

Microsoft®

Testing the Microsoft Identity and Access Management Solution



Microsoft®

Solutions for Security

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 MS – DOS, Windows, Windows NT, Active Directory Application Mode, Active Directory®, Exchange, Exchange Server, Host Integration Server 2000, Identity Integration Server 2003 Enterprise Edition, Internet Information Server 6.0, Jscript®, Management Console (MMC), Passport, Services for NetWare, Services for UNIX, SQL Server™, VBScript, Windows NT® 4.0, Windows NT® Server 4.0, Windows® 95, Windows® 2000, Windows® 2000 Server, Windows® Server 2003™, Windows® 2003 Authorization Manager, Windows® XP Professional are either registered trademarks or trademarks of Microsoft Corporation in the United States or other countries.

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

Testing the Microsoft Identity and Access Management Solution

Introduction

This document describes testing of the Microsoft Identity and Access Management (I&AM) solution, as outlined in the Implementation Guide. Use this guide as a reference to verify that the implementation of the solution works as expected. This will give you a high degree of confidence in the recommended solution, and give you a basis for testing your own solution.

Purpose of this Guide

The purpose of this guide is to provide you with an approach for implementing your solution either in a lab or production environment. The document is based on thorough laboratory testing of the Microsoft I&AM solution. The guide describes the testing scope, objectives, strategy, environment, tools, and cases, as well as provides the test results.

Test Scope

The testing for the Microsoft I&AM solution was applied to a scenario environment using a fictional company called Contoso Pharmaceuticals environment. The Planning Guide, Chapter 5, "The Contoso Pharmaceuticals Scenario," describes this environment and its expected functionality.

In Scope

The test team conducted the following types of tests to validate the solution in each phase of the test pass:

1. Document tests
2. Baseline tests
3. Functional tests
4. Vulnerability Assessment tests

The "Test Cases" section later in the document describes these tests.

Testing used following components prescribed by the solution:

- Microsoft® Identity Integration Server 2003, Enterprise Edition (MIIS 2003)
- Windows Server 2003™ with Active Directory® directory services (for an intranet and extranet directory)
- Microsoft Internet Information Services (IIS) 6.0 servers (for the extranet)
- Lotus Notes R5 (server and client)
- iPlanet Directory
- Solaris 9 workstation
- SAP Web Application Server version 6.20 (mini-edition)
- SAPGUI client on Microsoft Windows® XP

In addition, testing also verified that the solution causes no major or critical errors while the following servers performed their roles:

- Domain Controller (DC)
- IP configuration–Dynamic Host Configuration Protocol (DHCP)
- Name resolution services–Domain Name System (DNS)
- File services–File Server
- Web services–IIS
- E–mail services–Microsoft Exchange 2000
- Certificate services

Out of Scope

The following things were out of the testing scope of this solution:

1. Penetration testing of the secured environment based on the solution.
2. Performance testing of the secured environment based on the solution.
3. Scalable application testing for the business-to-consumer (B2C) and business-to-employee (B2E) scenarios. These applications were used to validate scenario functionality only.
4. Time-based vulnerability scenarios difficult to reproduce were not tested.
5. Extensive testing of the following services and components:
 - Active Directory
 - DHCP
 - DNS
 - Certificate infrastructure
 - Web and File servers
 - Exchange Server 2000
 - Firewall and Proxy servers
 - Router Device
 - Layer 2/ Layer 3 switches
 - SAP application
 - iPlanet Directory
 - Lotus Notes R5
 - Solaris 9 workstation client

Test Objectives

Testing was performed to meet the following four major objectives:

- Verify that the Planning Guide and Implementation Guide address the issues faced by the fictional Contoso Pharmaceutical scenario.
- Verify that all prescriptive guidance in the Implementation Guide is clear, complete, and technically correct.
- Verify that the solution functions as documented in the Implementation Guide.
- Verify that the Microsoft I&AM solution addresses the vulnerabilities defined in the Contoso environment.

