Microsoft Solutions for Security

Securing Wireless LANs with Certificate Services

Test Guide

Release 1.6

Microsoft

Test Guide Overview

The Test Guide explains the overall test strategy that Microsoft used to validate this solution, and describes the primary test cases that you can use to validate the solution in your own labs. The complete set of test cases for the solution is included.

The Test Guide contains the following chapter:

- Chapter 13: Testing the Solution

Table of Contents

13

Testing the Solution

Introduction

The Test Guide will help you to verify that your implementation of the *Securing Wireless LANs with Certificate Services* solution works as expected. The guidance in this chapter was developed and used by the Microsoft Solutions for Security (MSS) test team as part of the internal testing for the solution. The guidance describes the scope of the tests, test objectives and strategy, the test lab environment, the tools used, and the test cases. Lastly, it also reports the test results from the MSS labs.

Purpose of This Document

This purpose of this chapter is to provide you with a ready–made testing framework that you can use to test your own deployment of the solution. After you successfully run through the test cases, you should have a high degree of confidence that your deployed solution—whether in a test lab or in production—will work as expected.

Test Scope

The tested solution was based on the fictional company profile described in Chapter 3, “Secure Wireless LAN Solution Architecture.”

In Scope

The test team conducted different types of tests to validate the solution. Different combinations of these were tested in each test phase. The different types were:

- Baseline tests
- Functional tests
- Operation tests

The description of these tests is given in the “Test Cases” section later in this chapter.

The test team conducted these three test types on the following components as used in the solution:

- The PKI, comprising:
  - Root certification authority (CA)
  - Issuing CA
- Microsoft Internet Authentication Service (IAS)
- Wireless clients:
  - Microsoft® Windows® XP Professional with Service Pack 1 (SP1)
  - Windows XP Tablet PC Edition with SP1

In addition, the testing verified that after installing each component of the solution, the clients could access the following services with the same level of functionality as before. This was designed to show regression in functionality due to the introduction of any of the previously listed solution components or changes made to them during the configuration process:

- Network connectivity
- Domain controller
- IP configuration—Dynamic Host Configuration Protocol (DHCP)
- Name resolution services—Domain Name System (DNS)
- File services—File Server
- Web services—Internet Information Services (IIS)
- E-mail services—Microsoft Exchange 2000
- Wireless network access

Out of Scope

The following areas were excluded from the testing scope:

- Vulnerability assessment and penetration testing of the solution. A commercial security consultancy performed this assessment and testing.
- Integration with a third–party Public Key Infrastructure (PKI).
- Extensive testing of the following server roles (other than that needed to verify the correct behavior of the solution):
  - Domain controller, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS)
  - Exchange Server 2000
  - Web Server and File and Print server
  - Microsoft Operations Manager (MOM)
- Extensive testing of the following client services (again, these were used to verify solution functionality):
  - DNS and DHCP
  - File
  - Web
  - E–mail
- Clients running the following software were excluded from the testing scope:
  - Windows 2000 Professional
  - Pocket PCs running Windows CE
  - Microsoft Windows NT® version 4.0
  - Windows 9*x*
  - Non–Windows clients

Test Objectives

The test objectives were to verify the following:

1. That all prescriptive guidance in the solution is clear, complete, and technically correct.
2. That the solution provides a secure wireless LAN (WLAN) network using Certificate Services with no detrimental effect on any of your existing infrastructure functionality, performance, and security policy.
3. That you can easily deploy the solution. IT professionals who have attained the Windows 2000 (or Server 2003) Microsoft Certified Systems Engineer (MCSE) certification or have equivalent knowledge level and who are familiar with Certificate Services and IAS should be able to use this guidance.

Test Strategy

To achieve the test objectives, the test team developed a lab based on Woodgrove Bank, a fictional company of 15,000 users. The test lab environment is described later in the chapter. The tests consisted of the following stages:

- The solution was unit tested as part of the development process.
- System test pass one.
- System test pass two.
- System regression tests.

