6. Single Sign-On

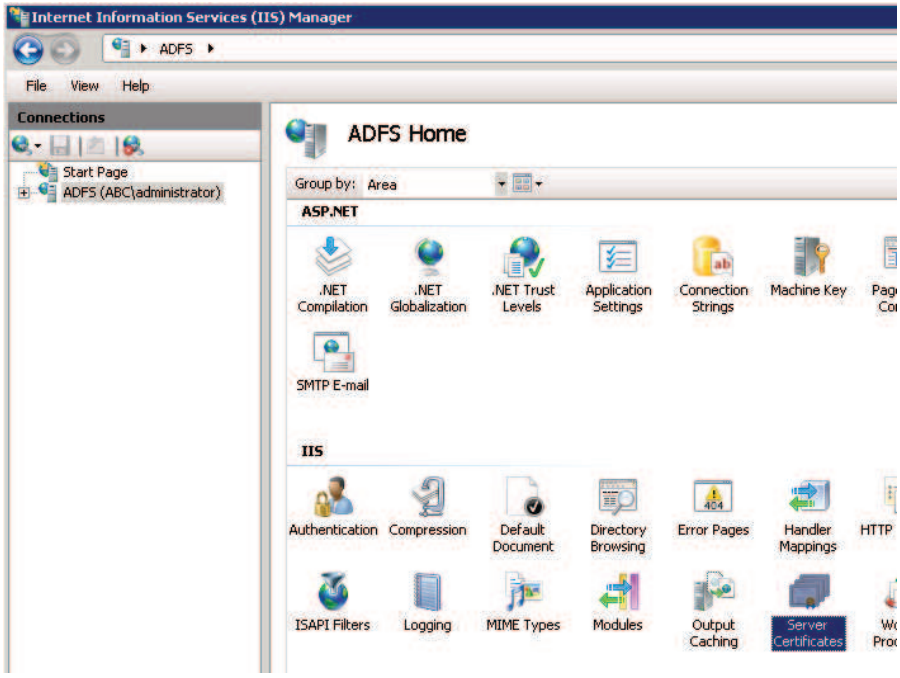
As stated in the design solution, we will implement SSO using ADFS 2.0 and test with *Internet Explorer*. We will also enable Integrated Windows Authentication (IWA) for IE so users do not have to log into WebEx if they have already logged into the domain on their PC. Since Active Directory Federation Services (ADFS) 2.0 is not supported on a domain controller, we have another VM we will use as Customer ABC's SAML server (adfs.abc.com), which also has IIS server (required for ADFS). Outside of a lab environment, an ADFS architecture might be performed using several servers including servers in a DMZ. But for this lab, we will keep it simple and utilize a single ADFS server. Company ABC's ADFS server will act as the Identity Provider (IdP) - or "Federation Server", or "SAML Server". We will configure the SAML as "Service Provider Initiated" where users start at the WebEx meeting site and are redirected to their IdP system (ADFS 2.0 Server) for authentication. The IdP authenticates the user and sends a SAML assertion back to the WebEx Meetings Server. The majority of WebEx customers use this method. **Some steps have been performed for you to reduce lab time. These steps are in bold GREEN.**

6.1 Installing and Configuring Windows 2008 ADFS 2.0 as the SAML Server

1. **Since IIS is required for ADFS, this was added as a role on adfs.abc.com server. This step is not shown.**

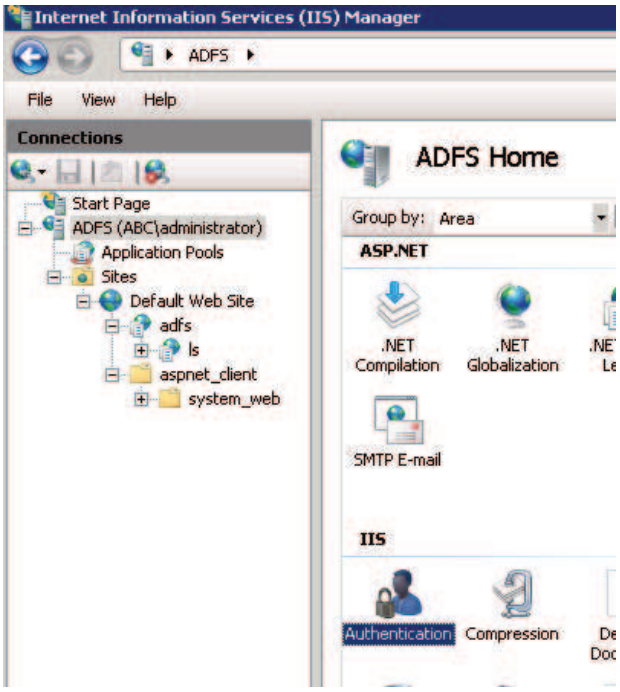
2. **ADFS 2.0 is not native to windows 2008 as a role to be added to the server. It must be downloaded and installed on the server. This step is not shown.**

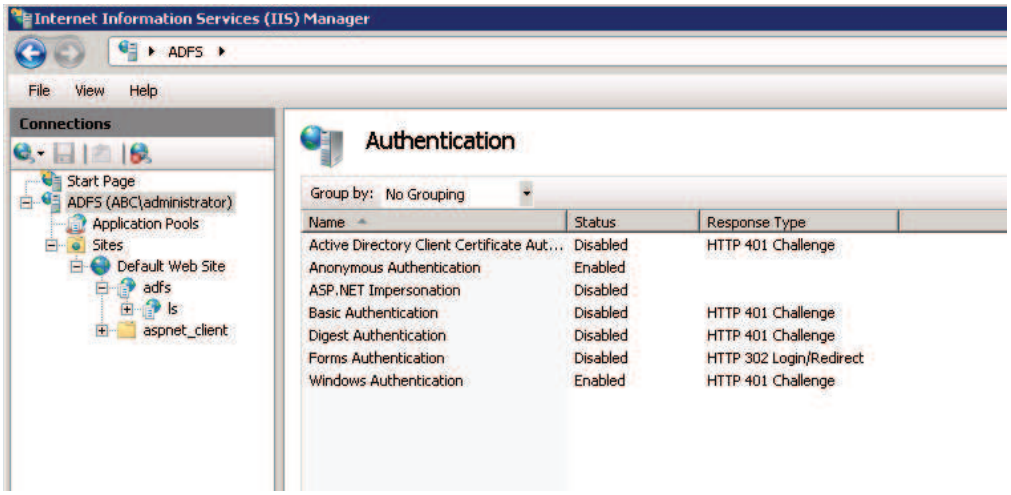
3. RDP into the ADFS server and log in as Administrator/C1sc0123 to the abc domain. ADFS requires a certificate. Normally in a production environment, a certificate would be procured or generated from PKI. Because we are in a lab, we will generate a self-signed certificate. Open IIS by clicking on the IIS Manager ICON on the desktop. Click on **ADFS (ABC\administrator)** top level tree in the left pane, and then open **Server Certificates**. On the right, click on **Create Self-Signed Certificate** and specify a **friendly name** for the certificate when asked. Then minimize IIS Manager.



When done generating the self-signed cert…

4. Now, we need to enable Windows Authentication on all Web Sites in IIS for the ADFS server. Go back to IIS Manager, click on the main **ADFS (ABC\administrator)** tree in the left pane (top level), double-click on the **Authentication** icon in the middle pane, and enable **Windows Authentication.** Afterwards, minimize IIS Manager.

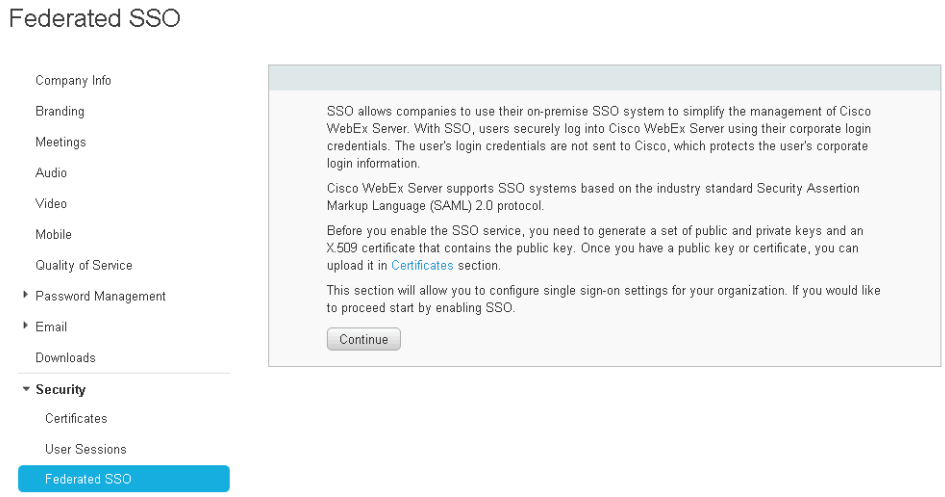




Return to Table of Contents

6.2 Configuring WebEx Meetings Server and ADFS 2.0 for SSO Operation

1. From the ADFS Server in the CWMS administrative screens, click on **Settings**, and expand **Security** on the left hand side. A message explaining SSO will come up where you simply click on Continue.

