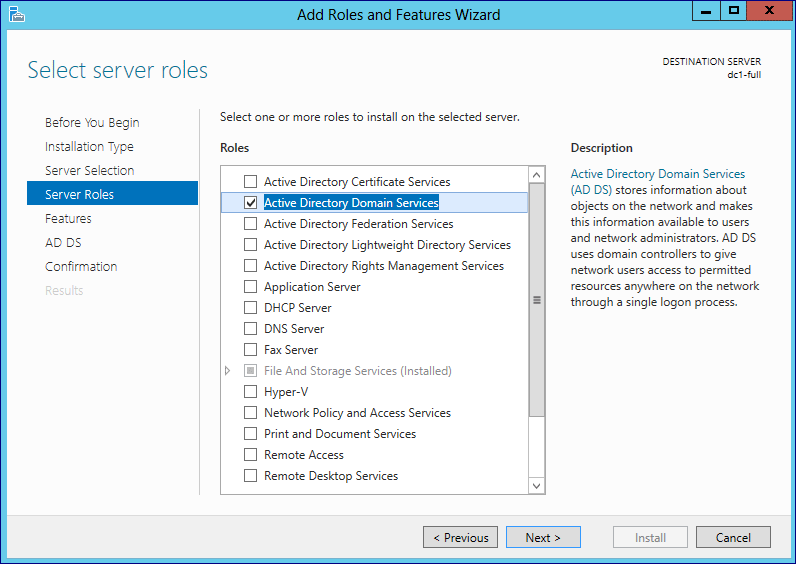
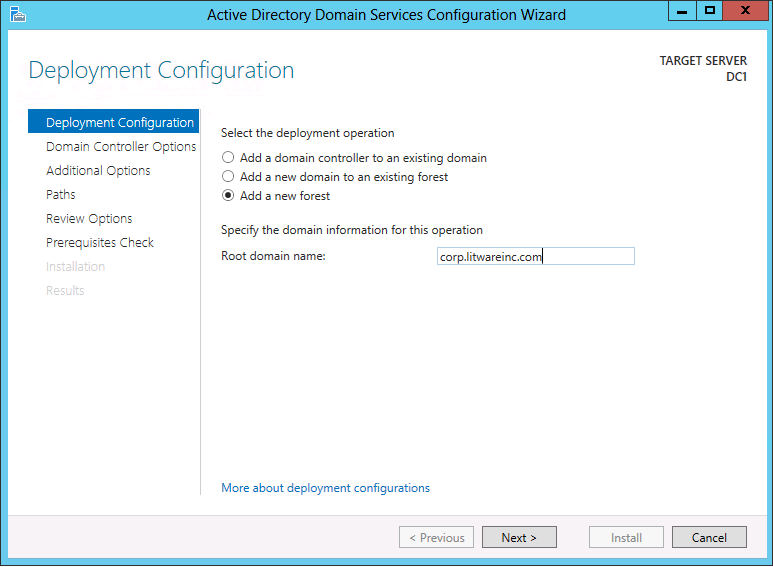
## ADFS Setup

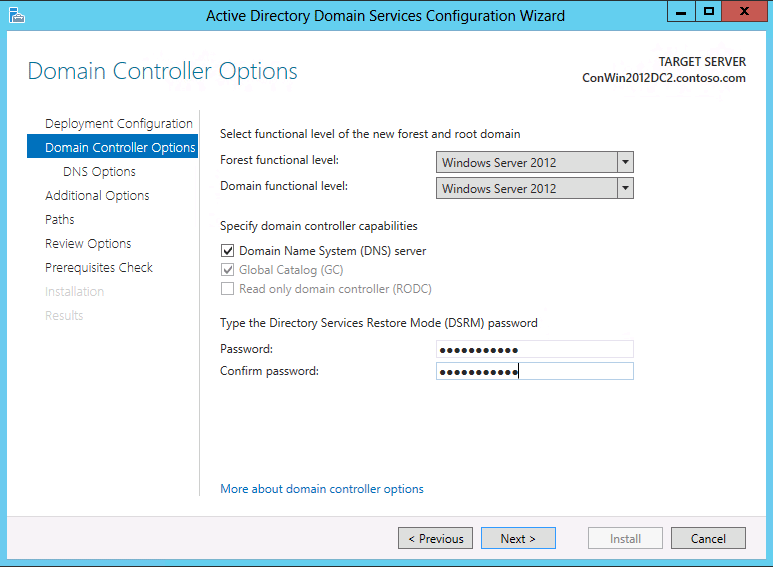
* **Configure the domain controller (DC1)**
  1. Install the AD DS role service and install Active Directory Domain Services (AD DS) to make your computer a domain controller.



