|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MS-ADFSPIP  Client Test Suite  User Guide | | | | |
| *Windows is built to be the most interoperable platform* | | | | |
| Description: Windows-brand_v_bL_png | **MICROSOFT CORPORATION**  ***May 20, 2014***  Send suggestions and comments about this document to intopdoc@microsoft.com.  Please include the name of the test suite with your feedback. | |  | |
| **Microsoft Confidential. ©** 2010 Microsoft Corporation. All rights reserved. These materials are confidential to and maintained as a trade secret by Microsoft Corporation. Information in these materials is restricted to Microsoft authorized recipients only. Any use, distribution or public discussion of, and any feedback to, these materials are subject to the terms of the attached license. By providing any feedback on these materials to Microsoft, you agree to the terms of that license. | | | |  |
|  | |

#### Microsoft Corporation Technical Documentation License Agreement (Standard)

**READ THIS!** THIS IS A LEGAL AGREEMENT BETWEEN MICROSOFT CORPORATION ("MICROSOFT") AND THE RECIPIENT OF THESE MATERIALS, WHETHER AN INDIVIDUAL OR AN ENTITY ("YOU"). IF YOU HAVE ACCESSED THIS AGREEMENT IN THE PROCESS OF DOWNLOADING MATERIALS ("MATERIALS") FROM A MICROSOFT WEB SITE, BY CLICKING "I ACCEPT", DOWNLOADING, USING OR PROVIDING FEEDBACK ON THE MATERIALS, YOU AGREE TO THESE TERMS. IF THIS AGREEMENT IS ATTACHED TO MATERIALS, BY ACCESSING, USING OR PROVIDING FEEDBACK ON THE ATTACHED MATERIALS, YOU AGREE TO THESE TERMS.

1. For good and valuable consideration, the receipt and sufficiency of which are acknowledged, You and Microsoft agree as follows:

(a) If You are an authorized representative of the corporation or other entity designated below ("**Company**"), and such Company has executed a Microsoft Corporation Non-Disclosure Agreement that is not limited to a specific subject matter or event ("**Microsoft NDA**"), You represent that You have authority to act on behalf of Company and agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that Company will treat the Confidential Information accordingly;

(b) If You are an individual, and have executed a Microsoft NDA, You agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that You will treat the Confidential Information accordingly; or

(c)If a Microsoft NDA has not been executed, You (if You are an individual), or Company (if You are an authorized representative of Company), as applicable, agrees: (a) to refrain from disclosing or distributing the Confidential Information to any third party for five (5) years from the date of disclosure of the Confidential Information by Microsoft to Company/You; (b) to refrain from reproducing or summarizing the Confidential Information; and (c) to take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, but no less than reasonable care, to keep confidential the Confidential Information. You/Company, however, may disclose Confidential Information in accordance with a judicial or other governmental order, provided You/Company either (i) gives Microsoft reasonable notice prior to such disclosure and to allow Microsoft a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Confidential Information shall not include any information, however designated, that: (i) is or subsequently becomes publicly available without Your/Company’s breach of any obligation owed to Microsoft; (ii) became known to You/Company prior to Microsoft’s disclosure of such information to You/Company pursuant to the terms of this Agreement; (iii) became known to You/Company from a source other than Microsoft other than by the breach of an obligation of confidentiality owed to Microsoft; or (iv) is independently developed by You/Company. For purposes of this paragraph, "Confidential Information" means nonpublic information that Microsoft designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential by Recipient. "Confidential Information" includes, without limitation, information in tangible or intangible form relating to and/or including released or unreleased Microsoft software or hardware products, the marketing or promotion of any Microsoft product, Microsoft's business policies or practices, and information received from others that Microsoft is obligated to treat as confidential.

2. You may review these Materials only (a) as a reference to assist You in planning and designing Your product, service or technology ("Product") to interface with a Microsoft Product as described in these Materials; and (b) to provide feedback on these Materials to Microsoft. All other rights are retained by Microsoft; this agreement does not give You rights under any Microsoft patents. You may not (i) duplicate any part of these Materials, (ii) remove this agreement or any notices from these Materials, or (iii) give any part of these Materials, or assign or otherwise provide Your rights under this agreement, to anyone else.

3. These Materials may contain preliminary information or inaccuracies, and may not correctly represent any associated Microsoft Product as commercially released. All Materials are provided entirely "AS IS." To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

4. If You are an entity and (a) merge into another entity or (b) a controlling ownership interest in You changes, Your right to use these Materials automatically terminates and You must destroy them.