Test Strategy

Testing the solution started with the Development Team building a lab instance based on the Contoso environment, and then carrying out unit testing. This was the proof-of-concept phase of the testing. The Test Team then built a test lab instance of the Contoso scenario to conduct two rounds of testing, followed by a final regression test pass. Each test pass included two incremental build phases:

1. Preparation
2. Implementation

Test Phases

The Test Team used the following logical, phased approach based on incremental steps in both the Preparation and Implementation phases. These incremental steps included:

1. Entry criteria: Start of the phase
2. Build phase
3. Tests execution
4. Exit criteria: End of the phase

After the Preparation phase, the servers were image backed up, and this logical milestone marked the initial stage of the configuration as the Contoso Before State Ready. This approach eliminated the need to rebuild the lab for consecutive test passes; the servers were rebuilt using the backup images. The solution test pass then consisted of the Implementation Phase. Further detail on these phases is provided in the following sections.

Any critical issues found in the first test pass were reported as bugs and resolved before testing progressed to the next phase. This strategy provided a high-quality solution and helped resolve critical issues quickly.

Figure 1.1 shows the phased test approach described in this section:

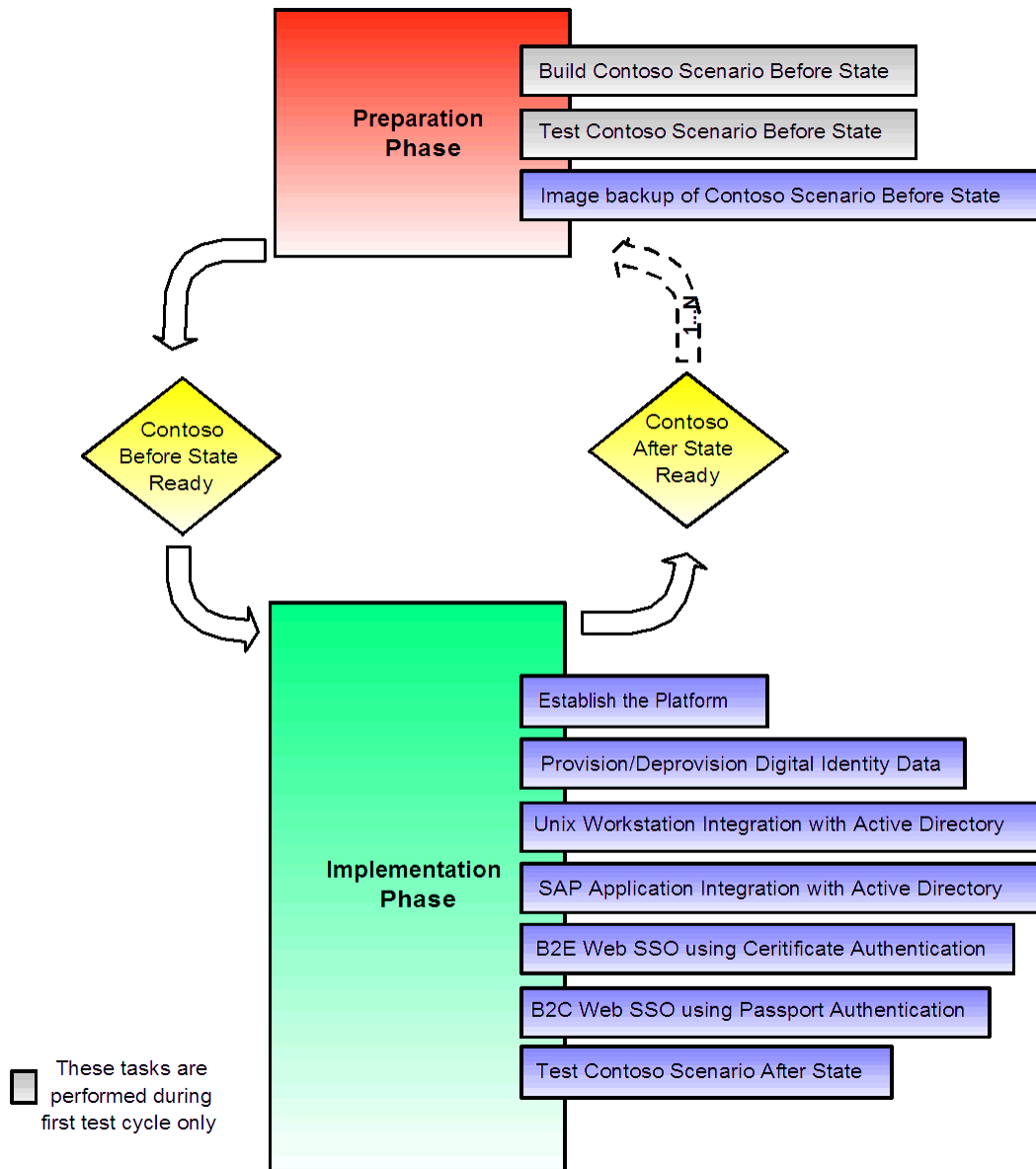


Figure 1.1
The phased test approach used to validate the Microsoft I&AM solution

Preparation Phase

The Preparation phase occurred only once, during the first test pass. The objective of this phase was to build the Contoso environment (Contoso's Before State) with the vulnerabilities described in the "Analyzing Issues and Requirements" sections of the Implementation Guide. The Before State then became the baseline for testing the solution. The steps in this phase were:

1. **Entry criteria:** This consisted of setting up the lab as shown in Figure 1.2, the network diagram, with the base operating system installed on all servers and clients.
2. **Build phase:** This step involved the installation and configuration of the different network components:
 - Manual server configuration of Windows infrastructure:
 - Intranet domain controllers
 - DNS and DHCP services
 - Intranet Web services
 - Intranet file and print service
 - Intranet certificate services infrastructure