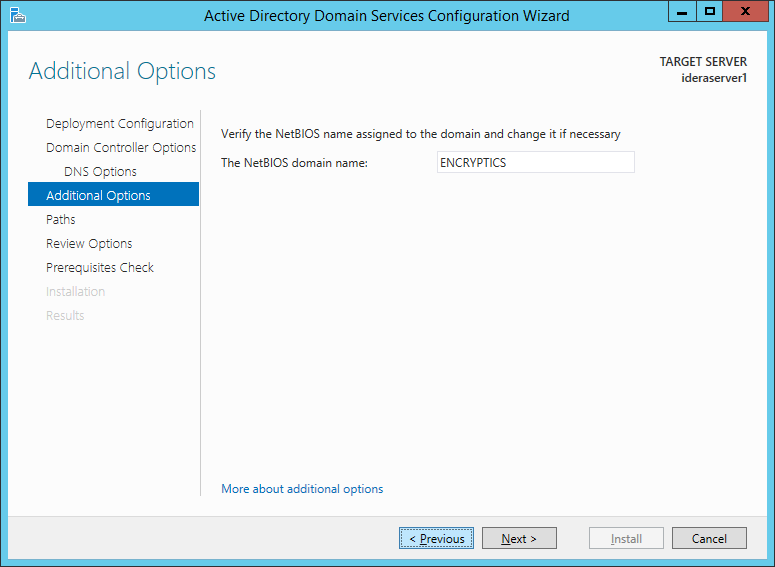
* 1. Configure forest domain



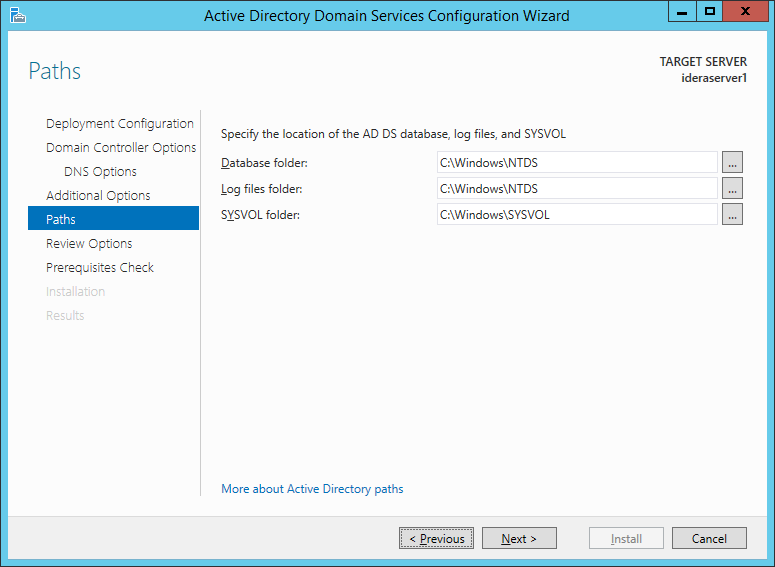
* 1. Provide Administrator password



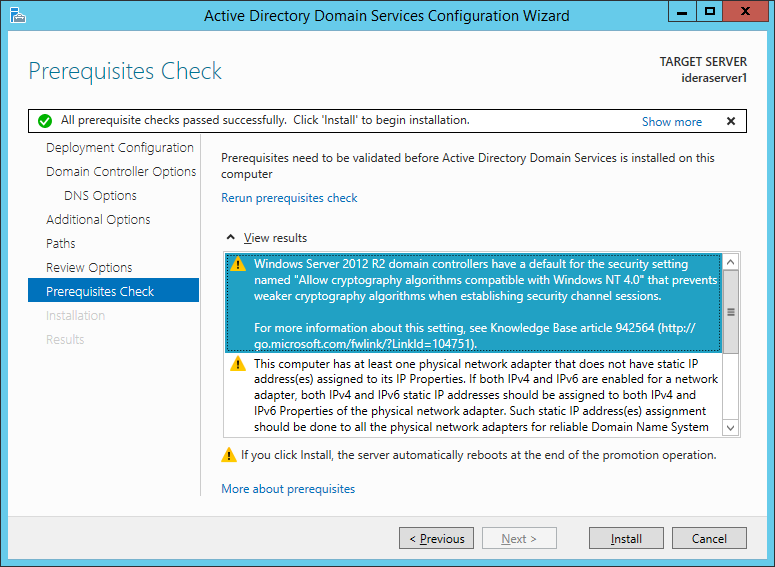
* 1. Click Next



* 1. Click Next

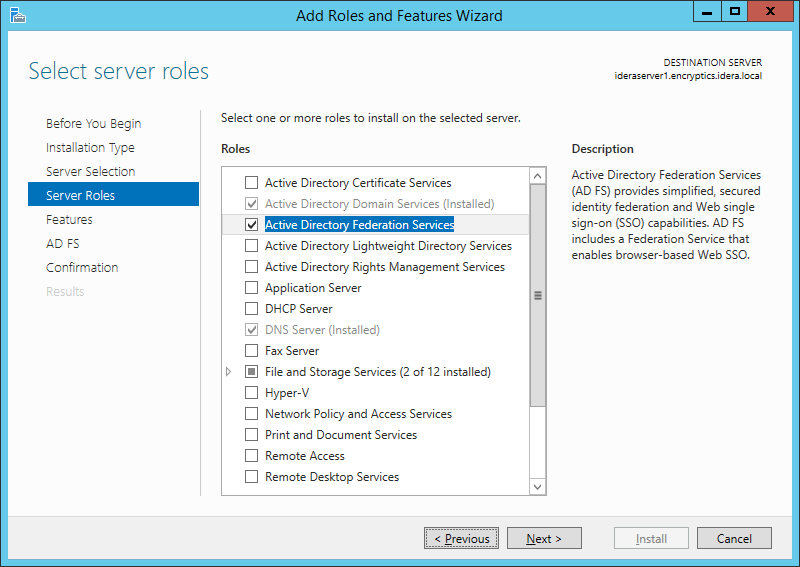


* 1. Click Install

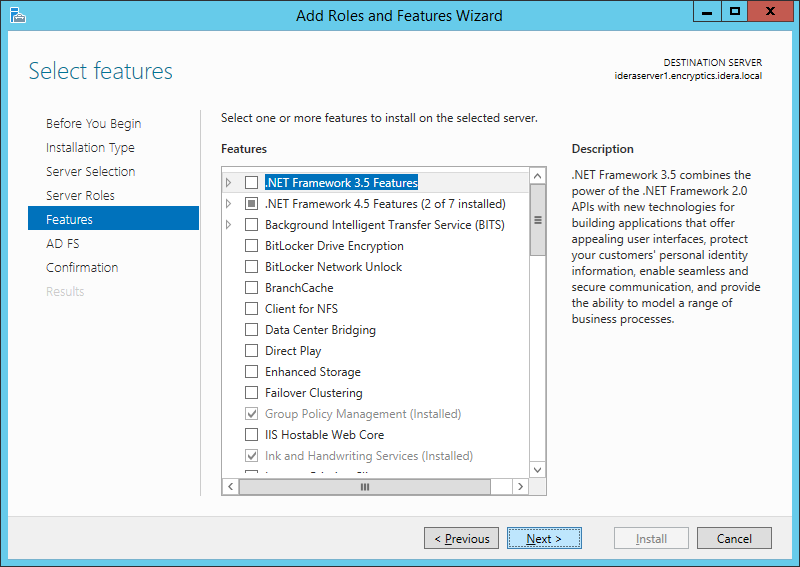


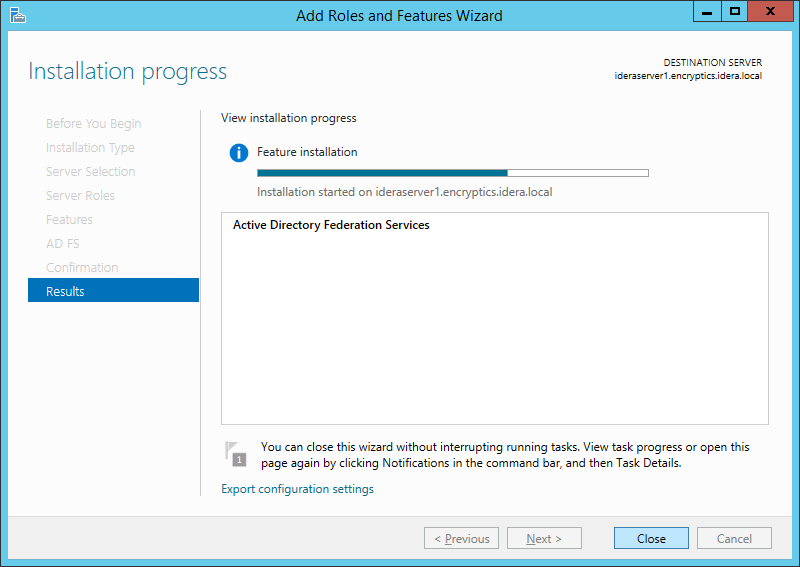
* **Install Valid Certificate**
  1. Make sure IIS is configure on host server and create a valid SSL certificate using IIS
  2. Enable https:// for IIS using valid certificate
