

Microsoft Solutions for Security

Testing the Windows XP Security Guide

Microsoft®

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e – mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e – mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Windows Server 2003, Active Directory, Excel, Exchange Server, Money, Visual Basic, Office, Outlook, Windows 98, Windows NT 4.0 Workstation, Windows 2000 Professional, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Introduction	1
Scope	1
Testing Objectives	1
Testing Strategy and Methodology	2
Strategy	2
Testing Environment and Tools	2
Test Cycles	3
Lab Network Diagrams	4
Types of Test Procedures	6
Base Deployment Tests	6
Interoperability Tests	7
Usability Tests	7
Pass and Fail Criteria	7
Security Build Phases	7
Test Prep Phase	7
Manual Server Configuration Phase	8
Group/Local Policy Configuration Phase	9
Test Execution Details	9
Chapter 2: Configuring the Active Directory Domain Infrastructure	9
Chapter 3: Security Settings for Windows XP Clients	10
Chapter 4: Administrative Templates for Windows XP	10
Chapter 5: Securing Stand–Alone Windows XP Clients	12
Chapter 6: Software Restriction Policy for Windows XP Clients	12
Release Criteria	13
Bug Classification	14
Summary	15

Introduction

The *Windows XP Security Guide* was tested in a lab environment to ensure that the technology works as expected and to have a high degree of confidence in the recommended solution.

The documentation was checked for consistency, and all recommended procedures were tested by the *Windows XP Security Guide* test team, thus ensuring that users of the solution save on costs and time associated with building and testing their own implementations of the solution.

Scope

The *Windows XP Security Guide* was tested in a lab environment based on the two scenarios described in Chapter 1, "Introduction to the Windows XP Security Guide." Testing was conducted based on the criteria described in the Testing Objectives section below.

A vulnerability assessment of the test lab environment secured by the *Windows XP Security Guide* solution was out of scope for the test team. Penetration testing was taken up by partners, details of which are presented in the Test Execution section below.

Testing Objectives

The objectives of the *Windows XP Security Guide* test team were to verify that:

- All statements made in the solution guide are accurate.
- All prescriptive guidance in *Windows XP Security Guide* is correct. The guidance should be repeatable and reliably usable by a Microsoft Certified Systems Engineer (MSCE) with two years of experience.
- The Domain Administrators and Local Administrators can use system tools after hardening Microsoft® Windows® XP.
- Domain Users and Local Users can access various applications, which are listed in the Testing Strategy and Methodology section below, after securing Windows XP.

Testing Strategy and Methodology

This section deals with the overall strategy of the test effort. It begins with an overview of the strategy and then presents the details on which test execution is based. These include a description of the test environments, tools and software used, progression of test cycles, security build phases of each test cycle and the tests executed in each security build phase.

Strategy

To achieve the testing objectives, the test team developed a test lab based on the two scenarios identified for hardening to different levels of security. The test team executed two test cycles to validate the guidance in the *Windows XP Security Guide*.

A test cycle was defined as a sequence of the following two incremental security build phases:

1. Manual Server configuration phase
2. Group/Local Policy configuration phase

The details of these phases are provided in the Security Build Phases section below, along with the Test Prep Phase section which describes the steps undertaken to ensure that the lab environment itself was free of any issues that could cause a misinterpretation of the actual test results after both the scenarios had been hardened through the two security build phases.

At various stages in a cycle, different sets of tests were executed from the pool below as further explained in the Types of Tests section.

- Base deployment tests.
- Interoperability tests
- Usability tests

For the complete details on how each chapter was tested and how the phases as well as the tests were sequenced, please refer to the Test Execution Details section below.

Testing Environment and Tools

The test environment consisted of Microsoft Windows Server™ 2003 Active Directory® directory services, Infrastructure Servers—Wins, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP)—file and printer servers, Microsoft Internet Information Server (IIS), Microsoft Exchange 2000 Server. The Level 2—lockdown Scenario, which is for the enterprise client environment, also contained the public key infrastructure (PKI) Certification Server and Microsoft Internet Authorization Server (IAS).

