# SharePoint 2013部署ADFS验证

本文基于KB <https://technet.microsoft.com/zh-cn/library/hh305235.aspx> 补充了ADFS配置部分，标出了需要注意的点

本文中的过程介绍如何配置 AD FS 以将其用作 SharePoint 2013 Web 应用程序的身份提供程序安全令牌服务 (IP-STS)。在此配置中，AD FS 颁发由声明组成的基于 SAML 的安全令牌，以便客户端计算机可访问使用基于声明的身份验证的 Web 应用程序。您可以使用备用身份提供程序来替代 AD FS，但该提供程序必须支持 WS 联合身份验证标准。

有关为什么要使用基于 SAML 的身份验证的信息，请参阅[在 SharePoint 2013 中规划用户身份验证方法](https://technet.microsoft.com/zh-cn/library/cc262350.aspx)。

您可将 AD FS 与 Windows Server 2012、Windows Server 2008 或 Windows Server 2008 R2 操作系统一起使用，构建一个联合身份管理解决方案，从而将分布式标识、身份验证和授权服务跨过组织和平台边界扩展到基于 Web 的应用程序。通过部署 AD FS，可将组织的现有身份管理功能扩展到 Internet。

有关在标准化的测试实验室中配置的这些过程的版本，请参阅[测试实验室指南：演示在 SharePoint Server 2013 中使用基于 SAML 的声明身份验证](https://technet.microsoft.com/zh-cn/library/jj219641.aspx)。

**开始之前**

开始此操作之前，您应熟悉下列文章中的概念：

* [在 SharePoint 2013 中规划用户身份验证方法](https://technet.microsoft.com/zh-cn/library/cc262350.aspx)

|  |
| --- |
| **注意注意：** |
| 因为 SharePoint 2013 在 Internet Information Services (IIS) 中作为网站运行，所以管理员和用户依赖于浏览器提供的辅助功能。SharePoint 2013 支持受支持的浏览器的辅助功能。有关详细信息，请参阅以下资源：   * [规划浏览器支持](http://go.microsoft.com/fwlink/p/?LinkId=246502) * [SharePoint 2013 的辅助功能](https://technet.microsoft.com/zh-cn/library/jj219681.aspx) * [SharePoint 2013 中的辅助功能](http://go.microsoft.com/fwlink/p/?LinkId=246501) * [键盘快捷方式](http://go.microsoft.com/fwlink/p/?LinkID=246504) * [触控](http://go.microsoft.com/fwlink/p/?LinkID=246506) |

**过程概述**

此配置包含必须按顺序执行的以下阶段：

* [阶段 1：安装和配置 AD FS 服务器](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#Phase1)
* [阶段 2：使用 Web 应用程序将 AD FS 配置为信赖方](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#Phase2)
* [阶段 3：将 SharePoint 2013 配置为将 AD FS 视为受信任的身份提供程序](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#Phase3)
* [阶段 4：将 Web 应用程序配置为将基于声明的身份验证和 AD FS 用作受信任的身份提供程序](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#Phase4)

在每个阶段，也必须按顺序执行一系列过程。

**阶段 1：安装和配置 AD FS 服务器**

此阶段包含以下过程：

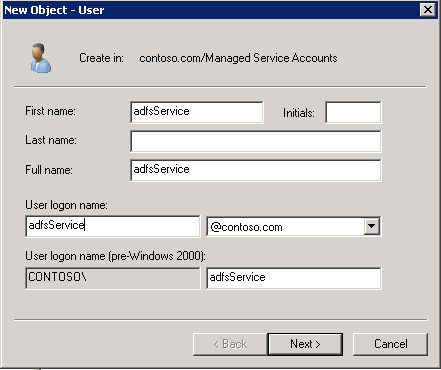
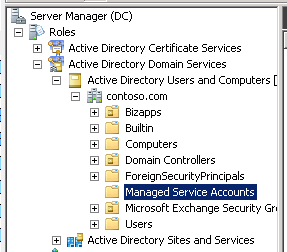
1. 获取域管理员账号
2. 为AD FS准备服务账号
3. 为AD FS准备证书
4. 设置服务器IP地址
5. 配置DNS条目
6. 安装AD FS
7. 配置AD FS

**获取域管理员账号**

首先需要获取的是 AD FS 服务运行所在的 Active Directory 域管理员帐户。对于测试环境，我们将使用默认的 contoso\administrator 帐户。在生产环境中，不建议使用默认的管理员帐户。根据您的公司策略，请求和接收域管理员帐户可能需要一些时间，因此务必要提前完成这一工作。