The base infrastructure servers for the tests included the following roles (some of these roles were combined on one server):

- Domain controller, DHCP, and DNS
- Web server and File & Print server
- Microsoft Exchange Server E–mail server
- Microsoft Outlook® Web Access server
- Active Directory® domain controller

These services were verified by conducting the baseline tests before any of the solution components were deployed. An image backup of each of the infrastructure servers was taken for use during the second test pass. The regression test used the same infrastructure as the second test pass.

The system test passes (one and two) were themselves divided into two incremental build phases as follows:

1. The PKI Certificate Services phase
2. The WLAN phase

A detailed description of these two phases follows later in this section.

The test team recorded bugs for any critical issues found during a given phase; all critical bugs were resolved in that phase before the testing moved to the next phase. This strategy helped the test team rapidly resolve critical issues, and save time and cost related to debugging issues.

Testing with multiple test passes (or cycles) also ensured that any non-critical issues found in test pass *N* were resolved in regression test pass *N+1* to provide a high quality solution. The solution was stable by the end of the third regression test cycle.

The following figure portrays the phased test approach to the solution in this guide:

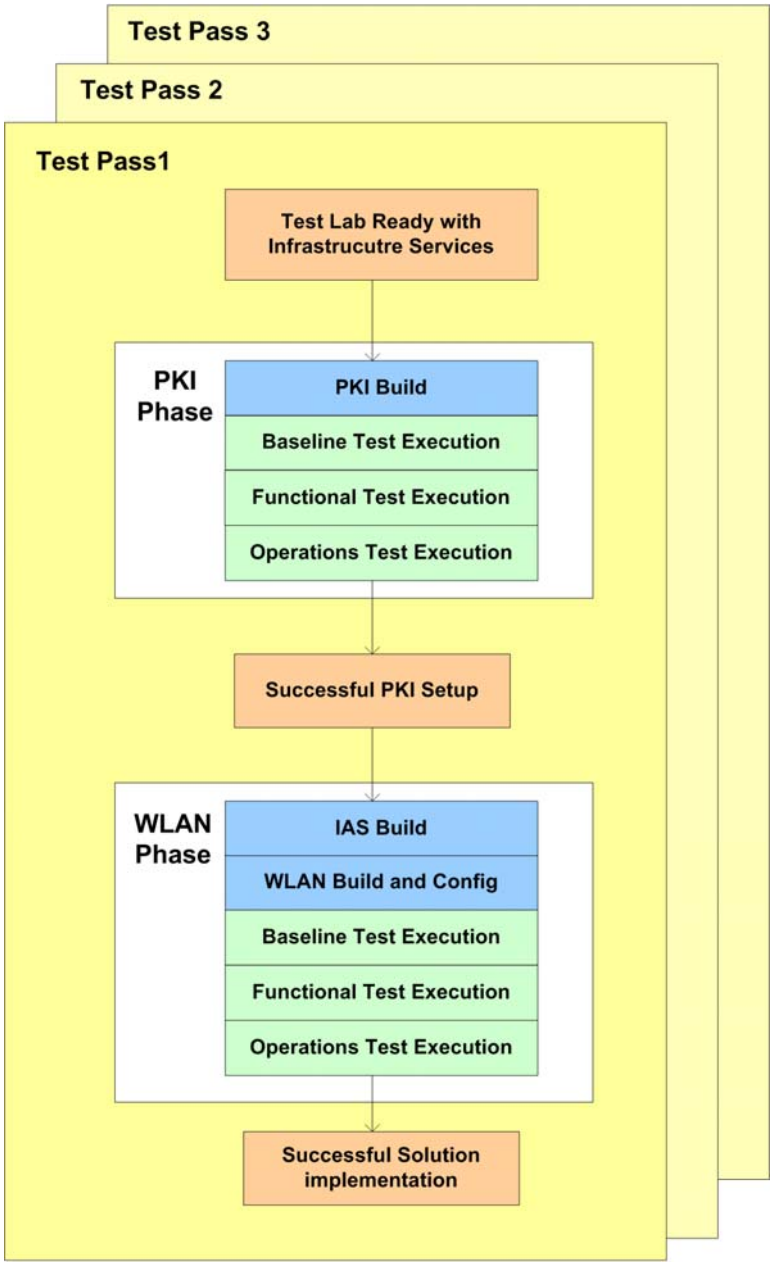

Figure 13.1
The phased test approach for the solution

Test Phases

Testing followed a logical phased approach. Each phase was incremental and had the following steps:

1. Entry criteria: Start of the phase
2. Component build
3. Different types of tests conducted on the build
4. Exit criteria: End of the phase

The PKI Phase

The entry criterion for this phase was successful execution of the baseline tests on the infrastructure servers. The steps involved in this first phase were as follows:

1. **PKI Build:** This step consisted of implementing Certificate Services for the network. It involved installing, building, and configuring the root CA and issuing CA servers. This was also the Component Build step for the phase.
2. **Baseline test execution:** This step ensured that the Certificate Services setup did not break the already existing infrastructure and client services.
3. **Functional test execution:** This step ensured that the CAs were implemented successfully in the test network, and that they were fully functional.
4. **Operations test execution:** This step ensured that the CAs could be managed and maintained by appropriate administration roles. These tests verified the various Certificate Services component operations procedures mentioned in the Solution Guide.

The exit criterion for this phase was successful completion of the all of the above mentioned tests.

The WLAN Phase

The build of the second incremental phase, the WLAN phase, began after successfully completing the PKI phase. Successful installation of the PKI phase was the entry criterion for this phase. The second step started with the installation of the IAS servers and then moved to configuring the WLAN components. The steps involved in this phase were:

1. **IAS Build:** This step consisted of installing and configuring the IAS servers in the network at both the headquarters (HQ) and at the branch office according to the guidance for the solution.
2. **WLAN components:** This step consisted of building and configuring the WLAN components.
3. **WLAN clients:** This step consisted of configuring the WLAN clients.
4. **Complete baseline test execution:** This step verified that there was no negative impact on the base infrastructure and client services.
5. **Complete functional test execution:** This step verified that the solution was successfully built and implemented. It included verifying the secure wireless access services in the network and their use of the PKI built in the previous phase.
6. **Complete operations test execution:** This step ensured that the secure network could now be managed and maintained. This included re-testing the Certificate Services components using operations and management tests.

The exit criterion for this phase was successful completion of all the above mentioned tests.

Test Environment

The test environment was designed to be a functional subset of the IT services that a company such as Woodgrove Bank would use. All key infrastructure services required by the solution were represented in the lab environment. The lab emulated a headquarters (HQ) office and a smaller branch office linked by a routed wide area network (WAN) connection. The following infrastructure servers were set up in the lab:

- Domain controller, DHCP, and DNS (HQ and Branch)
- Microsoft Exchange 2000 (on Windows Advanced Server 2000) at the HQ
- Web and File & Print at the HQ
- MOM at the HQ

The solution servers themselves consisted of the following:

- The Root CA at the HQ
- The Issuing CA at the HQ
- Primary and secondary IAS servers at headquarters, and a secondary IAS service installed on the branch office domain controller.

Hardware

The test lab hardware configuration of the server computers was based on the hardware profiles provided in the solution guidance, with the addition of the following:

- Standard desktop clients
- Standard portable computer clients
- Standard Tablet PC clients
- 802.1X capable wireless access points (APs) at the HQ and branch office
- Desktop computers for routing and WAN simulation
- Layer 3 Switch

Software

The base operating system used in the Test lab for all of the server roles (except Microsoft Exchange 2000) was Microsoft Windows Server™ 2003. In addition, the following software was used for testing:

- Windows 2000 Advanced Server with SP3
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Standard Edition
- Exchange 2000 with SP3
- Windows XP Professional with SP1
- Windows XP Professional with SP1 (Tablet version)
- MOM 2000 with SP1
- Microsoft SQL Server™ 2000 with SP3
- Outlook 2000 with SP1

To test secure wireless access, the test lab clients used the following operating system:

- Windows XP Professional with SP1
- Windows XP Tablet PC Edition with SP1

Network Diagram

The following diagram is a detailed schematic of the test environment.