For Level 2 (enterprise) and Level 3 (high security) lockdown scenarios the test environment consisted of three clients with the following operating system:

- Windows XP SP1 Desktop Clients
- Windows XP SP1 Laptop Clients

Test Cycles

Testing with multiple test cycles ensures that issues found in test cycle N are resolved in regressive test cycle $N + 1$. This ensures a high quality solution. The test team executed two test cycles, and at the end of the second test cycle the solution reached a stable state.

For the first test pass, a separate scenario was built in the lab that has:

- One server with Windows Server 2003 and the server roles installed (DC, DNS, DHCP, File, Print, and Web).
- One server with Windows Advanced Server 2000 and Exchange Server 2000 installed.
- Two laptops with Microsoft Windows XP® Professional – SP1 installed.
- Three desktops with Windows XP Professional – SP1 installed.

The following is the list of applications installed on the client machines in order to test them:

- Microsoft Office XP
- Adobe Acrobat Reader 5.0
- Roxio Easy CD Creator 5.0
- Apple QuickTime 6.0
- WinZip
- iHateSpam for Microsoft Outlook®
- Paint Shop Pro 6.0
- Microsoft Money 2003
- Microsoft Reader
- Microsoft ActiveSync 3.5
- eTrust antivirus 6.0.1
- Microsoft TechNet
- Attachmate myExtra!

For second test pass, two laptop and two desktop machines were plugged into Scenario 2 and Scenario 3 of the Securing Windows Server 2003 environment. These XP clients were tested in these environments against secured Windows 2003 servers: domain controller, DNS, DHCP, Web, file, print, certificate authority (CA), and IAS.

Lab Network Diagrams

The following diagram shows the scenario that was built in the lab for the first test round.

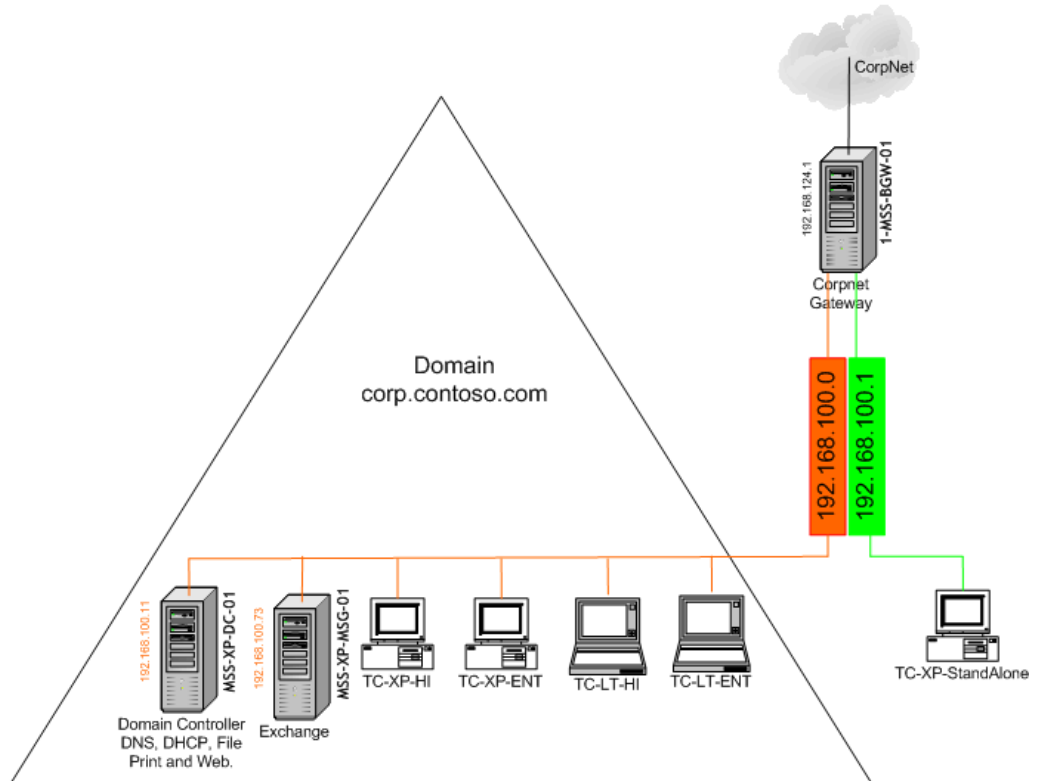


Figure 1.1
Lab diagram for the first test pass

The following figures show scenarios 2 and 3 of the Windows Server 2003 environment using Windows XP client machines (desktops and laptops):