### 为AD FS准备服务账号

在DC中，Active Directory Domain Services->域->Managed Service Accounts中，新建服务用户账号



在DC或者任意其他机器上（需要以域管理员账号）打开命令行，执行以下命令为新建的账号配置SPN

setspn -A host/fs.contoso.com CONTOSO\adfsService

adfs.contoso.com请使用后续 为AD FS服务准备的URL，此URL不能跟AD FS的FQDN相同。

此URL后续会用于申请证书。

账号为刚刚生成的服务账号

setspn -A HTTP/adfshost.contoso.com CONTOSO\adfsService

setspn -A HTTP/adfshost CONTOSO\adfsService

执行setspn -L CONTOSO\adfsService 查看是否添加成功

在AD FS服务器上，将此账号加入到本地管理员

**为AD FS准备证书**

如要成功设置 AD FS，您需要做的第二件事是为服务器身份验证获取 SSL SAN 证书。在生产环境中要使用一个公开可信的证书。

您可以从许多商业 CA 那里购买证书。您可以在该网页上找到 Microsoft 信任的 CA：<http://support.microsoft.com/kb/931125>。另一个选择是从企业 CA 获取证书。

如要购买证书，您需要访问 CA 的网站，遵循网站上的说明。每个 CA 都有不同的证书购买流程。

AD FS 证书需要是具有以下值的 SAN 证书：

<AD FS service name>.<domain>

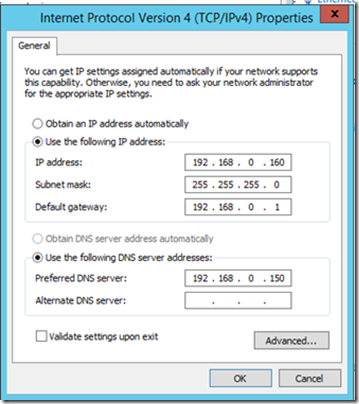
例如：

fs.contoso.com

注意：请不要使用<hostname>.<domain>的证书，否则后续配置ADFS时会报错

**设置服务器 IP 地址**

将**服务器 IP 改为静态 IP**

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/image_6.png)

### 配置 DNS 条目

您需要为 AD FS 创建一个 DNS 条目。这里创建的条目使用的URL跟之前申请证书时用得URL相同

<AD FS service name>.<domain>

例如：

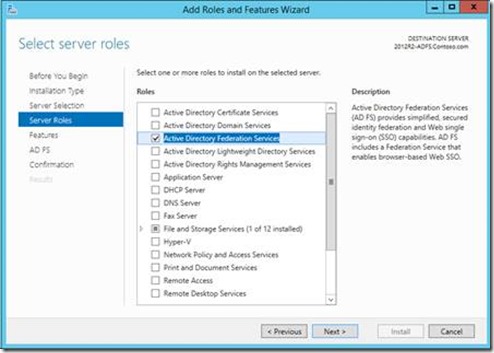
fs.contoso.com

注意：请一定要在 AD 中为 AD FS 创建 **A记录**

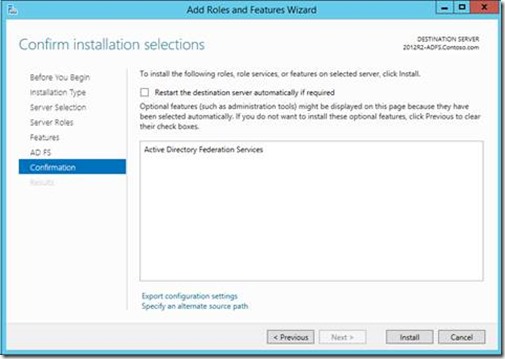
### 安装 AD FS

登录到计划安装 AD FS 的虚拟机或物理机并打开 Add Roles and Features Wizard。

如要安装 AD FS，选择 Server Roles 下的 Active Directory Federation Services 角色并单击 Next。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image002_2.jpg)

点击Next，看到以下确认页面。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image006_2.jpg)

### 配置 AD FS

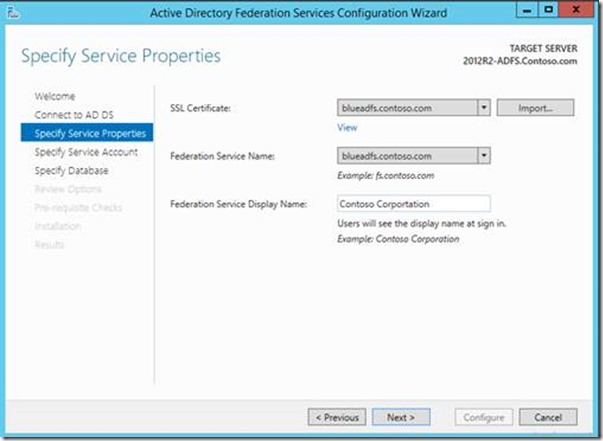
选择服务器管理器顶部的警告标志，单击 “Configure the federation service on this server” 链接。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image012_2.jpg)