  3. Install SSL certificate generated using 1st step on the client Machine in order to access host server securely.
  4. Make sure host server is accessible using FQDN from client.

* **Install the AD FS server role**
  1. Open server manager, click Add Roles and Features, proceed the step until you get Select server roles interface, and then click Active Directory Federation Services, then proceed with next.

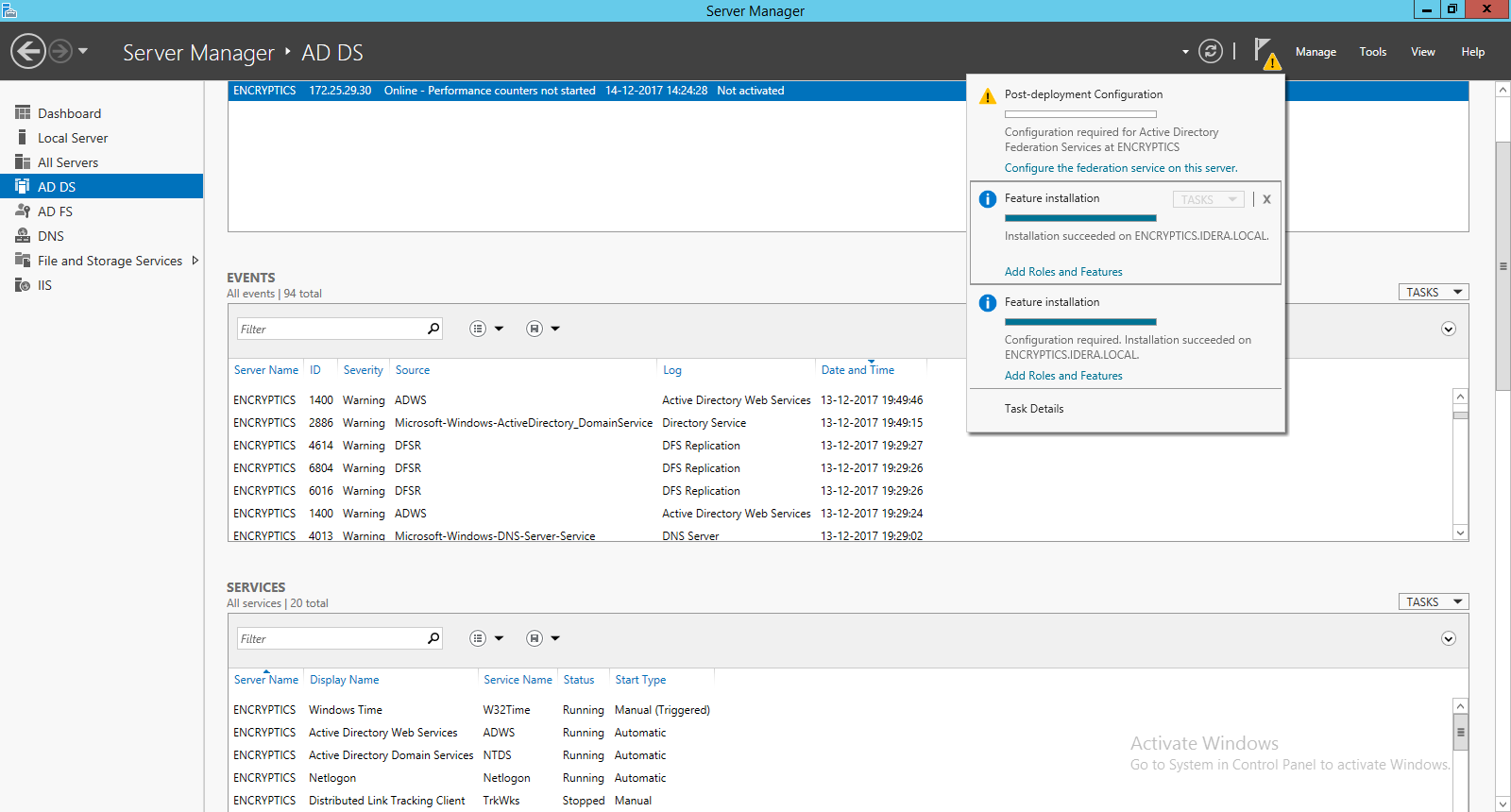


* 1. Click Next. On the Active Directory Federation Services (AD FS) interface, click Next and then click Install.