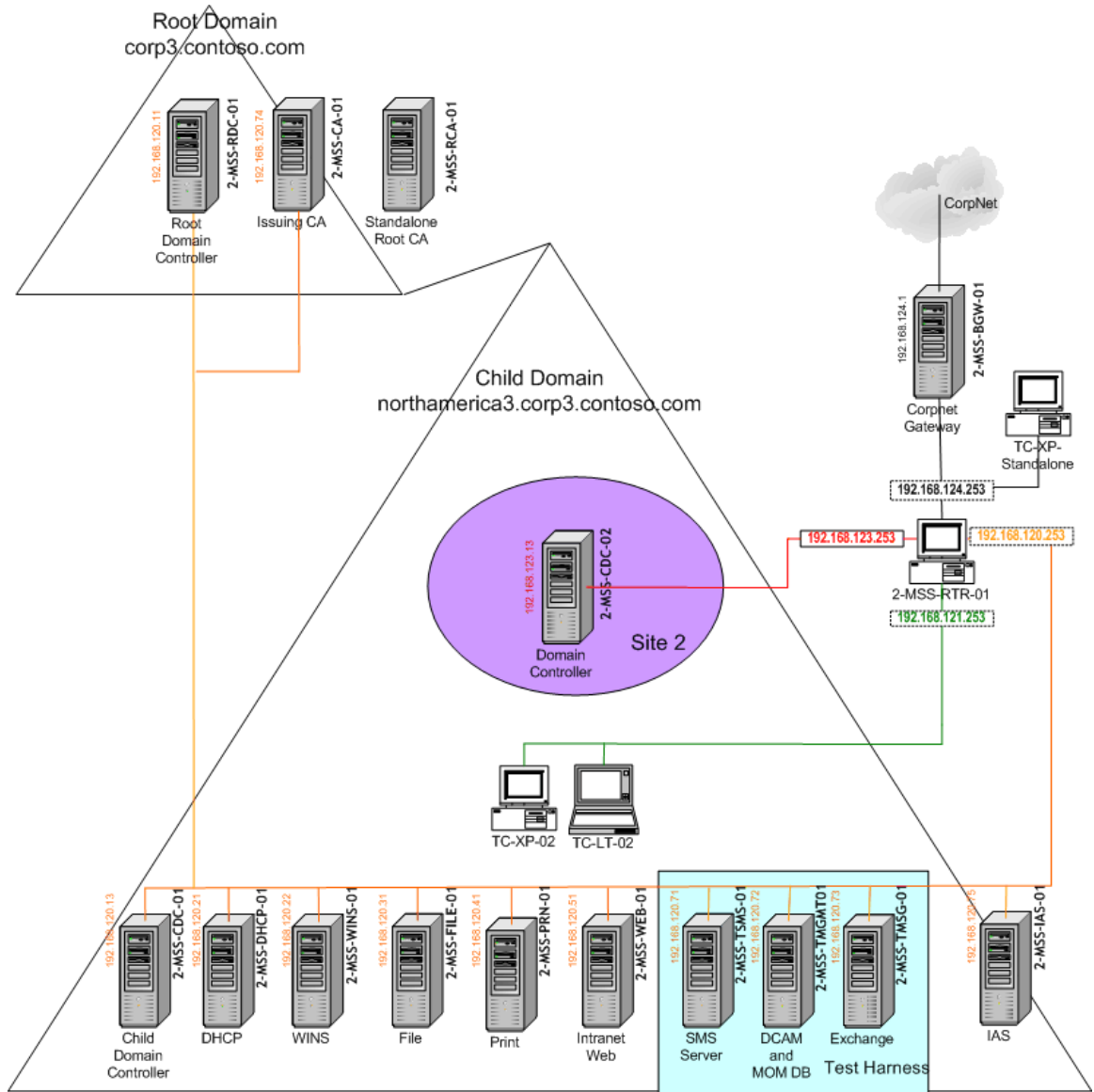


Figure 1.2
Lab diagram for enterprise scenario in the second test pass cycle

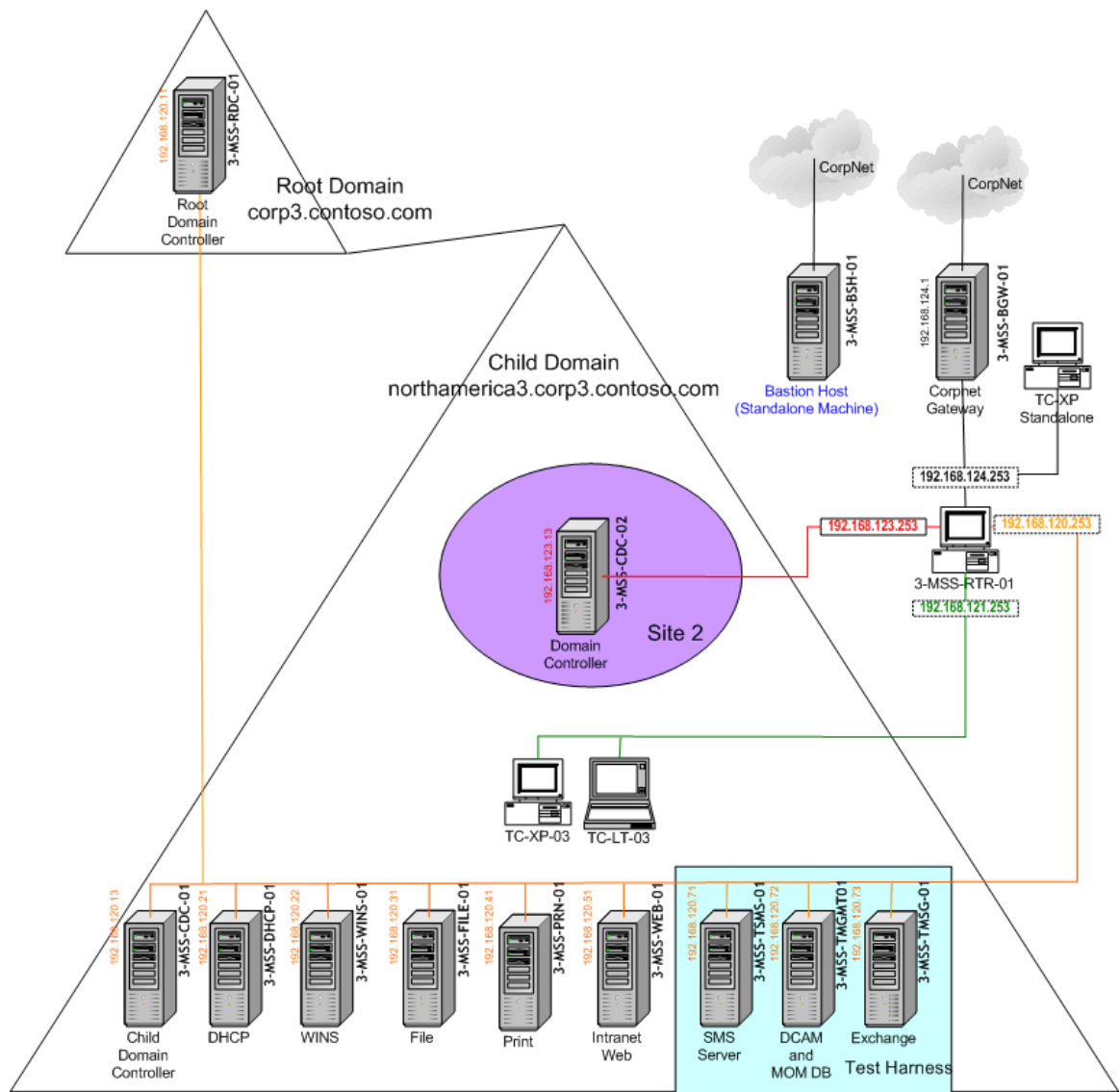


Figure 1.3
Lab diagram for high security scenario in the second test pass cycle

Types of Test Procedures

The test team performed the following tests as part of each security build phase to ensure that the build met the test objectives.