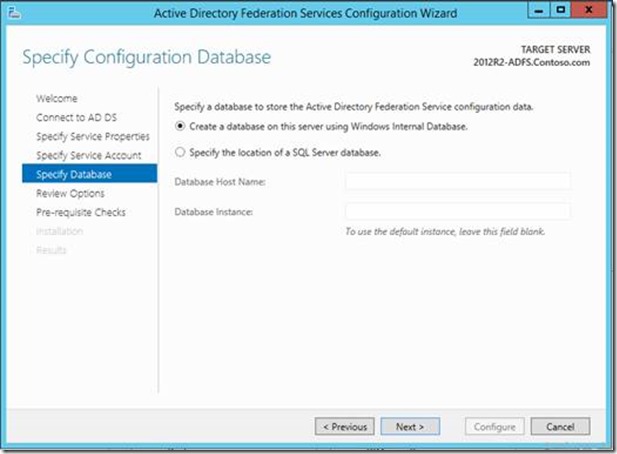
该链接会启动 Active Directory Federation Services 向导。

1. 欢迎屏幕之后的第一个页面将用于指定域管理员帐户，该帐户将用作专用 AD FS 帐户。
2. 接下来配置AD FS要使用的证书，并设置 Federation Service Name 的名称。

如前所述，这里使用的证书不能是<HostName>.<Domain>形式的证书，否则会配置失败

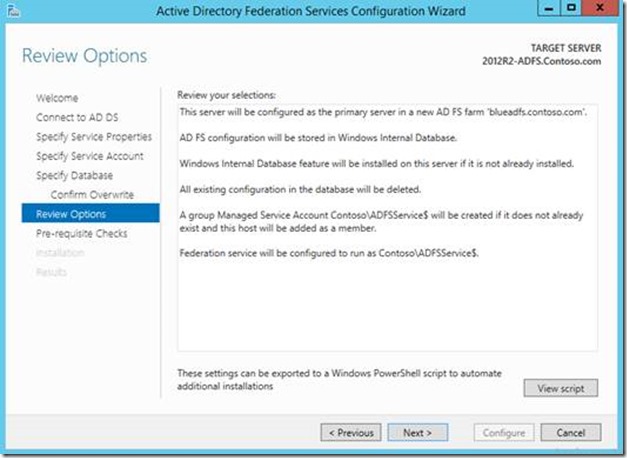
[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image014_2.jpg)

1. 使用之前配置到的服务账号
2. 选择使用 Windows 内部数据库并单击 Next。

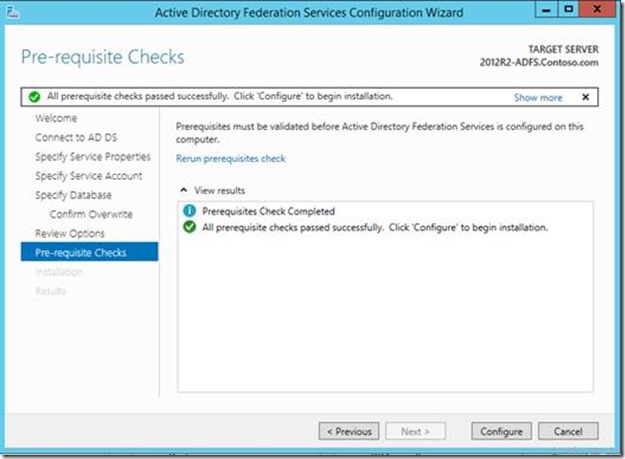
[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image018_2.jpg)