5. You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to these Materials. However, any Feedback you voluntarily provide may be used in Microsoft Products and related specifications or other documentation (collectively, "Microsoft Offerings") which in turn may be relied upon by other third parties to develop their own Products. Accordingly, if You do give Microsoft Feedback on any version of these Materials or the Microsoft Offerings to which they apply, You agree: (a) Microsoft may freely use, reproduce, license, distribute, and otherwise commercialize Your Feedback in any Microsoft Offering; (b) You also grant third parties, without charge, only those patent rights necessary to enable other Products to use or interface with any specific parts of a Microsoft Product that incorporate Your Feedback; and (c) You will not give Microsoft any Feedback (i) that You have reason to believe is subject to any patent, copyright or other intellectual property claim or right of any third party; or (ii) subject to license terms which seek to require any Microsoft Offering incorporating or derived from such Feedback, or other Microsoft intellectual property, to be licensed to or otherwise shared with any third party.

6. Microsoft has no obligation to maintain confidentiality of any Microsoft Offering, but otherwise the confidentiality of Your Feedback, including Your identity as the source of such Feedback, is governed by Your NDA.

7. This agreement is governed by the laws of the State of Washington. Any dispute involving it must be brought in the federal or state superior courts located in King County, Washington, and You waive any defenses allowing the dispute to be litigated elsewhere. If there is litigation, the losing party must pay the other party’s reasonable attorneys’ fees, costs and other expenses. If any part of this agreement is unenforceable, it will be considered modified to the extent necessary to make it enforceable, and the remainder shall continue in effect. This agreement is the entire agreement between You and Microsoft concerning these Materials; it may be changed only by a written document signed by both You and Microsoft.

Active Directory, Microsoft, PowerShell, Visual Studio, Windows, and Windows Server are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Introduction 1](#_Toc374100960)

[Known Issues 1](#_Toc374100961)

[License Information 1](#_Toc374100962)

[Further Assistance 1](#_Toc374100963)

[Quick Start Checklist 2](#_Toc374100964)

[How Do I? 3](#_Toc374100965)

[Requirements 3](#_Toc374100966)

[Environment 3](#_Toc374100967)

[Domain Controller & Certificate Authority (DCCA) 4](#_Toc374100968)

[OAuth & Device Registration Server (ADFS) 4](#_Toc374100969)

[Windows Client Device (SUT) 5](#_Toc374100970)

[Non-Windows Client Device (SUT) 5](#_Toc374100971)

[Driver Computer (DRIVER) 5](#_Toc374100972)

[Prerequisite Software 5](#_Toc374100973)

[Network Setup 6](#_Toc374100974)

[Domain Environment 6](#_Toc374100975)

[Verify Connectivity from the Driver Computer 8](#_Toc374100976)

[Computer Setup 9](#_Toc374100977)

[Set Up a DCCA Computer 9](#_Toc374100978)

[Set Up an ADFS Computer 11](#_Toc374100979)

[Set Up a Windows-based SUT Computer 11](#_Toc374100980)

[Set Up a Driver Computer 12](#_Toc374100981)

[Installed Files and Folders 12](#_Toc374100982)

[Configuration 14](#_Toc374100983)

[Configuring Windows-based Computers 14](#_Toc374100984)

[Configure the DCCA Computer 14](#_Toc374100985)

[Configure the ADFS Computer 16](#_Toc374100986)

[Configure the Widnows-based SUT Computer 18](#_Toc374100987)

[Configure the Driver Computer 20](#_Toc374100988)

[Configuring the Test Suite 20](#_Toc374100989)

[Required Configuration Settings 20](#_Toc374100990)

[Running Test Cases 23](#_Toc374100991)

[Run All Test Cases 23](#_Toc374100992)

[Run All BVT Test Cases 23](#_Toc374100993)

[Check Test Results 24](#_Toc374100994)

[Review the Log Files 24](#_Toc374100995)

[Manage the Generation of Log Files 24](#_Toc374100996)

[Debugging Test Cases 28](#_Toc374100997)

[Troubleshooting 29](#_Toc374100998)

[Unable to set the network to Private 29](#_Toc374100999)

[Unable to Specify UPN When Joining Workplace 30](#_Toc374101000)

[Cannot Workplace Join with Build-in Administrator 30](#_Toc374101001)

[Cannot Trigger SUT to Join Workplace 30](#_Toc374101002)

Introduction

This guide provides information about how to install, configure, and run MS-ADFSPIP Test Suite and its environment. This suite of tools is designed to test the implementations of Device Registration Discovery Protocol, as specified in Microsoft document [MS-DVRD], and Device Registration Enrollment Protocol, as specified in Microsoft document [MS-DVRE].  
This guide provides information about using this test suite on the Microsoft® Windows® operating system.

This suite of tools tests only the protocol implementation behaviors that are observed on the wire. For detailed information about the design of this test suite, see MS-ADFSPIP\_ClientTestDesignSpecification.docx.

## Known Issues

For detailed information about known issues related to this test suite, see the release notes in the installation folder.