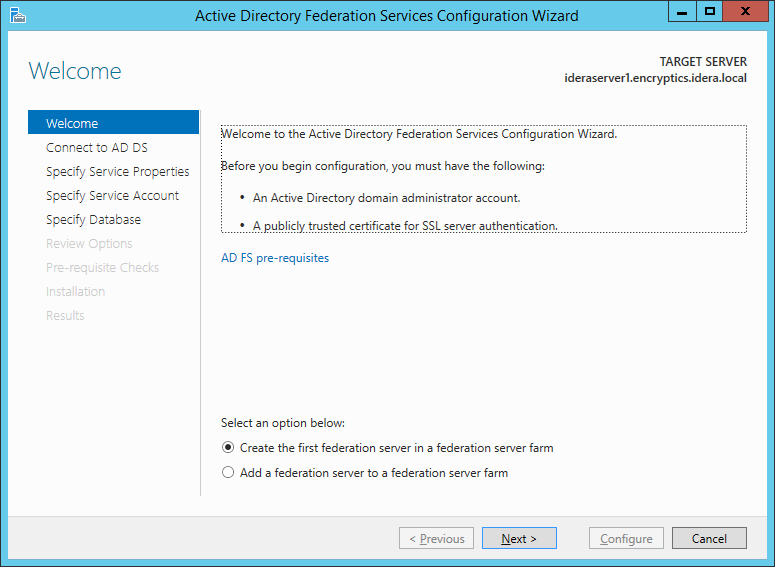




* **Configure the federation server**
  1. On the Server Manager Dashboard page, click the Notifications flag, and then click Configure the federation service on the server.
     + The Active Directory Federation Service Configuration Wizard opens.

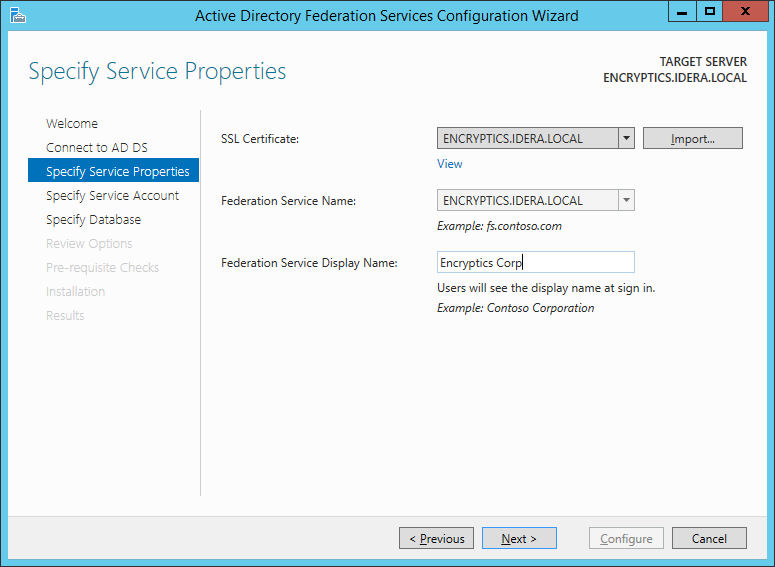


* 1. On the **Welcome** page, select **Create the first federation server in a federation server farm**, and then click **Next**.

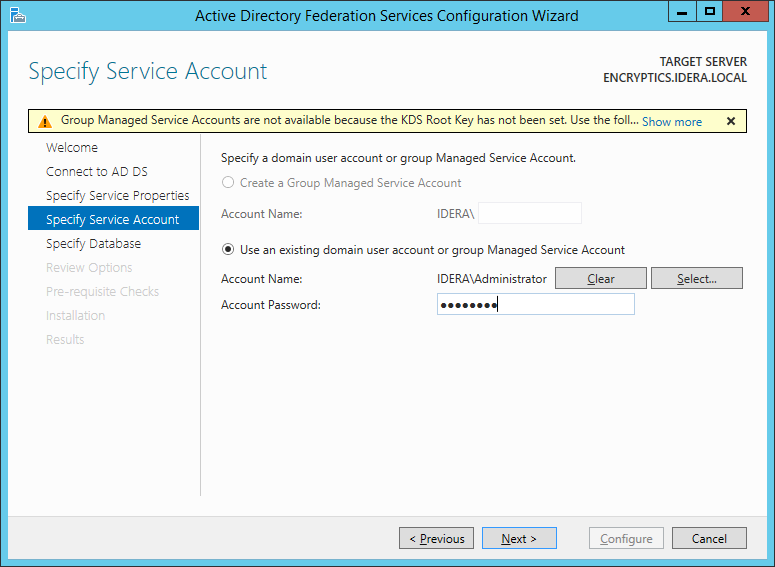


* 1. On the **Connect to AD DS** page, specify an account with domain administrator rights for the **contoso.com** Active Directory domain that this computer is joined to, and then click **Next**.