如果之前配置过AD FS，则会报出警告 提示已经有数据库存在，确认是否覆盖，直接选择覆盖即可。

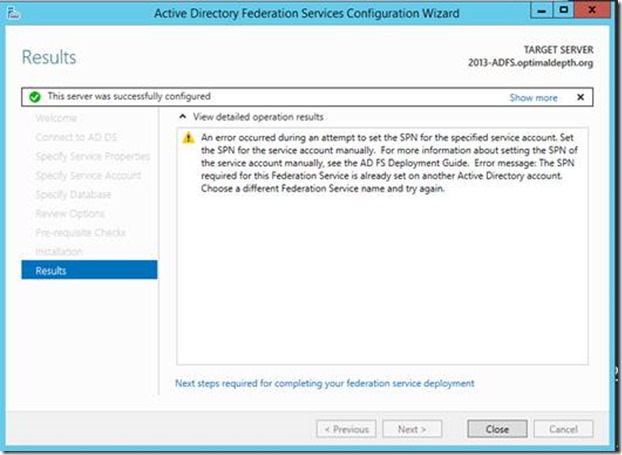
1. 审查页面将向您显示您选择的选项的概述。单击 Next。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image020_2.jpg)

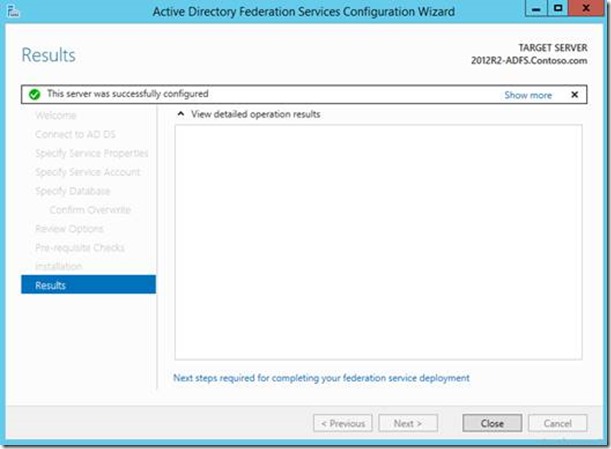
1. 下一个界面将是必备项检查页面。如果通过检查，单击 Configure。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image022_2.jpg)

如果您使用了 AD FS 服务器的名称或另一台现有服务器的名称，会收到如下所示的错误消息。您应当重新开始安装过程，选择一个与 AD FS 服务器或任何现有服务器的名称不同的名称。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image024_2.jpg)

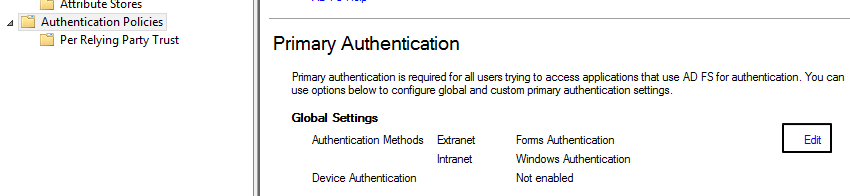
当配置成功完成时，您会看到以下表明 AD FS 配置成功的页面。

[](https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/47/85/metablogapi/clip_image026_2.jpg)

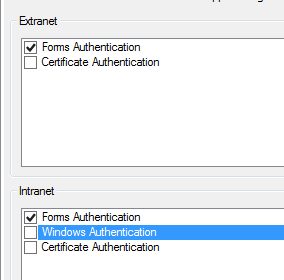
### 配置Form认证

一般情况下AD FS认证使用Form认证的居多，请在配置好AD FS之后，配置ADFS为Form认证。

AD FS上打开AD FS Management，找到Authentication Policies，点击右侧Primary Authentication中的Edit



上下两个都配置为Form Authentication



**阶段 2：使用 Web 应用程序将 AD FS 配置为信赖方**

此阶段包括以下过程：

1. [为信赖方配置 AD FS](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#relyparty)
2. [配置声明规则](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#claimrule)
3. [导出令牌签名证书](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#ExportCert)

**为信赖方配置 AD FS**

可使用本节中的过程配置信赖方。信赖方将定义 AD FS 识别信赖方应用程序并为其颁发声明的方式。

**为信赖方配置 AD FS**

1. 确认执行此过程的用户帐户是本地计算机上管理员组的成员。有关帐户和组成员身份的其他信息，请参阅[了解本地用户和组](http://go.microsoft.com/fwlink/p/?LinkId=780863)。
2. 在 AD FS 服务器上，打开 Active Directory 联合身份验证服务 (AD FS) 2.0 管理控制台。
3. 在导航窗格中展开“信任关系”，然后双击“信赖方信任”文件夹。
4. 在右侧窗格中单击“添加信赖方信任”。

