MS-CHAP v2 challenge and response: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response).
5. The IAS server sends back an MS-CHAP v2 success packet when the server has successfully authenticated the client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. The client responds with an MS-CHAP v2 success packet when the client has successfully authenticated the server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
7. The IAS server sends an EAP-TLV indicating successful authentication.
8. The client responds with an EAP-TLV status success message.
9. The server completes authentication and sends an EAP-Success message using plaintext. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

Packet sequence for a successful guest authentication

After PEAP stage one occurs and the TLS channel is created between the IAS server and the 802.1X wireless client, for the case of an authentication failure being converted to a successful guest authentication using WPS technology with PEAP-MS-CHAP v2, the RADIUS message sequence is:

1. The IAS server sends an identity request message to the client: EAP-Request/Identity.
2. The client responds with an identity response message: EAP-Response/Identity.
3. The IAS server sends an MS-CHAP v2 challenge message: EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge).
4. The client responds with an MS-CHAP v2 challenge and response: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response). The authentication fails and the WPS extension DLL on the server determines that the user authentication should succeed with limited access.
5. The IAS server sends back an MS-CHAP v2 success packet when the server has successfully authenticated the client: EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success).
6. The client responds with an MS-CHAP v2 success packet when the client has successfully authenticated the server: EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success).
7. The IAS server sends an EAP-TLV indicating successful authentication, as well as other TLVs, including a URL PEAP-TLV that provides the client with the URL of the provisioning server (or a URL to change password).
8. The client responds with an EAP-TLV status success message.
9. The server completes authentication and sends an EAP-Success message using plaintext. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

Packet sequence for other WPS cases (disabled, expired, and unknown accounts)

After PEAP stage one occurs and the TLS channel is created between the IAS server and the 802.1X wireless client, for other WPS cases (disabled, expired and unknown accounts) with PEAP-MS-CHAP v2, the RADIUS message sequence is:

1. The IAS server sends an identity request message to the client: EAP-Request/Identity.
2. The client responds with an identity response message: EAP-Response/Identity.
3. The IAS server discovers that the account is disabled, expired, or unknown. The WPS extension DLL on the server decides that the user authentication should succeed with limited access.
4. The IAS server sends an EAP-TLV indicating successful authentication, as well as other TLVs, including a URL PEAP-TLV that provides the client with the URL of the provisioning server.
5. The client responds with an EAP-TLV status success message.
6. The server completes authentication and sends an EAP-Success message using plaintext. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

For more information about PEAP, see "Protected EAP Protocol (PEAP)" at http://go.microsoft.com/fwlink/?LinkId=41301.

For more information about EAP-MS-CHAP v2, see “Microsoft EAP CHAP Extensions” at http://go.microsoft.com/fwlink/?LinkId=41306.

How to create an IAS extension DLL and a URL PEAP-TLV

There are two types of PEAP-TLVs used by IAS and WPS:

- **Status-Result PEAP-TLV with Type=3.** The Status-Result PEAP-TLV is sent by the IAS server and provides client computers with an authentication response (either accept or reject).
- **URL PEAP-TLV with Type=8.** The URL PEAP-TLV is sent by an IAS extension DLL that you create and install on your IAS servers. The URL PEAP-TLV provides client computers with the location of the provisioning server so that the client can download XML files from the server.

IAS always sends a Status-Result PEAP-TLV containing an authentication response. Depending upon circumstances outlined below, your IAS extension DLL might include a URL PEAP-TLV inside the same message as the Status-Result PEAP-TLV.

The process for providing your IAS servers with an extension DLL capable of processing messages is as follows:

- Create an IAS extension DLL that can identify and act upon access requests that should be provisioned and allowed, while passing through all other access requests without any modifications.
- Add the DLL to the Windows registry, so that IAS calls the DLL during the processing of each message. After your DLL identifies an access request upon which it needs to act, it changes the access request into a successful attempt (if the access request was previously marked for rejection), and the DLL will inject the URL PEAP-TLV into the response. In addition, the DLL might also add RADIUS Tunnel attributes or otherwise request that a network restriction be enforced for the current client. The PEAP-TLVs are sent inside the last PEAP Access-Challenge message; the overall authentication result, along with any RADIUS Tunnel attributes, is sent in the final Access-Accept message. The client uses the specified URL PEAP-TLV, which contains an HTTPS URL and an action parameter, to contact a provisioning server and obtain XML files.

URL PEAP-TLV values

The value of the URL PEAP-TLV, which is sent in the PEAP channel and is encrypted and integrity-checked, provides the client with the following information:

- The location of the provisioning information, in the form of an HTTPS URL, which is needed by the client to access the provisioning server. An example URL is: http://www.example.com/provisioning/master.xml.
- The action parameter, which represents the action the WISP requires of the client to access the WISP. This action and the pound sign character (#) are appended to the HTTPS URL sent in the URL PEAP-TLV. There are four possible actions that can be configured in a URL PEAP-TLV:

- **Sign up**. This value is passed by IAS to the client when the customer has authenticated as guest or attempts authentication as an unknown user and does not have a valid user account. An example value for the URL PEAP-TLV is: http://www.example.com/provisioning/master.xml#signup, where **#signup** is the parameter for this action.
- **Renewal**. This value is passed by IAS to the client when the customer's user account is expired and needs renewal before network access can be granted. An example value for the URL PEAP-TLV is: http://www.example.com/provisioning/master.xml#renewal, where **#renewal** is the parameter for this action.
- **Password change**. This value is passed by IAS to the client when the customer is required to change the account password. An example value for the URL PEAP-TLV is: http://www.example.com/provisioning/master.xml#passwordchange, where **#passwordchange** is the parameter for this action.
- **Force update**. This value is passed by IAS to the client when the WISP requires the Windows XP–based client to download an updated XML master file. This method of updating the XML master file on the client should be used only to correct errors; otherwise, the TTL expiry time in the XML master file is used to provide background updates. An example value for the URL PEAP-TLV is: http://www.example.com/provisioning/master.xml#forceupdate, where **#forceupdate** is the parameter for this action.

WPS technology response to URL PEAP-TLVs on client computers

WPS technology on client computers running Windows XP with SP2 evaluates which URL PEAP-TLV values sent by the IAS server are valid based upon whether the client has authenticated as guest or has authenticated with credentials for a valid user account.

When the client has authenticated as guest, WPS technology on the client accepts and utilizes a URL PEAP-TLV that includes the sign-up action parameter (#signup). This allows customers who do not yet have an account to do the following:

- Download the XML files that contain the sign-up wizard
- Run the sign-up wizard
- Create an account

This is the only circumstance under which WPS technology on the client will download and run the sign-up wizard.

When the client has authenticated with credentials for a valid user account, WPS technology on the client ignores a URL PEAP-TLV that contains the sign-up action parameter (#signup). WPS technology on the client will, however, respond to URL PEAP-TLVs that contain the renewal action parameter (#renewal), the password change action parameter (#passwordchange), and the force update action parameter (#forceupdate) by downloading the appropriate XML files and running the wizard specified by the action parameter.

IAS extension DLL types and functionality

IAS supports both authentication extension DLLs and authorization extension DLLs. Authentication DLLs validate credentials against a user account database; authorization DLLs are processed after authentication DLLs and are used to modify the result sent back to the client computer. IAS extension DLLs for WPS technology are authorization DLLs.