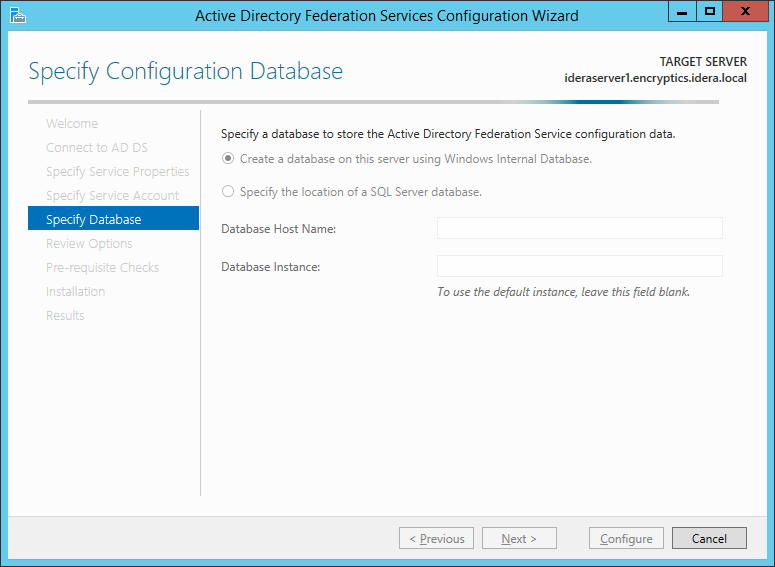
On the **Specify Service Properties** page, do the following, and then click **Next**:



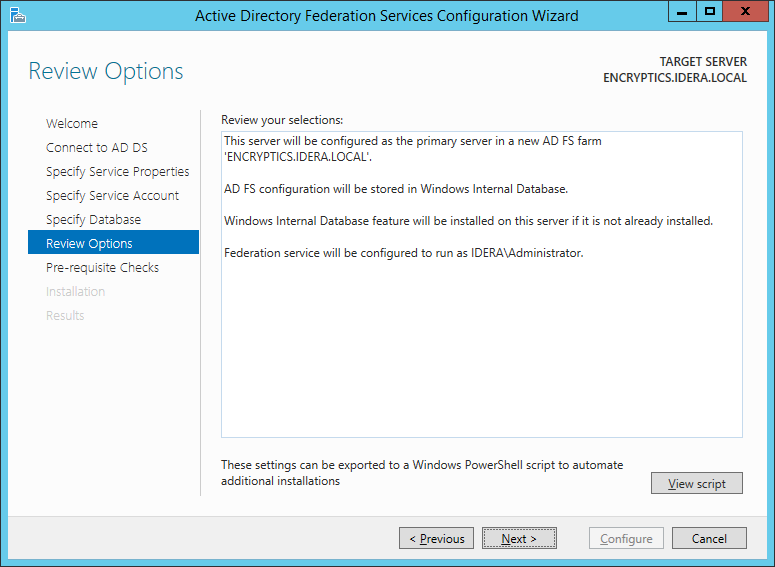
* + - Import the SSL certificate that you have obtained earlier. This certificate is the required service authentication certificate. Browse to the location of your SSL certificate.
    - To provide a name for your federation service, type **adfs1.contoso.com**. This value is the same value that you provided when you enrolled an SSL certificate in Active Directory Certificate Services (AD CS).
    - To provide a display name for your federation service, type **Encryptics**.
  1. On the **Specify Service Account** page, select **Use an existing domain user account or group Managed Service Account**, and then specify the Account name.



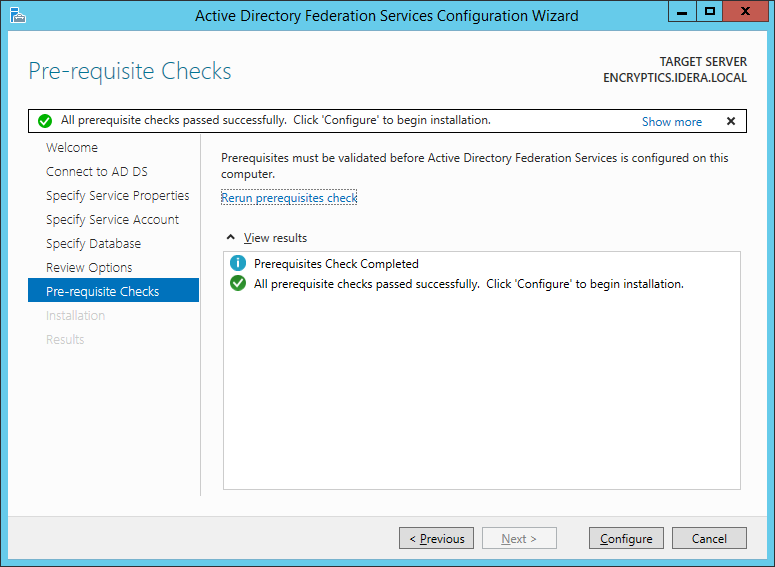
* 1. On the **Specify Configuration Database** page, select **Create a database on this server using Windows Internal Database**, and then click **Next**.



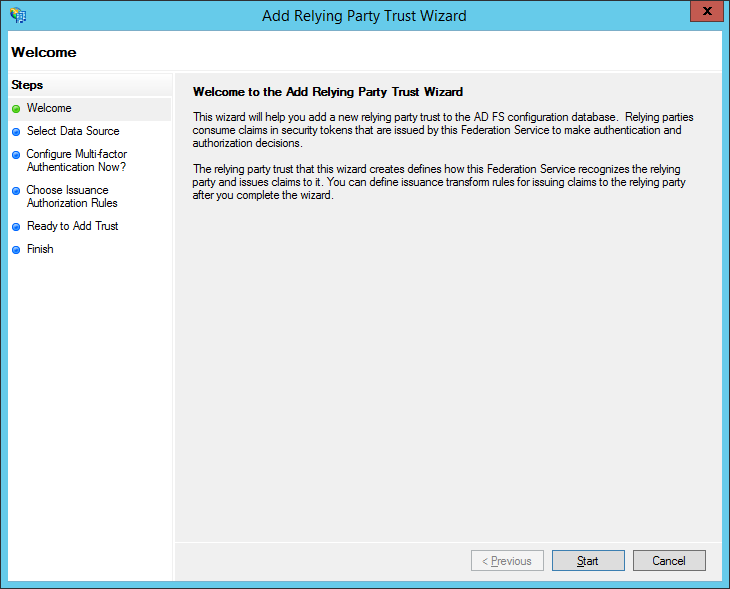
* 1. On the **Review Options** page, verify your configuration selections, and then click **Next**.



