

# Report Server & ASP.NET 集成ADFS

我们报表门户以及Report Server ADFS集成方案

## 分步指南

一共分为两步：

1. Report Server 和ADFS集成
2. 报表门户和ADFS集成

## 一、Report Server 和 ADFS集成

官方参考文档：<https://docs.microsoft.com/zh-cn/power-bi/report-server/connect-adfs-wap-report-server>

- 实际上Report Server 集成ADFS是为了解决外网的访问，适用于外网环境。
- 若需要搭建在内网环境，一共两种方案。

第一种方案：则需要内网有两台DNS服务器。

第二种方案：若内网没有两台DNS服务器，则需要每个用户电脑的host文件中添加DNS记录，将ADFS的DNS指向代理服务器ip（如：adfs.contosolab.com wap的ip）

注意配置项：

### 1.服务器域名

配置如下：

1. 一台代理服务器，服务器必须加域，并且和ADFS服务器同一个域下。安装Web 应用程序代理。
2. 为代理服务器配置公用DNS，指向代理服务器IP（<https://reports.contosolab.com>）。（此DNS将作为Report Server门户访问地址）
3. 为 AD FS 服务器配置公用 DNS 记录，指向代理服务器IP。（此DNS名称需要和ADFS内部的DNS名称一致）

配置白话解释：

- 实际是为代理服务器配置两个公共的DNS。公共的DNS为外网的DNS。
- 内网环境集成Report Server集成ADFS，则需要两台DNS服务器，

DNS1服务器配置为：为ADFS配置DNS（[adfs.contosolab.com](https://adfs.contosolab.com)）以指向ADFS的IP（若公司已有ADFS环境，无须重复配置）

DNS1服务器配置为：为WAP配置DNS（[reports.contosolab.com](https://reports.contosolab.com)）以指向WAP的IP

DNS2服务器配置为：为ADFS配置DNS（[adfs.contosolab.com](https://adfs.contosolab.com)）以指向WAP的IP（若没有内网没有两台DNS服务器，通过修改每个用户电脑的host文件，添加dns记录，将ADFS的DNS指向WAP的IP）

- 外网环境Report Server集成ADFS，则需要配置公共的DNS指向对应公共的IP

### 2.SPN配置参考

文档如下：（文档线上浏览有BUG，请下载查看）

[SPN配置文档.docx](#)

其他内容请参考官方链接

## 二、报表门户和ADFS集成

### 1.在ADFS配置配置报表门户的信赖方信任

官方文档：<https://docs.microsoft.com/zh-cn/aspnet/core/security/authentication/ws-federation?view=aspnetcore-6.0>

参考文档：[DIP 集成ADFS.docx](#)

配置完成后保存以下信息，在下面会用到

- ADFS令牌签名证书指纹
- 信赖方信任标识符

组织 终结点 代理终结点 注释 高级  
监视 标识符 加密 签名 已接受的声明

指定此信赖方信任的显示名称和标识符。

显示名称(S):  
bIP

信赖方标识符(I):  
添加(A)

示例:  
https://fs.contoso.com/adfs/services/trust

信赖方标识符(I):  
https://localhost:43331 删除(R)

确定 取消 应用(A)

## 2. 报表门户启用WS 联合身份验证

### 1. .NET FARMWORK版本

参考文档: <http://www.wjshs.net/hudun-p-5919630.html>

- 在报表门户中的web.config添加以下配置: ADFS授权地址: <https://<adfs地址>/adfs/ls> 、 <https://<adfs地址>/adfs/services/trust>

```
</modules>
</system.webServer>
<system.identityModel>
  <identityConfiguration>
    <audienceUri>
      <add value="http://localhost:11349/" />
    </audienceUri>
    <securityTokenHandlers>
      <add type="System.IdentityModel.Services.Tokens.MachineKeySessionSecurityTokenHandler, System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
      <remove type="System.IdentityModel.Tokens.SessionSecurityTokenHandler, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    </securityTokenHandlers>
    <certificateValidation certificateValidationMode="None" />
    <issuerNameRegistry type="System.IdentityModel.Tokens.ValidatingIssuerNameRegistry, System.IdentityModel.Tokens.ValidatingIssuerNameRegistry">
      <authority name="https://adfs.fisksoft.com/adfs/services/trust">
        <keys>
          <add thumbprint="875 [redacted] "fd" />
        </keys>
        <validIssuers>
          <add name="https://adfs.fisksoft.com/adfs/services/trust" />
        </validIssuers>
      </authority>
    </issuerNameRegistry>
  </identityConfiguration>
</system.identityModel>
<system.identityModel.services>
  <federationConfiguration>
    <cookieHandler requiresSsl="false" />
    <wsFederation passiveRedirectEnabled="true" issuer="https://adfs.fisksoft.com/adfs/ls/" realm="http://localhost:11349/" requireHttps="false" />
  </federationConfiguration>
</system.identityModel.services>
</configuration>
```

- 在代码中可以通过 `HttpContext.Current.User.Identity.Name` 获取当前登录用户

### 2. .NET Core版本

官方文档: <https://docs.microsoft.com/zh-cn/aspnet/core/security/authentication/ws-federation?view=aspnetcore-6.0>