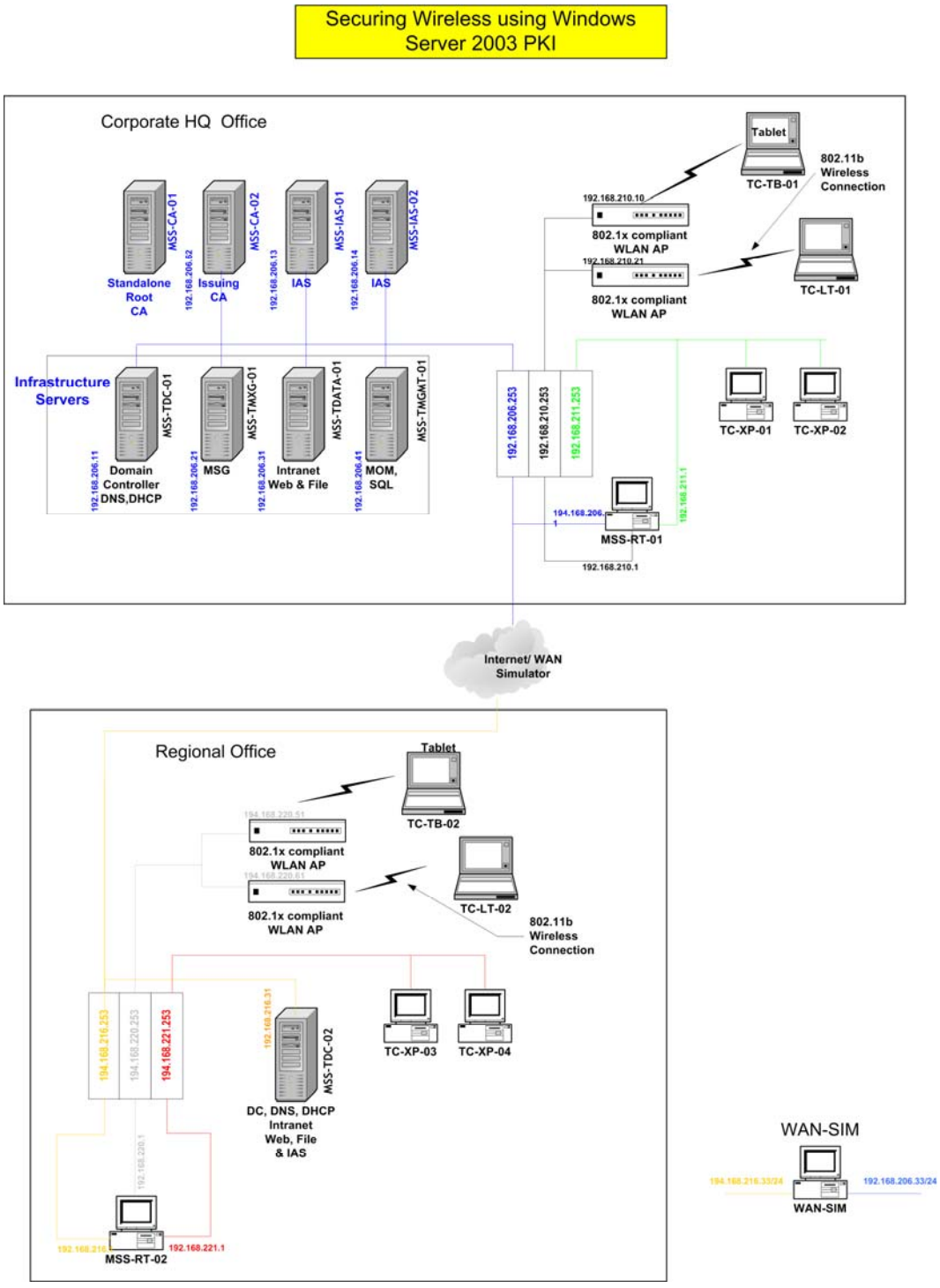

Figure 13.2
Test lab network diagram

Configurations and Settings

The previous figure displays the network that was built in the test lab to simulate the Woodgrove Bank scenario. In this scenario, there is a headquarters network containing the majority of the infrastructure and solution servers, and a branch office network with a single server running infrastructure and solution services for it. The WAN simulator computer introduces network latency and bandwidth restriction between these networks. The configuration and settings in the test lab were identical to those prescribed in the solution guidance.