这将打开 Active Directory 联合身份验证服务 (AD FS) 2.0 配置向导。

1. 在“欢迎使用添加信赖方信任向导”页上，单击“开始”。
2. 选择“手动输入有关信赖方的数据”，然后单击“下一步”。
3. 键入信赖方名称，然后单击“下一步”。
4. 确保选中“Active Directory 联合身份验证服务(AD FS) 2.0 配置文件”，然后单击“下一步”。
5. 不要使用加密证书。单击“下一步”。
6. 单击以选中“启用 WS 联合身份验证被动协议”复选框。
7. 在“WS 联合身份验证被动协议 URL”字段中，键入 Web 应用程序 URL 的名称，并追加 **/\_trust/**（例如，**https:// app1.contoso.com/\_trust/**）。单击“下一步”。

|  |
| --- |
| **注意注意：** |
| URL 的名称必须使用安全套接字层 (SSL)。 |

1. 键入信赖方信任标识符的名称（例如，**urn:sharepoint:contoso**），然后单击“添加”。单击“下一步”。请注意，这将是您在阶段 3 中配置新的 SPTrustedIdentityTokenIssuer 时的领域值。
2. 选择“允许所有用户访问此信赖方”。单击“下一步”。
3. 在“已准备好添加信任”页上，无需执行任何操作，直接单击“下一步”。
4. 在“完成”页上单击“关闭”。这将打开“规则编辑器”管理控制台。使用此控制台和下一过程将声明的映射从所选的目录源配置到 SharePoint 2013。

**配置声明规则**

使用此步骤中的过程将轻型目录访问协议 (LDAP) 属性的值作为声明进行发送，并指定属性将映射到传出声明类型的方式。

**配置声明规则**

1. 确认执行此过程的用户帐户是本地计算机上管理员组的成员。有关帐户和组成员身份的其他信息，请参阅[默认本地组](http://go.microsoft.com/fwlink/p/?LinkId=780864)。
2. 在“颁发转换规则”选项卡上，单击“添加规则”。
3. 在“选择规则模板”页上，选择“将 LDAP 属性作为声明进行发送”。单击“下一步”。
4. 在“配置规则”页上，在“声明规则名称”字段中键入声明规则的名称。
5. 从“属性存储”下拉列表中选择“Active Directory”。
6. 在“将 LDAP 属性映射到传出声明类型”部分的“LDAP 属性”下，选择“E-Mail-Addresses”。
7. 在“传出声明类型”下，选择“电子邮件地址”。
8. 在“LDAP 属性”下，选择“User-Principal-Name”。
9. 在“传出声明类型”下，选择“UPN”。
10. 单击“完成”，然后单击“确定”。

**导出令牌签名证书**

可使用本节中的过程导出您要用来建立信任关系的 AD FS 服务器的令牌签名证书，然后将该证书复制到 SharePoint 2013 能够访问的位置。

**导出令牌签名证书**

1. 确认执行此过程的用户帐户是本地计算机上管理员组的成员。有关帐户和组成员身份的其他信息，请参阅[默认本地组](http://go.microsoft.com/fwlink/p/?LinkId=780864)
2. 在 AD FS 服务器上，打开 Active Directory 联合身份验证服务 (AD FS) 2.0 管理控制台。
3. 在导航窗格中展开“服务”，然后单击“证书”文件夹。
4. 在“令牌签名”下，单击“主要”列中指示的主要令牌证书。
5. 在右侧窗格中单击“查看证书链接”。这将显示证书的属性。
6. 单击“详细信息”选项卡。
7. 单击“复制到文件”。这将启动“证书导出向导”。
8. 在“欢迎使用证书导出向导”页上，单击“下一步”。
9. 在“导出私钥”页上，单击“否，不要导出私钥”，然后单击“下一步”。
10. 在“导出文件格式”页上，选择“DER 编码二进制 X.509 (.CER)”，然后单击“下一步”。
11. 在“要导出的文件”页上，键入您要导出的文件的名称和位置，然后单击“下一步”。例如，输入 **C:\ADFS.cer**。
12. 在“正在完成证书导出向导”页上，单击“完成”。

**阶段 3：将 SharePoint 2013 配置为将 AD FS 视为受信任的身份提供程序**

此阶段包括以下过程：

1. [导出多个父证书](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#multicerts)
2. [通过使用 Windows PowerShell 导入令牌签名证书](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#import)
3. [使用 Windows PowerShell 为声明映射定义唯一标识符](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#claimmapping)
4. [新建身份验证提供程序](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#AuthProvider)