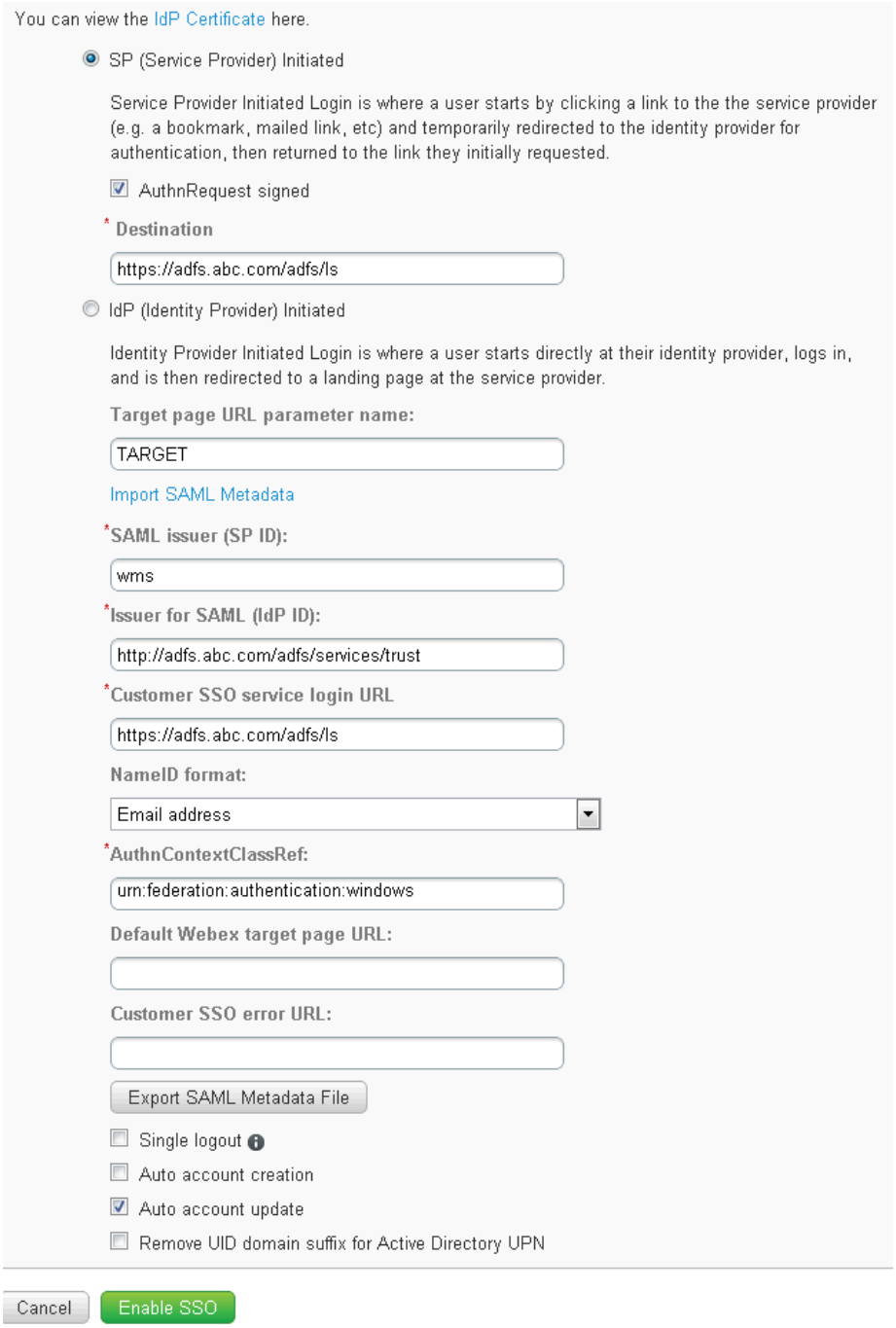


2. While inside the SSO Configurations screen, fill in the following as shown **EXACTLY**. Failure to do so will result in errors. For now, do not select Auto Account Creation . Finally, click on the **Enable SSO** button:

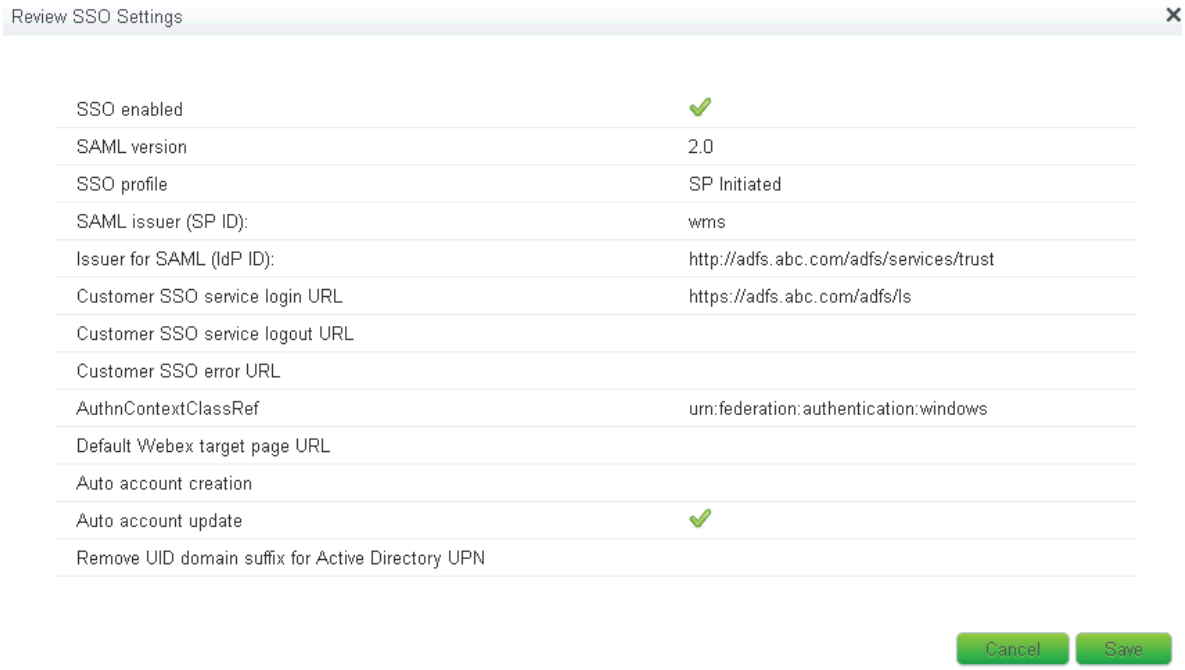
   Note that the **SAML Issuer (SP ID)** is actually just a name or a tag and can be anything, however it must be reflected accurately in ADFS in order for SSO to function properly. For your cut and pasting pleasure:

AuthnRequest Signed Destination	https://adfs.abc.com/adfs/ls
Target Page URL parameter name	TARGET
SAML issuer (SP ID)	wms
Issuer for SAML (IdP ID)	http://adfs.abc.com/adfs/services/trust
Customer SSO Service Login URL	https://adfs.abc.com/adfs/ls
NameID format	select “Email address”
AuthnContextClassRef	urn:federation:authentication:windows

Auto Account Update on



3. A “Review SSO Settings” dialog box will appear. Review your settings and click on **Save**. SSO enablement does not require CWMS to be in Maintenance Mode. Also, this will not affect the administrator password which will stay local. If you have issues saving, switch browsers.

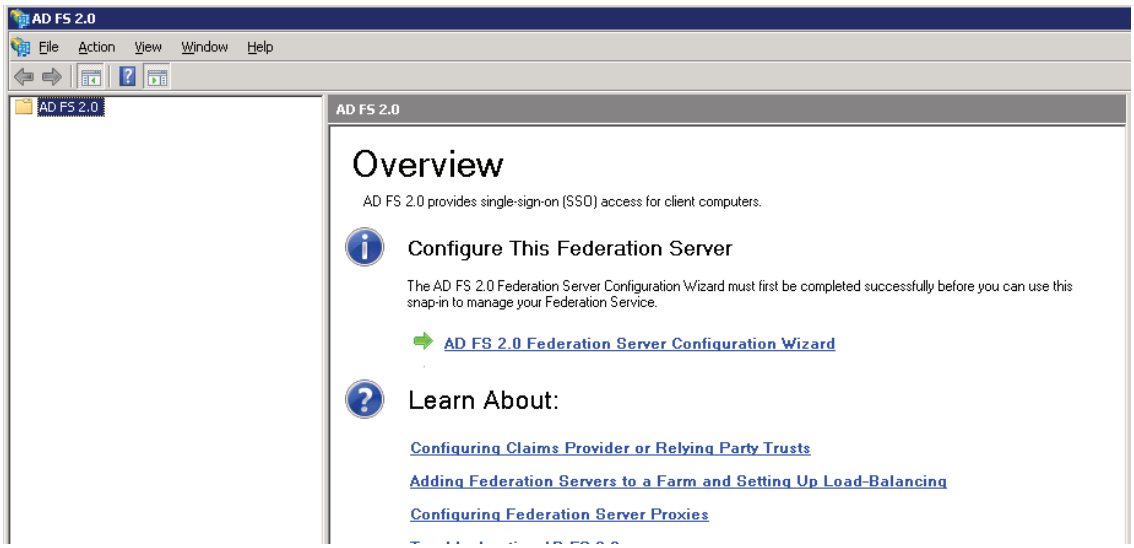


4. Next, we will export the ***signed*** Metadata from WebEx Meetings Server so we can simplify the ADFS configuration in a later step. Since it is signed, we will not have to separately import a certificate on the ADFS server. While still RDP'd into your ADFS server and in the **Federated SSO** configuration screen, click on the **Export SAML Metadata File** button and save the .xml file onto the desktop when asked (not shown). You can minimize this browser after you have saved the file.

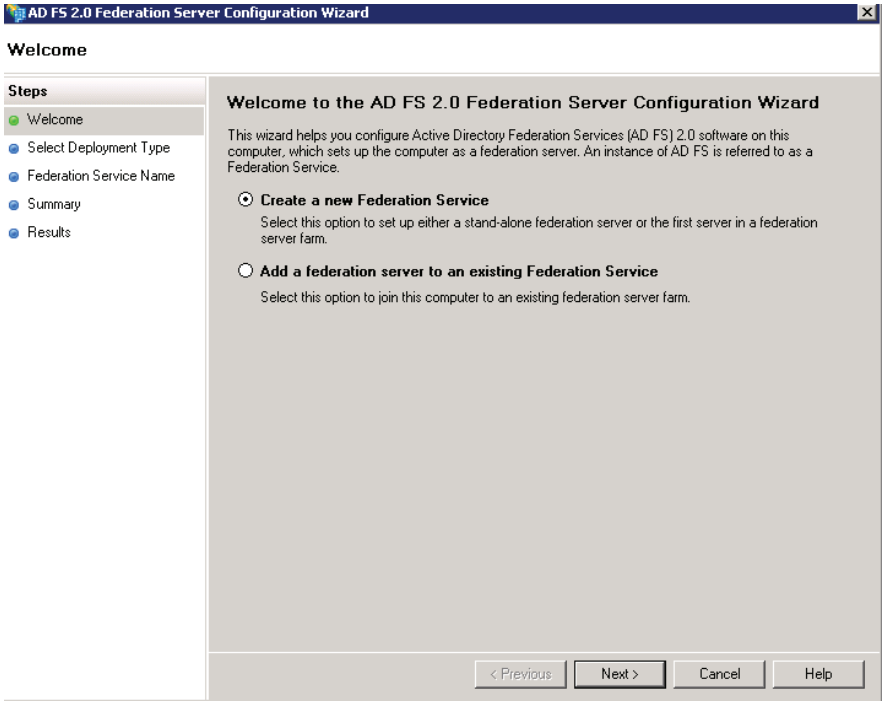
5. Now, we would normally begin the ADFS 2.0 installation, however ADFS 2.0 was already installed for you. Proceed to the next step.

6. Double click on the ADFS **2.0 Management** icon on your desktop.

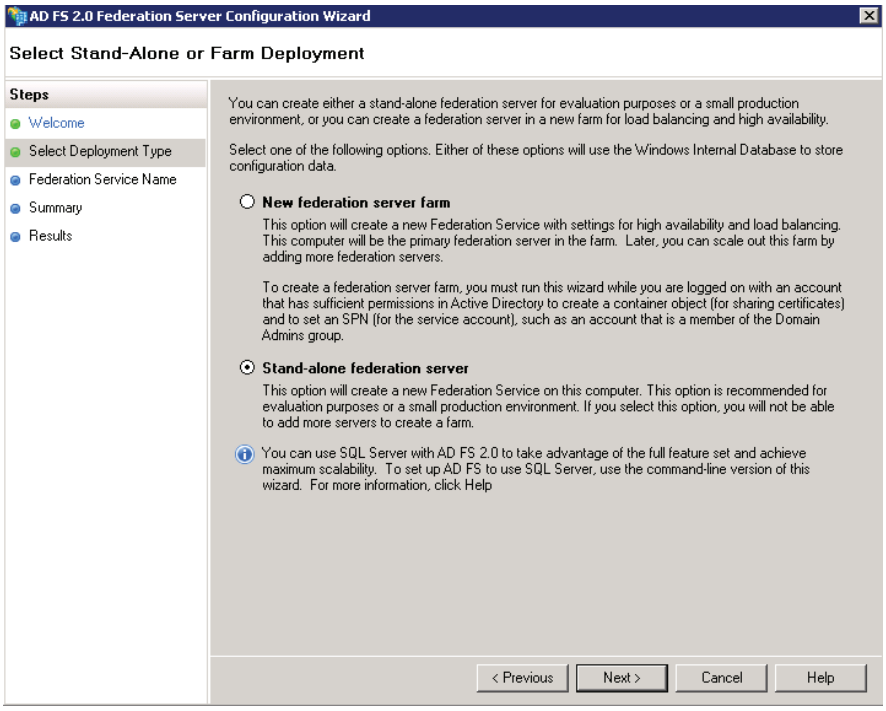
7. ADFS knows it's not fully configured, so click on the **AD FS 2.0 Federation Server Configuration Wizard** in the middle of the window.