Test Tools

This section describes the different kinds of tools used during the solution testing. Most of these tools are available with the installation guidance for the operating system. Otherwise, you can install them from the Support\Tools folder on the Windows Server 2003 installation media.

Software

The following tools were used while testing:

- Certutil—This is a powerful multipurpose Certificate Services utility tool that you can use to setup, configure, and troubleshoot CAs.
- Certreq—This tool is used to manually request a certificate from a CA, and it is available from the Windows Server 2003 installation media.
- Ldifde—This tool is used to import and export Active Directory information using LDAP Data Interchange Format (LDIF) files. This tool was used for some certificate template related operations in the solution.
- Ntbackup—This tool is used to restore and backup files, and it is available on the Windows Server 2003 installation media.

System Monitoring

The following system monitoring tools were used during testing:

- Dcdiag—This tool analyzes the state of domain controllers in an Active Directory forest and reports any problems to assist in troubleshooting.
- Jetpack—This tool is used to verify DHCP database consistency.
- Agenthelper—This tool is a MOM utility that verifies the OnePoint service is running on the MOM managed agents.
- PerfMon—This tool allows you to view system performance logs, alerts, and counters.
- NetMon—This tool captures and filters frames from network traffic to and from the computer on which this utility is installed.
- IASparse—This tool interprets IAS log files, and details the various Remote Authentication Dial-In User Service (RADIUS) parameters.
- EventViewer—This tool allows you to view, filter, and export the Windows Application, Security, and System monitoring logs.
- MOM MMC—This is the MOM Management console that monitors for information, warnings, alerts, errors, and critical error logs for the agents that the MOM server manages.
- PKIHealth—This tool is used to diagnose CRL Distribution Point (CDP) and Authority Information Access (AIA) problems for all CAs across the organization.

Custom Scripts

The following scripts were used at various solution-defined stages during the testing:

- ca_setup.wsf—This script contains the job commands that are required while configuring and building the Certificate services.
- ca_setup.vbs—This script contains the functional code to implement the jobs defined in the ca_setup.wsf script.

- ca_monitor.wsf—This script contains the job commands required for monitoring CA services.
- ca_monitor.vbs—This script contains the functional code to implement the jobs defined in ca_monitor.wsf.
- ca_operations.wsf—This script contains the job commands required while performing Certificate services operational and monitoring tasks.
- ca_operations.vbs—This script contains the functional code to implement the jobs defined in the ca_operations.wsf script.
- constants.vbs—This script contains constant parameters for Certificate services that are used in other scripts.
- helper.vbs—This script contains common functions and variables used by scripts related to Certificate, IAS and WLAN.
- IASAccessPrep.txt—This text file contains the header rows that are added the IAS log files to convert them into MS Access files.
- IASClientExport.bat—This batch file dumps the RADIUS client configuration of the IAS server into a text configuration file on the A:\ drive.
- IASClientImport.bat—This batch file imports the RADIUS client configuration from a text configuration file on the A:\ drive to the IAS server.
- IASExport.bat—This batch file dumps the IAS specific configurations into a text configuration file.
- IASImport.bat—This batch file imports IAS specific configurations from a text configuration file to the IAS server.
- ias_tools.wsf—This script contains job commands that are required while configuring IAS servers.
- ias_tools.vbs—This script contains the functional code to implement the jobs defined in the ias_tools.wsf script.
- IAS_Data.bat—This batch file contains a command that is required while configuring the IAS servers for the solution.
- pkiparms.vbs—This script contains user specific constants that are used during the Certificate Services configuration process.
- wl_tools.wsf—This script contains job commands that are required while configuring the WLAN components.
- wl_tools.vbs—This script contains the functional code to implement the jobs defined in the wl_tools.wsf script.