## License Information

For licensing information, see the End User License Agreement (EULA) that was provided with this test suite. The EULA is contained in the EULA.rtf file in the installation folder.

## Further Assistance

If you need further information about this test suite or assistance in troubleshooting issues related to this test suite, contact intopdoc@microsoft.com.

# Quick Start Checklist

The following checklist summarizes the steps you need to complete to get the test suite up and running. The checklist also provides references to documentation that can help you get started.

| **Check** | **Task** | **Topic** |
| --- | --- | --- |
| □ | Download the test suite for the protocol implementation | For a list of the files that the download package contains, see [Installed Files and Folders](#_Setup_of_the). |
| □ | Confirm that your test environment and computers meet the requirements of the test suite | For information about the requirements of the test suite, see [Requirements](#_Requirements). |
| □ | Install the software prerequisites | For information about software that must be installed on the computers in your test environment before the test suite is installed, see [Prerequisite Software](#_Prerequisite_Software). |
| □ | Set up a Domain Controller & Certificate Authority (DCCA) | See [Set Up a DCCA](#_Set_Up_DCCA) Computer. |
| □ | Set up an OAuth & Device Registration Server (ADFS) | See [Set Up an ADFS](#_Additional_Domain_Controller) Computer. |
| □ | Set up a Windows Client Computer (SUT) | See [Set Up a Windows-based SUT](#_Set_Up_SUT) Computer. |
| □ | Set up a Driver Computer (DRIVER) | See [Set Up a Driver Computer](#_Set_Up_DRIVER) |
| □ | Set up the network | See [Network Setup](#_Network_Setup). |
| □ | Verify the connection from the driver computer to the SUT and other computers | See [Verify Connectivity from the Driver Computer](#_Verify_Connectivity_from). |
| □ | Configure the DCCA Computer | See [Configure the DCCA](#_Install_and_configure) Computer. |
| □ | Configure the ADFS Computer | See [Configure the ADFS](#_Configure_the_DRS) Computer. |
| □ | Configure the SUT Comptuer | See [Configure the Windows-based SUT](#_Configure_the_RODC_1) Computer. |
| □ | Configure the Driver Computer | See [Configure the Driver Computer](#_Configure_the_Driver_3) . |
| □ | Configure the Test Suite settings | See [Configuring the Test Suite](#_Configuring_the_Test). |

# How Do I?

Use the following quick reference to learn how to complete common tasks.

|  |  |
| --- | --- |
| **How do I…?** | **For more information…** |
| Set up the test environment | [Network Setup](#_Network_Setup_1) and [Computer Setup](#_Computer_Setup) |
| Verify the connection from the driver computer to other computers in the test environment | [Verify Connectivity from the Driver Computer](#_Verify_Connectivity_from_1) |
| Configure the Domain Controller & Certificate Authority | See [Configure the DCCA](#_Configure_the_DCCA) Computer. |
| Configure the Device Registration Server | See [Configure the ADFS](#_Configure_the_DRS) Computer. |
| Configure the Client Computer | See [Configure the Windows-based SUT](#_Configure_the_RODC_1) Computer. |
| Configure the Driver Computer | See [Configure the Driver Computer](#_Configure_the_Driver_3). |
| Configure the Test Suite settings | See [Configuring the Test Suite](#_Configuring_the_Test). |
| Run test cases | See [Running Test Cases](#_Running_Test_Cases). |
| Debug my own test cases | See [Debugging Test Cases](#_Debugging_Test_Cases). |
| Get the results of test runs | See [Check Test Results](#_Check_Test_Results_1). |
| Troubleshoot problems | See [Troubleshooting](#_Troubleshooting). |

# Requirements

This section describes the requirements for the test environment that are used to run this test suite.

Note

The requirements in this section apply only to the Windows-based computers in the test environment. Note that the driver computer must use a Windows-based operating system.

## Environment

Run this test suite in a domain environment that contains the following computers, physical or virtual:

Note

If virtual machines with Windows are used, please make sure the Windows computers’ Security Identifiers (SIDs) are different.

* A computer set up as the domain controller and certificate authority, named DCCA, running Microsoft® Windows Server® 2012 R2, Enterprise Edition.
* A computer set up as the ADFS server (Active Directory Federation Service), named ADFS, running Microsoft® Windows Server® 2012 R2, Enterprise Edition.
* A computer set up as the application proxy, named SUT. If the device is a computer running Windows, it should be running Microsoft® Windows Server® 2012 R2, Enterprise Edition.
* A driver computer, named DRIVER, running Microsoft® Windows 8.1.