When IAS starts, it automatically loads all registered extension DLLs. Extension DLLs can then inspect and modify every RADIUS message received and sent by IAS. When you create your IAS extension DLL, make sure that it can perform the following functions within the IAS processing cycle:

- Recognize particular types of authentication attempts (both accepted and rejected attempts).
- Convert these types of authentication attempts into accepted attempts based on the WPS technology business rules that you have defined in IAS remote access policies and in your sign-up wizard, renewal wizard, and other XML files.
- Add provisioning information, such as a URL PEAP-TLV containing the URL of the provisioning server and an action parameter, to the responses sent to client computers connected to your Wi-Fi hotspots.
- Provide information that allows IAS to isolate clients to a network where they can access resources, such as the provisioning server and the IAS server, used when signing up for accounts.

As with all extension DLLs, a WPS technology extension DLL must first identify and ignore all RADIUS messages that are not relevant to its function. When the DLL recognizes a message that it might need to modify, it must inspect the following:

- The type of message being processed.
- The current authentication result.
- The user name being authenticated.

Then, based on the business logic appropriate to your deployment of WPS technology, the extension DLL should decide whether the response should:

- Be converted into a successful authentication attempt.
- Have provisioning information added to the message, and/or:
- Indicate to a layer three network device (for example, a wireless access point) that the client computer should be allowed restricted access to the network.

Finally, the WPS technology extension DLL should perform any changes that it determines are appropriate.

> **Important**
>
> The extension DLL must not return an error to IAS. In addition, the extension DLL should always allow RADIUS messages to continue to be processed; it should not unilaterally decide to drop a packet.

As previously described, provisioning information consists of a RADIUS ratEAPTLV attribute (type 273), containing a URL PEAP-TLV whose value contains a URL string and an action parameter.

APIs

A WPS Extension DLL must implement the following API functions, which are called by IAS:

- **RadiusExtensionInit()** This API allows the DLL to perform one-time initialization actions.
- **RadiusExtensionTerm()** This API allows the DLL to perform one-time clean-up and termination actions.
- **RadiusExtensionProcess2()** This API is called for every RADIUS message received by IAS.

IAS extension DLL actions

The following structures, attribute names, and attribute values are defined in the SDK header file authif.h. For more information, see MSDN.

- **pECB** The **RADIUS_EXTENSION_CONTROL_BLOCK** pointer parameter passed into RadiusExtensionProcess2().
- **pRequest** The **RADIUS_ATTRIBUTE_ARRAY** pointer containing the RADIUS attributes that make up the RADIUS request packet from the client host.
- **pResponse(X)** The **RADIUS_ATTRIBUTE_ARRAY** pointer containing the RADIUS attributes that make up the RADIUS response packet of the specified type (e.g., pResponse(REJECT)).

Your WPS technology IAS extension DLL must perform the following actions:

1. **Message Filter**. The WPS extension DLL should ignore all messages, except those that match the following criteria:
   a. The message must be at the authorization stage of IAS processing.
   pECB->repPoint == repAuthorization
   b. The inbound message must be an ACCESS_REQUEST.
   pECB->rcRequestType == rcAccessRequest
   c. The outbound message must be an ACCESS_CHALLENGE.
   pECB->rcResponseType == rcAccessChallenge
   d. The response message must contain a RADIUS ratEAPTLV attribute (type 273).
   To perform this check, the DLL must scan all RADIUS attributes in the response to discover whether the attribute ratEAPTLV (type 273) is present.
2. **Message Inspection**. The WPS extension DLL should obtain the following information about the authentication attempt:
   a. RADIUS connection request policy (CRP) used to process this request (RADIUS attribute ratPolicyName = 270 = remote access policy name; ratCRPPolicyName = 275 = connection request policy name).
   b. Reject Reason Code (RADIUS attribute ratRejectReasonCode (type 274))
   c. Username (checking both ratUserName (type 1) and ratFQUserName (type 269))
   d. Overall authentication result, from the RADIUS ratEAPTLV attribute (type 273) containing the Status-Result TLV (type=3) (possible values: Success(1) or Failure(2))
3. **Message Analysis**. The following business logic is recommended, but can be adapted as appropriate:

a. You can design the DLL to choose to perform completely different business logic based on the RADIUS connection request policy name used to process the request. This allows you to configure the IAS server with remote access policies that identify users based on any supported criteria, then have the extension DLL impose greater or fewer restrictions for different types of accounts based on the remote access policy that was used.

b. Within a request the Reject Reason Code should take precedence over the other values. If this RADIUS attribute is present, the message should be processed according to the reason code specified. This can have one of the following values:

i. rrrcAccountUnknown(1)
The authentication attempt is using a user name that does not correspond to any known account. (Suggested action parameter: "signup")

ii. rrrcAccountDisabled(2)
The authentication attempt is using a user name that corresponds to an account that has been disabled by an administrator. (Suggested action parameter: "signup")

iii. rrrcAccountExpired(3)
The authentication attempt is using a user name that corresponds to an account that has been expired, either by exceeding its natural expiration lifetime or by administrative action. (Suggested action parameter: "renew")

iv. rrrcAuthenticationFailure(4)
The authentication attempt is using a user name and password pair that are incorrect for the corresponding account. (Suggested action parameter: "signup")

You can design the DLL to choose how to respond to each of these types of failures independently, based on the business logic appropriate to your needs.

The DLL may choose to respond to all types of failures equally, to respond to some types of failures differently than others, or to ignore one or more types of failures. The suggested behavior for the extension DLL is that for each type, the failure is converted to a success and provisioning information is added with the action parameters listed above.

c. The user name should have the next level of precedence. This is where the DLL can determine whether the current authentication attempt is using a guest account or a valid user account.

i. Guest account attempts should be handled by both the DLL and an IAS connection request policy - the DLL should add the provisioning information, while the connection request policy should add network restriction information.

ii. Normal user authentication attempts must be recognized as such, but the DLL must not make a decision until it has considered the overall authentication result.

d. For Normal user authentication, the overall authentication result must be checked.

i. If the attempt was successful, the response may be modified as described above; typically, however, it should not be modified.

- Adding provisioning information would cause users who are allowed onto the network to also receive a balloon asking for an account sign-up, renewal, or password change. In situations when these behaviors are desired, then provisioning information may be added.

- Adding restricted network information would mean that users who have proven that they have valid credentials would only have access to a limited part of the network. In situations when these behaviors are desired, then restricted network information may be added.

ii. If the attempt was unsuccessful, for a reason not already specified by the Reject Reason Code, then the attempt must not be modified. Attempts that are rejected without a corresponding Reject Reason Code are typically rejected for true error conditions; this can include requests attempting to use an EAP type not configured on the IAS server, corrupted messages, and so forth - all true errors where an Accept response should not be sent to the end user.