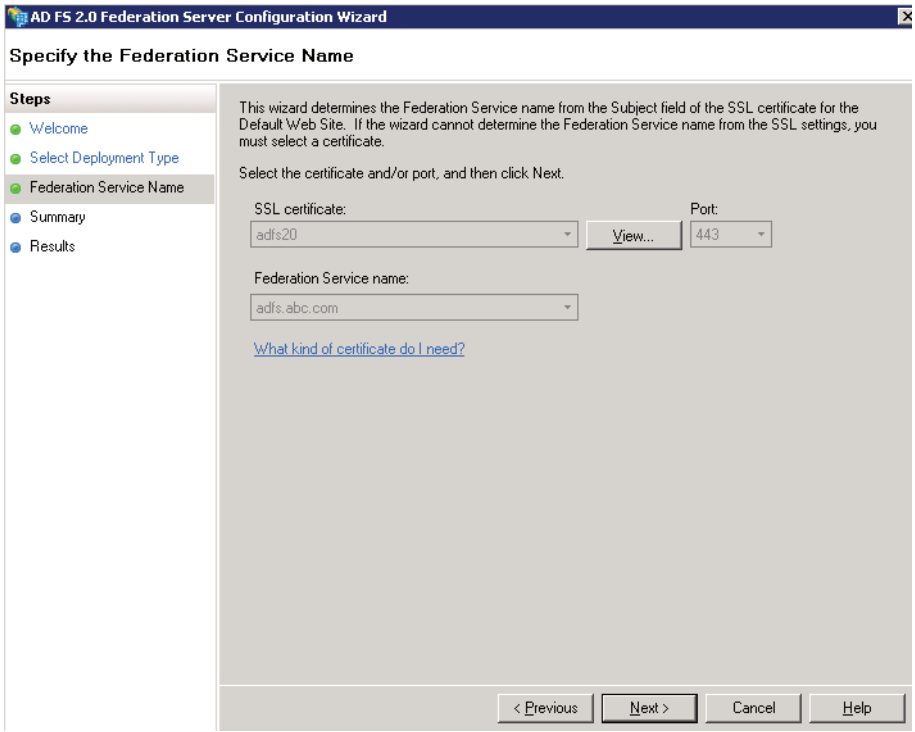
8. You will see the wizard pop up. Leave **Create a new Federation Service** selected, and click on **Next.**



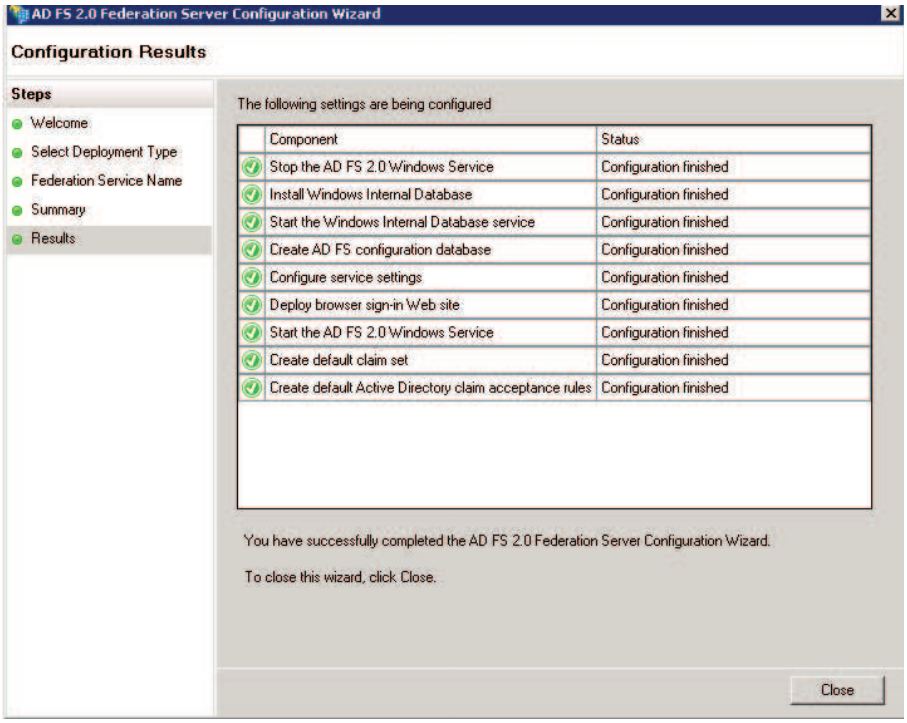
9. Select **Stand-alone federation server**, and click on **Next.**

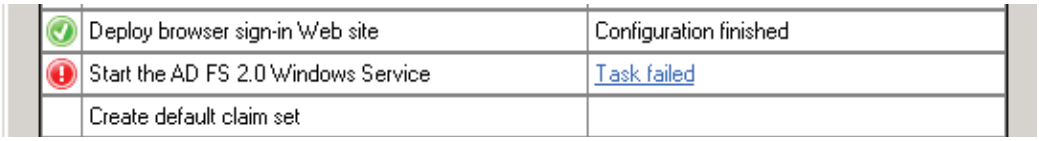


10. As you can see, the certificate we generated before is in **SSL Certificate field.** Click **Next Twice.**

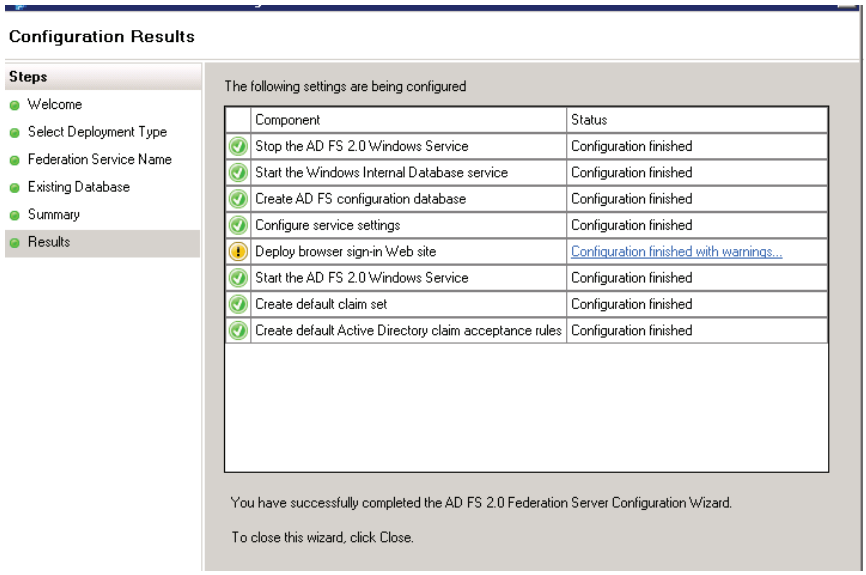


11. The wizard will begin installing the necessary components as shown below, but probably with errors. Click on **Close** when it is finished.

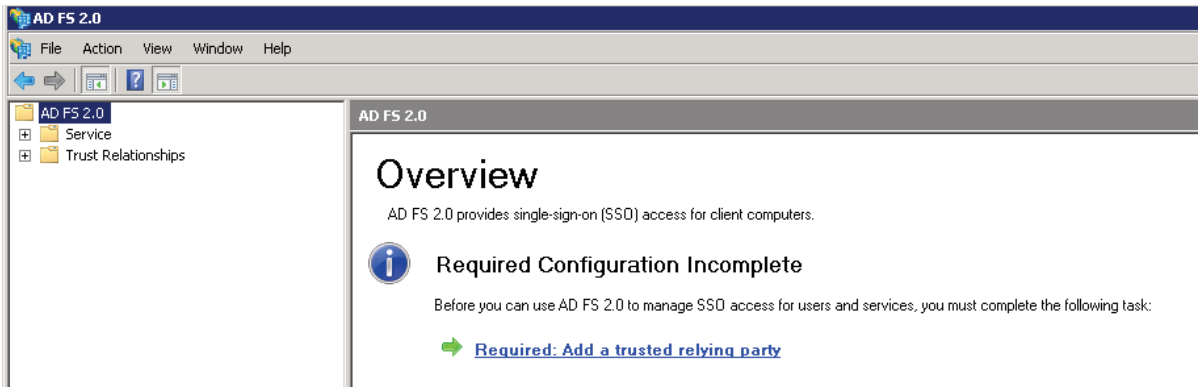




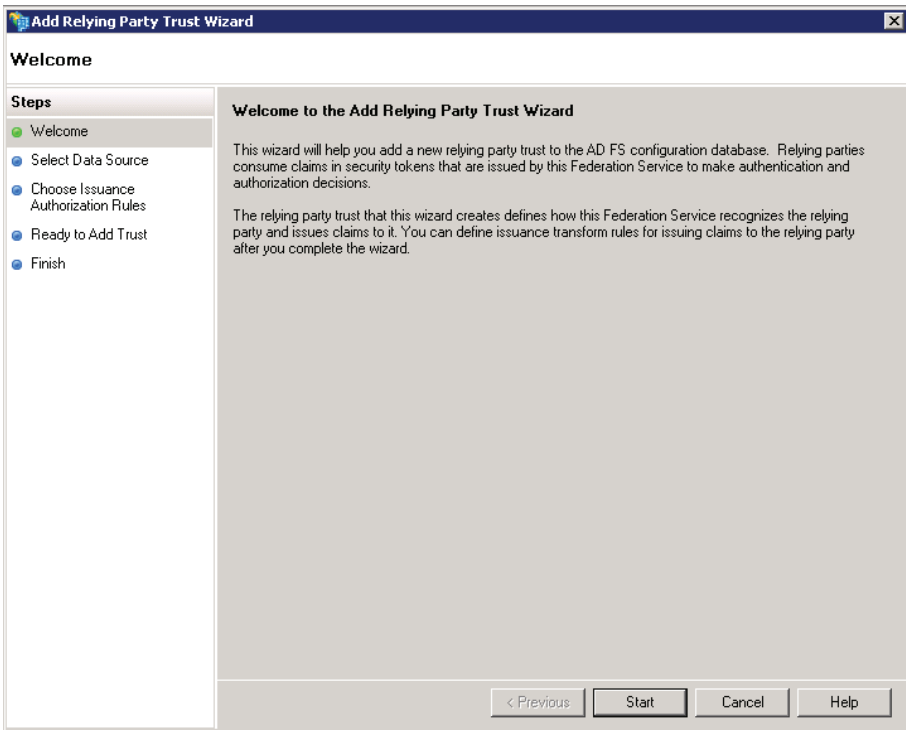
Note: If you receive an error on the "Start the ADFS 2.0 Windows Service", simply re-run the wizard, confirm the deletion of the previous database, and you should be OK (even if the configuration results show yet another Microsoft warning).