## Domain Controller & Certificate Authority (DCCA)

The minimum requirements for the DCCA are as follows.

| **Requirement** | **Description** |
| --- | --- |
| Operating system | Microsoft® Windows Server® 2012 R2, Enterprise Edition |
| Services | Active Directory Domain Services (AD DS)  Active Directory Certificate Service (AD CS) |
| Memory | 1 GB RAM |
| Disk space | 60 GB |

## Active Directory Federation Server (ADFS)

The minimum requirements for the ADFS are as follows.

| **Requirement** | **Description** |
| --- | --- |
| Operating system | Microsoft® Windows Server® 2012 R2, Enterprise Edition |
| Services | Active Directory Federation Service (AD FS) |
| Memory | 1 GB RAM |
| Disk space | 60 GB |

## Windows Web Application Proxy (SUT)

The minimum requirements for the SUT are as follows.

| **Requirement** | **Description** |
| --- | --- |
| Operating system | Microsoft® Windows Server® 2012 R2, Enterprise Edition |
| Services | Web Application Proxy |
| Memory | 1 GB RAM |
| Disk space | 60 GB |

## Non-Windows Web Application Proxy (SUT)

The minimum requirements for the SUT are as follows.

| **Requirement** | **Description** |
| --- | --- |
| Operating system | Non-Windows operating systems |
| Feature | Implement Web Application Proxy feature. |

## Driver Computer (DRIVER)

The minimum requirements for the DRIVER computer are as follows.

| **Requirement** | **Description** |
| --- | --- |
| Operating system | Microsoft® Windows 8.1 |
| Memory | 1 GB RAM |
| Disk space | 60 GB |

## Prerequisite Software

All of the following software must be installed on the driver computer *before* the test suite.

|  |
| --- |
| **Required Software that is Included with test suite** |
| Protocol Test Framework (build 1.0.2220.0 or later) |
|  |
| **Required Software that is Not Included with test suite** |
| Microsoft® Visual Studio® 2012 Ultimate, Premium, or Professional. |

# Network Setup

Run this test suite in a domain environment using either physical or virtual machines. This section describes the test environment using physical computers.

For information about configuring a virtual machine, see <http://www.microsoft.com/virtualization/en/us/solution-appliance-test.aspx>. The configuration of virtual machines for use with this test suite is out of the scope of this guide.

## Domain Environment

The domain environment requires interactions between the following computers and server roles.

* The DCCA runs an implementation of the domain controller and certificate authority. The DCCA provides the domain environment for the testing, and also the functionality to authorize certificate which is used to identify server and client in device registration process.
* The ADFS runs the active directory federation services, which is a backend server used to generate real access token.
* The SUT runs an implementation of the web application proxy, which is being tested.
* The DRIVER runs the test cases by acting as a synthetic server which responses to the requests from the proxy, which is regarded as the client, to test the proxy’s behavior.

The following figure shows the domain environment.



This following table shows the recommanded IP setting between the machine, all the computer set the static IP for IPV4 and can ping with other computer.

|  |  |
| --- | --- |
| **Computer** | **IP setting** |
| DCCA | IPv4: 192.168.1.1  DNS: 127.0.0.1 |
| ADFS | IPv4: 192.168.1.2  DNS: 192.168.1.1 |
| SUT | IPv4: 192.168.1.10  DNS: 192.168.1.1 |
| DRIVER | IPv4: 192.168.1.100  DNS: 192.168.1.1 |

## Verify Connectivity from the Driver Computer

After you install the environment, verify the connection from the driver computer to the SUT machines, and between all other computers in the test environment. The following provides a general list of steps you can use to check for connectivity between two Windows-based computers. For further information, see the administration guide for your operating system.

To check the connection from the driver computer

Note

Disable active firewalls in the test environment.

1. Click the **Start** button, and then click **Run**.
2. In the **Run** dialog box, type **cmd** and then click **OK**.
3. At the command prompt, type **ping** followed by the hostname or IP address of the SUT, and then press **Enter**. The following example checks the connection to a SUT with IP address 192.168.1.10:

> ping 192.168.1.10

1. Repeat these steps until you confirm connectivity between all computers in the test environment.

Do not proceed with the configuration of the test suite until connectivity is confirmed. Any issues with network connectivity must be resolved before you configure the test suite.

# Computer Setup

This section explains how to set up the computers for the test environment.

Note

All values mentioned in below sections are recommend name, if you use other names you can update them to [PTF config](#_Configuring_the_Test)

## Set Up a DCCA Computer

This section provides information about how to set up a domain controller & certificate authority for use with this test suite.

To set up a Windows-based DCCA:

1. Install **Active Directory Domain Services** and promote this server to a domain controller. Set the name of the root domain to **contoso.com**, and set administrator password to **Password01!**
2. Install **Active Directory Certificate Services** with role service **Certificate Authority**.

## Set Up an ADFS Computer

This section provides information about how to set up the OAuthe and device registration server for use with this test suite.