**导出多个父证书**

若要完成 AD FS 服务器的配置，请将 .CER 文件复制到运行 AD FS 的计算机。

令牌签名证书可能会在其证书链中包含一个或多个父证书。如果是这样，则必须将链中的每个证书添加到受信任的根证书颁发机构的 SharePoint 2013 列表。

若要确定是否存在一个或多个父证书，请按以下步骤操作。

|  |
| --- |
| **注意注意：** |
| 除非将所有证书导出到根证书颁发机构，否则应重复这些步骤。 |

**导出多个父证书**

1. 确认执行此过程的用户帐户是本地计算机上管理员组的成员。有关帐户和组成员身份的其他信息，请参阅[默认本地组](http://go.microsoft.com/fwlink/p/?LinkId=780864)
2. 打开 Active Directory 联合身份验证服务 (AD FS) 2.0 管理控制台。
3. 在导航窗格中展开“服务”，然后单击“证书”文件夹。
4. 在“令牌签名”下，单击“主要”列中指示的主要令牌证书。
5. 在右侧窗格中单击“查看证书链接”。这将显示证书的属性。
6. 单击“证书”选项卡。这将显示链中的任何其他证书。
7. 单击“详细信息”选项卡。
8. 单击“复制到文件”。这将启动“证书导出向导”。
9. 在“欢迎使用证书导出向导”页上，单击“下一步”。
10. 在“导出私钥”页上，单击“否，不要导出私钥”，然后单击“下一步”。
11. 在“导出文件格式”页上，选择“DER 编码二进制 X.509 (.CER)”，然后单击“下一步”。
12. 在“要导出的文件”页上，键入您要导出的文件的名称和位置，然后单击“下一步”。例如，输入 **C:\adfsParent.cer**。
13. 在“正在完成证书导出向导”页上，单击“完成”。

**通过使用 Windows PowerShell 导入令牌签名证书**

可使用这一部分将令牌签名证书导入到驻留在 SharePoint Server 上的受信任根证书颁发机构列表。必须针对链中的每个令牌签名证书重复此步骤，直至到达根证书颁发机构。

**通过使用 Windows PowerShell 导入令牌签名证书**

1. 确认您具有以下成员身份：
   * SQL Server 实例上的 **securityadmin** 固定服务器角色。
   * 要更新的所有数据库上的 **db\_owner** 固定数据库角色。
   * 运行 Windows PowerShell cmdlet 的服务器上的 Administrators 组。
   * 添加至少具有以上最小权限的成员。

管理员可以使用 **Add-SPShellAdmin** cmdlet 授予使用 SharePoint 2013 产品 cmdlet 的权限。

|  |
| --- |
| **注意注意：** |
| 如果您不具有这些权限，请联系您的安装管理员或 SQL Server 管理员来请求权限。有关 Windows PowerShell 权限的其他信息，请参阅 [Add-SPShellAdmin](https://technet.microsoft.com/zh-cn/library/ff607596.aspx)。 |

1. 启动 SharePoint 2013 命令行管理程序。
   * 对于 Windows Server 2008 R2：
     + 在 SharePoint 2013 环境中，在“开始”菜单上，单击“所有程序”，单击“Microsoft SharePoint 2013 产品”，然后单击“SharePoint 2013 命令行管理程序”。
   * 对于 Windows Server 2012：
     + 在 SharePoint 2013 环境中，在“开始”屏幕上，单击“SharePoint 2013 命令行管理程序”。

如果“SharePoint 2013 命令行管理程序”不在“开始”屏幕上：

* + - 右键单击“计算机”，单击“所有应用程序”，然后单击“SharePoint 2013 命令行管理程序”。

有关如何与 Windows Server 2012 进行交互的详细信息，请参阅 [Windows Server 2012 R2 和 Windows Server 2012 中的常见管理任务和导航](http://go.microsoft.com/fwlink/p/?LinkId=276950)。

1. 从 Windows PowerShell 命令提示符处，导入令牌签名证书的父证书（即，根证书颁发机构证书），如以下语法中所示：

$root = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("<PathToParentCert>")

New-SPTrustedRootAuthority -Name "Token Signing Cert Parent" -Certificate $root

1. 从 Windows PowerShell 命令提示符处，导入从 AD FS 服务器复制的令牌签名证书，如以下语法中所示：

$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("<PathToSigningCert>")

New-SPTrustedRootAuthority -Name "Token Signing Cert" -Certificate $cert

有关 **New-SPTrustedRootAuthority** cmdlet 的其他信息，请参阅 [New-SPTrustedRootAuthority](https://technet.microsoft.com/zh-cn/library/ff607586.aspx)

**使用 Windows PowerShell 为声明映射定义唯一标识符**

可使用本节中的过程定义声明映射的唯一标识符。通常，此信息采用电子邮件地址的格式，并且受信任 STS 的管理员必须提供此信息，因为只有 STS 的所有者才知道始终对每个用户唯一的声明类型。