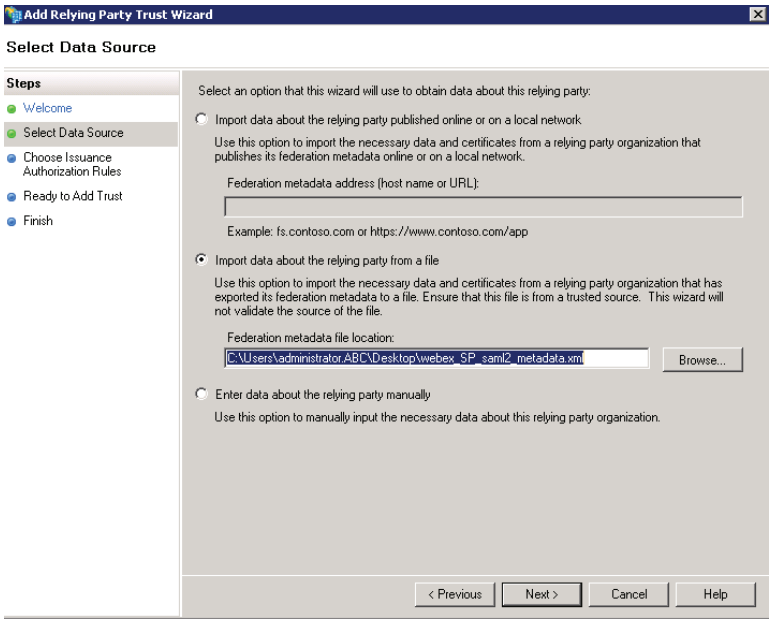
12. After it is complete, you will notice in the main ADFS 2.0 management window that it knows it has an incomplete configuration. We need to add a trusted relying party, in our case, your WebEx site. Click on **Required: Add a trusted relying party** in the middle of the screen to start a new configuration wizard, and then click **Start.**



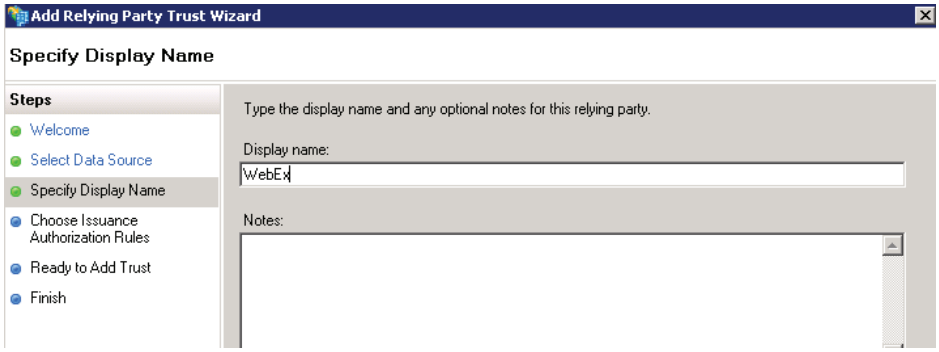
A new wizard will begin…



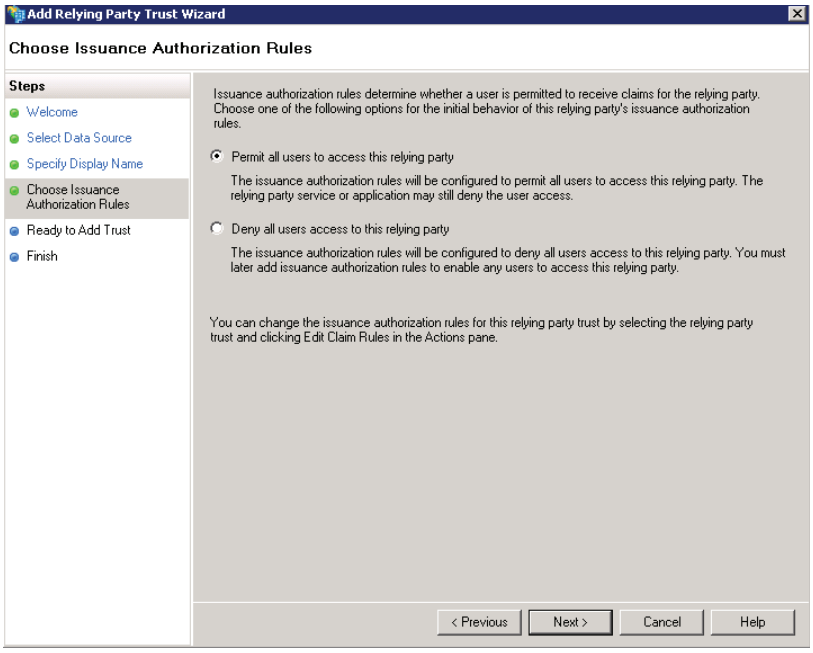
13. Next, we will "auto-configure" much of ADFS 2.0 with the WebEx SP FAS information using CWMS's SSO metadata file we saved from the previous step. Therefore, select **Import data about the relying party from a file**, browse to the .XML metadata file on the desktop and click on **Next.**



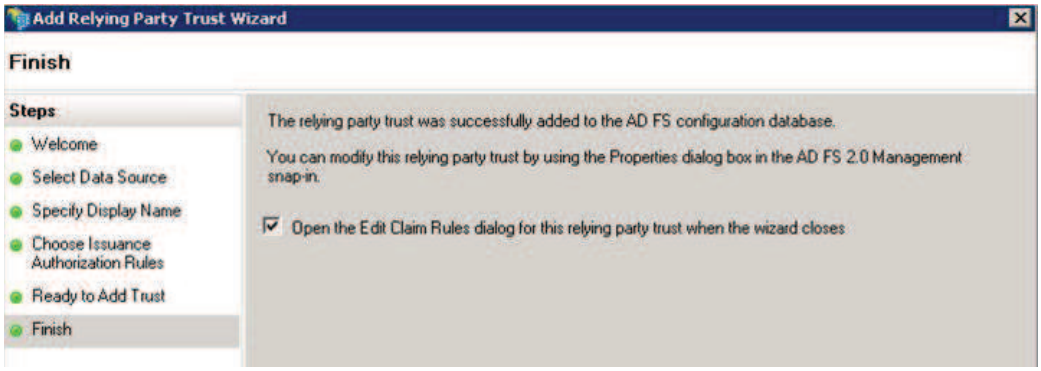
14. Give it a friendly name, like **WebEx**, and click on **Next.**



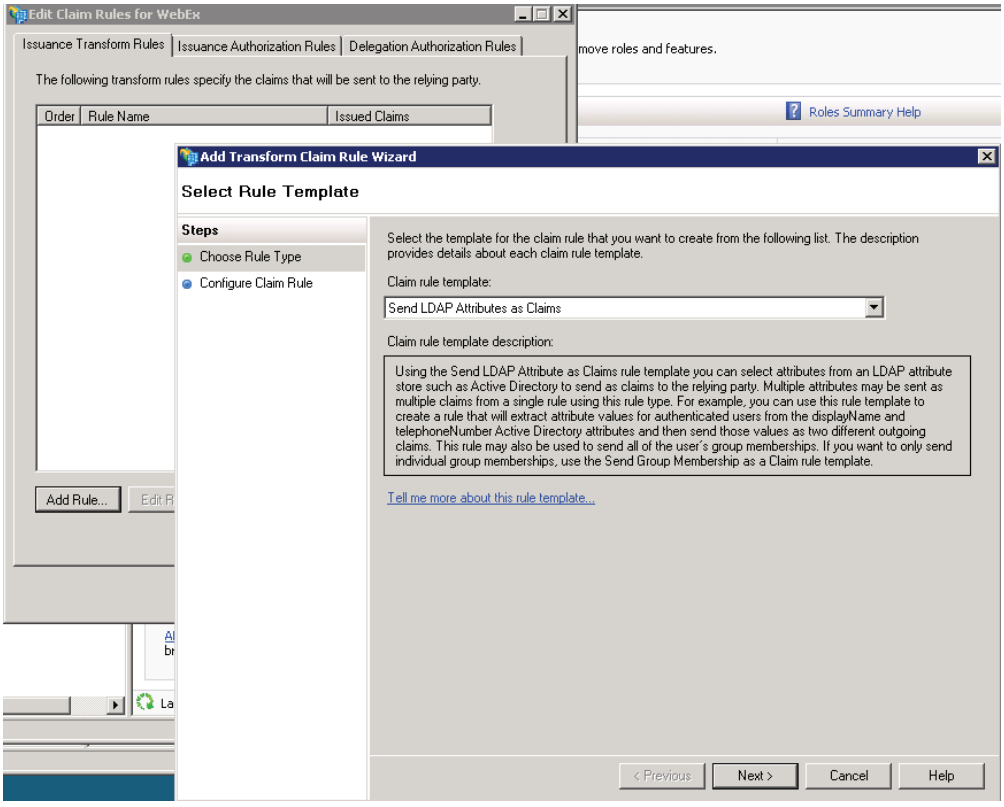
15. Leave the **Permit all users to access this relying party** radio button selected, and click on **Next *twice*.**



16. Here, leave the default checkbox selected (Open Edit Claim Rules….) and click on **Close.**

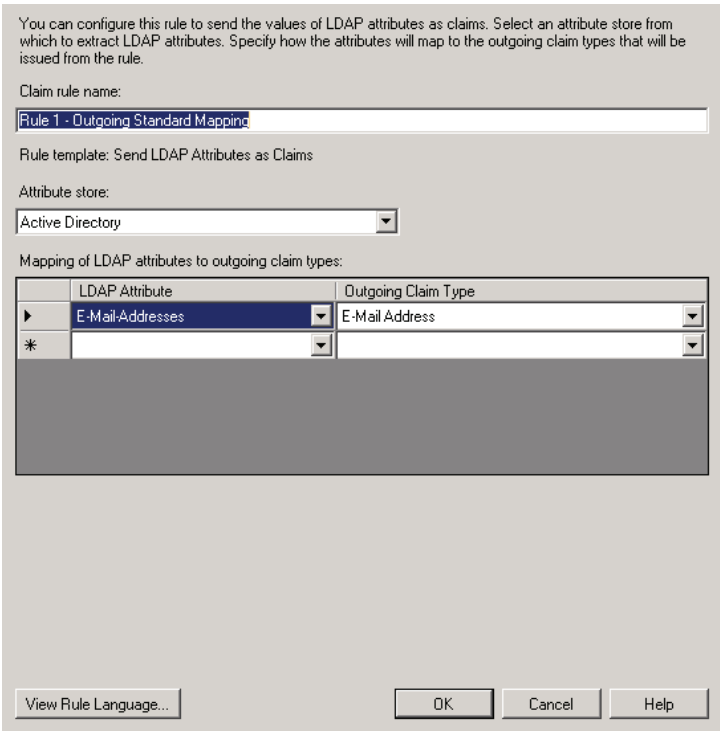


17. After the Wizard closes, the **Edit Claim Rules for WebEx** dialog box comes up ("WebEx" being the relying party we just added). This rule will map LDAP attributes to WebEx user attributes for the SAML 2.0 authentication and auto account creation process. While on the **Issuance Transform Rules** tab, Select **Add Rule**, then you will see the following:

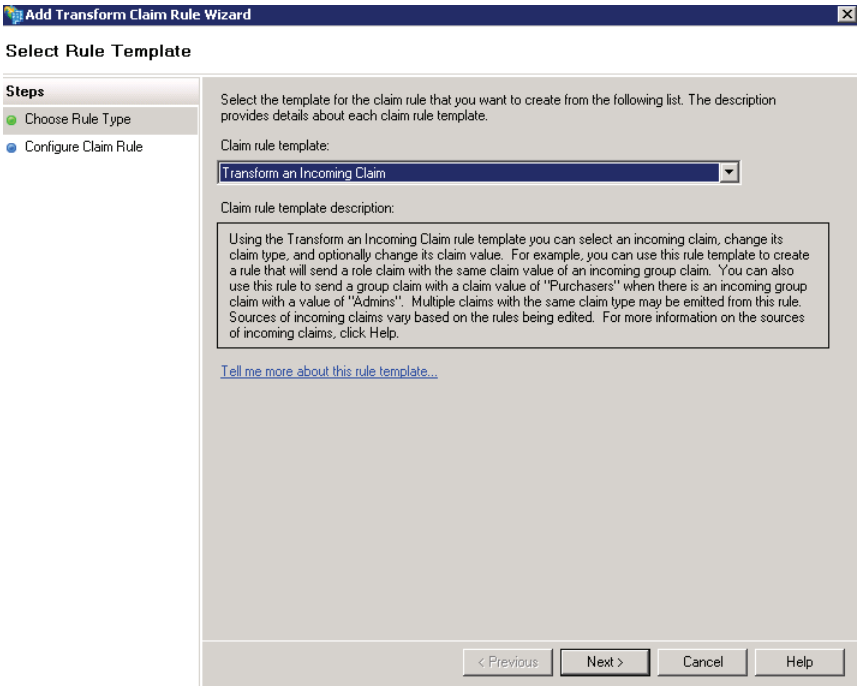


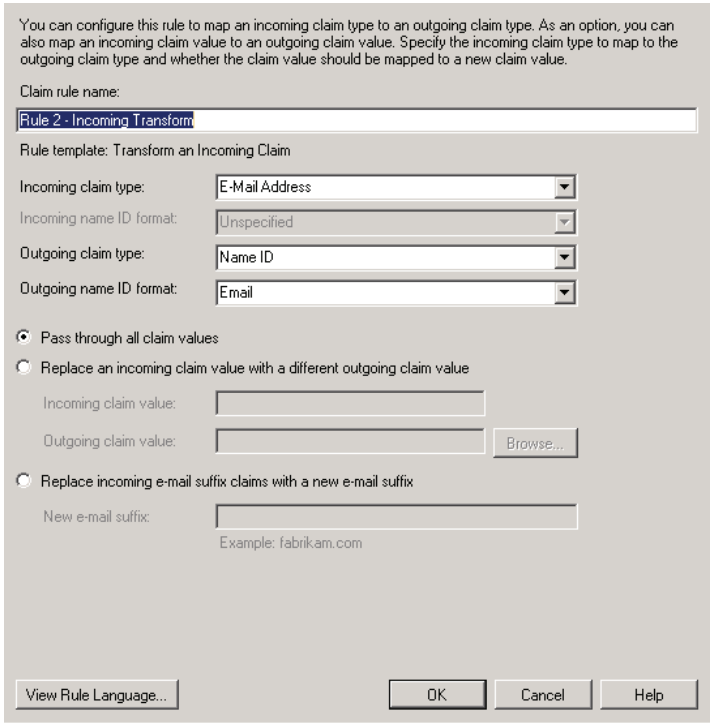
18. We will create 3 rules. Not all entries are in the drop down box and must be typed out. Create the rules *exactly* as follows

a. After clicking Add Rule as shown above, leave the Claim rule template as "**Send LDAP Attributes as Claims**" and click on **Next** (shown above). Now fill the rest out as follows and click on **OK**:

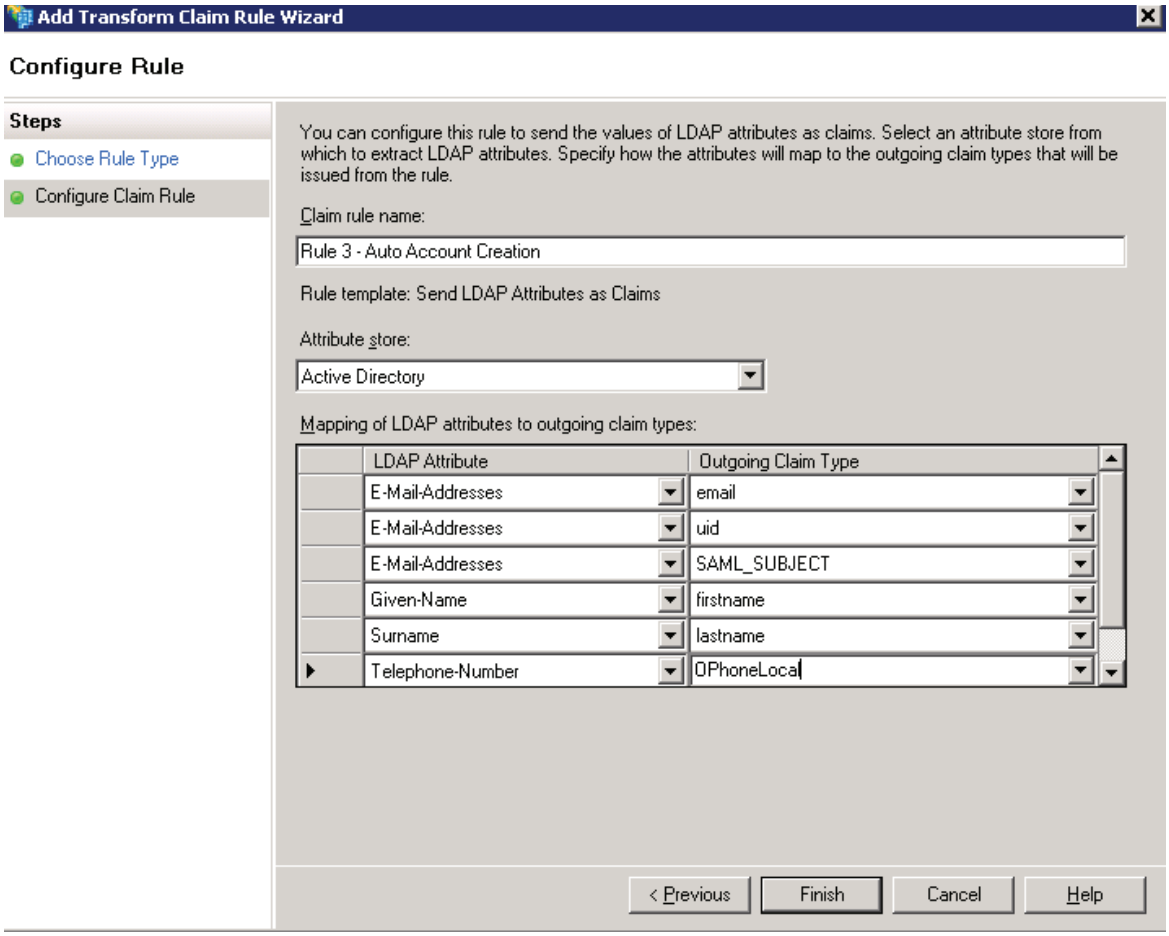


b. Click on **Add Rule** again, but this time select **Transform an Incoming Claim**, click on **Next** and fill out the rest of the entries exactly as shown in the second screen shot.


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Claim rule template:
Transform an Incoming Claim
Claim rule template description:
Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.
Tell me more about this rule template...
< Previous
Next >
Cancel
Help

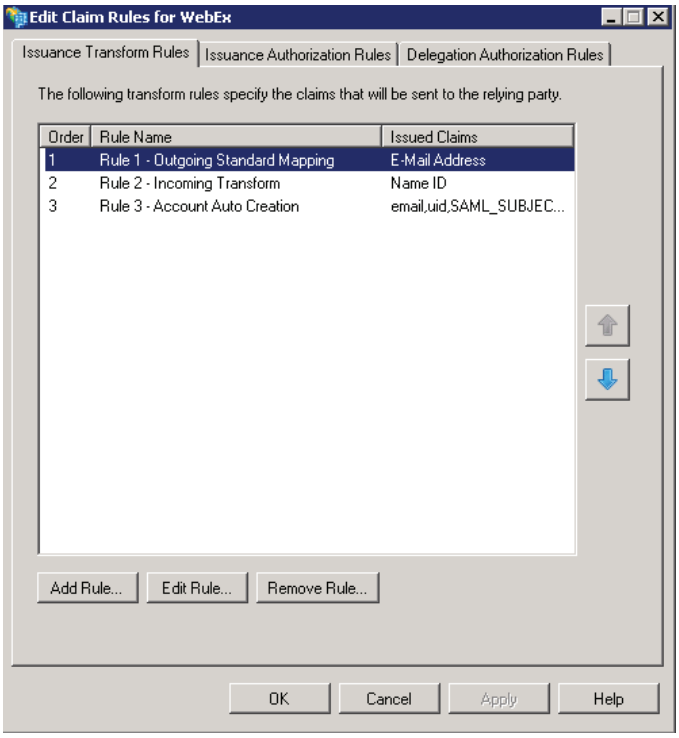

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.
Claim rule name:
Rule 2 - Incoming Transform
Rule template: Transform an Incoming Claim
Incoming claim type:
E-Mail Address
Incoming name ID format:
Unspecified
Outgoing claim type:
Name ID
Outgoing name ID format:
Email
Pass through all claim values
Replace an incoming claim value with a different outgoing claim value
Incoming claim value:
Outgoing claim value:
Browse...
Replace incoming e-mail suffix claims with a new e-mail suffix
New e-mail suffix:
Example: fabrikam.com
View Rule Language...
OK
Cancel
Help

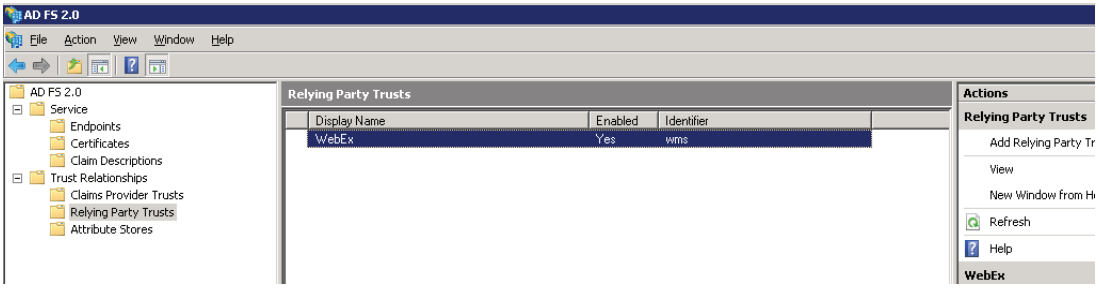
c. For your third and final rule, clicking Add Rule as shown above, leave the Claim rule template as "**Send LDAP Attributes as Claims**" and click on **Next** and fill out the mappings exactly as follows (note that the outgoing claim types must be typed in much of the time, as it all depends on the schema on the remote end), then click on **OK**:



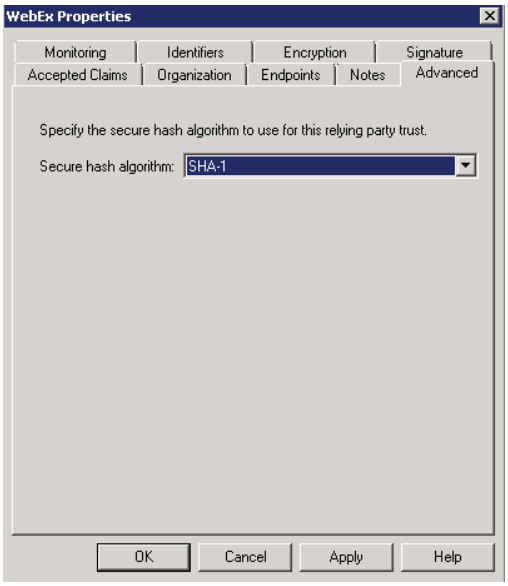
Note: CWMS, like WebEx in the cloud, out-dials the country code plus the phone number. The TelephoneNumber AD attribute is the typical attribute where office phone numbers exist. In the above mapping, this can be changed to any AD attribute of your choosing. AD actually has no native attribute for country code, which is a standard LDAP field WebEx Meetings Server is expecting in conjunction with the phone number (the combination of which is standard E.164 format). Therefore, what is displayed above maps user's numbers in AD (which don't have a "+1" in it). CWMS server, using the +1 default country code as a default value, combines this and uses it for out-dialing. If your TelephoneNumber AD attribute has a +1 in it, then have your AD team write a script to populate another attribute field with the same number without the country code or special characters, then use this attribute for the mapping. This way, the phone number will be right when CWMS tries to out-dial the number. CWMS, at the time of its release, should handle the special characters. Therefore, the solution could also be handled in CUCM using translation patterns.

d. You should see the following when complete. Select **OK** again

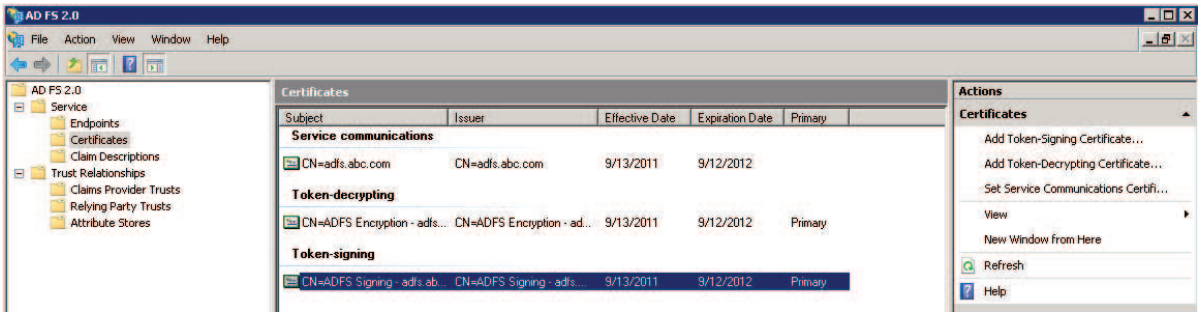




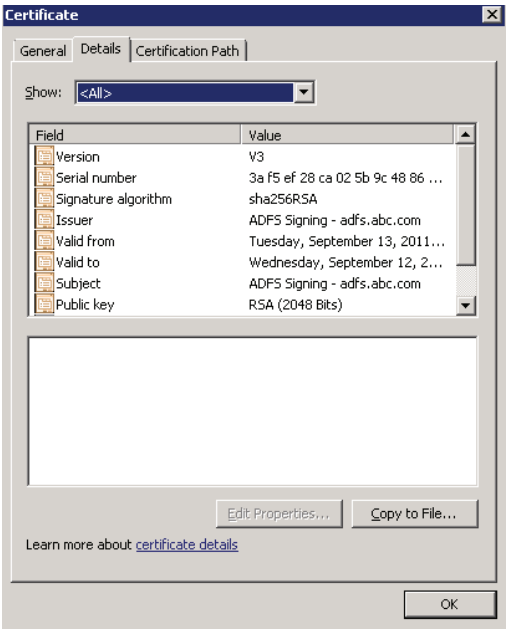
19. Double click on the the **WebEx** relying party trust to open the properties box, select **Advanced**, and change the **Secure hash algorithm** to **SHA-1**. Then click on **OK.**

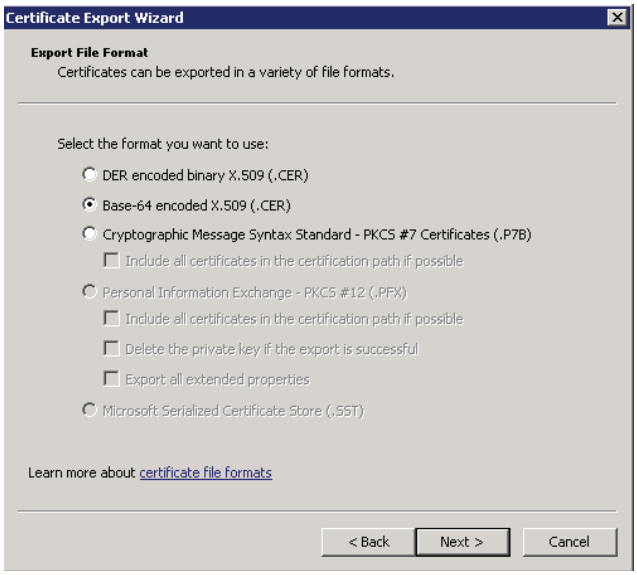


20. Now, since we generated a self-signed certificate in IIS earlier (instead of buying one or getting one from our non-existent Public Key Infrastructure), we need to export the Token-Signing key used by ADFS 2.0 for import into WebEx Meetings Server in a later step. In the left pane, expand **Service** and select **Certificates**, then double click on the **Token-signing** certificate.

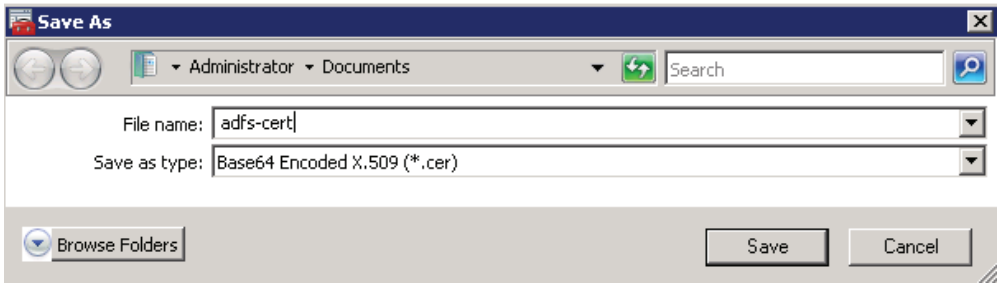


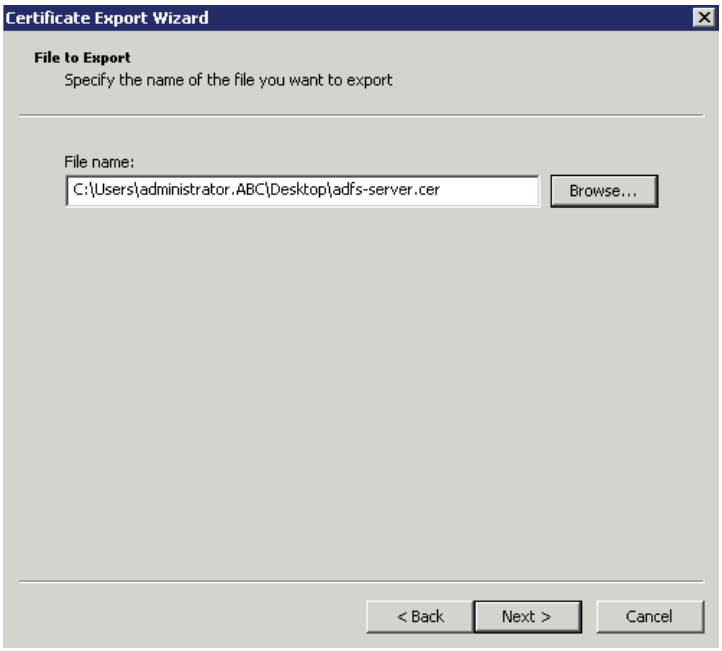
21. Click on the **Details** Tab of this certificates information window and click on the **Copy to File** button to start the **Certificate Export Wizard.** Then click on **Next** twice, making sure it is **BASE-64 Encoded X.509.**





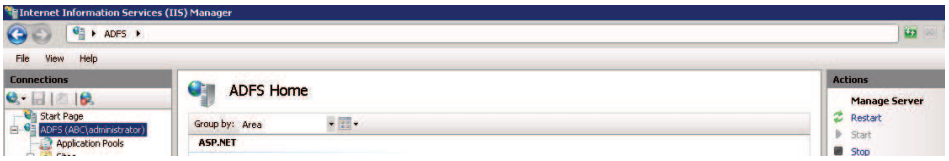
22. Save the file to the desktop and give it a name, then click **Next** and **Finish.** You can also close the Certificate window.


Save As
Administrator ▸ Documents
Search
File name: adfs-cert
Save as type: Base64 Encoded X.509 (*.cer)
Browse Folders
Save
Cancel

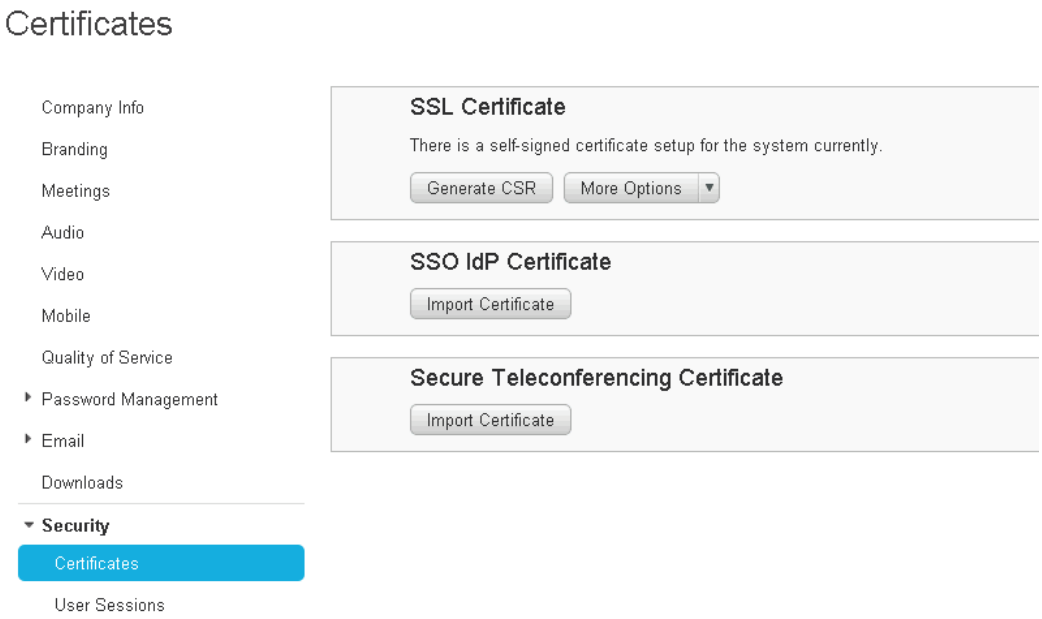

Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\administrator.ABC\Desktop\adfs-server.cer
Browse...
< Back
Next >
Cancel