To set up a Windows-based ADFS:

1. Install **Active Directory Federation Services.**

## Set Up a Windows-based SUT Computer

This section provides information about how to set up a client computer (SUT) for use with this test suite.

To set up a Windows-based Client

1. Install **MS-ADFSPIP-TestSuite-ClientEP.msi** with option **Install and configure Windows System Under Test (SUT).**

## Set Up a Driver Computer

This section describes how to set up the driver computer.

Important

Microsoft Visual Studio 2012 and Protocol Test Framework must be installed on the driver computer before you run the test suite installer.

To set up the driver computer:

1. Install **MS-ADFSPIP-TestSuite-ClientEP.msi** with option **Install Test Suite on Driver Computer**.

## Installed Files and Folders

The installation process adds the following folders and files to the driver computer at C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\TestSuite\<version#>\.

Note

This path may vary based on your installation location.

The <*version#>* placeholder indicates the installed build of the test suite.

| **File or Folder** | **Description** |
| --- | --- |
| Batch | Command files you can use to run individual test cases or all test cases. |
| Bin | Test suite binaries and configuration files. |
| Docs | **[MS-ADFSPIP].pdf** – The version of the technical document that this test suite is based on.  **MS-ADFSPIP\_ClientUserGuide.docx** – A user guide that explains how to install and configure computers to run test cases.  **MS-ADFSPIP\_ClientTestDesignSpecification.docx** – An overview document containing conceptual information about a protocol including probable use, relationships to other protocols, message flow, state diagrams, a short list of properties, and a test approach describing justification and adapter approach.  Note  The driver computer should include Microsoft Office or other programs that can open and display these documents. If it does not, you can copy these documents to a computer equipped with applications that can. |
| Scripts | Scripts that are used to set up and configure the computers. |
| Source | Test suite source code. |
| EULA.rtf | The End User License Agreement. |

# Configuration

This section explains how to configure the test environment.

## Configuring Windows-based Computers

This section explains how to configure computers for a Windows-based test environment.

### Configure the DCCA Computer

This section provides a general list of steps that you can use to configure DCCA in a Windows-based test environment.

To configure the DCCA:

1. Log on to the DCCA computer as **domain Administrator**.
2. Turn off **Windows Firewall.**
3. Disable **DCP** and **AIA** on **Certificate Authority**.
4. Modify "**Web Server**" certificate template to allow "**Domain Computers**" group to issue it.
5. In **DNS Manager**, add a **new host** named **adfs** with IP address pointing to the driver, i.e. **192.168.1.100**; add a **new host** named **webapp** pointing also to the driver; add an **alias** named **enterpriseregistration** pointing to **adfs.contoso.com**.
6. Create a user, e.g. **adfsuser**, to be used for ADFS.

### Configure the ADFS Computer

This section provides a general list of steps that you can use to configure the ADFS in a Windows-based test environment.

To configure the ADFS

1. Join the computer to domain **contoso.com.**
2. Log on to the ADFS computer as **domain administrator.**
3. Turn off **Windows Firewall.**
4. Request a new **Web Server certificate**; set the **subject name** to be of type **Common name** and value **adfs.contoso.com**; add an **alternative name** with type **DNS** and value **adfs.contoso.com**; add another **alternative name** with type **DNS** and value **enterpriseregistration.contoso.com**; make private key exportable.
5. Configure AD FS to use **Farm mode**, use "**adfs.contoso.com**" as name, use "**adfsuser**" to host service, and select certificate from Step 4 as service certificate.
6. Enable **device registration service**.
7. Export the **certificate** in Step 4 with **private key**.\
8. Add “fed1” relying party trust.

### Configure the Widnows-based SUT Computer

This section provides a general list of steps that you can use to configure the SUT computer in a Windows-based test environment. **Do not initially join the SUT computer to the domain. And do not use the build-in Administrator account.** (See [Troubleshooting](#_Troubleshooting) if you encounter problems)

To configure the Windows-based SUT:

1. Turn off **Windows Firewall.**
2. Make sure the **Network Location** is **Private**, and turn off **password protected sharing.**
3. Change **PowerShell execution policy** to **Unrestricted.**
4. Enable **PSRemoting.**
5. Import **ADFS certificate**.
6. Request an **Web Server Certificate** with **subject name** set to **webapp.contoso.com**.
7. Create a folder, say C:\Temp, and share the folder with **Everyone** with **Read/Write** permission.
8. Copy all the scripts from C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint \<version#>\Scripts to C:\Temp. Run **RemoteExecutionListener.ps1.**
9. Add RemoteExecutionListener.ps1 into start-up run registry section.

### Configure the Driver Computer

This section provides a general list of steps that you can use to configure the driver computer in a Windows-based test environment.