Base Deployment Tests

These test cases were used to verify the correctness of procedures and functions for building security on Windows XP. This helped identify inconsistencies between the security guide, the functional design specification document, and other documents provided along with the security guide. These tests were done prior to Windows XP hardening. No test cases were exclusively designed for this purpose and testing was informal in nature.

Interoperability Tests

These test cases were used to verify that the clients could continue to use the core services from all servers after they had been hardened. These services include: accessing a file which is shared on the file server, printing a document using a network printer, accessing a Web page which resides on the Web server, getting a new Internet Protocol (IP) address from the DHCP Server.

Usability Tests

These test cases were used to verify that the clients could still continue to use various applications—such as Microsoft Office and Adobe Acrobat Reader—after having been hardened. These test cases were also used to verify that the clients could access Web sites such as <http://www.microsoft.com> and <http://msdn.microsoft.com>.

Pass and Fail Criteria

Before of testing, the following criteria were defined to ensure defect–prevention and bug resolution:

- All test cases must pass with expected results as outlined in the individual test case spreadsheets.
- A test case is considered to have passed if the actual result matched the expected result documented for the case. If the actual result does not match the expected result, it was treated as a failed test case and a bug was created and a severity score assigned.
- If a test case failed, it was not assumed that the solution guidance was necessarily defective. For example, misinterpretation of product documentation, incomplete documentation, or inaccurate documentation could cause failures. Each failure was analyzed to discover its cause based on actual results and the results described in project documentation; as well as being escalated to the correct Microsoft owners of the respective products.

Security Build Phases

A security build phase had a clear set of procedures. Any critical issues found in a build phase were raised as bugs and resolved in that phase before the test team moved to the next incremental build phase. This ensured that critical issues were resolved quickly. This saved time and the cost of debugging issues found in the test lab in later phases.

The following subsections describe the Test Prep phase and the two Security Build phases.

Test Prep Phase

Before executing the build phases, a Test Prep phase was executed. This phase consisted of setting up the base network to which the solution was applied, and consisted of the following steps.

- ▶ **To test the preparatory phase:**
 1. Set up the lab according to the network diagram with the base operating system installed on all servers and clients.
 2. Configure each server role.
 3. Install all third–party applications on the clients.
 4. Execute an interoperability test to verify client accessibility of a limited set of services provided by domain controllers and member servers—DNS, DHCP, file, print, and Web.
 5. Execute all the installed applications to verify that there is no installation problem and all the applications run properly.
 6. Check the event log to ensure that there are no errors.
 7. Take ghost images of builds based on the successful execution of the above mentioned tests with appropriate results. This ghosted environment was used as the baseline for testing the solution.

Manual Server Configuration Phase

This is often the first security build phase. It consists of the following security build procedures.

- ▶ **To test the manual server configuration phase:**
 1. The Microsoft Management Console (MMC) for the Computer Management is used to change the prescribed settings, such as the local administrator account and password on each member server in the security guide. Use the following steps to secure the Domain Accounts (guest and administrator accounts):
 - a. Disable the guest account.
 - b. Ensure that the built – in administrator account has a complex password, has been renamed, and has had its default account description removed.
 - c. Follow the security guide’s prescription on additional steps to secure the domain accounts.
 2. Follow all other applicable manual hardening procedures as prescribed by each chapter of the guide.
 3. In case of the stand–alone Windows XP client, manually create a secure database.

Group/Local Policy Configuration Phase

In this phase the Group Policy objects (GPO) were applied at the domain, site, and Organizational Unit (OU) level. GPOs are applied to different OUs, such as the Windows XP OU, Windows XP desktop OU, Windows XP laptop OU, and Domain Users OU. In the case of the stand-alone Windows XP clients, Local Policy is configured. This phase consists of the following security build procedures.

- ▶ **To test the Group/Local Policy configuration phase:**
 1. Create OUs to support Group Policy recommendations in the security guide.
 2. Move the Windows XP clients and desktops to the appropriate OU.
 3. Identify the domain users and move them to the appropriate OU in order to apply the Administrative Templates.
 4. Add a new GPO link for each OU. You might need to move the GPO links higher up in the priority list in cases where a default GPO link is already present.
 5. Import the security template into the GPO.
 6. Apply the Group Policy on the particular OU in accordance with the chapter and scenario that is being tested.