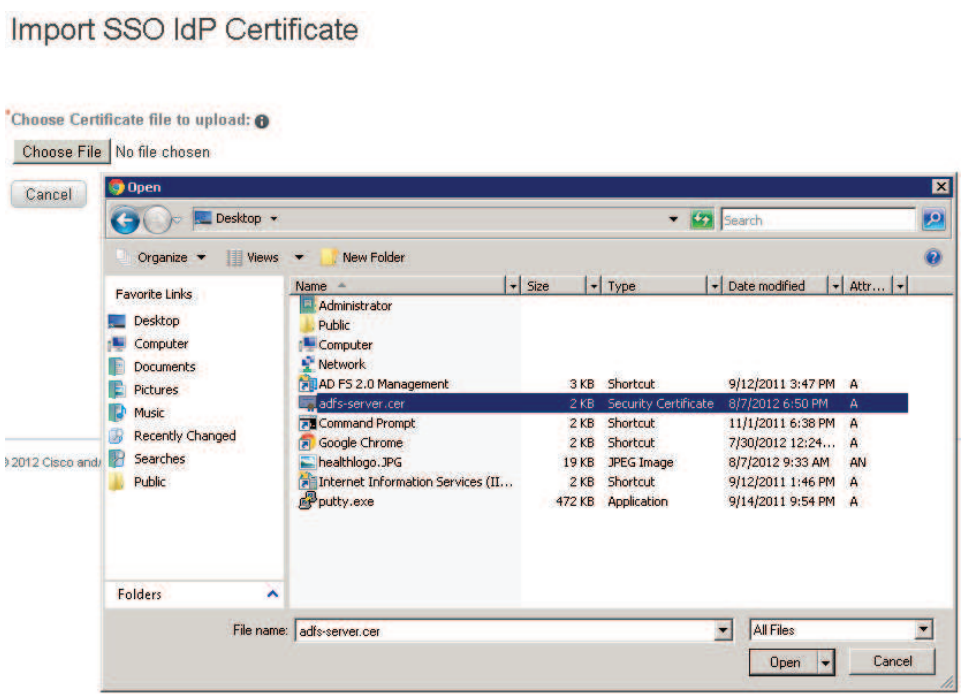

Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Use
Export Keys No
Include all certificates in the certification path No
File Format DER En
< Back
Finish
Cancel

23. After, go to **IIS Manager**, click on the main **ADFS (ABC\administrator)** tree in the left pane (top level) again, and click on **Restart** on the right side of the window to restart IIS.



24. On your ADFS Server, maximize your CWMS Admin browser and go back to your **SSO configuration** in the administration pages. Under **SSO IdP Certificate**, **import** the newly exported ADFS server certificate that is currently on your desktop. Browse to the desktop, choose the certificate, and click on **Open** and then click on **Upload**. When finished, click on **Done** as shown below:



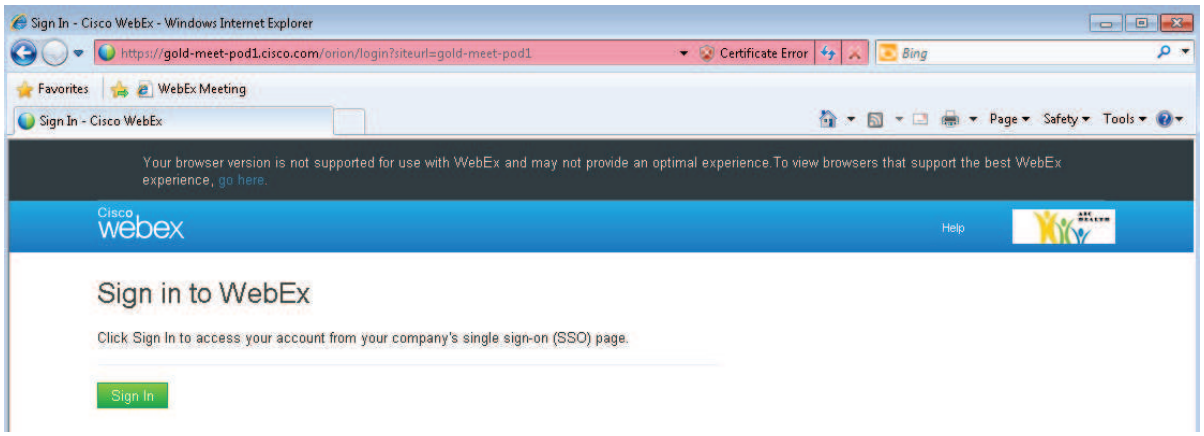


Return to Table of Contents

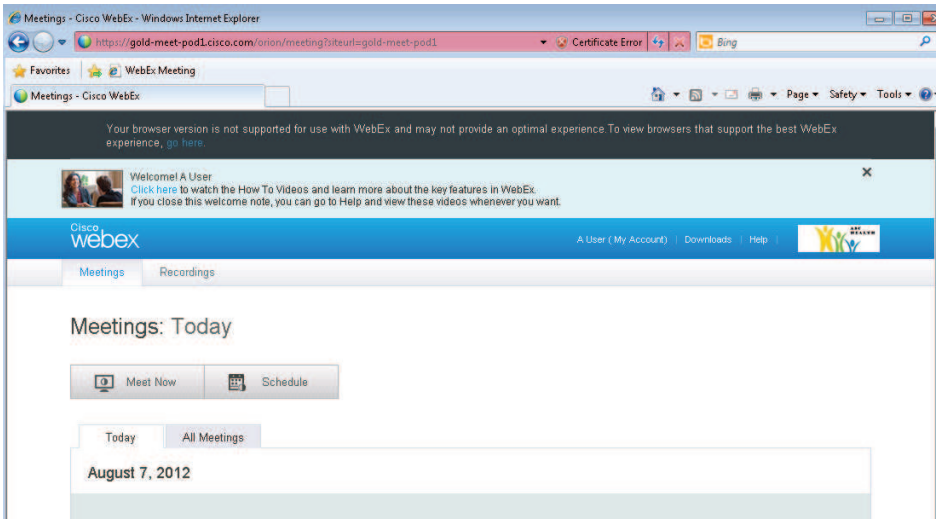
6.3 Testing and Fine-Tuning SSO on the Clients

We will test SSO using IE

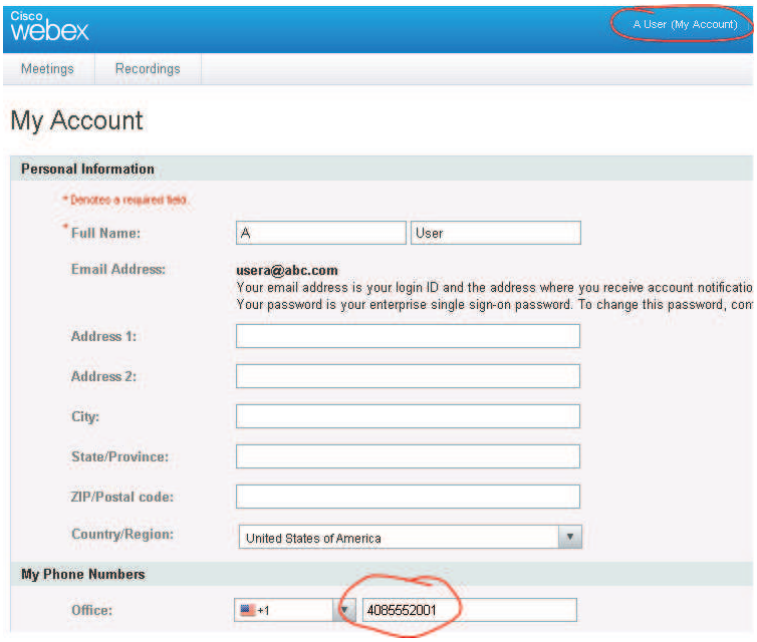
1. On **wkstn1**, open **Internet Explorer** and browse to https://gold-meet-podx.cisco.com, where **"x"** is your pod number. Accept any certificate warnings you see before and after clicking on **Sign In.**



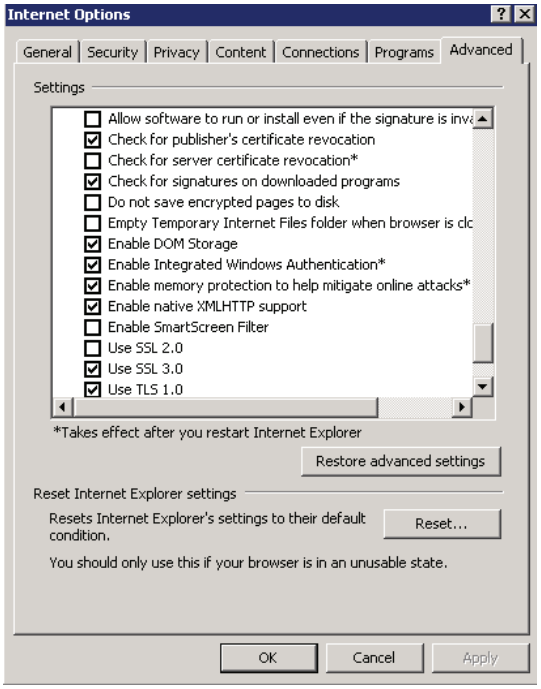
2. Hopefully, you've successfully logged in to IE. You should see the screen below. After a successful login, proceed to the next step.



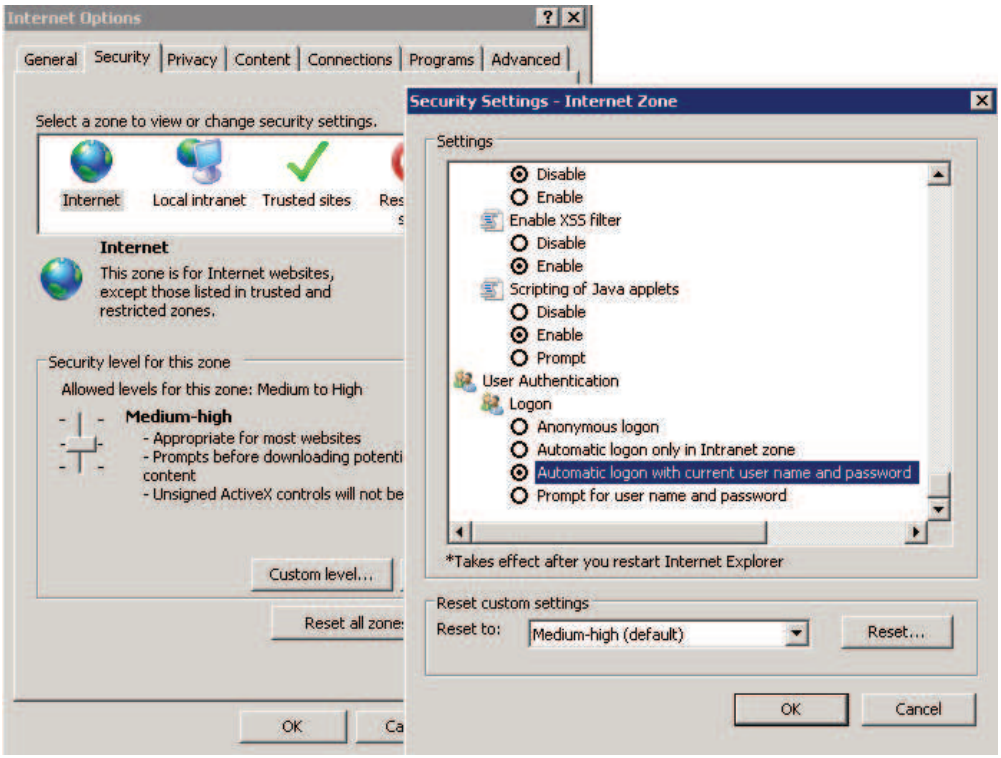
3. Click on the “My Account” link at the top right of your user page and notice that your phone number has been updated. This is because on the Federated SSO page, we selected **Auto Account Update.**