To configure the driver computer

1. Join the computer to domain **contoso.com**.
2. Log on to the driver computer as **domain administrator.**
3. Disable **Windows Firewall**.
4. Change **PowerShell execution policy** to **Unrestricted**.
5. Import **ADFS certificate**.
6. Set local DNS record, pointing ADFS and WebApp to the proxy’s IP.

## Configuring the Test Suite

This test suite is installed with default configuration settings. You may need to change these settings if you use a customized test environment or if you customize your test runs.

You can configure the test suite for various purposes including, for example, to:

* Define the settings of the test environment, including computer names and IP addresses.
* Define the basic options used in the test suite, for example, the protocol version or the version of the target operating system.
* Define the folders and formats used for output from test runs.
* Define scripts to run before and after each test run.
* Define the case which will break test enviroment
* Set time limits on discrete test tasks and for test runs.

To change configuration settings, edit the MS-ADFSPIP\_ClientTestSuite.deployment.ptfconfig file.

### Required Configuration Settings

The following table describes the configuration properties used in the test suite configuration file and their values. These properties are required.

| **Property** | **Description** |
| --- | --- |
| **Common.TestDeployment** | The bool value incidating whether testing deployment senerio or not.  The default value is “True”. |
| **Common.SUT.IPAddress** | The IPv4 address of the SUT computer.  The default value is "192.168.1.10”. |
| **Common.SUT.** **MaxDelayBetweenOperationsInSeconds** | The maximum delay in seconds between two successive operations, for example, sending device registration discovery request and sending OAuth request, on the client device.  This value should be less than 60 seconds, unless the client implementation has very big performance issue.  The default value is "60". |
| **Common.SUT.Share** | The shared folder path on the client.  The default value is “\\192.168.1.10\temp”. |
| **Common.SUT.IsWindows** | The bool value indicating whether the client runs Windows operating system.  The default value is “True". |
| **Common.OAuthService1.Endpoint** | The 1st OAuth service endpoint.  The default value is “https://adfs.contoso.com/adfs/oauth2/authorize”. |
| **Common.OAuthService1.Identifier** | The 1st OAuth service identifier.  The default value is “http://adfs.contoso.com/adfs/services/trust”. |
| **Common.OAuthService2.Endpoint** | The 2nd OAuth service endpoint.  The default value is “https://adfs.contoso.com/adfs/oauth2/token”. |
| **Common.OAuthService2.Identifier** | The 2nd OAuth service identifier.  The default value is “http://adfs.account.com/adfs/services/trust”. |
| **Common.DiscoveryService.DNSName** | The discovery service endpoint.  The default value is “enterpriseregistration.contoso.com”. |
| **Common.EnrollmentService.ResourceId** | The enrollment service resource Id.  The default value is “urn:ms-drs:adfs.contoso.com”. |
| **Common.PassiveService.Endpoint** | The passive service endpoint.  The default value is "https://adfs.contoso.com/adfs/ls". |
| **Common.TLSServerCertificate.FilePath** | The local copy of the ADFS server certificate with private key.  The default value is “c:\\Adfs.pfx”. |
| **Common.TLSServerCertificate.Password** | The password for the .pfx certificate.  The default value is “123”. |
| **Common.User.Name** | The user name used to registration.  The default value is “TestUser”. |
| **Common.User.Domain** | The registration user domain.  The default value is “contoso.com”. |
| **Common.User.Password** | The password for the registration user.  The default value is “Password01!”. |
| **Common.DRS.Ip** | The IPv4 address of the real DRS in backend.  The default value is “192.168.1.2”. |
| **Common.TLSHostName** | The TLS host name of the real DRS.  The default value is “enterpriseregistration.contoso.com”. |

# Running Test Cases

This test suite includes command files that you can use to complete some basic test cases. Each test case verifies the protocol implementation based on a given scenario.

You can find and run these test cases in the following directory:

C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Batch

You can run these command files at the command prompt, or by selecting and clicking one or more of the files from the directory.

Note

* Check the values in MS-ADFSPIP\_ClientTestSuite.deployment.ptfconfig under C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Bin are correct

## Run All Test Cases

Use the steps below to run all test cases.

To run all test cases

* From the desktop of the driver computer, double-click the **Run MS-ADFSPIP Client\_AllTestCases** shortcut. This shortcut is created during the installation process.

Alternatively, go to C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Batch, and double-click the **RunAllTestCases.cmd** file.

## Run All BVT Test Cases

Use the steps below to run all BVT test cases

To run all test cases

* From the desktop of the driver computer, double-click the **Run MS-ADFSPIP Client\_BVTTestCases** shortcut. This shortcut is created during the installation process.

Alternatively, go to C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Batch, and double-click the **RunBVTTestCases.cmd** file.

## Check Test Results

The handling of test results involves both the review of log files and the management of their generation. This section describes those topics.