These scripts are all included with the solution download package.

Test Cases

This section details the tests used to verify the solution and ensure that the solution fulfilled its objectives. In addition, this section includes the test case Pass and Fail criteria. The core tests listed are a small subset of the full set of test cases. The full test case list is documented in two Microsoft Excel spreadsheets that are included with the download package for the solution (see references for the spreadsheet files on next page).

The test scenarios in the following list were tested after the lab was completely built according to the solution guidance. The domain users and computers were added to the appropriate certificate services and wireless access security groups and users were connected to the network with a wired connection and allowed to log on once so that Group Policy was correctly applied to the wireless client computers.

The following core scenarios were tested in the lab to validate the solution:

- **Certificate auto-enrollment for users and computers**—When a user logs on to the domain using a wired network connection, Group Policy is applied for both the user and computer. User and computer authentication certificates are correctly issued by the issuing CA, and that the certificates are available in the personal certificate stores of the user profile and the computer.
- **Root and issuing CA certificates in the trusted root store**—When a user logs in to the domain with a wired connection, Group Policy is applied for the user and computer. The user and computer certificate stores are verified using the Certificates MMC; under the Trusted Root Certificate Authorities folder, the presence of the Root CA Certificate is verified. The presence of an Issuing CA certificate under the Intermediate Certification Authorities also is verified.
- **The IAS server authentication certificate**—When the build is complete and the IAS servers are added to the appropriate security groups and organizational units (OU), the IAS servers were restarted (restart was required so that the computers could obtain new group memberships). Each IAS server receives a new server authentication certificate. This was verified using the Certificates MMC to view the computer certificate store.
- **The Root and Issuing CA certificates and CRLs are available on the Web server**—From Internet Explorer on a client computer, the Web server's PKI virtual directory was accessed to verify that the client could view the Root and Issuing CA's certificates and CRLs. This verification should match the Hypertext Transfer Protocol (HTTP) location configured in the client's certificate under the **Details** tab.
- **Wireless access to the network using authentication certificates**—After a user received the new and valid user and computer authentication certificates the wireless network card was plugged in and the wired connection was removed. After the computer was restarted, computer authentication to the WLAN occurred. The computer authentication to the WLAN was verified by looking in the IAS server system event log. Then, the user could log in to the domain over the WLAN. User authentication to the WLAN was verified by a system event log entry generated on the IAS server.

- **IAS server availability for branch office users**—When the Branch office IAS service is unavailable, users can authenticate against one of the IAS servers at headquarters. The setup for this test was to have the headquarters' IAS server serve as the secondary IAS server on the wireless APs of the branch office. Then, the IAS service in the branch office was switched off. Users could still authenticate and connect to the WLAN. The authentication was confirmed by looking at the authentication events logged to the system event log on the headquarters' IAS server.

Details on the different types of test cases that the Test team executed for the solution are described in the following sections.

Baseline Tests

These tests validate the base infrastructure services. They include basic tests on server and client functionality that were referred to during the system testing.

From the client's perspective, the baseline tests included testing of basic client services, such as authenticating to the domain and accessing a file server, Web server, and E–mail server. The baseline tests were rerun after each phase of the solution build to verify that applying the solution configuration did not cause any problems for the existing functionality of the environment.

From the servers' perspective, the baseline tests verified that the servers were properly functioning and that there was no negative impact on their roles after implementing the solution components.

For more information about the test cases used for the baseline test phase, see the Baseline Test Cases.xls file included with the solution.

Functional Tests

These tests were designed to verify that the solution could be built as documented and would provide the expected functionality. The functional test cases included verifying the functions, status, and interoperability of the PKI, IAS, and WLAN components and services as prescribed by the solution guidance.