4. **Message Modification**. The following changes can be performed on the response message:

   a. Convert to success.
   Find the RADIUS ratEAPTLV attribute (type 273) that contains the Status-Result TLV (type 3), then directly set its data value to Success(1) (modifying the value in place). Because this data value contains a short int in network byte order, you can use the following line of code for the assignment stage:
   pEapTlvIn->Value[1] = MS_PEAP_AVP_VALUE_SUCCESS;

   b. Add provisioning information.
   Allocate enough memory for an EAP-TLV structure, set the type to URL PEAP-TLV (type 8), set the length as appropriate, and copy the URL string into the TLV's value buffer. Then, add a RADIUS ratEAPTLV attribute (type 273) whose data value points to the EAP-TLV data structure.

   c. Add restricted-network attributes.
   This involves adding RADIUS attributes to the response, to indicate to the Wi-Fi hotspot's network hardware that network restrictions should be associated with the given end-user's client computer. These restrictions can be imposed by the 802.11 wireless access point or by a network switch or router between the access point and the rest of the network.
   Different network hardware provides different methods for imposing network restrictions; the attributes to be added will depend on the network hardware in use.
   For example, if VLANs are deployed for client isolation,, then the following RADIUS attributes could be added to the response, to direct the network hardware to place the client on VLAN 0:

   - ratFramedProtocol (type 7) = PPP(1)
   - ratTunnelType (type 64) = TUNNEL_TYPE_VLAN(13)
   - ratMediumType (type 65) = TUNNEL_MEDIUM_TYPE_802 (6)
   - ratTunnelPrivateGroupID (type 81) = "0" (0x30, 0x00)
   - ratTunnelTag (type 4170) = [obtain value from hardware-specific documentation]

For more information about creating an IAS extension DLL, see the following topics:

- RADIUS_EXTENSION_CONTROL_BLOCK (Internet Authentication Service Extensions: Platform SDK) at http://go.microsoft.com/fwlink/?LinkId=20041. The RADIUS_EXTENSION_CONTROL_BLOCK structure provides information about the current RADIUS request. It also provides functions for obtaining the attributes associated with the request, and for setting the disposition of the request.
- GetRequest (Internet Authentication Service Extensions: Platform SDK) at http://go.microsoft.com/fwlink/?LinkId=20042. The GetRequest function returns the attributes received in the RADIUS request process and any internal attributes describing the request state.
- RadiusExtensionTerm (Internet Authentication Service Extensions: Platform SDK) at http://go.microsoft.com/fwlink/?LinkId=20043. The RadiusExtensionTerm function is called by IAS prior to unloading the Extension DLL. Use RadiusExtensionTerm to perform any clean-up operations for the Extension DLL.
- Internet Authentication Service Extensions at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ias/ias/ias_start_page.asp

To order a Platform Software Development Kit (SDK) CD, see Microsoft Platform SDK at http://go.microsoft.com/fwlink/?LinkId=20044.

PEAP-TLV Packets

The Protected Extensible Authentication Protocol (PEAP), described in RFC 2284, provides a standard mechanism for support of multiple authentication types. Using PEAP-TLV, it is possible for various types of data to be passed directly between the IAS server and the PEAP client, and to provide functionality that is not included in RFC 2284 without defining a multiplicity of new PEAP types. The following table describes PEAP-TLV packet types:

Packet Types	Packet Description
PEAP-TLV URI Packet	Contains a Type-Length-Value object (TLV).
PEAP-TLV Result Packet	Provides support for acknowledged success and failure messages

Packet details

The following section provides detailed descriptions of the PEAP-TLV URI Packet and the PEAP-TLV Result Packet.

PEAP-TLV URI Packet

The PEAP-TLV URI packet contains a Type-Length-Value (TLV) object.

Fields

MandatoryRequirement

Data type: **BINARY**

Mandatory TLV packet, set to 1.

Value	Meaning
0	Non-mandatory TLV
1	Mandatory TLV

TLVReserved

Length: 1
Data type: **BINARY**
Reserved. Value is zero.

TLVType

Length: 14
Data type: **BINARY**
TLV attribute type.

Value	Meaning
0	Reserved
1	Reserved
2	Reserved
3	Acknowledged result

TLVValueLength

Data type: **UCHAR**
Length of **TLVValue** field.

TLVValue

Data type: **UCHAR**
URI to a master document.

Value	Meaning*
https://www.example.com/provisioning/master.xml#signup	1
https://www.example.com/provisioning/master.xml#renewal	2
https://www.example.com/provisioning/master.xml#passwordchange	3
https://www.example.com/provisioning/master.xml#forceupdate	4

*Meaning definitions

1. Signup should be returned by the ISP in the TLV when the user name in the authentication is guest or an unknown user name.
2. Renewal should be returned by the ISP in the TLV when the user name’s account needs renewal by the user
3. Passwordchange should be returned by the ISP in the TLV when the user should change the password for the account.
4. Forceupdate should be returned by the ISP in the TLV when the ISP needs the client to update the provisioning files as soon as possible. This should not normally be used to update the files; the TTL expiry time in the master file should be used to allow the files to be updated in the background instead. Forceupdate should be used only to correct an error in the XML files.

PEAP-TLV Result Packet

The PEAP-TLV Result Packet provides support for acknowledged success and failure messages.

Fields

MandatoryRequirement
Length: 1
Data type: **BINARY**
Mandatory TLV packet, set to 1.

TLVReserved

Length: 1
Data type: **BINARY**
Reserved. Value is zero.

TLVPacketType

Length: 14
Data type: **BINARY**
TLV packet type. Value is 3.

TLVStatusLength

Data type: **USHORT**
Length of the **TLVStatus** field. Value is 2.

TLVStatus

Data type: **USHORT**
TLV status.

Value	Meaning
1	Success
2	Failure

Backward compatibility

PEAP-TLV is a "special case" type, more similar to the Identity and Notification types than to the authentication types such as MD5-Challenge (RFC 2284). PEAP-TLV differs from the Identity and Notification types in that a peer may respond to an EAP-TLV request with a Nak Response. This is allowed for backward compatibility with implementations that do not support the PEAP-TLV type.

Beta Documentation Note

The following two scenarios — a WISP using IP filters for client isolation and an HSP using IP filters for client isolation — are currently in development and have not been implemented or tested. They are provided as general depictions of possible implementations of WPS technology at a later date.

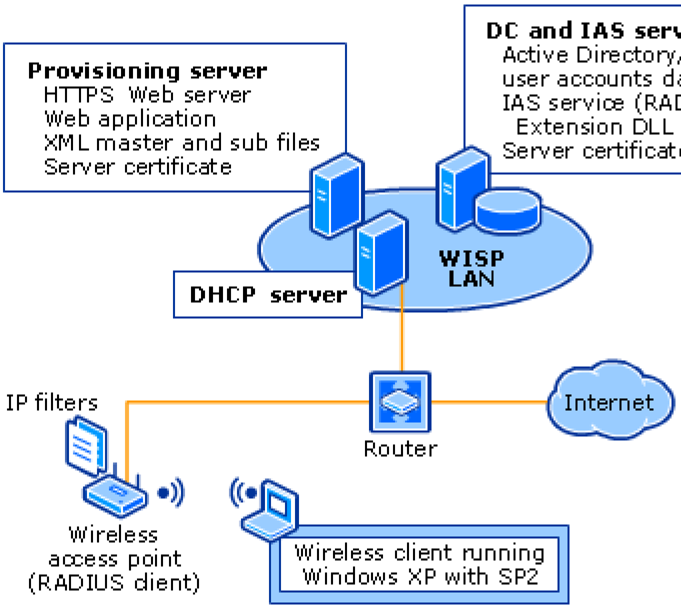
WPS technology for a WISP with IP filters

If your organization is an enterprise or a WISP, you can deploy WPS technology by using IP filters for client computer isolation. In this circumstance, client computers are provided access to network resources, such as the provisioning server and IAS servers, and IP filters block access to the Internet until the customer establishes a paid account. After the account is established, the IP filters are lifted, and traffic is allowed between the client computer and the Internet.

In the sections that follow, the components of a WISP network using IP filters are described, and how the components work together during new customer sign-up are detailed.

