# Protocol Scenarios

MS-ADFSPIP is used for protecting AD FS server and supporting pre-authentication when user access web resource inside company network. There are 4 roles in this system: AD FS Server, Proxy, and Web Application server. These 3 are inside a company network. There is a client outside the company network, used by user to access Web Application server inside company network. There are 3 scenarios involves different roles of this protocol:

## Proxy deployment

This scenario is used when a Proxy is registered to AD FS Server and retrieve configuration before it can process requests from user.

Call sequence:

1. Proxy establish trust relationship with AD FS Server by sending a certificate
2. Proxy get AD FS Server configuration
3. Proxy get and update web application store data

## Manage web applications

This scenario is used to describe how a Proxy admin tool can check, add, and delete web application publish information. There is no complex sequence. Proxy admin tool can choose any of below operations after the TLS connection to AD FS server is established

1. Admin tool adds a new record into store
2. Admin tool retrieves all records
3. Admin tool deletes a record

## Pre-authenticate users

This scenario is used when user access web application via Proxy, Proxy should request user to pre-authenticate

Call sequence:

1. User from client machine sends http request to Proxy to access a web application resource
2. Proxy verifies the request is not pre-authenticated so rely a HTTP 307 message to client to redirect it to AD FS Server
3. User authenticates with AD FS Server
4. STS verifies the request is from a valid Proxy and then issue security token to user

## Proxy Renew Trust

This scenario is used when Proxy restarts or current certificate will expire, Proxy sends new certificate to renew the trust relationship with AD FS Server

Call sequence:

1. Proxy sends both old certificate and new certificate to AD FS Server to renew trust relationship
2. AD FS Server sends response to Proxy

# Test Scope and requirements

Test suite will test whether Proxy implementation can finish scenarios in section 1.

For Windows implementation, choose Proxy powershell APIs.

# Test Approach

Traditional test case. Test suite will play AD FS Server, Web Application server, and Client machine roles.

# Test Scenarios

|  |  |
| --- | --- |
| Scenario Name | ProxyDeployment |
| Covered messages | Proxy/EstablishTrust  Proxy/WebApplicationProxy/Trust  Proxy/GetConfiguration  Proxy/WebApplicationProxy/Store  Proxy/WebApplicationProxy/Store/ |
| Scenario steps | * Proxy uses “Proxy/EstablishTrust” message to establish a new relationship with AD FS Server * Proxy uses “Proxy/WebApplicationProxy/Trust” message to create a trust identifier for Proxy * Proxy uses “Proxy/GetConfiguration” message to retrieve AD FS Server configuration * Proxy uses “Proxy/WebApplicationProxy/Store” message to get current version of data store * Proxy uses “Proxy/WebApplicationProxy/Store/” message to add a new record into data store |

|  |  |
| --- | --- |
| Scenario Name | SearchWebApplication |
| Covered messages | Proxy/RelyingPartyTrusts/ |
| Scenario steps | * IT Admin tool uses “Proxy/RelyingPartyTrusts/” message to find out all published web applications |

|  |  |
| --- | --- |
| Scenario Name | AddWebApplication |
| Covered messages | Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings |
| Scenario steps | * IT Admin tool uses “Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings” message to publish a web application |

|  |  |
| --- | --- |
| Scenario Name | DeleteWebApplication |
| Covered messages | Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings |
| Scenario steps | * IT Admin tool uses “Proxy/RelyingPartyTrusts/” message to delete a published web application |

|  |  |
| --- | --- |
| Scenario Name | UserAccessViaProxy |
| Covered messages | Pre-authentication message |
| Scenario steps | * User from client machine send a HTTP GET request to Proxy but actually to access a published web application * Proxy verifies there is one published web application matches user request, so it responses a HTTP 307 formated as Pre-authentication message |

|  |  |
| --- | --- |
| Scenario Name | ProxyRenewTrust |
| Covered messages | Proxy/RenewTrust |
| Scenario steps | * Proxy uses “Proxy/RenewTrust” message to renew the certificate with AD FS Server * AD FS Server sends back the response |

# Test Cases

## BVT

### Deployment\_InitialStore\_Success

|  |  |
| --- | --- |
| Test Case Name | Deployment\_InitialStore\_Success |
| Description | Test Proxy can successfully complete the deployment and get required configuration before start running |
| Priority | 0 |
| Test Steps | **Trigger Proxy start deployment**  **Proxy tries to establish trust with Driver**  **Driver returns HTTP 200 to acknowledge trust is established**  **Proxy tries to get AD FS configuration**  **Driver verifies Proxy is using the trust certificate and returns configuration data**  **Proxy tries to get store version**  **Driver verifies Proxy is using the trust certificate and returns version 1**  **Proxy tries to get version 1 store data**  **Driver verifies Proxy is using the trust certificate and returns data**  **Verifies Proxy starts running** |

### PublishApplication\_Success

|  |  |
| --- | --- |
| Test Case Name | PublishApplication\_Success |
| Description | Test Proxy can successfully get all published web applications and publish new web application. |
| Priority | 0 |
| Test Steps | **Trigger proxy client to add a new web application.**  **Proxy client tries to retrieve all published web applications.**  **Driver verifies that the client request is valid using the trusted certificate, and returns a list of relying party trusts.**  **Proxy client tries to create a new set of publishing settings on a relying party trust.**  **Driver verifies that the request is valid and using the trusted certificate, then returns HTTP 200.**  **Driver verifies the application is successfully published on the proxy.** |

### RemoveApplication\_Success

|  |  |
| --- | --- |
| Test Case Name | RemoveApplication\_Success |
| Description | Test Proxy can successfully remove a published web applications. |
| Priority | 0 |
| Test Steps | **Trigger the proxy client to remove a published web application.**  **Proxy tries to remove the published web application.**  **Driver verifies that the request is valid and using the trusted certificate, then returns HTTP 200.**  **Driver verifies the application is successfully removed from the proxy.** |

### PreAuthentication\_WorkplaceJoined\_Federation\_AsProxy\_Success

|  |  |
| --- | --- |
| Test Case Name | PreAuthentication\_WorkplaceJoined\_Federation\_AsProxy\_Success |
| Description | Client can successfully access web application via proxy with pre-authentication. |
| Priority | 0 |
| Test Steps | **Trigger the proxy to redeploy web application proxy role.**  **Trigger the proxy to publish a web application.**  **Driver sends web access request to the proxy.**  **Driver verifies proxy can successfully perform pre-authentication and message forwarding.** |

### RenewTrust\_Success

|  |  |
| --- | --- |
| Test Case Name | RenewTrust\_Success |
| Description | Proxy can successfully renew trust with the server. |
| Priority | 0 |
| Test Steps | **Trigger the proxy to reinstall web application proxy role after deployment.**  **Driver waiting for renew trust request.**  **Driver verifies that the renew request is valid.**  **Driver verifies proxy has successfully renewed trust.** |