 - Extranet domain controller
 - Extranet Web services
 - Perimeter Internet security and acceleration service for firewall and proxy servers
 - Microsoft SQL Server™ 2000 database for applications
 - Configuring PIX firewall
 - Configuring the Edge router
 - Configuring line-of-business (LOB) applications on the extranet Web servers
 - Configuring the iPlanet Directory server
 - Configuring the Lotus Notes Directory server
 - Configuring the SAP server
 - Configuring the Windows XP and Solaris 9 clients
 - Configuring the SAPGUI on the Windows XP client
 - Developing, deploying, and configuring the following ASP.NET applications:
 - The Customer Trial application and related Active Server Pages (ASP) pages.
 - The Sales Contact application.
3. **Test execution:** This step included the following tests:
4. Verifying that Contoso's Before State infrastructure functioned without errors and ensuring that no service failures occurred while executing the Baseline tests.
5. Executing the Vulnerability Assessment test scenarios.
6. **Exit criteria:** After successfully executing the above tests, an image of each server was taken to back each one up for consecutive test passes going forward in the test process.

Implementation Phase

The objective of the Implementation phase was to resolve Contoso's vulnerabilities by implementing the Microsoft I&AM solution. The steps in this phase included:

1. **Entry criteria:** Inspection was done to ensure no major or critical errors had occurred after each image backup of the servers was complete.
2. **Build phase:** This step tested the Implementation Guide documentation. The Implementation Guide was used for the following:
3. Configuring the external and infrastructure Active Directory and configuration of Certificate services.
4. Installing and configuring MIIS 2003 server:
 - Provisioning and deprovisioning digital identity data.
5. UNIX workstation and SAP application integration with Active Directory using the Kerberos version 5 protocol scenario.
6. Business-to-Employee Web Single Sign On using the Certificate Authentication scenario.
7. Business-to-Consumer Web Single Sign On using Passport Authentication scenario.

Note: Steps a and b must be completed before starting the remaining scenario.

8. **Test execution:** This step included the following the tests:
9. Functional
10. Vulnerability
11. Baseline
12. **Exit criteria:** Successful completion of the above tests marked the end of this phase and completed the test pass.