### Review the Log Files

You can find the log files in the "TestResults" directory, a subdirectory of the test suite installation directory. The log files that contain test suite results use a \*.trx file name, in which the asterisk ("\*") character represents the user name, the protocol name, or both.

Additional log files are used for generating requirement coverage reports and diagnosing test issues. Their settings can be found in the \*.ptfconfig or \*.deployment.ptfconfig files. The file names, corresponding paths, and formats can be set in the Sinks node of the configuration file.

The following instruction provides an example of how to cause log entries for the "Debug" logging sink not to be written into the MS-ADFSPIP\_Log.txt file in the current directory:

<File id="Debug" directory=".\" file="MS-ADFSPIP\_Log.txt" format="text"/>

### Manage the Generation of Log Files

The log files contain a range of information including, but not limited to, the following:

* Test computer client and server names
* Internet Protocol (IP) addresses
* User names and passwords
* Domain names and test domain names
* DHCP and DNS servers, pipes, and mail slots
* Security Identifiers (SIDs)
* Globally unique identifiers (GUIDs) of domain controllers
* Port numbers
* User account settings associated with Windows Active Directory
* Name of sites which are present or nonexistent.

None of this information is sent to Microsoft.

If you do not need the log files for debugging, you can delete them. You can also control the generation of all log files for the test suite, except for \*.trx files.

The following describes how to stop the generation of log files using the file name extensions of .txt and .xml. This process should be followed *before* you run test cases in Visual Studio.

To prevent the generation of .txt and .xml type log files

Note

This procedure assumes that the test suite was installed at the root directory **C:**. MS-ADFSPIP represents the protocol name.

1. Open the MS-ADFSPIP\_ClientTestSuite.ptfconfig file. You can find this configuration file at the path C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Source\Client\TestCode\TestSuite. Or, if you use batch files to run your test cases, you can find this file at C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Bin.
2. Locate the Sinks node and comment out all the entries.
3. Locate the Profile node and comment out all the entries.
4. Locate the Profile node and add the following entries:

<Rule kind="CheckSucceeded" sink="Console" delete="false" />

<Rule kind="Checkpoint" sink="Console" delete="false"/>

<Rule kind="Comment" sink="Console" delete="false"/>

<Rule kind="Debug" sink="Console" delete="false" />

<!-- Show for XML log -->

<Rule kind="CheckSucceeded" sink="XMLLog" delete="false"/>

<Rule kind="Comment" sink="XMLLog" delete="false"/>

<Rule kind="Checkpoint" sink="XMLLog" delete="false"/>

<Rule kind="Debug" sink="XMLLog" delete="false"/>

<Rule kind="EnterMethod" sink="XMLLog" delete="false"/>

<Rule kind="ExitMethod" sink="XMLLog" delete="false" />

<Rule kind="CheckSucceeded" sink="BeaconLog" delete="false"/>

<Rule kind="Checkpoint" sink="BeaconLog" delete="false"/>

<Rule kind="Comment" sink="BeaconLog" delete="false"/>

<Rule kind="Debug" sink="BeaconLog" delete="false" />

<Rule kind="CheckSucceeded" sink="Debug" delete="false"/>

<Rule kind="Checkpoint" sink="Debug" delete="false"/>

<Rule kind="Comment" sink="Debug" delete="false"/>

<Rule kind="Debug" sink="Debug" delete="false" />

The following gives an example of an MS-ADFSPIP\_ClientTestSuite.ptfconfig in which the Sinks and Profile nodes are commented out.

<Sinks>

<File id="Debug" directory=".\" file="MS-ADFSPIP\_Log.txt" format="text"/>

<File id="XMLLog" directory=".\" file="MS-ADFSPIP\_Log.xml" format="xml"/>

<Console id="Console" />

<Sink id="BeaconLog" type="Microsoft.Protocols.TestTools.Logging.BeaconLogSink" assembly="Microsoft.Protocols.TestTools"/>

</Sinks>

<Profiles>

<Profile name="Verbose" extends="Error">

<!-- Show on Console -->

<Rule kind="CheckSucceeded" sink="Console" delete="false" />

<Rule kind="Checkpoint" sink="Console" delete="false"/>

<Rule kind="Comment" sink="Console" delete="false"/>

<Rule kind="Debug" sink="Console" delete="false" />

<!-- Show for XML log -->

<Rule kind="CheckSucceeded" sink="XMLLog" delete="false"/>

<Rule kind="Comment" sink="XMLLog" delete="false"/>

<Rule kind="Checkpoint" sink="XMLLog" delete="false"/>

<Rule kind="Debug" sink="XMLLog" delete="false"/>

<Rule kind="EnterMethod" sink="XMLLog" delete="false"/>

<Rule kind="ExitMethod" sink="XMLLog" delete="false" />

<Rule kind="CheckSucceeded" sink="BeaconLog" delete="false"/>

<Rule kind="Checkpoint" sink="BeaconLog" delete="false"/>

<Rule kind="Comment" sink="BeaconLog" delete="false"/>

<Rule kind="Debug" sink="BeaconLog" delete="false" />

<Rule kind="CheckSucceeded" sink="Debug" delete="false"/>

<Rule kind="Checkpoint" sink="Debug" delete="false"/>

<Rule kind="Comment" sink="Debug" delete="false"/>

<Rule kind="Debug" sink="Debug" delete="false" />

</Profile>

</Profiles>

For further information about logging in the Protocol Test Framework (PTF), see the *PTF User Guide* in the PTF installation directory.