**使用 Windows PowerShell 为声明映射定义唯一标识符**

1. 从 Windows PowerShell 命令提示符处，创建一个电子邮件地址声明映射，如以下语法中所示：

$emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming

1. 从 Windows PowerShell 命令提示符处，创建 UPN 声明映射，如以下语法中所示：

$upnClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" -IncomingClaimTypeDisplayName "UPN" -SameAsIncoming

1. 从 Windows PowerShell 命令提示符处，创建角色声明映射，如以下语法中所示：

$roleClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -IncomingClaimTypeDisplayName "Role" -SameAsIncoming

此声明映射用于服务器到服务器身份验证应用场景。有关详细信息，请参阅[SharePoint 2013 中的服务器到服务器身份验证的规划](https://technet.microsoft.com/zh-cn/library/jj219546.aspx)。

1. 从 Windows PowerShell 命令提示符处，创建主 SID 声明映射，如以下语法中所示：

$sidClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid" -IncomingClaimTypeDisplayName "SID" -SameAsIncoming

此声明映射用于服务器到服务器身份验证应用场景。

有关 **New-SPClaimTypeMapping** cmdlet 的其他信息，请参阅 [New-SPClaimTypeMapping](https://technet.microsoft.com/zh-cn/library/ff607650.aspx)

**新建身份验证提供程序**

可使用本节中的过程创建一个新的 SPTrustedIdentityTokenIssuer。

**使用 Windows PowerShell 创建新的身份验证提供程序**

从 Windows PowerShell 命令提示符处，创建一个新的身份验证提供程序，如以下语法中所示。

$realm = "urn:sharepoint:<WebAppName>"

$signInURL = "https://<YourADFSServerName>/adfs/ls"

$ap = New-SPTrustedIdentityTokenIssuer -Name <ProviderName> -Description <ProviderDescription> -realm $realm -ImportTrustCertificate $cert -ClaimsMappings $emailClaimMap,$upnClaimMap,$roleClaimMap,$sidClaimMap -SignInUrl $signInURL -IdentifierClaim $emailClaimmap.InputClaimType

$realm 变量是 AD FS 中配置的信赖方信任标识符的名称，$cert 变量是[使用 Windows PowerShell 导入令牌签名证书](https://technet.microsoft.com/zh-cn/library/hh305235.aspx" \l "import)一节中使用的变量。**SignInUrl** 参数用于 AD FS 服务器。

在 ClaimsMappings 列表中包含 $roleClaimMap 和 $sidClaimMap，以用于服务器到服务器身份验证应用场景。

有关 **New-SPTrustedIdentityTokenIssuer** cmdlet 的其他信息，请参阅 [New-SPTrustedIdentityTokenIssuer](https://technet.microsoft.com/zh-cn/library/ff607628.aspx)

**阶段 4：将 Web 应用程序配置为将基于声明的身份验证和 AD FS 用作受信任的身份提供程序**

此阶段包括以下过程：

1. [将现有 Web 应用程序与 AD FS 身份提供程序关联](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#CreateWebApp)
2. [使用 AD FS 身份提供程序创建新的 Web 应用程序](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#NewWebApp)
3. [启用令牌重放保护](https://technet.microsoft.com/zh-cn/library/hh305235.aspx#ReplayProt)

**将现有 Web 应用程序与 AD FS 身份提供程序关联**

若要将现有的 Web 应用程序配置为使用 SAML 登录，则必须更改声明身份验证类型部分中的可信身份提供程序。

**将现有的 Web 应用程序配置为使用 AD FS 身份提供程序**

1. 确认执行此过程的用户帐户是 SharePoint 组“服务器场管理员”的成员。
2. 在管理中心的主页上，单击“应用程序管理”。
3. 在“应用程序管理”页上的“Web 应用程序”部分，单击“管理 Web 应用程序”。
4. 单击适当的 Web 应用程序。
5. 从功能区中单击“身份验证提供程序”。
6. 在“区域”下单击区域的名称，例如 Default。
7. 在“编辑验证”页上的“声明身份验证类型”部分，选择“信任的身份提供程序”，然后单击 SAML 提供程序的名称（New-SPTrustedIdentityTokenIssuer 命令中的 *<ProviderName>*。单击“确定”。
8. 接下来，您必须为此 Web 应用程序启用 SSL。可以通过为“https://”版本的 Web 应用程序 URL 添加备用访问映射，然后在 Internet Information Services (IIS) 管理器控制台中为 https 绑定配置网站来完成此操作。有关如何为 IIS 设置 SSl 的详细信息，请参阅[如何在 IIS 7.0 上设置 SSL](http://go.microsoft.com/fwlink/p/?LinkId=187887)。

**使用 AD FS 身份提供程序创建新的 Web 应用程序**

在创建新的 Web 应用程序以使用 SAML 登录时，您必须为 AD FS 受信任身份提供程序配置声明身份验证。请参阅[在 SharePoint 2013 中创建基于声明的 Web 应用程序](https://technet.microsoft.com/zh-cn/library/ee806885.aspx)并执行以下操作：

* 在“新建 Web 应用程序”对话框的“安全配置”部分，为“使用安全套接字层(SSL)”选择“是”。

有关如何为 IIS 设置 SSL 的信息，请参阅[如何在 IIS 7.0 上设置 SSL](http://go.microsoft.com/fwlink/p/?LinkId=187887)。

* 在“新建 Web 应用程序”对话框的“声明身份验证类型”部分，选择“信任的身份提供程序”，然后单击 SAML 提供程序的名称（来自 New-SPTrustedIdentityTokenIssuer 命令的 *<ProviderName>*）。

**配置访问 Web 应用程序的权限**

要允许用户通过使用电子邮件地址作为其基于 SAML 的标识（如具有 **-IdentifierClaim $emailClaimmap.InputClaimType** 参数的 New-SPTrustedIdentityTokenIssuer 命令中所指定），您必须将具有适当权限的用户电子邮件地址添加到 Web 应用程序。

使用以下过程来为 Web 应用程序配置基于电子邮件地址的权限。

**为 Web 应用程序配置基于电子邮件地址的权限**

1. 在管理中心的主页上，单击“应用程序管理”。
2. 在“应用程序管理”页上的“Web 应用程序”部分，单击“管理 Web 应用程序”。
3. 单击适当的 Web 应用程序，然后单击“用户策略”。
4. 在“Web 应用程序的策略”中，单击“添加用户”。
5. 在“添加用户”对话框中，单击“区域”中的适当区域，然后单击“下一步”。
6. 在“添加用户”对话框中，单击“用户”框右下方的“浏览”图标。
7. 在“选择人员和组”对话框中，在“查找”中键入用户帐户的电子邮件地址，然后单击“搜索”图标。
8. 在搜索结果中，依次单击 AD FS 标识提供程序名称下的“电子邮件地址”、“显示名称”下的用户电子邮件地址、“添加”，然后单击“确定”。
9. 在“权限”中，单击适当的权限级别。
10. 对具有相同权限级别的其他用户电子邮件地址重复第 6 步至第 9 步。
11. 单击“完成”，然后单击“确定”。

**启用令牌重放保护**

要为使用基于 SAML 的声明身份验证的 SharePoint 2013 Web 应用程序提供额外安全保护，您可以使用 Windows Identity Foundation (WIF) 令牌重放检测功能。令牌重放保护可以防止攻击者试图截取和使用用户的安全令牌。有关详细信息，请参阅[如何：启用令牌重放检测](http://go.microsoft.com/fwlink/p/?LinkId=506806)。

使用此部分中的步骤在为 SAML 声明身份验证配置的 Sharepoint Web 应用程序上启用重放检测。

**启用重放保护**

1. 在运行 SharePoint 2013 的服务器上，打开 Internet Information Services (IIS) 管理器管理单元。
2. 在 Internet Information Services (IIS) 管理器的控制台树中，右键单击与 Web 应用程序的名称对应的网站，然后单击“浏览”。
3. 在文件夹窗口中，双击“Web.Config”文件。
4. 在“<Configuration>”部分中，找到“<microsoft.identityModel>”部分。
5. 将以下内容作为新的部分添加到“<microsoft.identityModel>”部分中：

<service>

<tokenReplayDetection enabled="true" capacity="<NumberOfTokensToBeCached>" expirationPeriod="<TokenCacheExpiration>">

</service>

其中：

* + <NumberOfTokensToBeCached> 是指存储在令牌重放检测缓存中的令牌数。
  + <TokenCacheExpiration> 是指删除重放检测缓存中的令牌之后的时间，使用 <小时>:<分>:<秒> 格式。

1. 将您的更改保存到 Web.Config 文件。

如果运行 SharePoint 2013 的服务器场位于负载平衡器之后，启用令牌重放检测将在负载平衡器中请求会话粘滞，即使 SharePoint 2013 Web 应用程序并无此要求。要避免会话粘滞请求，请使用 [ACS 安全准则](http://go.microsoft.com/fwlink/p/?LinkId=277159)中的信息。