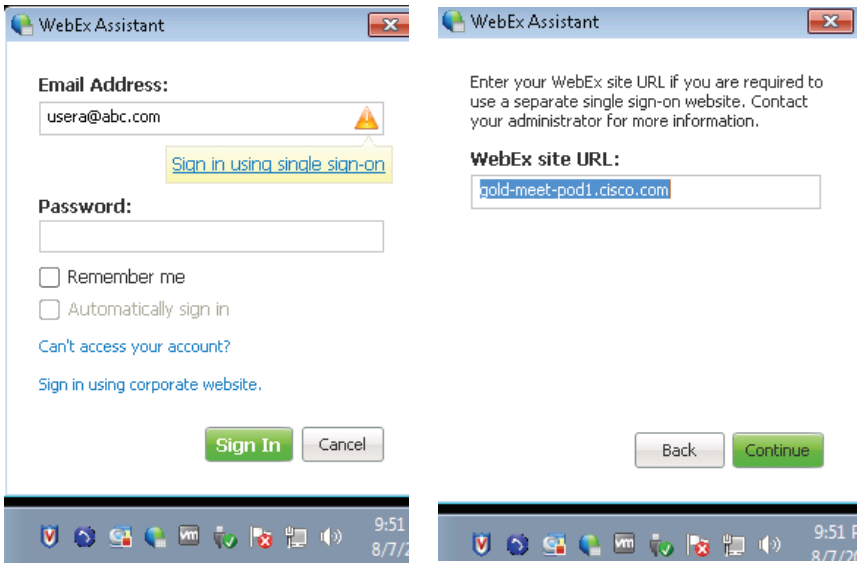
4. If you were prompted for a username and password above, its because Integrated Windows Authentication (IWA) was not on. While still in wkstn1, go to **Tools, Internet Options**, then to the **Advanced** tab. Scroll to the bottom, and note that **Enable Integrated Windows Authentication** is checked.



5. Other settings to note are as follows. Click on the **Security** tab, select the **Internet zone**, click on **Custom Level**, scroll to the bottom, and select **Automatic logon with current user name and password**. Select **OK**, then select **yes** when the warning pops up. Do the same thing for the **Local Intranet**. When finished, select **OK** to close the **Internet Options** window and **close down IE completely.**



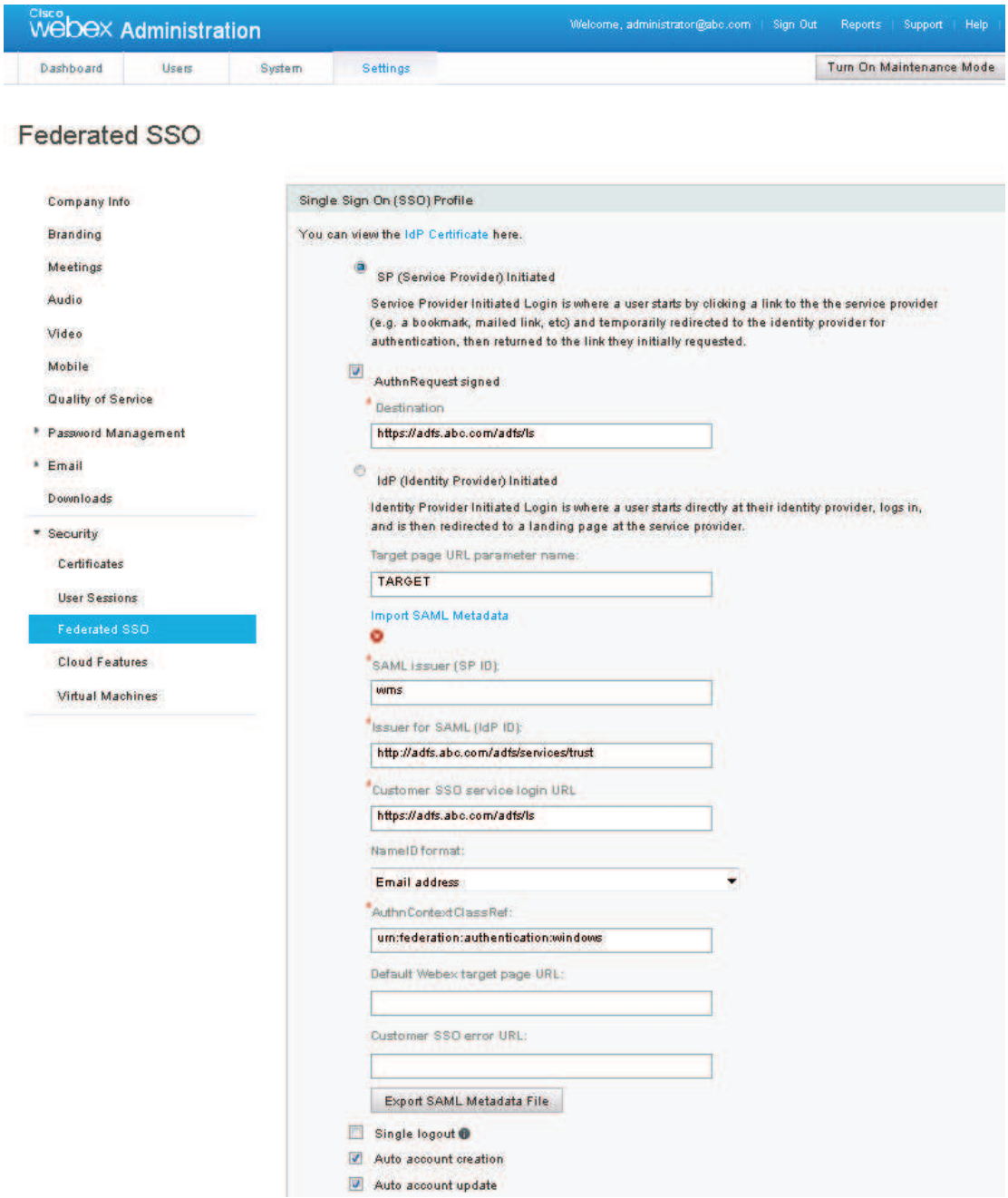
6. Now, go ahead and fix WebEx Assistant (running in the system tray) which, depending on timers, is currently trying to log in, or is idle. If it is not in error, right click on it and **sign out.** If it has already popped up in error (trying sign in with the old local password for usera, but failing), click on "**Sign in using single sign-on**" and make sure that **gold-meet-podx.cisco.com** is in the WebEx site URL field. Then click **Continue** and accept any certificate warnings.



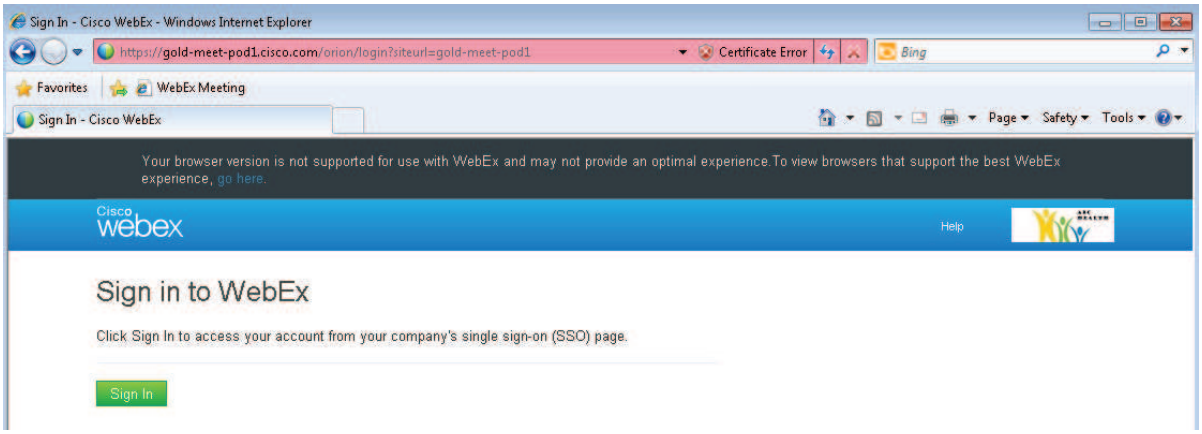
7. You have completed WebEx SSO. Now, we will work on the rest of the user(s) while enabling auto account creation.

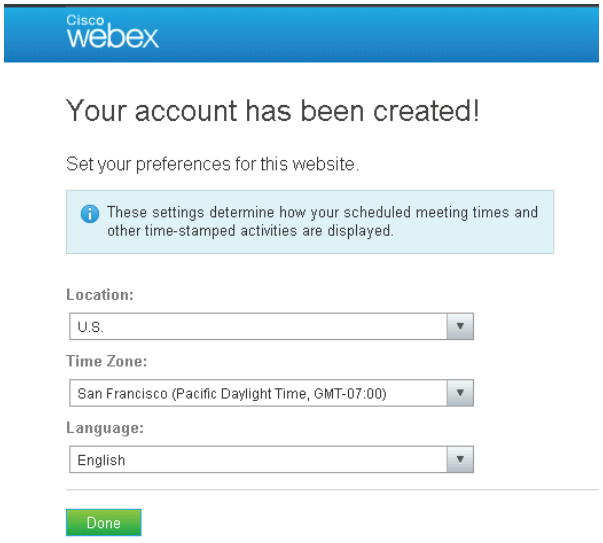
6.4 Auto Account Creation with SSO

1. Where ever you are, browse to the meetingsadmin.abc.com and go to the SSO section under Settings. The administrator account is always a local account and password, so use **C1sc0123*.** **Enable Auto Account Creation,** then **Save.**



2. Now, go to **wkstn2** and open up **Internet Explorer**, which is already set up for IWA. Browse to https://gold-meet-pod**x**.cisco.com, where **"x"** is your pod number. Accept any certificate warnings you see before and after clicking on **Sign In** below**.** You should not be prompted for any credentials, and you should see a screen that says "**Your account has been created**!".





3. The rest is not shown. Follow through with the setup of **WebEx Assistant** and log into it **using SSO**. Look out for any certificate warnings you need to accept, as the "Sign-in using Single Sign-On" link will not appear until the certificate is accepted. If you are asked to set preferences, go through the motions , but you will not have to do anything as SSO/AD integration will populate things for you. Refer to previous slides for WebEx Assistant configuration if needed.

4. You have completed the SSO portion of the lab

Note that it is not possible to delete users. You can only deactivate them. If you ever choose to remove SSO from the Federated SSO page, to set the local password accounts that were auto-created, simply deactivate and reactivate the user and they will be sent an email to create a password.

Return to Table of Contents