Components of WPS technology for a WISP using IP filters

When an ISP deploys Wi-Fi hotspots as a WISP, WPS technology can be configured with IP filters for client computer isolation during the account sign-up process. The following illustration depicts the components of a WISP network using IP filters for client computer isolation.



Components of a WISP network using IP filters

This configuration consists of the following components.

Wireless client

A computer running Windows XP Home Edition with SP2, Windows XP Professional with SP2, or Windows XP Tablet PC Edition with SP2. The wireless client connects to the WISP network, which is in a public location and is accessible to customers with portable computers and wireless network adapters.

Wireless access point (RADIUS client)

The wireless access point is configured as a RADIUS client to the IAS server deployed on the WISP LAN. The wireless access points used for WPS technology must meet the following requirements:

- Support for the IEEE standard 802.1X authentication.
- Support for Wi-Fi Protected Access (WPA) is preferred.
- The ability to implement client isolation by applying IP filters to the connection with the client.
- Support for RADIUS authentication and RADIUS accounting, including:

- Support for the Class attribute as defined in RFC 2865, “Remote Authentication Dial-in User Service (RADIUS),” to allow session correlation for RADIUS authentication and accounting records. For session correlation, when you configure RADIUS accounting at your IAS server or proxy, you must log all accounting data that allow applications (such as billing applications) to query the database, correlate related fields, and return a cohesive view of each session in the query results. At a minimum, to provide session correlation, you must log the following IAS accounting data: NAS-IP-Address; NAS-Identifier (you need both NAS-IP-Address and NAS-Identifier because the access server can send either attribute); Class; Acct-Session-Id; Acct-Multi-Session-Id; Packet-Type; Acct-Status-Type; Acct-Interim-Interval; NAS-Port; and Event-Timestamp.
- Support for accounting interim requests, which are sent periodically by some access servers during a user session, that can be logged. This type of request can be used when the Acct-Interim-Interval RADIUS attribute is configured to support periodic requests in the remote access profile on the IAS server. The access server, in this case a wireless access point, must support the use of accounting interim requests if you want the interim requests to be logged on the IAS server.
- Support for IP address range filtering.
- Support for dynamic retransmit timeout (RTO) estimation or exponential backoff to handle congestion and delays in a wide area network (WAN) environment.

In addition, there are some filtering features that the access points should support to provide enhanced security for the network. These filtering options include:

- **DHCP filtering.** The access point must filter on IP ports to prevent the transmission of DHCP broadcast messages in the instance that the client is a DHCP server. The access point must block the client from sending IP packets from port 68 to the network.
- **DNS filtering.** The access point must filter on IP ports to prevent a client from performing as a DNS server. The access point must block the client from sending IP packets from port 53 to the network.

IP filters

IP filters that isolate client computers connecting as guest are configured in the remote access policy on the WISP IAS server, and are applied to the client connection by the wireless access point. The IP filters must grant the client computer access to the provisioning server and block access to all other locations.

Router

The router must provide multiple ports for connection to access points, the WISP LAN, and the Internet.

Provisioning server

The WISP provisioning server is configured with the following components.

HTTPS Web server

The Internet Information Services (IIS) or third-party Web server must be deployed with HTTPS.

Web application

The WISP Web server is configured with an account processing Web application that processes data provided during customer sign-up or account renewal. When a customer uses the sign-up wizard on a client computer to create and pay for a WISP account, the customer enters data, such as name, address, and credit card information, that is converted to an XML document on the client. Windows XP sends this XML document to the WISP provisioning server.

The account processing Web application on the provisioning server must be capable of accepting and processing the XML documents containing the user data. For example, the account processing Web application must dynamically create an account in the Active Directory user accounts database, and must contain a credit card verification component to process customers' payment information. The account processing Web application must permit new customers to sign up and to permit existing customers to renew their subscriptions for service.

XML master file and subfiles

The WISP provisioning server stores the XML master file and subfiles that provide the client with all configuration information needed to access the network, create an account, pay for the account, and ultimately access the Internet. For more information about the XML master file and subfiles, see "XML schemas" in this paper.

Server certificate

For server authentication to client computers, the WISP provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust.

Domain controller and IAS server

The WISP domain controller and IAS server is configured with the following components.

Active Directory

The user accounts database on the domain controller must be an Active Directory user accounts database or a database that uses Lightweight Directory Access Protocol (LDAP) and supports dynamic creation of user accounts. When a customer signs up for an account using the sign-up wizard, the account processing Web application on the provisioning server creates a new account in the user accounts database, and adds the user to a group that has clearly defined access privileges that match the type of account the customer purchased when signing up.

If you use an accounts database other than Active Directory, IAS authentication and authorization extension DLLs must be written and installed for this process to function correctly.

For information about configuring Active Directory replication, see "Active Directory replication" in this paper.

Internet Authentication Service (IAS)

IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy, and is used to authenticate and authorize users connecting to your network. IAS is configured with remote access policies that allow guest authentication for non-domain member computers and users. It is also configured to provide IP filters to RADIUS clients (access points) that apply the filters to client connections during guest authentication. IAS also provides unrestricted access to users with valid accounts.

Extension DLL and URL PEAP-TLV

An IAS authentication extension DLL defining a URL PEAP-TLV provides IAS with the ability to send the location of the provisioning server to client computers. PEAP-Type-Length-Value (PEAP-TLV) is an Extensible Authentication Protocol (EAP) authentication type that allows the IAS server to pass information to client computers attempting to connect to your network.

In this circumstance, the value contained in the PEAP-TLV is an HTTPS Uniform Resource Locator (URL) that provides client computers running Windows XP with SP2 with the location of the WISP provisioning server. With this URL and parameter, Windows XP can download the WISP XML files to the client computer.

In addition to the URL of the provisioning server, the URL PEAP-TLV includes an action parameter. The action parameter directs the client to perform a specific task. The action parameter included in the URL PEAP-TLV defines tasks such as new customer sign-up, existing account renewal, and password change.

For more information, see “How to create an IAS extension DLL and a URL PEAP-TLV” in this paper.

Server certificate

For server authentication to client computers, the WISP IAS server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and is issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust. If you install IAS and Active Directory on the same computer, the computer must have a certificate. If you install IAS and Active Directory on different computers, only the IAS server needs a certificate.

DHCP server

The DHCP server must be able to assign valid public IP addresses to computers accessing the network through the wireless access points.

How a WISP works using IP filters

The Internet connection process with WPS technology for a WISP with IP filtering differs depending on whether the customer attempting to connect is a new customer or an existing customer. The following example describes the process for a new customer. In addition, how IAS handles an expired account is explained.

New customer connection example

When a new customer connects to a WISP and establishes an account, the following four basic stages occur:

1. The customer discovers the WISP network at a Wi-Fi hotspot
2. The customer authenticates as guest
3. The client is provisioned and the customer establishes an account

4. The customer is authenticated with the new account credentials
5. IP filters are removed and the customer gains access to the Internet

In the next section we will look at these stages in more detail.

1. The customer discovers the WISP network at a Wi-Fi hotspot

When a customer arrives at the WISP Wi-Fi hotspot with a portable computer running Windows XP Home Edition with SP1, Windows XP Professional with SP1, or Windows XP Tablet PC Edition with SP1, the computer comes within range of the WISP access point beacon.

The Wireless Auto Configuration service on the client computer detects the beacon information from the access point, which is enabled with broadcast Secure Set Identifier (SSID). The SSID is equivalent to the network name.