Test Environment

The test lab contained an instance of the Contoso Pharmaceuticals environment, which included the following:

- The following server roles were on Microsoft Windows Server 2003™ Enterprise Edition:
 - Domain Controllers (intranet and extranet)
 - DNS and DHCP
 - Web
 - File and Print
 - Internet Security and Acceleration Firewall and Proxy
 - Root certificate authority (CA)
 - Intermediate CA
 - Issuing CA
 - MIIS 2003
 - Lotus Notes R5
 - iPlanet Directory
 - SQL 2000 database
 - SAP server
 - Microsoft Windows® 2000
 - Exchange 2000 for messaging
 - Cisco Network devices
 - Cisco 515 PIX firewall
 - Cisco 3600 series router

The test lab instance included the following clients:

- Microsoft Windows XP desktops
- Solaris 9 workstations

Hardware

The lab hardware configuration of the server computers running the Windows Server 2003 Enterprise Edition operating system was based on the prescribed hardware profile given in the product documentation. The following additional hardware details were employed in the lab:

- Regular desktop clients
- Sun Ultra 1 Workstation for Solaris 9 client
- Cisco 515 PIX firewall
- Cisco 3600 series router
- Layer 3 Switch

Software

Windows Server 2003 provided the base operating system for all of the server roles used in the scenario with the exception of Microsoft Exchange 2000 with SP3. The Test Team also used the following additional software:

- Microsoft Windows® 2000 Advanced Server with SP3
- Windows XP Professional with SP1
- SQL Server 2000 with SP3
- Lotus Notes R5 (client and server)
- iPlanet Directory Server 5.1
- Lotus Domino R5
- Solaris 9 workstation
- SAP Web Application Server 6.20–Mini Edition
- SAPGUI 6.2