# Debugging Test Cases

You can use the Visual Studio solution (.sln) file included with this test suite to debug additional test cases that you create for your protocol implementation.

Note

* Check the values in MS-ADFSPIP\_ClientTestSuite.deployment.ptfconfig under C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Source\Client\TestCode\TestSuite are correct

To debug a test case

1. On the driver computer, use Microsoft® Visual Studio® to open the following solution file:

C:\MicrosoftProtocolTests\MS-ADFSPIP\Client-Endpoint\<version#>\Source\Client\TestCode\MS-ADFSPIP\_Client.sln

1. In Visual Studio, in the Solution Explorer window, right-click the **Solution** **‘MS-ADFSPIP\_Client’**, and select **Build Solution**.
2. In the Solution Items folder, click **MS-ADFSPIP\_Client.vsmdi**, and then select the names of the test scenarios that you want to debug.

# Troubleshooting

This section describes how to troubleshoot common issues in running test cases.

## Unable to set the network to Private

|  |  |
| --- | --- |
| PROBLEM | The Network Location is set to Public and unable to change to Private. |
| CAUSE | The Network Location feature provides an easy way to customize your firewall settings based on whether you trust or don’t trust the computers around you. There are three Network Location types - Private, Public and Domain. If your computer is a member of the domain then you won’t be able to change the Network Location type. If your computer is standalone or part of the workgroup, then you can choose what type of network location do you want - Public or Private. Private means that you are a member of the trusted network and you can lower your network security a little bit. Public means that you have no trust for the network outside, and you should not let your guard down.  The network location is per connection/network card. Every time a new connection is added - the dialog will appear, asking you to choose the network location type. However, there is no direct way to change the network location once it is set at the first time. We can only use PowerShell script to change it.  Setting the correct network location type is very important for Windows PowerShell Remoting. You cannot enable Windows PowerShell Remoting on your machine if your connections are set to Public. It means you won’t be able to connect to this machine using Windows PowerShell Remoting. |
| RESOLUTION | Try to run the following PowerShell script:  # Skip network location setting for pre-Vista operating systems  if([environment]::OSVersion.version.Major -lt 6) { return }   # Skip network location setting if local machine is joined to a domain.  if(1,3,4,5 -contains (Get-WmiObject win32\_computersystem).DomainRole) { return }   # Get network connections  $networkListManager = [Activator]::CreateInstance([Type]::GetTypeFromCLSID([Guid]"{DCB00C01-570F-4A9B-8D69-199FDBA5723B}"))  $connections = $networkListManager.GetNetworkConnections()   # Set network location to Private for all networks  $connections | % {$\_.GetNetwork().SetCategory(1)} |

## Unable to Specify UPN When Joining Workplace

|  |  |
| --- | --- |
| PROBLEM | When performing Workplace Join, there is no prompt shown on UI asking for user account or password information. |
| CAUSE | It is probably because the computer has joined domain. If the computer has joined domain, Windows use WIA to retrieve user credential information, so no prompt will be shown. |
| RESOLUTION | If you want to use customized account information, quit the computer from domain, and logon with local account. |

## Cannot Workplace Join with Build-in Administrator

|  |  |
| --- | --- |
| PROBLEM | When log on user is the build-in Administrator account, Workplace Join failed after receiving discovery result. |
| CAUSE | It is by design that build-in Administrator cannot use Workplace Join. |
| RESOLUTION | Log on with other accounts. |

## Cannot Trigger SUT to Join Workplace

|  |  |
| --- | --- |
| PROBLEM | The scripts to trigger Windows-based SUT to join workplace do not work properly. |
| CAUSE | The scripts to trigger a Windows-based SUT to join workplace are done by sending keystokes to simulate the actual Workplace Join operations.  Many uncertain facts will effect this kind of UI automation, such as whether the Windows is activated, or if there is process interrupt the automation. |
| RESOLUTION | Make sure the automation scripts are running on a clean system, and no other user processes are running except the listener script.  Check the Windows UI, if there are changes in UI related to Workplace Join, the scripts will fail. Modify the scripts to make sure the keystoke sequence matches the actual UI operations. |