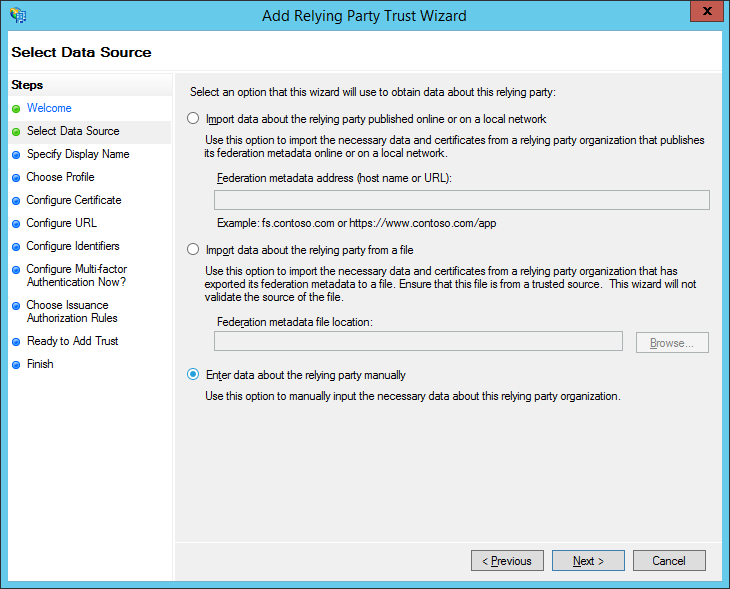
* 1. On the **Pre-requisite Checks** page, verify that all prerequisite checks were successfully completed, and then click **Configure**.



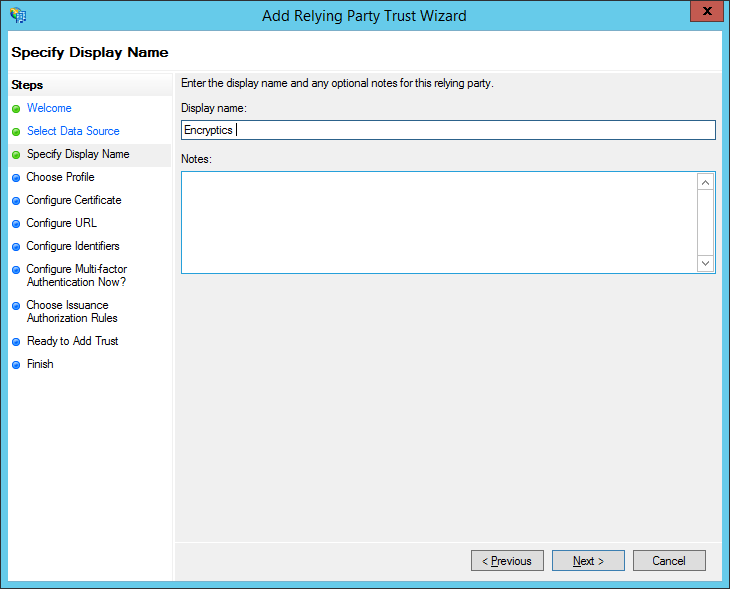
* 1. On the **Results** page, review the results, check whether the configuration has completed successfully.
* **Create a relying party trust on your federation server**
  1. On you federation server, in the **AD FS Management console**, navigate to **Relying Party Trusts**, and then click **Add Relying Party Trust**.



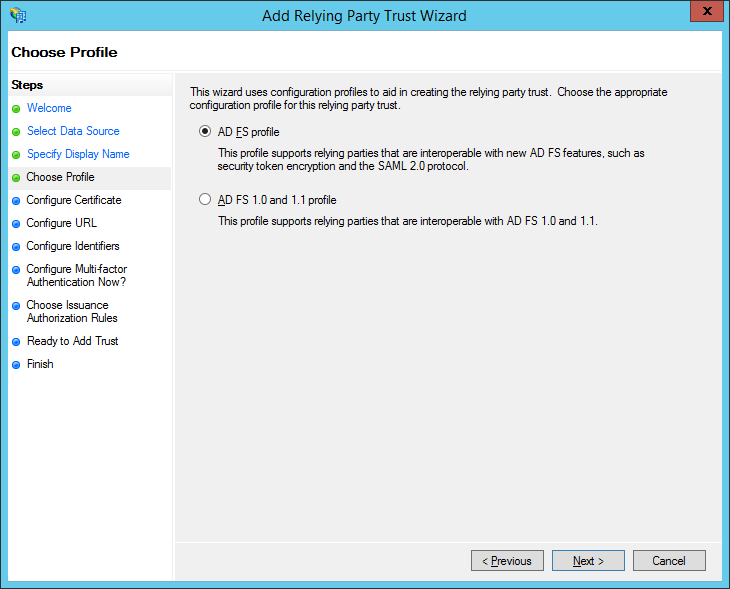
* 1. On the **Select Data Source** page, select **Enter data about relying party manually,** and then click **Next.**



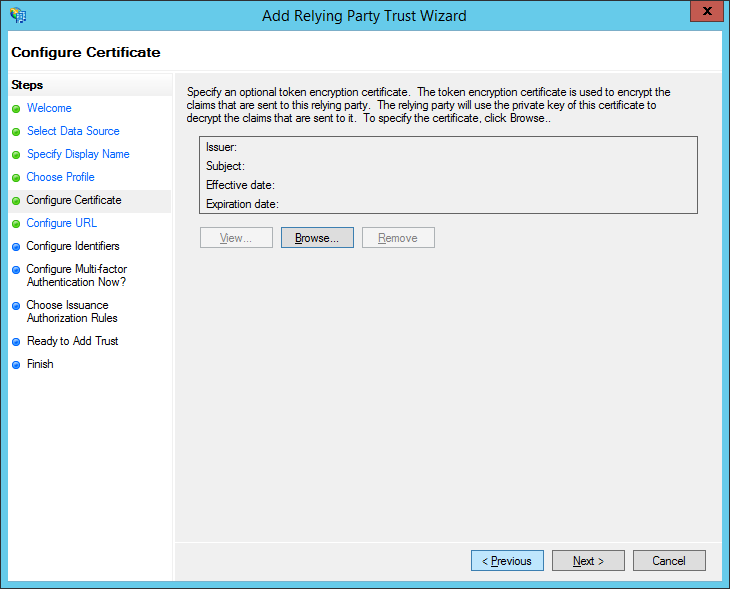
* 1. On the **Specify Display Name** page, specify the **display name** for your relying party trust, **claimapp**, and then click **Next**.