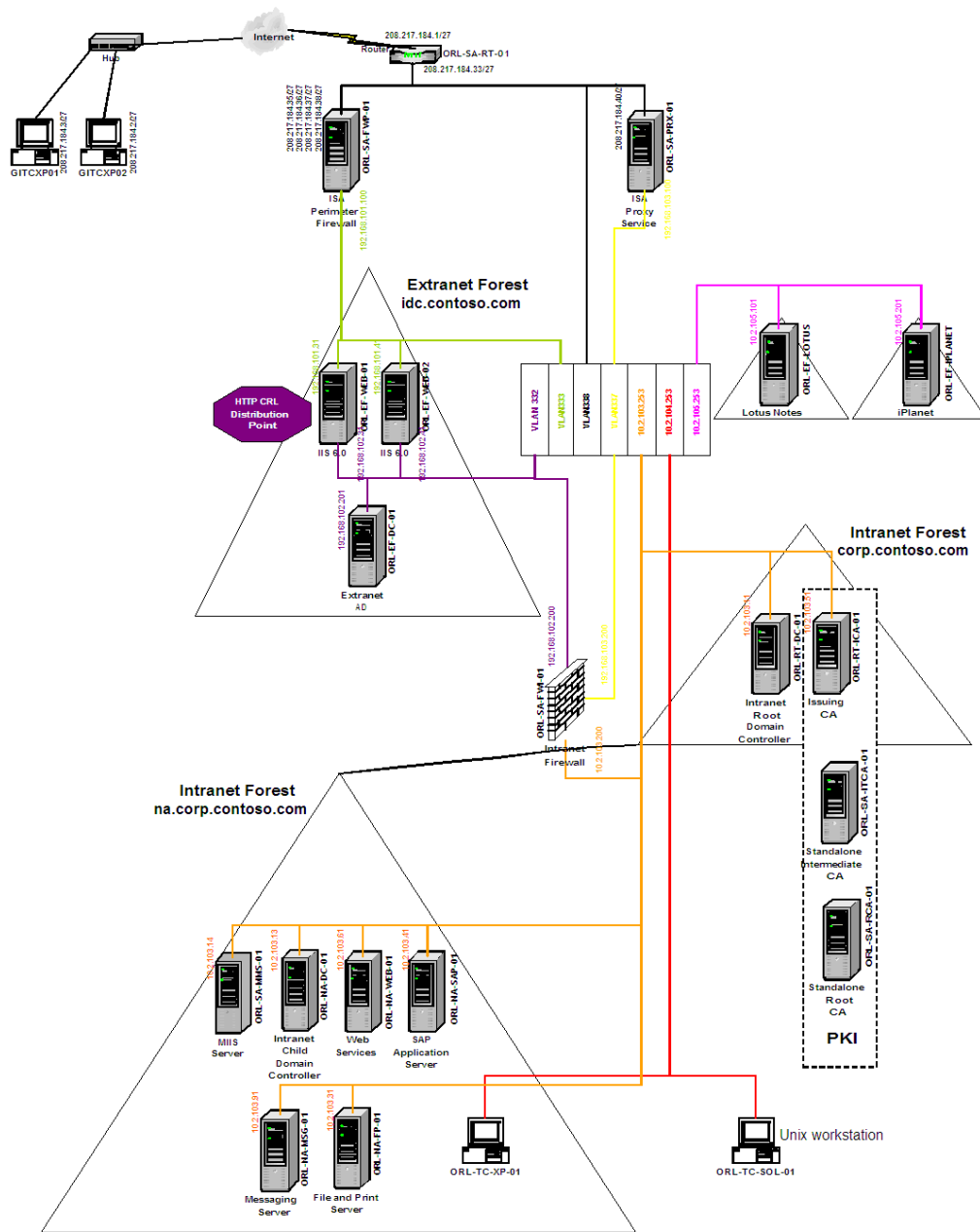


Figure 1.2
The test lab network diagram

Configurations and Settings

Figure 1.2 shows the test lab network setup used to simulate the Contoso Pharmaceuticals environment. Refer to Chapter 2 of the Implementation Guide, "Establishing the Platform," for more details on the network architecture.

Test Tools

This section describes the different tools used during the solution testing. Most of these are available after Windows Server 2003 installs. You can obtain all of the tools from the Support\Tools folder in the Windows Server 2003 installation media.

Software

The following tools were used while testing the solution:

- **ADSIEdit:** This low level editor for Active Directory allows you to view, add, delete, and move objects and attributes within the Active Directory.
- **Ldp.exe:** You can use this tool to search Active Directory using Lightweight Directory Access Protocol (LDAP) filters. You can also use Ldp to add, delete, and modify objects in Active Directory and to perform extended LDAP operations.

System Monitoring

The following system monitoring tools were used during testing:

- **Dcdiag:** Analyzes the state of domain controllers in a forest or enterprise and reports any problems to assist in troubleshooting.
- **Klist:** Solaris command line tool that lists user Kerberos tickets.
- **Kinit:** Solaris command line tool that obtains new Kerberos tickets for users.
- **NetMon:** Captures and filters frames of network traffic going in and out a computer in which this utility is installed.
- **EventViewer log:** Application, security, and system monitoring tool that captures logs related to these functions.

Tests Conducted

This section details the tests you can use to verify the I&AM solution. Additionally, this section includes test case Pass and Fail criteria.

The following were the core scenarios tested to validate the solution. In addition, sales users were connected to the internal network before accessing the extranet Web page for the Sales Contact application via the Internet. This was done so they could obtain user authentication certificates.

- **User account provisioning in different directory stores:** Once the configuration of MIIS 2003 server is complete according to the guidance in Chapter 3, "Digital Identity Aggregation and Provisioning with MIIS 2003," in the Implementation guide, verify that a new user account is provisioned in the following directories as configured in the Workflow Application:
 - Infrastructure Directory
 - External Directory
 - Lotus Notes
 - iPlanet Directory
- **User account deprovisioning in different directory stores:** Once the configuration of MIIS 2003 server is complete according to the guidance in Chapter 3, "Digital Identity Aggregation and Provisioning with MIIS 2003," in the Implementation Guide, verify that an existing user account is deprovisioned in different directory stores as configured in the Workflow application.
- **Verify that Lotus Notes users are added as 'Contacts' in the Infrastructure Directory:** Based on the steps in Chapter 3 of the Implementation guide.
- **Verify SAP users are able to log in to the SAP server without giving their credentials:** Once the appropriate SAP user account is created on the SAP server, and in the intranet Active Directory, the SAP user logs on to the SAP server. Verify that the system uses the Kerberos protocol and authenticates the user without requiring credentials.
- **Verify the Sales employee can access the Sales Contact application via the Internet using single sign on (SSO):** This scenario requires that the user has:
 - The appropriate extranet Active Directory account created by MIIS 2003.
 - Membership in the Sales group, which has permissions to access the Sales Contact application.
 - A valid user authentication certificate issued by the Issuing CA.