The customer is informed by Windows XP that a wireless network is available. The customer views information in Windows XP, and if interested, the customer clicks **Connect**.

2. The customer authenticates as guest

Wireless Auto Configuration uses 802.1X and PEAP guest authentication to connect to the WISP network through the access point, automatically passing a null user name and a blank password to the WISP IAS server.

The IAS server is the PEAP authenticator and TLS endpoint for customers who connect as guest, and the TLS tunnel is created between the client and the IAS server. All subsequent messages between client and server pass through this tunnel.

Server authentication is performed when the IAS server verifies its identity to the client computer using a certificate that contains the Server Authentication purpose in Enhanced Key Usage (EKU) extensions. This certificate is issued by a public trusted root certification authority (CA).

The IAS server authenticates and authorizes the customer as guest. In the Access-Challenge message that the IAS server sends to the client is a URL PEAP-TLV. The URL PEAP-TLV is a container with a value that is the URL of the provisioning server. This URL provides the client with the location of the XML master file.

The IAS server also sends IP filters in the form of Vendor Specific Attributes (VSAs) to the access point. These IP filters are applied to the client connection by the access point and are used to isolate the client; the filters block access to all network resources except the WISP provisioning server.

The customer client computer receives an IP address lease from the DHCP server. The address is from a public IP address range configured in a scope on the DHCP server.

3. The client is provisioned and the customer creates an account

The XML master file on the provisioning server contains pointers to the XML subfiles. Windows XP downloads the XML master file and subfiles. When the XML sign-up schema is downloaded, the sign-up wizard is launched on the client to allow the customer to create and pay for an account with the WISP.

Using the sign-up wizard on the client computer, the customer steps through the process of signing up for an account. The data entered by the customer is converted by Windows XP into an XML document.

The XML document containing the customer's sign-up data is sent by Windows XP to the Web application on the WISP provisioning server.

The Web application processes the customer payment information. Once payment is verified and sign-up information is completed successfully, the Web application creates a user account in Active Directory, and permissions are applied to the user account by assigning group membership based on the account type chosen by the customer.

An XML document containing the new account credentials is sent from the WISP provisioning server to the client computer. The client computer uses the credentials to configure Wireless Auto Configuration and 802.1X under the name of the WISP.

4. The customer is authenticated with the new account credentials

Wireless Auto Configuration restarts the association to the SSID for the WISP. Wireless Auto Configuration finds the correct 802.11 profile which was downloaded with the other WISP information. Wireless Auto Configuration re-associates with the access point using the correct profile.

802.1X restarts the authentication process using PEAP-MS-CHAP v2 and the new account credentials.

As the client starts the authentication process with PEAP-MS-CHAP v2 authentication, a TLS channel is created between the customer's client computer and the WISP IAS server.

In the second stage of PEAP-MS-CHAP v2 authentication, the WISP IAS server authenticates and authorizes the connection request against the new account in the Active Directory user accounts database. The IAS server sends an Access-Accept message to the access point.

5. IP filters are removed and the customer gains access to the Internet

Because IP filters are used to isolate the client, the IAS server message causes the access server to remove the IP filters from the client connection, granting the customer access to the Internet.

How IAS handles an expired account

You can determine the types of account plans that you want to offer your customers. These plans can range from fees based on hourly use to accounts with life spans as long as a day, a month, or longer.

It is important for IAS to determine whether a connecting or connected client computer has a valid account, and to take the appropriate action if the customer's account is expired. The following example illustrates how IAS determines that a twenty-four hour account is current, and how WPS technology behaves when the account expires.

Twenty-four hour connect option example

When the customer arrives at the WISP, the customer chooses an access account that has a one day (24 hour) lifespan. The customer and client computer proceed through the account creation process described above, and then connect to the Internet. The following process occurs:

- In the Access-Accept message sent by the IAS server, the IAS server sets a session timeout of 60 minutes for the client computer connection to the access point.
- After 60 minutes, the access point requests that the client reauthenticate. The client reauthenticates successfully and the customer's session is not interrupted.

- Each 60 minutes thereafter, the access point requests that the client reauthenticate. During each authentication the IAS server checks the current time against the expiry time for the user account to discover whether the customer is authorized to access the network.
- On the last re-authentication, at hour 23 in the account lifespan and before 24 hours have passed, the IAS authorization check fails and the IAS server sends a URL PEAP-TLV to the client that contains the account renewal action parameter and an HTTPS URL for an XML master file. The URL PEAP-TLV supplies the customer with the location of the provisioning server where the customer can renew the account.
- Upon receiving the URL in the URL PEAP-TLV, 802.1X requests that Windows XP display the account renewal application to the customer.
- The customer renews the account and 802.1X initiates authentication with the account credentials.
- During authentication with the IAS server, the IAS server authenticates and authorizes the customer against the user accounts database, and sends an Access-Accept message containing a session timeout of 60 minutes to the access point.
- During this process, because the account has not expired, the customer maintains connection to the Internet.

If the customer does not complete the renewal process before the 24 hour account lifespan is reached, then the access point reapplies IP filters and customer access to the Internet is terminated. The customer is then provided with the option of renewing the account for continued access.

Note

This scenario is currently in development and has not been implemented or tested. It is provided as a general depiction of a possible implementation of WPS technology.

WPS technology for an HSP with IP filters

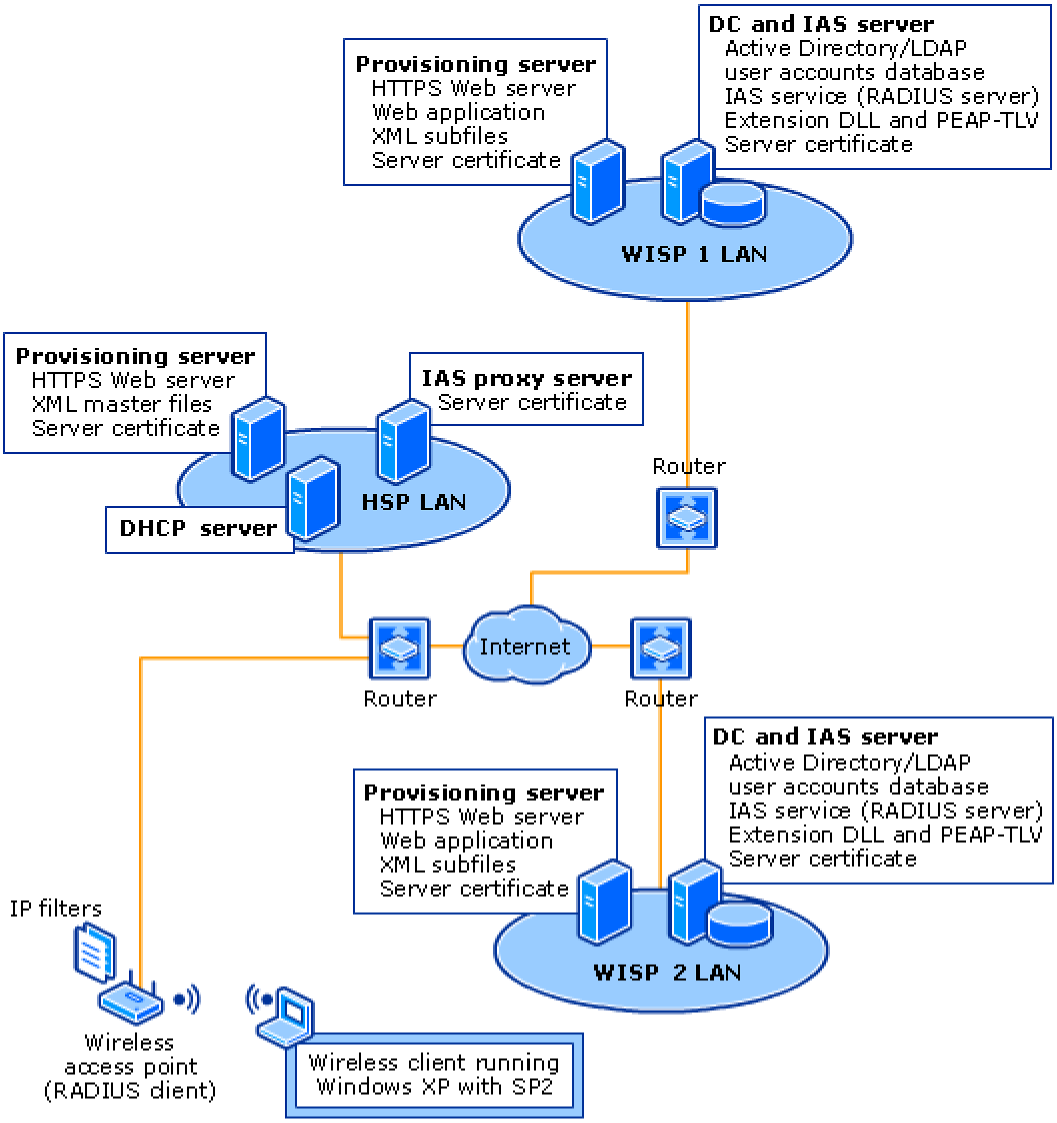
If your organization is an HSP, you can deploy WPS technology by using IP filters for client computer isolation. In this circumstance, client computers are provided access to HSP and WISP network resources, such as provisioning servers and IAS servers, and IP filters block access to the Internet until the customer establishes a paid account. After the account is established, the IP filters are lifted, and traffic is allowed between the client computer and the Internet.

In the sections that follow, the components of an HSP network using IP filters are described, and how the components work together during new customer sign-up are detailed.

Components of WPS technology for an HSP network using IP filters

A Hotspot Service Provider (HSP) can deploy WPS technology with IP filters for

client computer isolation during the account sign-up process.
The following illustration depicts the components of an HSP network using IP filters for client computer isolation.



Components of an HSP network using IP filters

This configuration consists of the following components.

Wireless client

A computer running Windows XP Home Edition with SP2, Windows XP Professional with SP2, or Windows XP Tablet PC Edition with SP2. The wireless client connects to the HSP network, which is in a public location and is accessible to customers with portable computers and wireless network adapters.

Wireless access point (RADIUS client)

The wireless access point is configured as a RADIUS client to the IAS proxy server deployed on the HSP LAN. The wireless access points used by an HSP for WPS technology must meet the following requirements:

- Support for the IEEE standard 802.1X authentication.
- Support for Wi-Fi Protected Access (WPA) is preferred

- The ability to implement client isolation by applying IP filters to the connection with the client.
- Support for RADIUS authentication and RADIUS accounting, including:
    - Support for the Class attribute as defined in RFC 2865, “Remote Authentication Dial-in User Service (RADIUS),” to allow session correlation for RADIUS authentication and accounting records. For session correlation, when you configure RADIUS accounting at your IAS server or proxy, you must log all accounting data that allow applications (such as billing applications) to query the database, correlate related fields, and return a cohesive view of each session in the query results. At a minimum, to provide session correlation, you must log the following IAS accounting data: NAS-IP-Address; NAS-Identifier (you need both NAS-IP-Address and NAS-Identifier because the access server can send either attribute); Class; Acct-Session-Id; Acct-Multi-Session-Id; Packet-Type; Acct-Status-Type; Acct-Interim-Interval; NAS-Port; and Event-Timestamp.
    - Support for accounting interim requests, which are sent periodically by some access servers during a user session, that can be logged. This type of request can be used when the Acct-Interim-Interval RADIUS attribute is configured to support periodic requests in the remote access profile on the IAS server. The access server, in this case a wireless access point, must support the use of accounting interim requests if you want the interim requests to be logged on the IAS server.
    - Support for IP address range filtering.
    - Support for dynamic retransmit timeout (RTO) estimation or exponential backoff to handle congestion and delays in a wide area network (WAN) environment.

In addition, there are some filtering features that the access points must support to provide enhanced security for the network. These filtering options include:

- **DHCP filtering.** The access point must filter on IP ports to prevent the transmission of DHCP broadcast messages in the instance that the client is a DHCP server. The access point must block the client from sending IP packets from port 68 to the network.
- **DNS filtering.** The access point must filter on IP ports to prevent a client from performing as a DNS server. The access point must block the client from sending IP packets from port 53 to the network.

IP filters

IP filters that isolate client computers connecting as guest are configured in the remote access policy on the HSP IAS proxy server, and are applied to the client connection by the wireless access point. The IP filters must grant the client computer access to the provisioning server at the HSP and the WISP, and must block access to all other locations.

Router

The router must provide multiple ports for connection to access points, the HSP LAN, and the Internet or a WISP, depending on your configuration.

HSP LAN

The HSP local area network (LAN) consists of the following components.

Provisioning server

The HSP provisioning server is configured with the following components.

HTTPS Web server

The Internet Information Services (IIS) or third-party Web server must be deployed with HTTPS.

HSP XML master files

HSP XML master files are stored on the HSP provisioning server. Because an HSP can provide customers with a choice of Internet access plans with a variety of WISPs, one XML master file is configured at the HSP and stored on the HSP provisioning server for each WISP available to HSP customers. Each HSP XML master file contains a master XML schema that describes a list of URLs to other XML documents, which are XML subfiles stored on WISP provisioning servers. The XML master schema also describes properties of the WISP for which the XML master file was created and the Time-To-Live (TTL) for the XML master file before it is updated by the HSP provisioning server from the WISP provisioning server. The XML master file schema is:

- **The domain name of the WISP.** For example, if Microsoft Corporation is the WISP, the domain name is “microsoft.com.”
- **The friendly name of the WISP.** For example, Microsoft Corporation.
- **The TTL for the XML master file.** When client computers connect to the HSP provisioning server and download the master file, the TTL value tells Wireless Provisioning Services on the client computer when to request an update of the master file from the HSP provisioning server.
- **The list of URLs that point to XML subfiles.** The XML subfiles are located on the WISP provisioning server for which the XML master file was created. Only HTTPS URLs are supported for use within the XML schema, and by WISP provisioning servers. The name of the XML schema described in the subfile is included, as is the version number for the subfile. Possible subfile names include: Signup, SSID, EAP, Location, and Help. For more information, see “XML Schemas” in this paper.

Server certificate

For server authentication to client computers, the provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers connecting to the HSP wireless LAN. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust.

IAS proxy server

The HSP IAS proxy server is configured with the following components.

Internet Authentication Service (IAS)

The IAS proxy server must be a computer running Windows Server 2003, Standard

Edition with Service Pack 1 (SP1); Windows Server 2003, Enterprise Edition with SP1; or Windows Server 2003, Datacenter Edition with SP1; and Internet Authentication Service (IAS). IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) proxy and server.

The IAS proxy functions both as an IAS proxy and as an IAS server. The IAS proxy server is configured to locally process connection requests for users that authenticate as guest, and to forward non-guest authentication and accounting requests to the IAS servers located at individual WISPS based on the realm name configuration specified in **Connection Request Policies** in the IAS console.

On the IAS proxy, the IAS servers at each WISP are added to a remote RADIUS server group, with a minimum of one remote RADIUS server group created for each WISP. Because Windows Server 2003, Standard Edition, permits the creation of only two remote RADIUS server groups, an HSP offering Internet connectivity to more than two WISPs must deploy IAS proxies and servers running Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition.

Server certificate

For server authentication to client computers, the provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers connecting to the HSP wireless LAN. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust.

DHCP server

The DHCP server must be able to assign valid public IP addresses to computers accessing the network through the wireless access points.

WISP 1 LAN

The WISP 1 LAN is configured with the following components.

Provisioning server

The WISP provisioning server is configured with the following components.

HTTPS Web server

Like the HSP Web server, the WISP Web server must use HTTPS. The WISP provisioning server stores XML subfiles that are downloaded over HTTPS by client computers running Windows XP with SP2.

Web application

The WISP Web server is configured with an account processing Web application. When a customer uses the sign-up wizard on the client computer to create and pay for an account, the customer enters data, such as name, address, and credit card information, that is converted to an XML document and sent to the WISP provisioning server.

The account processing Web application on the provisioning server must be capable of accepting and processing the XML documents containing the user data. For example, the account processing Web application must dynamically create an account in the Active Directory user accounts database, and must contain a credit card verification component to process customers' payment information. The account processing Web application must permit new customers to sign up and to permit existing customers to renew their subscriptions for service.

XML subfiles

The WISP provisioning server maintains the XML subfiles that provide the client with all configuration information needed to access the network, create an account, pay for the account, and ultimately access the Internet. For more information about XML subfiles, see “XML schemas” in this paper.

Server certificate

For server authentication to client computers, the provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers connecting to the HSP wireless LAN. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust.

Domain controller and IAS server

The WISP domain controller and IAS server is configured with the following components.

Active Directory

The user accounts database on the domain controller must be an Active Directory user accounts database or a database that uses Lightweight Directory Access Protocol (LDAP) and supports dynamic creation of user accounts. When a customer signs up for an account, the account processing Web application on the provisioning server creates a new account in the user accounts database, and adds the user to a group that has clearly defined access privileges that match the type of account the customer purchased when signing up.

If you use an accounts database other than Active Directory, IAS authentication and authorization extensions must be written and installed for this process to function correctly.

For information about configuring Active Directory replication, see “Active Directory replication” in this paper.

Internet Authentication Service (IAS)

IAS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy, and is used to authenticate and authorize users connecting to your network. IAS is configured with remote access policies that allow guest authentication for non-domain member computers and users. It is also configured to provide IP filters to RADIUS clients (access points) that apply the filters to client connections during guest authentication. IAS also provides unrestricted access to users with valid accounts.

Server certificate

For server authentication to client computers, the provisioning server must maintain a valid certificate in its certificate store. The certificate must contain the Server Authentication purpose in Enhanced Key Usage (EKU) extensions and be issued by a public certification authority (CA), such as Verisign or Thawte, that is trusted by client computers connecting to the HSP wireless LAN. The Trusted Root Certification Authorities certificate store on computers running Windows XP is installed by default with a multitude of certificates issued by public CAs. You must obtain your server certificate from one of the public CAs for which clients already have trust. If you install IAS and Active Directory on the same computer, the computer must have a certificate. If you install IAS and Active Directory on different computers, only the IAS server needs a certificate.

Extension DLL and URL PEAP-TLV

An IAS extension DLL defining a URL PEAP-TLV provides IAS with the ability to send the location of the provisioning server to client computers.

PEAP-Type-Length-Value (PEAP-TLV) is an Extensible Authentication Protocol (EAP) authentication type that allows the IAS server to pass information to client computers attempting to connect to your network.

In this circumstance, the value contained in the PEAP-TLV is an HTTPS Uniform Resource Locator (URL) that provides client computers running Windows XP with the location of the WISP provisioning server. With this URL, Windows XP can download the WISP XML files to the client computer.

In addition to the URL of the provisioning server, the URL PEAP-TLV includes an action parameter. The action parameter directs the client to perform a specific task. The action parameter included in the URL PEAP-TLV defines tasks such as new customer sign-up, existing account renewal, and password change.

For more information, see “How to create an IAS extension DLL and a URL PEAP-TLV” in this paper.

WISP 2 LAN

The WISP 2 LAN is identical to the WISP 1 LAN described above, and is depicted in “Components of an HSP network using IP filters” to illustrate that an HSP can provide service offers to customers from multiple WISPs.

How an HSP works with IP filtering

The Internet connection process with WPS technology for an HSP with IP filtering differs depending on whether the customer attempting to connect is a new customer or an existing customer. The following example describes the process for a new customer. In addition, how IAS handles an expired account is explained.

New customer connection example

When a new customer connects to an HSP and establishes an account with a WISP, the following five basic stages occur:

1. The customer discovers the HSP network at a Wi-Fi hotspot
2. The customer authenticates as guest
3. The client is provisioned with the HSP XML master file
4. The customer selects a WISP and establishes an account
5. The customer is authenticated with the new account credentials

In the next section we will look at these stages in more detail.

1. The customer discovers the HSP network at a Wi-Fi hotspot

When a customer arrives at the HSP hotspot with a portable computer running Windows XP Home Edition with SP2, Windows XP Tablet PC Edition with SP2, or Windows XP Professional with SP2, the computer comes within range of the HSP access point beacon.

The Wireless Auto Configuration service on the client computer detects the beacon information from the access point, which is enabled with broadcast Secure Set Identifier (SSID). The SSID is equivalent to the network name.

The customer is informed by Windows XP that a wireless network is available. The customer views information in Windows XP, and if interested, the customer clicks **Connect**.

2. The customer authenticates as guest

Wireless Auto Configuration uses 802.1X and PEAP guest authentication to connect to the HSP network through the access point, automatically passing a null user name and a blank password to the HSP IAS proxy.

The IAS proxy is configured both as a proxy and as an IAS server. The IAS proxy/server is configured to locally process users that authenticate as guest, and to forward other messages to the WISP IAS servers based on the value of the User-Name attribute in the Access-Request message.

The HSP IAS proxy server acts as an IAS server for guest authentication, processing these requests locally rather than acting as a proxy and forwarding them. The HSP IAS proxy server is therefore the PEAP authenticator and TLS endpoint for customers who connect as guest, and the TLS tunnel is created between the client and the HSP IAS server. All subsequent messages between client and server pass through this tunnel.

Server authentication is performed when the HSP IAS server verifies its identity to the client computer using a certificate that contains the Server Authentication purpose in Enhanced Key Usage (EKU) extensions. This certificate is issued by a public trusted root CA.

The HSP IAS proxy server authenticates and authorizes the customer as guest. In the Access-Challenge message that the IAS server sends to the client is a URL PEAP-TLV. The URL PEAP-TLV is a container with a value that is the URL of the HSP provisioning server. This URL provides the client with the location of the HSP XML master file.

The HSP IAS proxy server also sends IP filters in the form of Vendor Specific Attributes (VSAs) to the access point. These IP filters are applied to the client connection by the access point and are used to isolate the client; the filters block access to all network resources except the HSP provisioning server and the WISP provisioning servers.