Test Execution Details

Chapters 2 through 6 of the *Windows XP Security Guide* provide recommendations for securing the domain, Windows XP desktops, Windows XP laptops and Windows XP stand-alone clients in both the high security and enterprise environments. These are accompanied by Excel workbooks in the form of security templates, administrative templates and automated scripts. Automated scripts are used for importing templates into the local GPO in the secure stand-alone client. Based on these recommendations, this section of the test guide explains the details of test execution for validating the guidance contained in chapters 2 through 6 of the guide.

Chapter 2: Configuring the Active Directory Domain Infrastructure

Use the following procedure to test this chapter.

- ▶ **To test the baseline:**
 1. Perform a sanity run of around 20 percent of the interoperability test cases to make sure that the ghost image is proper and functioning. A successful sanity run confirms that the entry criterion is met.
 2. Execute the base deployment tests and check for the consistency with other security guides.
- ▶ **To start the manual configuration phase:**
 1. Synchronize the time of all the Windows XP member servers and the Windows XP client computers with the domain controller.
 2. Disable the guest account.
 3. Rename the administrator and the guest account.
 4. Change the administrator password.

- **To implement the Group Policy configuration:**
1. In the northamerica.corp.contoso.com domain, create an OU called **Windows XP OU**. In the **Windows XP OU**, create the following two OUs: **Desktop OU** and **Laptop OU**.
 2. Move the Windows XP desktops to the **Desktop OU** and Windows XP laptops to the **Laptop OU**.
 3. In the northamerica.corp.contoso.com domain, create an OU called **Domain Users OU** and move the domain users to this OU.
 4. Link a new GPO to the domain. Click the **Up** button to have the highest priority for the new GPO, and then import the domain.inf security template into it.

Note: In the enterprise environment, import the Enterprise Client – Domain.inf security template, and in the High Security environment, import the High Security – Domain.inf.

You are now ready to execute the interoperability and usability tests.

Chapter 3: Security Settings for Windows XP Clients

This chapter covers the primary settings configured via Group Policy in a Windows Server 2003 domain. This chapter prescribes the settings that will ensure that the desktops and laptops in the organization running Windows XP are secure.

Use the following procedure to test this chapter.

- **To test the security settings:**
1. Execute the base deployment tests to verify that all the recommendations in the guide are appropriate to your environment. Modify the security template settings as needed before you proceed.
 2. Link a new GPO to the **Desktop OU**. For the Enterprise Client environment, import the Enterprise client–desktop.inf security template into the GPO, and for the High Security environment, import the High Security –desktop.inf security template into the GPO.
 3. Link a new GPO to the **Laptop OU**. For the Enterprise Client environment, import the Enterprise client–Laptop.inf security template into the GPO, and for the High Security environment, import the High Security –Laptop.inf security template into the GPO.
 4. Execute the interoperability and usability tests.

Chapter 4: Administrative Templates for Windows XP

This chapter covers the process of configuring and applying additional security settings to Microsoft Windows XP using administrative templates.

Use the following procedure to test this chapter.



To test the template execution:

1. Execute the base deployment tests and check for consistency with other security guides.
2. Link a new GPO to the **Windows XP OU**, and then import the following Administrative Templates to this GPO:
 - Access10.adm
 - Excel10.adm
 - Fp10.adm
 - Gal10.adm
 - Instlr11.adm
 - Ppt10.adm
 - Pub10.adm
 - Office10.adm
 - Outlk10.adm
 - Word10.adm.
3. Link this GPO to the **Domain Users OU**.
4. Apply the **Computer configuration settings** and **User configuration settings** according to the prescription given in the guide. These include the following:
 - Internet Explorer computer settings.
 - Internet Explorer user settings.
 - Windows Explorer settings.
 - System user settings.
 - System computer settings.
 - Windows update security settings to manage application of patches and hot fixes.
 - Microsoft Office XP: Custom maintenance wizard settings.
 - Microsoft Office XP: Security settings.
5. Execute the interoperability and usability tests.

Chapter 5: Securing Stand–Alone Windows XP Clients

This chapter covers the primary security settings set via Local Computer Policy. The prescribed setting values will ensure that stand–alone desktops and laptops in the organization running Windows XP Professional are secure.