Verify that when users access the application from the Internet, they are authenticated and do not require to enter their logon credentials.

- **Verify employees not in the Sales group cannot access the Sales Contact application:** Ensure that the user has:
 - A valid user authentication certificate.
 - Is not a member of the Sales group in the extranet Active Directory.
 Verify user authentication fails for a user who tried to access the Sales Contact application from the Internet.
- **Verify a customer with a valid Microsoft .NET Passport account can access the Product Trial application using SSO:** For this to happen, a customer who has registered for Contoso's Product Trial application creates a .NET Passport account. Verify that with this account, the customer can access the Customer Trial application on the Contoso home page after supplying his or her .NET Passport account ID to successfully log in to the site.

For more details on the complete set of test scenarios used by the test team, see the job aid on test cases that accompanies this solution. The following sections of this guide describe the types of tests executed by the Test Team.

Documentation Tests

These tests validated that the statements, procedures, and functions documented in the prescriptive implementation guidance are accurate, unambiguous, and complete. The Implementation Guide itself is the test scenario for these tests.

Baseline Tests

These tests checked the base client/server infrastructure services. The tests verified that there were no major or critical errors in the test lab instance build for Contoso's Before State. These included very basic tests on the following services:

- Intranet domain controllers service functions
- DNS and DHCP service
- Intranet Web services
- Messaging service
- Intranet file and print service
- Certificate services infrastructure
- Extranet domain controller
- Extranet Web services
- Perimeter internet security and acceleration service for firewall, and proxy services
- SQL Server database for applications
- Customer Trial ASP.NET application and related ASP pages
- Sales Contact ASP.NET application

For more information about the test cases, see the Baseline Test Cases.xls job aid.

Functional Tests

These tests verified that the system built according to the guidance in the Implementation Guide worked as expected. These tests also verified interoperability functionality as required. These tests contained test cases for the following scenarios:

1. Establishing the platform
2. Digital Identity aggregation and provisioning with MIIS 2003:
 1. The provisioning and deprovisioning digital identity data scenario
3. UNIX workstation and SAP application integration with Active Directory using the Kerberos protocol
4. B2E Web SSO using certificate authentication
5. B2C Web SSO using Passport authentication

For more details on the complete set of test cases used by the Test Team, see the Functional Test Cases.xls job aid included in the Tools and Templates folder that downloads with this solution.

Vulnerability Assessment Tests

These test cases verified vulnerabilities identified in the Contoso Before State Scenario as described in the "Analyzing Issues and Requirements" sections of the Implementation guide. These tests were used to prove how the solution mitigates them using the technologies that comprise the I&AM solution. Most of these tests might not be reproducible in your test environment due to either time constraints on reproducing them, or such tests being out of scope of test lab environment. However, these tests are included with this solution for your reference to compare them scenarios that fit your environment.

For more information on the test cases that the Test Team used, see the Vulnerability Assessment Test Cases.xls job aid that accompanies this guide.

Test Release

The primary release criteria for the solution were linked to the severity and priority of open bugs. The following defines the release criteria for bugs the Test Team encountered while validating the solution:

- No open bugs at the Severity 3 or Priority 2 level could exist before release.
- The solution guide content was free of comments and revision marks. The leadership team addressed all open bugs and determined their impacts before release.
- All test cases in the test lab environment were successfully completed.
- The solution content was without conflicting statements.