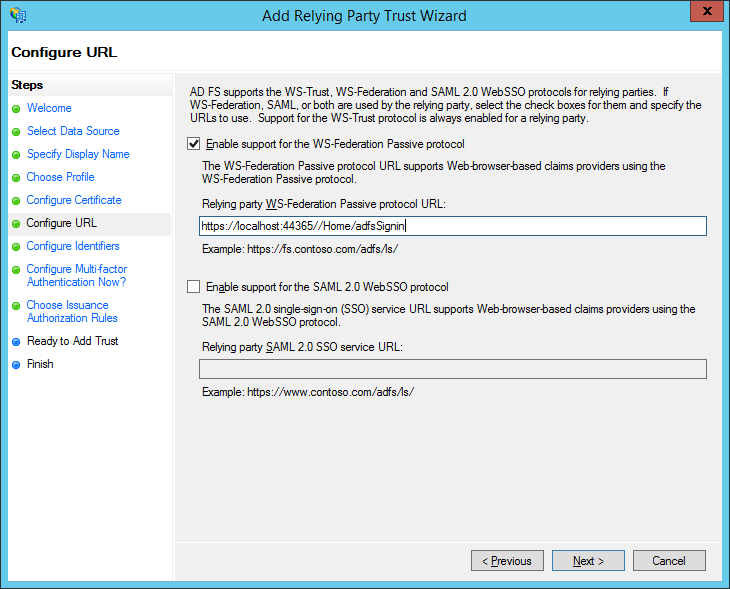
* 1. On **Choose Profile** select AD FS Profile, and then click **Next.**



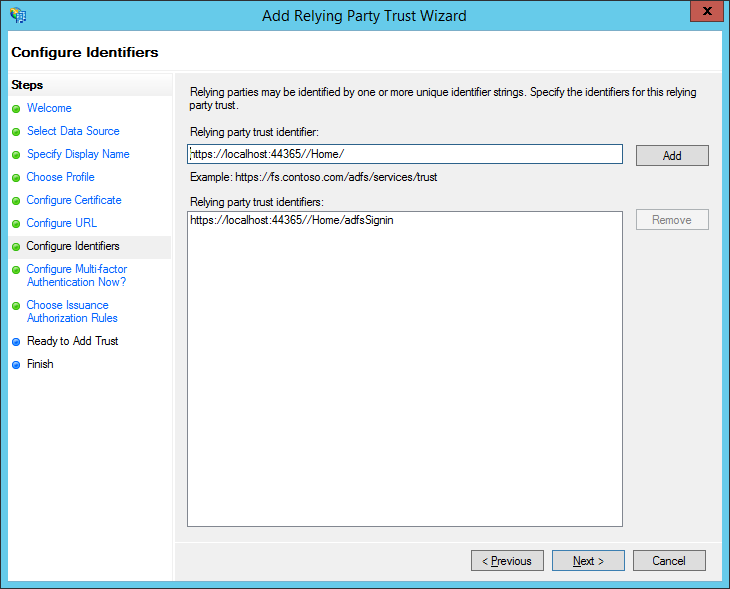
* 1. Click next



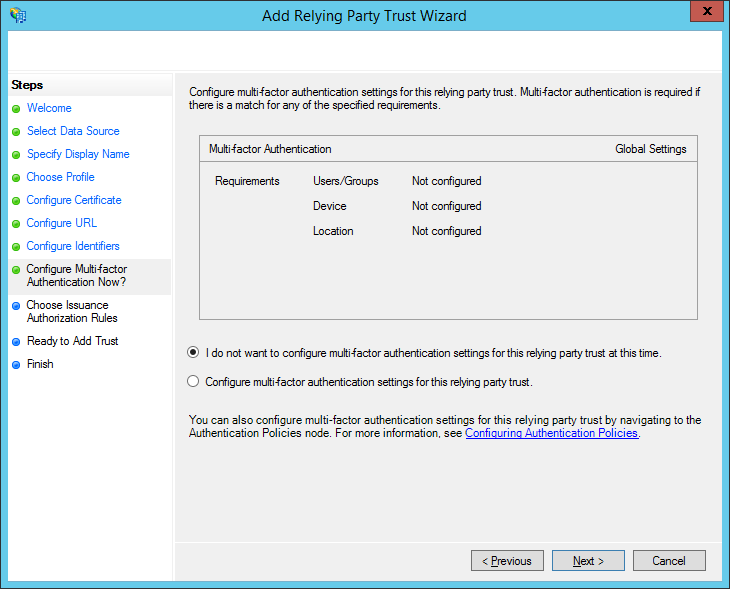
* 1. On the **Configuration URL** check Enable support for the WS-Federation Passive protocol and provide end point URL and click **Next.**