Use the following procedure to test this chapter.



To test stand–alone Windows XP clients:

1. Execute the base deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Create a security database using the Security Configuration and Analysis snap–in. This security database will be used to write to Local Policy.
3. Apply the security settings included in the stand–alone security template files using the Security Configuration and Analysis snap–in. It is necessary to use the Security Configuration and Analysis snap–in instead of the Local Computer Policy snap–in. It is not possible to import the security template using Local Computer Policy snap–in because security settings for System Services cannot be applied using this snap–in.
4. Run the automated scripts in the Excel workbooks included with this guide to import security templates.
5. Execute the interoperability and usability tests.

Chapter 6: Software Restriction Policy for Windows XP Clients

This chapter allows administrators to identify and control the software running in their domain using a policy–driven mechanism called Software Restriction Policy.

Use the following procedure to test this chapter.



To test the Software Restriction Policy:

1. Execute the base deployment tests to confirm that all recommendations in the guide are appropriate for your environment.
2. Locate the OU that was created for the Windows XP desktops and laptops. In the case of stand–alone clients, the settings are located in the Local Security Policy. Create a new GPO for the **Windows XP OU**. Remember, this new GPO is only used for the Software Restriction Policy.
3. Set the Software Restriction Policy by doing the following:
 - a. Create a default Software Restriction Policy.
 - b. Set up the path rules.
 - c. Set the policy options, such as enforcement, designated file types, and trusted publishers according to the prescriptions given in the security guide.
4. After reviewing the policy settings, reset the default policy setting to **Disallowed**.
5. Execute the interoperability and usability tests.

Release Criteria

The primary release criterion for the *Windows XP Security Guide* was tied to the severity of bugs that were still open. However, other issues that were not being tracked through bugs were also discussed. The criteria for release are:

1. No bugs are open with severity levels 1 and 2.
2. All open bugs are triaged by the leadership team, and their impacts are fully understood.
3. Solution guides are free of comments, revision marks, and so on.
4. Solution successfully passes all test cases in the test lab environment.
5. Solution contents have no conflicting statements.

Bug Classification

The bug severity scale is described in the table below. The scale is from 1 to 4, where 1 represents the highest severity, and 4 is the lowest.

Table 1.1: Bug Severity Classification

Severity	Most Common Types	Conditions Required
1	<ul style="list-style-type: none"> –Bug blocked build or further testing. –Bug caused unexpected user accessibility. –Steps defined in the documentation were not clear. –Results or behavior of a function or process contradicts expected results (as documented in functional specification). –Major mismatch between the security template files and the functional specification. 	<ul style="list-style-type: none"> –Solution did not work. –User could not begin to use significant parts of the system. –User had access privileges that should not be allowed. –User access was blocked to certain server that should be allowed. –Expected results were not achieved. –Testing can't proceed without being addressed.
2	<ul style="list-style-type: none"> –Steps defined in the guide are not clear. –Documented functionality is missing (in this case, test was blocked). –Documentation is missing or inadequate. –Inconsistency between security template files and content in the guide but security template file is in sync with functional specification. 	<ul style="list-style-type: none"> –User had no simple workaround to mend situation. –User could not easily figure out workaround. –Primary business requirements could not be met by the system.
3	<ul style="list-style-type: none"> –Documented format issue. –Minor documentation errors and inaccuracies. –Text misspellings. 	<ul style="list-style-type: none"> –User has a simple workaround to mend situation. –User can easily figure out workaround. –Bug does not cause a bad user experience. –Primary business requirements are still functional.
4	<ul style="list-style-type: none"> –Suggestions. –Future enhancements. 	<ul style="list-style-type: none"> –Clearly not a bug related to this version.

1.

Summary

This document enables an organization implementing the *Windows XP Security Guide* to test its implementation of the solution. The actual experience of the Windows XP Security Guide Test Team is captured in this document. It details the scope, objectives, and strategy used for testing the *Windows XP Security Guide*. The test environment, test case details, release criteria, and test results are included in this document.

All of the test cases executed by the test team passed with expected results. The test team was able to confirm that after applying the prescription provided by the *Windows XP Security Guide* for the client scenarios defined in the guide, requisite functionality that the servers were expected to provide was indeed available.