The customer client computer receives an IP address lease from the HSP DHCP server. The address is from a public IP address range configured in a scope on the DHCP server.

3. The client is provisioned with the HSP XML master file

The HSP master XML file on the HSP provisioning server contains pointers to multiple WISP master XML files, which in turn contain pointers to each respective WISP’s XML subfiles. Windows XP downloads the HSP XML master file.

Windows displays to the customer a list of WISPs whose services are offered by the HSP.

For this example, the customer selects services from WISP 1.

4. The customer selects a WISP

After the customer selects the WISP, Windows XP connects to the WISP and, using the Background Intelligent Transfer Service, downloads the WISP XML master file and subfiles. When the XML sign-up schema is downloaded, the sign-up wizard is opened on the client to allow the customer to create and pay for an account with the WISP.

Using the sign-up wizard on the client computer, the customer steps through the process of signing up for an account with WISP 1. The data entered by the customer is converted by Windows XP into an XML document.

The XML document containing the customer's sign-up data is sent by Windows XP to the Web application on the WISP 1 provisioning server.

The Web application processes the customer payment information. Once payment is verified and sign-up information is completed successfully, the Web application creates a user account in Active Directory, and permissions are applied to the user account by assigning group membership based on the account type chosen by the customer.

An XML document containing the new account credentials is sent from the WISP provisioning server to the client computer. The client computer uses the credentials to configure Wireless Auto Configuration and 802.1X under the name of the WISP.

5. The customer is authenticated using the new account credentials and gains Internet access

Wireless Auto Configuration restarts the association to the SSID for the HSP.

Wireless Auto Configuration finds the correct 802.11 profile which was downloaded with the other WISP information. Wireless Auto Configuration re-associates using the correct profile.

802.1X restarts the authentication process using PEAP-MS-CHAP v2 and the new account credentials.

As the client starts the authentication process, the HSP IAS proxy forwards messages between the client and the WISP IAS server. The connection request policies on the HSP IAS proxy are configured to forward requests to WISP 1 where the ISP's name exists in the realm portion of the RADIUS User-Name attribute. For example, if "user@wisp1.example" is the user name, the IAS proxy server uses the realm portion of the user name, "wisp1.example," to choose the IAS server that should receive the connection request.

In the first stage of PEAP-MS-CHAP v2 authentication, a TLS channel is created between the customer's client computer and the WISP 1 IAS server.

In the second stage of PEAP-MS-CHAP v2 authentication, the WISP 1 IAS server authenticates and authorizes the connection request against the new account in the user accounts database. The WISP IAS server sends an Access-Accept message that is forwarded by the HSP IAS proxy to the HSP access point.

Because IP filters are used to isolate the client, the IAS server message causes the access server to remove the IP filters from the client connection, granting the customer access to the Internet.

How IAS handles an expired account

Each WISP that offers connectivity through an HSP can determine the types of account plans to offer customers. These plans can range from fees based on hourly use to accounts with lifespans as long as a day, a month, or longer.

It is important for IAS to determine whether a connecting or connected client computer has a valid account, and to take the appropriate action if the customer's account is expired. The following example illustrates how IAS determines that a twenty-four hour account is current, and how WPS technology behaves when the account expires.

Twenty-four hour connect option example

When the customer arrives at the HSP, the customer chooses an access account with WISP 1 that has a one-day (24-hour) lifespan. The customer and client computer proceed through the account creation process described above, and then connect to the Internet. The following process occurs:

- In the Access-Accept message sent by the WISP 1 IAS server, the IAS server sets a session timeout of 60 minutes for the client computer connection to the access point.
- After 60 minutes, the access point requests that the client reauthenticate. The client reauthenticates successfully and the customer's session is not interrupted.
- Each 60 minutes thereafter, the access point requests that the client reauthenticate. During each authentication the IAS server checks the current time against the expiry time for the user account to discover whether the customer is authorized to access the network.
- On the last re-authentication, at hour 23 in the account lifespan and before 24 hours have passed, the IAS authorization check fails and the IAS server sends a URL PEAP-TLV message to the client that contains the account renewal action parameter and an HTTPS URL for an XML master file. The URL PEAP-TLV supplies the customer with the location of the provisioning server where the customer can renew the account.
- Upon receiving the URL in the URL PEAP-TLV, 802.1X requests that Windows XP display the account renewal application to the customer.
- The customer renews the account and 802.1X initiates authentication using the account credentials.
- During authentication with the WISP 1 IAS server, the IAS server authenticates and authorizes the customer against the user accounts database, and sends an Access-Accept message containing a session timeout of 60 minutes to the access point.
- During this process, because the account has not expired, the customer maintains connection to the Internet.

If the customer does not complete the renewal process before the 24 hour account lifespan is reached, then the access point reapplies IP filters and customer access to the Internet is terminated. The customer is then provided with the option of renewing the account for continued access.

Note

This scenario is currently in development and has not been implemented or tested. It is provided as a general depiction of a possible implementation of WPS technology.

Summary

When you deploy Wireless Provisioning Services technology, you can provide wireless Internet access to new and existing customers at Wi-Fi hotspots in public locations, such as airports and shopping malls. Customers can connect to your network, create and pay for an account, and connect to the Internet without knowing about your services prior to their arrival at Wi-Fi hotspot locations and without manually configuring their wireless computers. To deploy WPS technology, you must use Windows Server 2003, SP1 and Internet Authentication Service (IAS), and your customers must use computers running Windows XP with Service Pack 2 (SP2). Your IAS server must be configured with an IAS extension DLL and URL PEAP-TLV; these technologies allow the IAS server to inform client computers of the location of your provisioning server in IAS Access-Accept messages. In addition, you must deploy an HTTPS provisioning server that provides client computers with network and other configuration parameters described in a collection of XML schemas and provided to client computers in the form of XML master and subfiles. The provisioning server must also maintain a Web application that parses data entered by customers, verifies credit card information, and can dynamically create a user account in an Active Directory or LDAP compatible user accounts database.

Related Links

See the following resources for further information:

- Wireless Provisioning Services at http://go.microsoft.com/fwlink/?LinkId=41058
- WPS Authoring Tool at http://go.microsoft.com/fwlink/?LinkId=40535
- Using the WPS Authoring Tool at http://go.microsoft.com/fwlink/?LinkId=41067
- Windows Server 2003 Internet Authentication Service at http://go.microsoft.com/fwlink/?LinkId=20133
- Deploying SQL Server Logging with Windows Server 2003 Internet Authentication Service (IAS) at http://go.microsoft.com/fwlink/?LinkId=41039
- Remote Access Logging at http://go.microsoft.com/fwlink/?LinkId=41038
- Internet Authentication Service Extensions at http://go.microsoft.com/fwlink/?LinkId=34431
- Internet Authentication Service Reference at http://go.microsoft.com/fwlink/?LinkId=34429
- Windows Server 2003 Wi-Fi at http://go.microsoft.com/fwlink/?LinkId=5969
- SQL Server at http://go.microsoft.com/fwlink/?LinkId=20014
- Windows XP Professional at http://go.microsoft.com/fwlink/?LinkId=20127
- Windows XP Tablet PC Edition at http://go.microsoft.com/fwlink/?LinkId=20128
- Windows XP Home Edition at http://go.microsoft.com/fwlink/?LinkId=20130

For the latest information about Windows Server 2003, see the Windows Server 2003 Web site at http://go.microsoft.com/fwlink/?LinkId=20045.