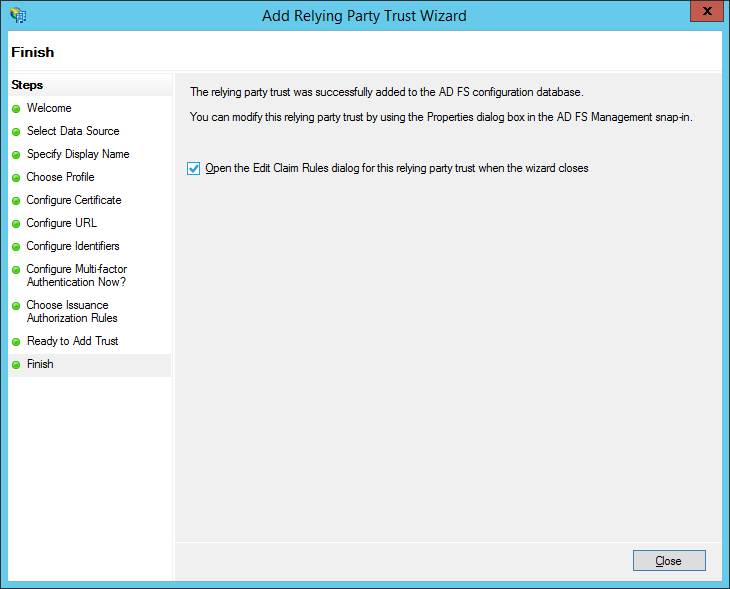
* 1. On the **Configuration Identifier** provide unique App Id and click **Next.**



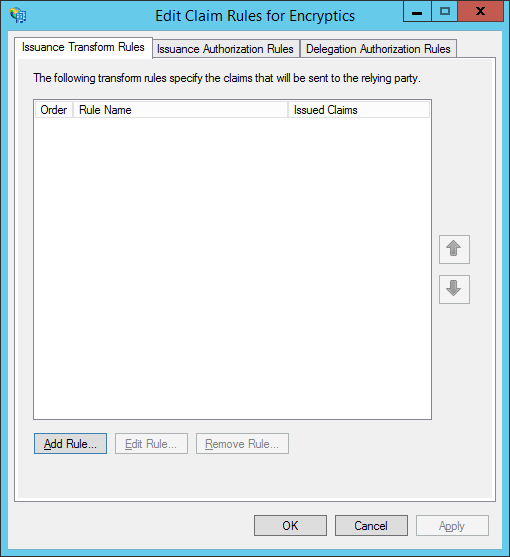
* 1. On the **Configure Multi-factor Authentication Now?** page, select **I do not want to specify multi-factor authentication setting for this relying party trust at this time**, and then click **Next**



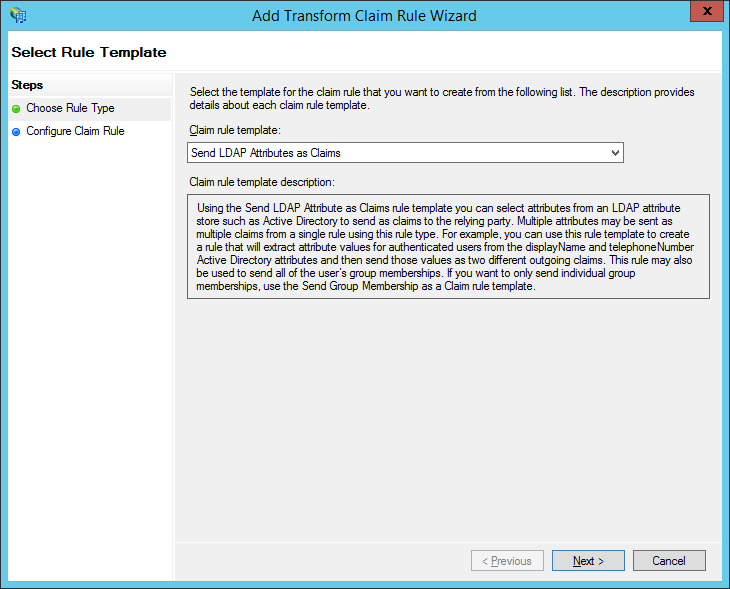
* 1. On the **Choose Issuance Authorization Rules** page, select **Permit all users to access this relying party**, and then click **Next**.
  2. On the **Ready to Add Trust** page, click **Next**.



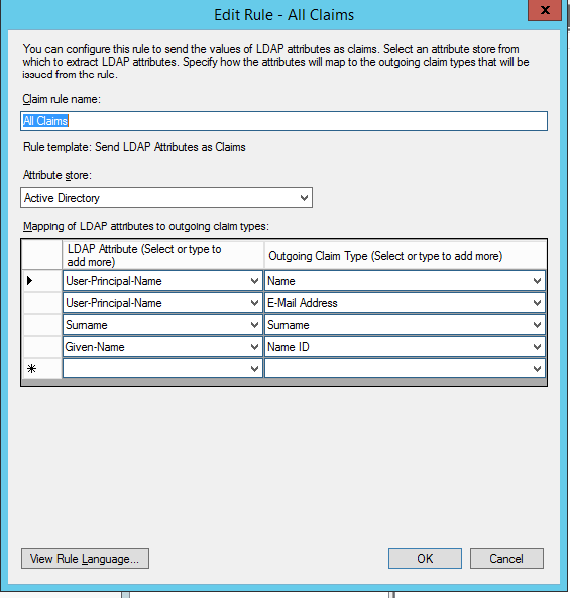
* 1. On the **Edit Claim Rules** dialog box, click **Add Rule**.



* 1. On the **Choose Rule Type** page, select **Send LDAP Attributes as Claims**, and then click **Next**.



* 1. On the **Configure Claim Rule** page, in the **Claim rule name** box, type **All Claims**. In the **Attribute Store** select **Active Directory**, and add attributes define in table.



|  |  |
| --- | --- |
| LDAP Attribute | Outgoing Claims |
| User-Principal-Name | Name |
| User-Principal-Name | E-mail Address |
| Surname | Surname |
| Given-Name | Name ID |
| Telephone-Number | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/phone |
| State-or-Province Name | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/state |
| streetAddress | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetAddress |
| postalCode | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalCode |
| mobile | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobile |
| co | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country |
| l | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/city |
| facsimileTelephoneNumber | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/facsimileTelephoneNumber |

* 1. Click **Finish**.
  2. Click **Apply** on **Edit Claim Rule**.
  3. Update adfsMetadataAddress value with https://<adfs host server>/federationmetadata/2007-06/federationmetadata.xml in webconfig
  4. Update adfsWtrelam value with Relying party Identifier