Bug Classification

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

Table 1.1: Bug Classification

Rating	Severity Definition	Priority Definition
1	The bug causes system crash or data loss.	Must fix as soon as possible. The bug is blocking further progress.
2	The bug causes major functionality or other severe problems; product crashes in obscure cases.	Should fix soon, before product release.
3	The bug causes minor functionality problems; may affect "fit and finish."	Fix if time; somewhat trivial. May be postponed.
4	The bug contains typographical errors, unclear wording, or error messages in low visibility fields.	The bug impacts the solution quality but does not prevent release.

Testing Results

All of the test cases passed with expected results. No open bugs at the Severity 2 level or greater, or with Priority 2 or greater remained open before release. This demonstrates that the test objectives were successfully met, and that the solution demonstrates how to achieve identity and access management, using the Contoso Pharmaceuticals as the fictional example used to illustrate the solution.

Diagnostic Information

Chapters 3 through 6 of the Implementation Guide provide more detail on the methods and procedures the Test Team used to validate the solution.

Use the following chapter tips to troubleshoot issues while implementing the solution to fit the needs of your organization.

Chapter 3: Digital Identity Aggregation and Provisioning with MIIS 2003

Chapter 3 contains diagnostic information to use at various stages to trouble shoot any issues while configuring MIIS 2003.

Chapter 4: Workstation and Application Integration Using the Kerberos Protocol

The following steps are necessary to ensure a working solution:

- Before Solaris users can change their UNIX passwords, they must obtain a Kerberos TGT ticket. Use the klist and kinit command line tools to obtain the Kerberos tickets.
- While adding the SNC_LIB variable to the Environment Variables, ensure that the new variable is added to the list of "System Variables" and not "User Variables" in the same pane. Otherwise, the Kerberos authentication protocol will fail.
- For any SAP user accounts created either in Active Directory or in the SAP server, be sure to enter their names in the same case as they were entered in Active Directory. Otherwise you may experience logon issues.

Chapter 5: Business-to-Employee Web Single Sign on Using Certificate Authentication

The following steps are necessary to ensure a working solution:

- While configuring the extranet IIS Web servers to enable Hypertext Transfer Protocol, Secure (HTTPS), add all CA certificates up to the Root level on the local computer's certificate store, ensure that this is done in the appropriate location for this under the Trusted Root Certificate Authorities folder. Failing to do this will prevent IIS from authenticating any sales employees attempting to access the site with their user certificates.
- Ensure that the issuing CA regularly publishes the Certificate Revocation Lists (CRLs) that are updated on the HTTP location. Failing to do so will prevent sales employees from accessing the Sales Contact application.
- When provisioning the Sales user account in the Extranet Active Directory through Management Agents, ensure that the user object's "AltSecurityIdentities" and "UPN" attributes in Extranet Active Directory are correctly mapped to the "Subject" field in the user certificate, and "UPN" in the intranet Active Directory account.

Chapter 6: Business-to-Consumer Web Single Sign On Using Passport Authentication

The following steps are necessary to ensure a working solution:

- While setting up the .NET Passport site ID in the Passport Manager Administration utility, if the site ID does not appear after running the downloaded site ID executables, manually change the site ID number in the Passport Manager Administration utility, and then verify that it works correctly.
- During the installation of the .NET Passport Site ID executable in the Passport Manager, ensure that the Web server has connectivity to the Internet and IIS 6.0 is stopped.

More Information

More information can be found in the Planning, and Implementation guides for the Microsoft I&AM solution. The following information sources were the latest available on topics closely related to testing the solution at the time this guide was released to the public.

For more information on Microsoft .NET Passport and free sign up, see:
<http://www.passport.net/Consumer/default.asp?lc=1033>

For more information on .NET Passport Member services, see:
<http://memberservices.passport.net/default.srf>

For more information on *Passport SDK* downloads, see:
<http://msdn.microsoft.com/library/default.asp?url=/downloads/list/websrvpass.asp>

For more information on Microsoft Identity Integration Server 2003 homepage, see:
<http://www.microsoft.com/windowserver2003/technologis/directory/miis/default.mspix>

For more information on operational information focused on PKI, see:
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/win2003/pkiwire/ops/swlanog2.asp>