For more information about the test cases used in the functional test phase, see the Functional & Operational Test Cases.xls file included with the solution.

Operation Tests

These tests validated the operations, maintenance, and manageability of the servers in the solution. These factors are documented in the management procedures of the Operations Guide in Chapter 11, "Managing the Public Key Infrastructure," and Chapter 12, "Managing the RADIUS and Wireless LAN Security Infrastructure."

For more information about the test cases used in the operational test phase, see the Functional & Operational Test Cases.xls file included with the solution.

Release Criteria

The primary release of the solution was linked to the severity and priority of open bugs according to the following criteria:

- No open Severity 1 or Severity 2 bugs.
- No open Priority 1 or Priority 2 bugs of any severity.
- All of the solution guides were free of comments and revisions.
- All open bugs were triaged by the leadership team.
- All test cases in the test lab environment were successfully completed.
- All of the solution content was without conflicting statements.

Bug Classification

The following table defines the bug severity and priority definitions that were used in the Test lab.

Table 13.1: Bug Classification

Rating	Severity definition	Priority definition
1	The bug causes system crash or data loss.	The bug must be fixed as soon as possible. The bug is blocking further progress in this area.
2	The bug causes major functionality or other severe problems; product crashes in obscure cases.	The team should fix the bug before product release.
3	The bug causes minor functionality problems; may affect quality.	Fix the bug if there is time; somewhat trivial. May be postponed.
4	The bug documents typographical errors, unclear wording, or error messages in low visibility fields.	Not defined.

Testing Results

All of the test cases passed with positive results. There were no open Severity 1 and 2 bugs and none with a level of Priority 2 or higher. This demonstrates that the test objectives were successfully met and that the solution is ready for public release.

Diagnostic Information

The following tips were helpful while troubleshooting issues during testing:

- Create HKCU\Software\Microsoft\Cryptography\Autoenrollment\AEEventLogLevel {**DWORD** set to **0**}. Then auto-enrollment will log to the Application Event log. Create the same registry key at HKLM for computer enrollment.
- Make sure that the shared secret on the wireless AP and IAS server is the same and correct (use copy and paste from the secrets file). Otherwise, the AP will not authenticate to the IAS server as a RADIUS client. This will result in error logs on the IAS server with one or the other following messages:
  - Invalid Authenticator

  - or -
  - Message authenticator attribute that is not valid.
- If the IAS server generates a warning log with Event ID 2 citing the following reason: Authentication was not successful because an unknown user name or incorrect password was used, ensure that the Remote Access Policy for Wireless is correctly configured on the IAS server. Also verify that the user has been added to the appropriate wireless security groups.
- If the IAS server generates a warning log with Event ID 2 citing the following reason: A certificate chain processed correctly, but one of the CA certificates is not trusted by the policy provider, verify that you can validate the IAS server certificate and user certificate against the current Issuing CA certificate. Also ensure that the valid Root CA and Issuing CA certificates are present in user's certificate store.
- If the SCHANNEL generates a warning log with Event ID 36877 citing the following reason: The certificate received from the remote client application has not validated correctly. The error code is 0x80096004. The attached data contains the client certificate, ensure that the user and computer wireless authentication certificate has not expired or been revoked.
- Refer to the "Troubleshooting" sections in the Operations Guide chapters for more diagnostic information.

More Information

You can find more information about the testing in the solution's Planning, Build, and Operations guides. The following links also provided useful reference information while troubleshooting issues during the testing:

- For information about troubleshooting, see the white paper "Troubleshooting Windows XP IEEE 802.11 Wireless Access" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspx.
- For information about certificate auto-enrollment in Windows XP, see the white paper "Certificate Autoenrollment in Windows XP" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/certenrl.mspx.
- For information about PKI enhancements, see the white paper "PKI Enhancements in Windows XP Professional and Windows Server 2003" at http://www.microsoft.com/technet/prodtechnol/winxppro/plan/pkienh.mspx.
- For a Windows XP wireless deployment technology and component overview, see the article "Windows XP Wireless Deployment Technology and Component Overview" at www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx.