



Federated Identity Management Guide

Federated Identity Management Guide

Version: 3.0
Revision: May 2015
Contributors: Doug Leavitt - API Product Manager

About inContact: inContact, Inc. (NASDAQ: SAAS) has helped over 750 contact centers around the globe create profitable customer experiences through its powerful portfolio of cloud-based contact center software solutions. The company's services and solutions enable contact centers to operate more efficiently, optimize the cost and quality of every customer interaction, create new pathways to profit, and ensure ongoing customer-centric business improvement and growth. The inContact Platform has grown from a powerful ACD with skills-based routing, CTI, and IVR with speech recognition to include an innovative online hiring solution, workforce management functionality, and a customer feedback and survey solution. Because the inContact Platform is delivered through a Software-as-a-Service (SaaS) model, inContact customers can realize significant cost savings and flexibility compared to premises-based alternatives. To learn more, visit www.inContact.com.

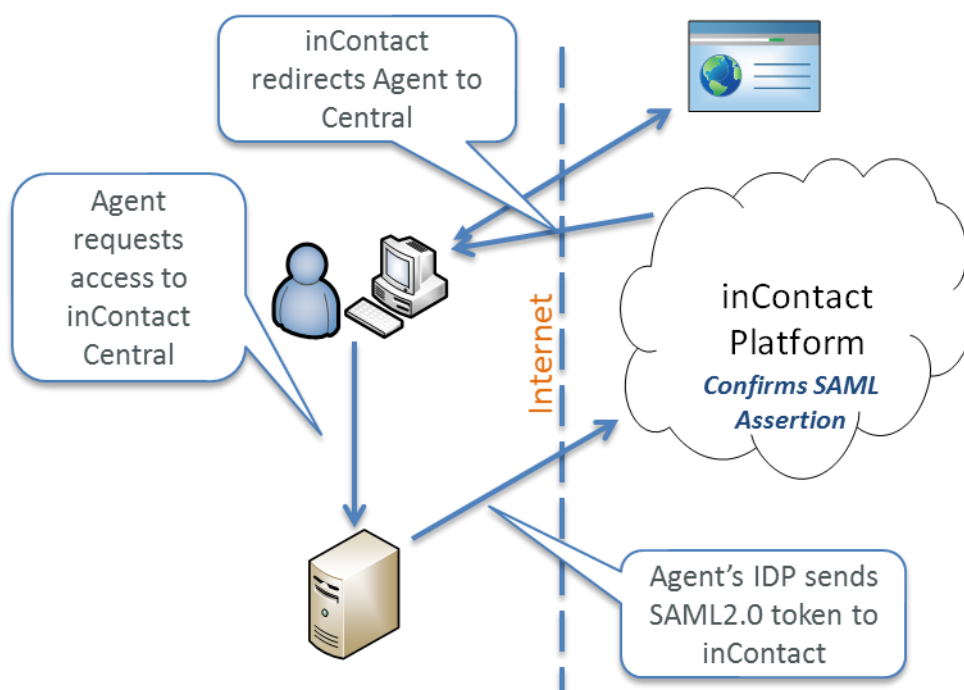
Copyright: ©2015 inContact, Inc.
Disclaimer: inContact reserves the right to update or append this document, as needed.

Contents

Federated Identity Management for inContact Central	1
Configuring your inContact Business Unit	2
Enabling Federated Identity for a Business Unit	2
Uploading Security Certificate	3
Configuring Users for Federated Identity Management.....	3
SAML2.0 Assertion Examples.....	5
Generating a Security Certificate from ADFS	8
Creating a Self-Signed Certificate from IIS	8
Importing Certificate into ADFS	9
Enabling Primary Key Access for ADFS	12
Configure a Service Provider in ADFS	15
Creating a Relying Party Trust.....	15
Configuring Claim Rules for a Trust in ADFS.....	19

Federated Identity Management for inContact Central

Federated Identity Management is the ability to use a trust relationship between your Identity Provider (IDP) authentication systems and the inContact platform through inContact Central. This capability allows your company to register its IDP with the inContact platform through the use of a secure certificate. Once this trust relationship is established, your IDP is authorized to send an Authorization assertion using the Security Assertion Markup Language 2.0 standard (SAML2.0). Upon the successful receipt of this assertion, your authenticated user will be logged into inContact Central fully authenticated from your IDP.



inContact currently supports IDP initiated authentication which means that customers or partners who want to use Federated Identity Management will ***need to provide for their Users a way to initiate the SAML2.0 assertion for login to Central***. We do not currently support a Service Provider initiated pattern, however that access pattern is under consideration for future releases.

Users can be individually configured to use Federated Identity Management, however any user that is configured to use Federated Identity Management will no longer be able to log directly into inContact Central through <https://login.incontact.com>. Once the user is logged into inContact Central through Federated Identity Management, they will have all the same privileges that they would have, if they had logged in directly to <https://login.incontact.com>.

In order to start using Federated Identity Management for inContact Central, please contact your inContact Customer Service Representative to enable this feature for your business unit and discuss in more detail your efforts to take advantage of this capability.

NOTE: It is recommended that you only enable Federated Identity Management for Users who will exclusively use Thin Agent. If you wish to use this Users who use both Thin Agent as well as other applications such as Power Agent or SFDC Agent, you will need to do some custom configuration to make that function.

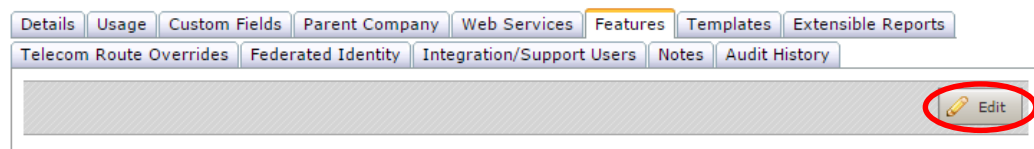
Configuring your inContact Business Unit

There are several steps you will need to take in order to use Federated Identity Management in your inContact Business Unit. You will need to do this in conjunction with your inContact Customer Support representative as this feature must be enabled by them for your Business Unit.

Enabling Federated Identity for a Business Unit

To enable Federated Identity Management for your Business Unit, you will need to request that the Federated Identity feature is enabled by contacting your inContact customer support representative.

1. Open the Business Unit configuration page by clicking on the Admin -> Business Units menu option and selecting your business unit.
2. Edit the properties from the Features tab.

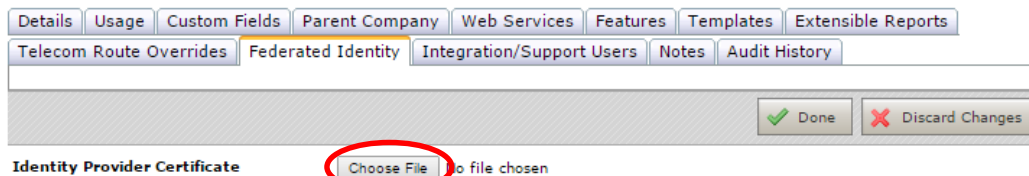


3. Under the Core section there is a feature labeled "Federated Identity" which will need to be enabled.

Uploading Security Certificate

Once you have enabled the Federated Identity Management feature for your Business Unit, you will need to upload a Security Certificate that you will use when you send the Authentication assertion from your IDP.

1. Open the Business Unit configuration page by clicking on the Admin -> Business Units menu option and selecting your business unit.
2. Open the properties from the Federated Identity tab and select Choose File for the Identity Provider Certificate.



3. Select the Security Certificate that is generated from your IDP system. For this guide we will provide you with instructions on how to generate a Security Certificate using Active Directory Federation Services.

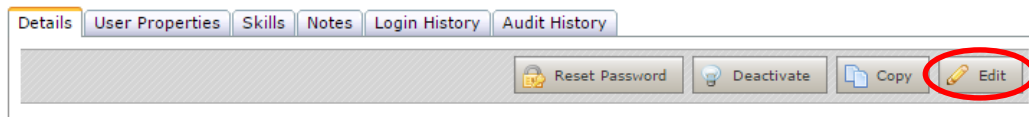
NOTE: If you are using ADFS as your Identity Provider with IIS you will find instructions on how to create a security certificate from IIS and import it into ADFS at [Generating a Security Certificate from ADFS](#).

Configuring Users for Federated Identity Management

Once you have uploaded the security certificate that you will use to send an authentication assertion to the inContact platform, you will need to configure each user that you want to use Federated Identity Management to have a Federated Identity value that will be used to identify the user from the authentication assertion.

NOTE: If a user is configured with a Federated Identity value, they will no longer be allowed to login directly at <https://login.incontact.com>. They will only be able to login through your IDP initiated authentication request.

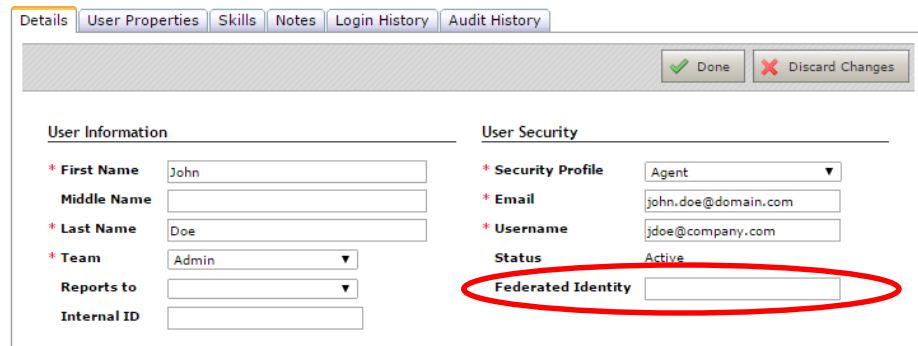
1. Edit the User configuration page by clicking on the Manage -> Users menu option and selecting the existing user or creating a new user and modifying the Details tab.



2. In the Details tab you will see a value called Federated Identity. In this field you must enter the unique value that will be passed in as part of the authentication assertion. This value will need to be tied to the user requesting access to inContact in your IDP system.

NOTE: When your IDP makes an Authentication Assertion to the inContact platform it **MUST** contain an LDAP claim with the same Federated Identity value configured for the user. The claim values being:

- “Name ID” - Required and must match Federated Identity
- “SecurityProfileID” – Optional and must match a valid security profile in your Business Unit. This security profile will be mapped to your inContact user and used going forward. If no claim is present, the current security profile mapped to this user in inContact Central will be used.



The screenshot shows the 'Details' tab of a user profile in the inContact system. The form is divided into two main sections: 'User Information' and 'User Security'. The 'Federated Identity' field in the 'User Security' section is highlighted with a red oval.

User Information	User Security
* First Name: John	* Security Profile: Agent
Middle Name:	* Email: john.doe@domain.com
* Last Name: Doe	* Username: jdoe@company.com
* Team: Admin	Status: Active
Reports to:	Federated Identity:
Internal ID:	

SAML2.0 Assertion Examples

Federated Identity Management will support any Identity Provider that can send the appropriate SAML2.0 assertion. We have provided a sample Metadata and Assertion that you can use to model the SAML2.0 assertion needing to be created from your Identity Provider.

SAML2.0 Metadata Example:

```
<md:EntityDescriptor
  ID="_7D262754554DAB8B49CDE184EF7809E6"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#_7D262754554DAB8B49CDE184EF7809E6">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <InclusiveNamespaces
            PrefixList="#default md saml ds xs xsi"
            xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>dg2D+g0AmFCkBDhndILImCj0Mw=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>DV7J...DbWA==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIC...dRtO</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
  <md:SPSSODescriptor
    ID="_9965E3E789FED5C36339DEAEB6D64D6"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    AuthnRequestsSigned="true"
    WantAssertionsSigned="false">
    <md:KeyDescriptor use="signing">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIIC...dRtO</X509Certificate>
        </X509Data>
      </KeyInfo>
    </md:KeyDescriptor>
    <md:AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://api.incontact.com/InContactAuthorizationServer/FederatedIdLogin?
        BusNo={BusNo} & ClusterNo={ClusterNo}"
      index="0"
      isDefault="true" />
    </md:AssertionConsumerService>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">inContact - http://www.incontact.com/
  </md:OrganizationName>
```



```
<md:OrganizationDisplayName xml:lang="en">inContact</md:OrganizationDisplayName>
<md:OrganizationURL xml:lang="en">http://www.incontact.com/</md:OrganizationURL>
</md:Organization>
<md:ContactPerson>
  <md:Company>inContact</md:Company>
  <md:EmailAddress>John.Doe@customer.com</md:EmailAddress>
</md:ContactPerson>
</md:EntityDescriptor>
```

SAML2.0 Assertion Example from ADFS 2:

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="_06cd8382-cc88-4141-83e1-1f10c4e38a5a"
  Version="2.0"
  IssueInstant="2015-05-26T10:08:45.260Z"
  Destination="https://api.incontact.com/InContactAuthorizationServer/FederatedIdLogin?BusNo=123&ClusterNo=1234"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    http://wst-dc.cloudapp.net/adfs/services/trust
  </Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <Assertion
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_e35f3031-25d5-4d50-8181-8f771ac7d856"
    IssueInstant="2015-05-26T10:08:45.260Z"
    Version="2.0">
    <Issuer>http://wst-dc.cloudapp.net/adfs/services/trust</Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod
          Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#_e35f3031-25d5-4d50-8181-8f771ac7d856">
          <ds:Transforms>
            <ds:Transform
              Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <ds:DigestValue>dm/BEL2iMFqleIhtUZP3hYN8bc0=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>rhuJ...yHjc1Dw==</ds:SignatureValue>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIC...dRtO</ds:X509Certificate>
        </ds:X509Data>
      </KeyInfo>
    </ds:Signature>
    <Subject>
      <NameID>John.Doe@customer.com</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <SubjectConfirmationData NotOnOrAfter="2015-05-26T10:13:45.260Z"
        Recipient="https://api.incontact.com/InContactAuthorizationServer/FederatedIdLogin?BusNo=123&ClusterNo=1234" />
      </SubjectConfirmation>
```

```
</Subject>
<Conditions
  NotBefore="2015-05-26T10:08:45.260Z"
  NotOnOrAfter="2015-05-26T11:08:45.260Z">
  <AudienceRestriction>
    <Audience>https://api.incontact.com/</Audience>
  </AudienceRestriction>
</Conditions>
<AttributeStatement>
  <Attribute Name="SecurityProfileID">
    <AttributeValue>6</AttributeValue>
  </Attribute>
</AttributeStatement>
<AuthnStatement>
  AuthnInstant="2015-05-26T09:14:22.040Z"
  SessionIndex="_e35f3031-25d5-4d50-8181-8f771ac7d856">
  <AuthnContext>
    <AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </AuthnContextClassRef>
  </AuthnContext>
</AuthnStatement>
</Assertion>
</samlp:Response>
```

Generating a Security Certificate from ADFS

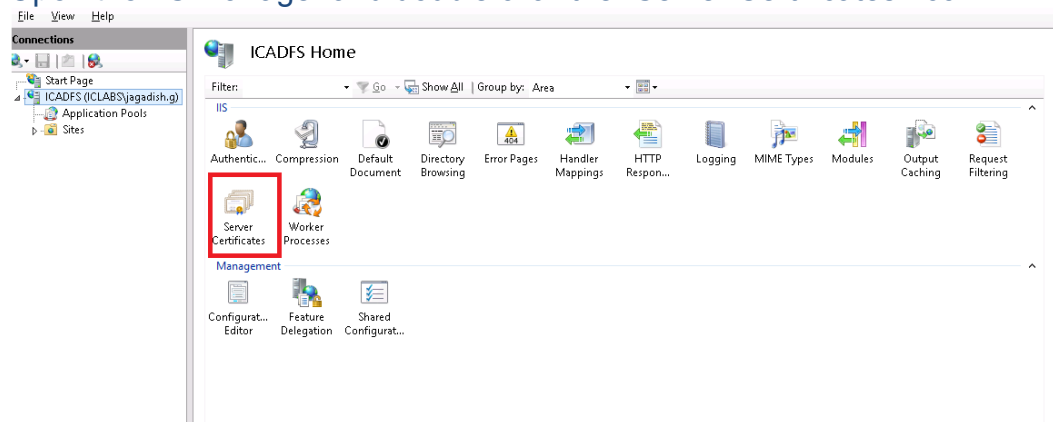
The inContact Federated Identity Management feature will work with any IDP that is enabled to send SAML2.0 assertions using a Security Certificate generated from that system. inContact has validated this functionality using IIS and ADFS2.0 running on Windows 2008 Server operating system. The steps below use this configuration as an example of how to generate a Security Certificate for use with the Federated Identity Management feature.

NOTE: This is just an example and your ADFS setup may be different. Consult your ADFS documentation and admin to resolve any differences with the examples below

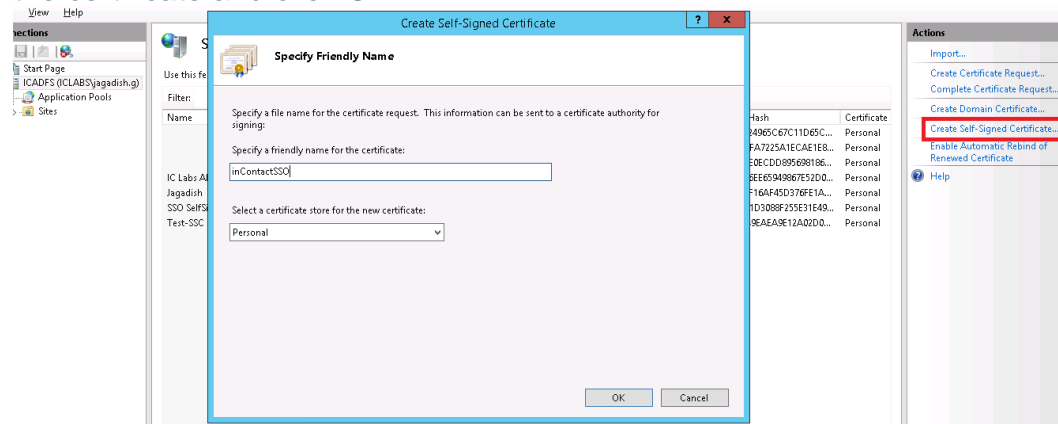
Creating a Self-Signed Certificate from IIS

To create a Self-Signed Certificate that can be uploaded to the inContact Business Unit Federated Identity tab under Admin -> Business Unit.

1. Open the IIS Manager and double click the "Server Certificates" icon.



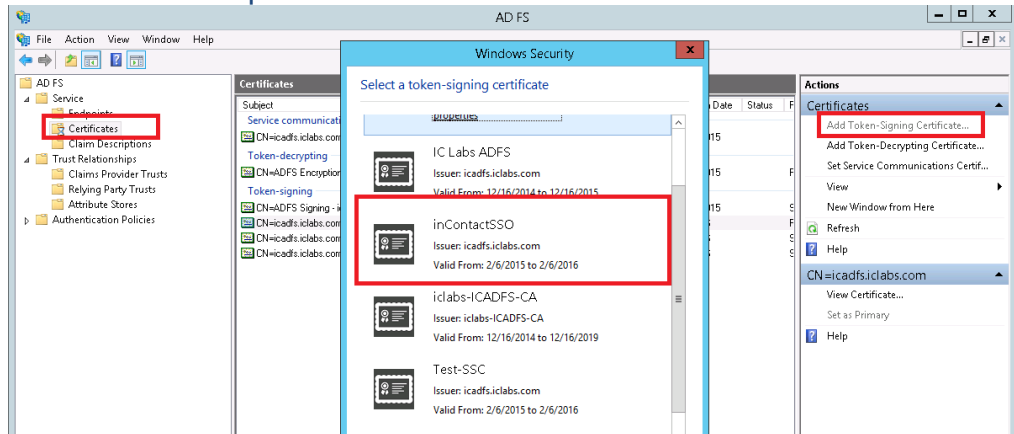
2. Click "Create Self-Signed Certificate" on the Actions pane. Enter a name for the certificate and click OK.



Importing Certificate into ADFS

Once your Certificate has been created, you will need to import this certificate into ADFS using the Management Console.

1. Open the ADFS Management Console and navigate to the Services -> Certificates and click on the “Add Token-Signing Certificates” command from the Actions pane.

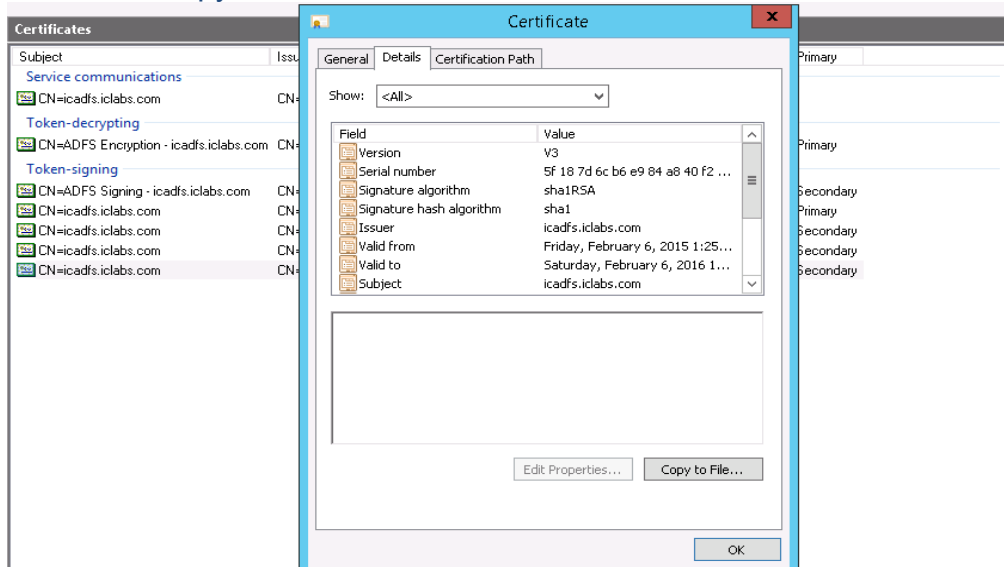


2. Select the Certificate created from IIS Manager and click OK. The Certificate will be added under the “Token-Signing” section.

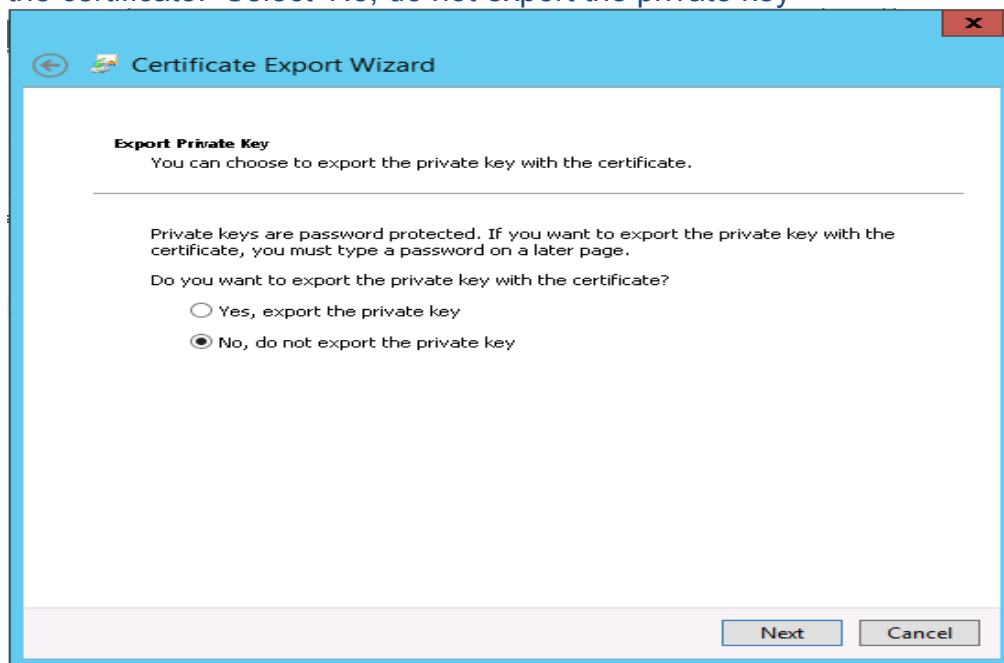
NOTE: If you are asked to ensure that the service account has access to the primary key, you will need to enable this access using the steps in [‘Enabling Primary Key Access for ADFS’](#)

3. Select the Certificate created from IIS Manager and select ‘Set as Primary’.

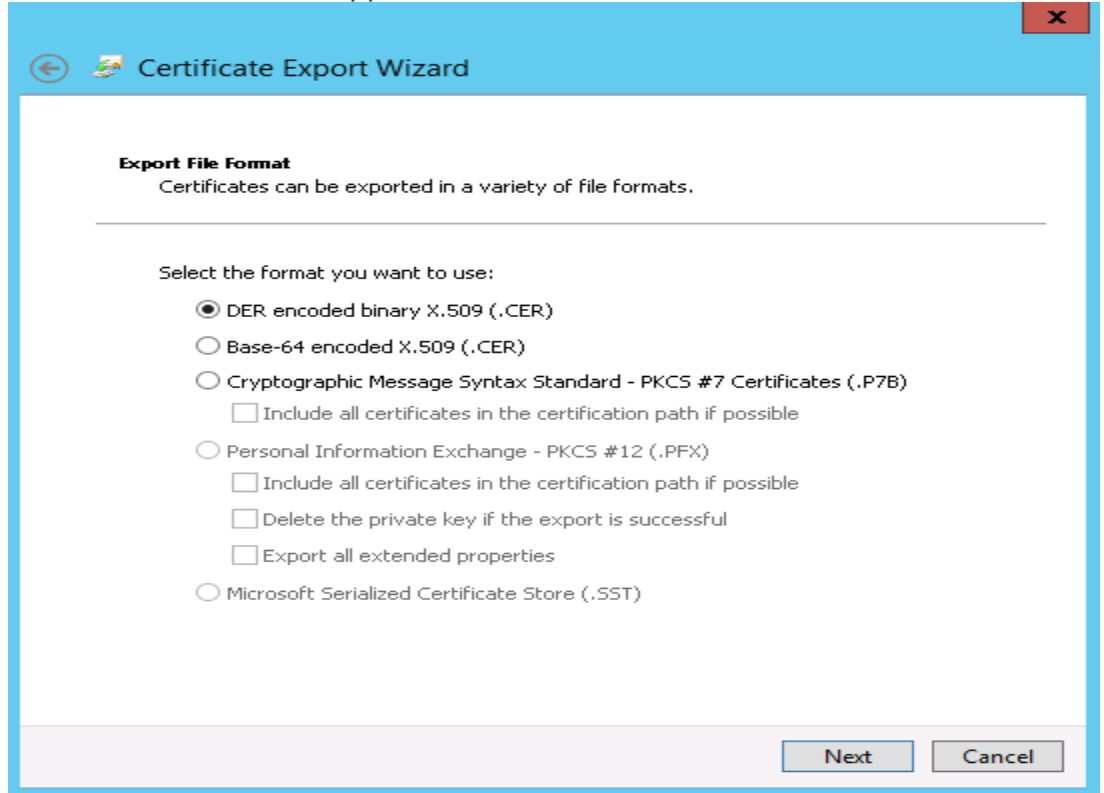
4. To save the certificate, right-click the certificate and click 'View Certificate' then click 'Copy to File'.



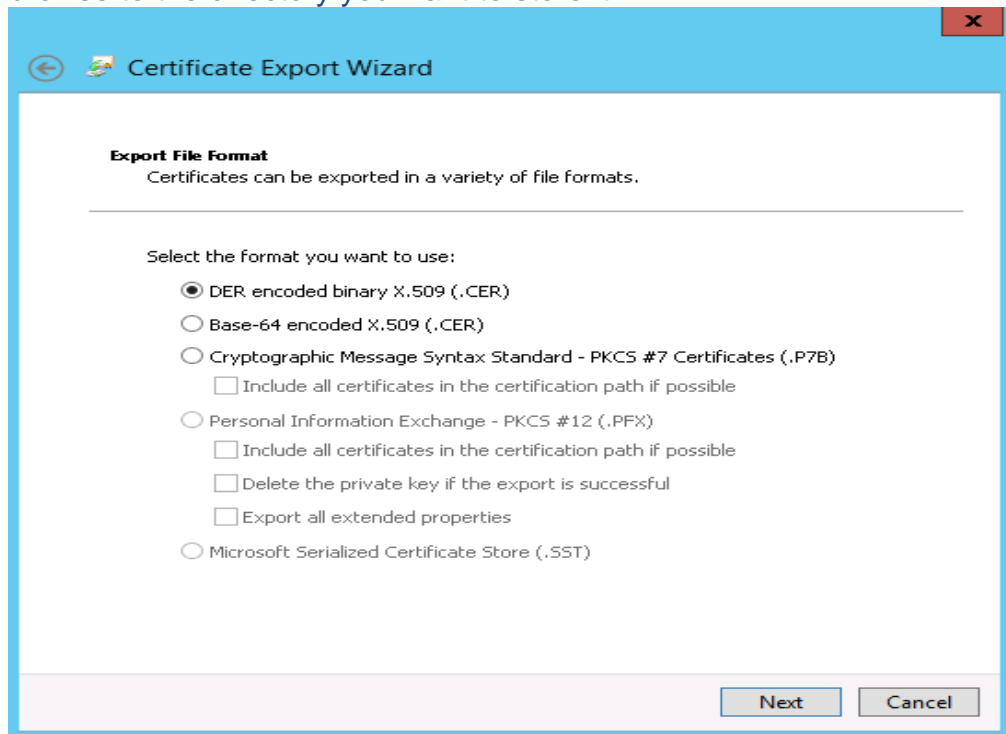
5. The Certificate Export Wizard will prompt you to export a private key with the certificate. Select 'No, do not export the private key'



6. Select what type of encryption you would like to use with your security certificate. inContact supports X.509 certificates.



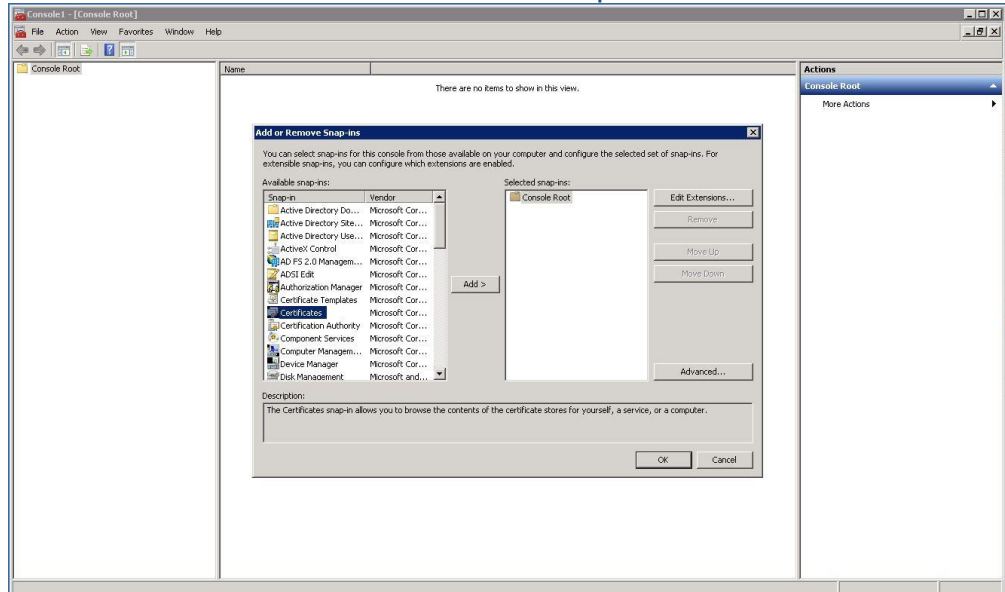
7. Provide the name of the file you want to save the certificate under and browse to the directory you want to store it in.



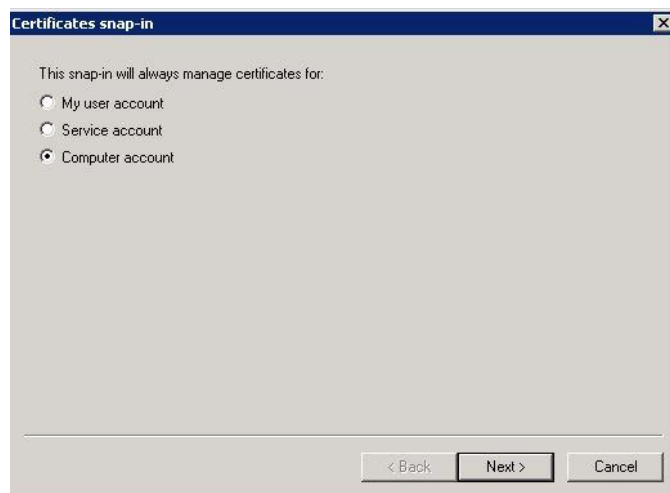
Enabling Primary Key Access for ADFS

To enable Primary Key access on your server for ADFS you can follow these steps.

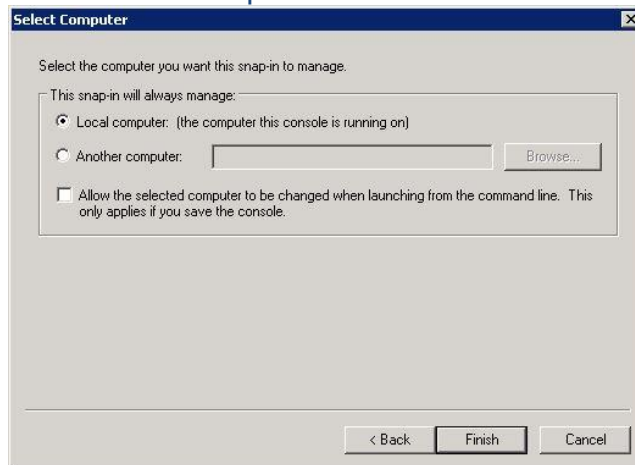
1. Launch mmc console by selecting 'Start' from the task bar and typing mmc in the Search Programs and Files text box.
2. After mmc launches, select 'Add/Remove Snap-in' from the file menu and select 'Certificates' from the available snap-ins.



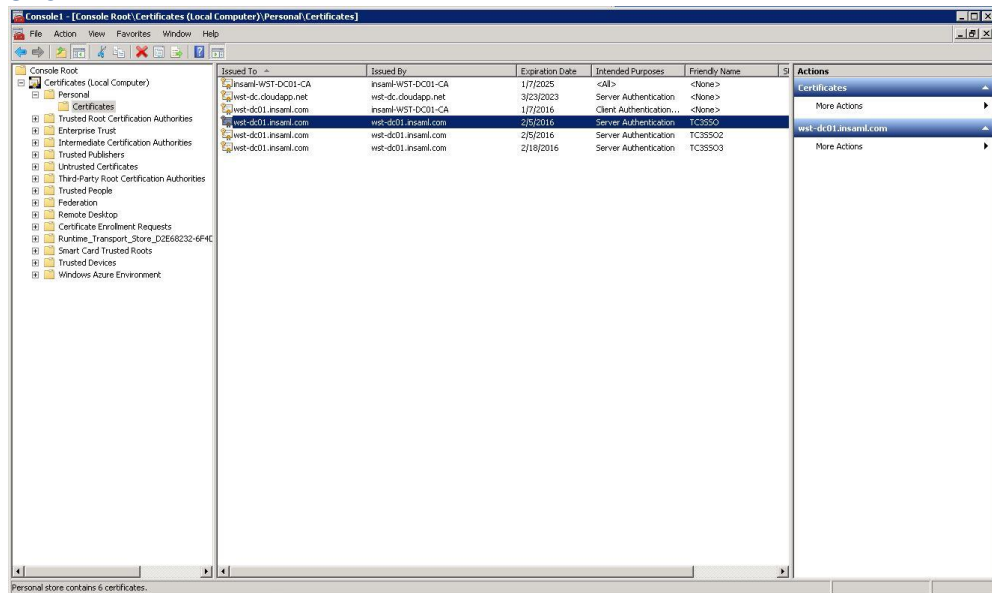
3. Click 'Add' and then select 'Computer Account' and click 'Next' as shown below.



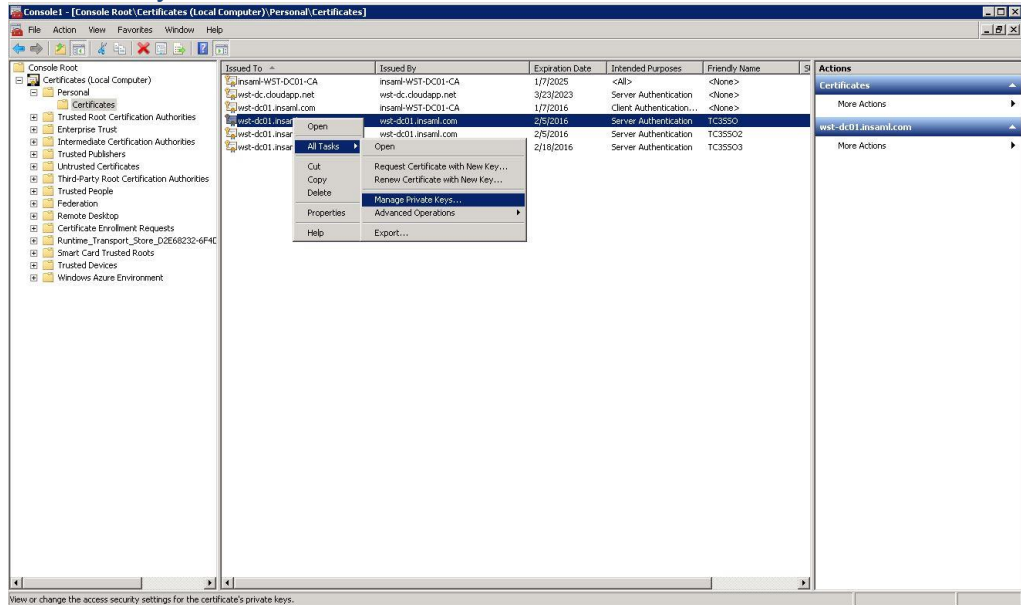
4. Click 'Local Computer' and click finish.



5. In the mmc console, select 'Personal' and then 'Certificates' in the left panel and then select the newly created certificate in the right panel as shown.



6. Right-click on the certificate and select 'All Tasks' and then 'Manage Private Keys' as shown.



7. Grant read access to the necessary accounts. These may be NETWORK SERVICE and adfsprxy. Check your service configuration if you are unsure.

Configure a Service Provider in ADFS

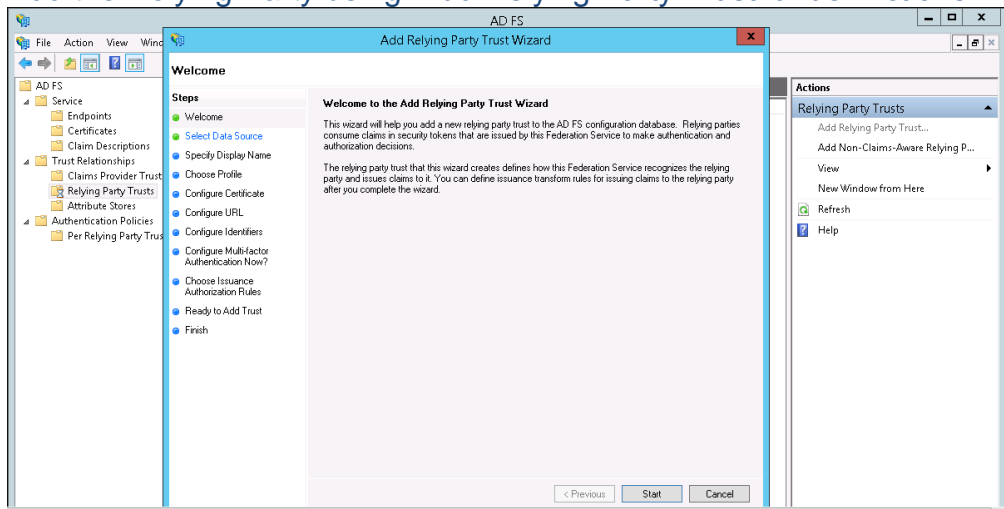
The inContact Federated Identity Management feature will work with any IDP that is enabled to send SAML2.0 assertions using a Security Certificate generated from that system. In addition to uploading this certificate, you will also need to configure your IDP to communicate with inContact as a Service Provider. In the instructions below we will show you an example of how to do this in ADFS.

NOTE: *This is just an example and your ADFS setup may be different. Consult your ADFS documentation and admin to resolve any differences with the examples below*

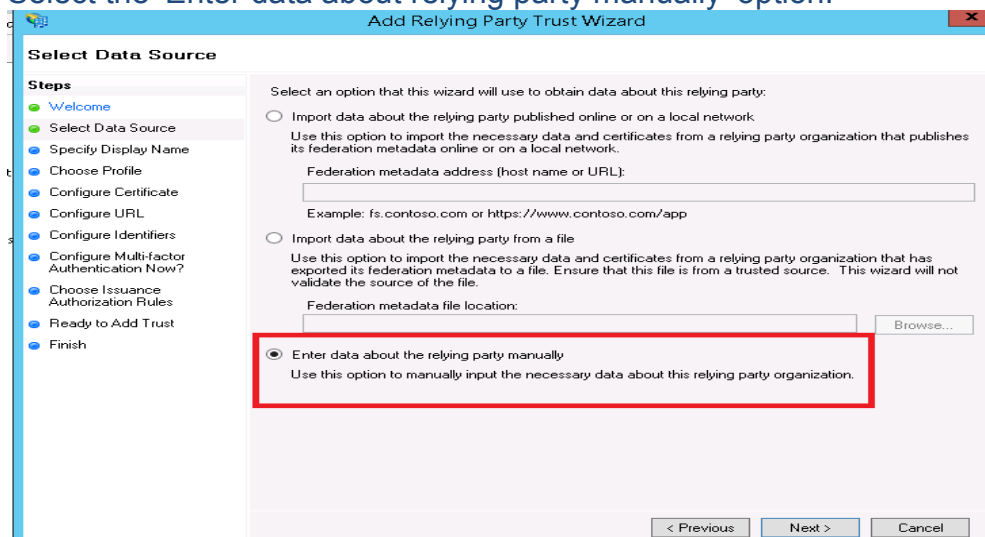
Creating a Relying Party Trust

To create a trust relationship between inContact and your ADFS system you must register a Relying Party Trust

1. Open the ADFS Management Console and navigate to Trust Relationships -> Relying Party Trusts.
2. Add the Relying Party using 'Add Relying Party Trust' under Actions



- Click 'Start' and the wizard will prompt you to select a data source. Select the 'Enter data about relying party manually' option.



Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

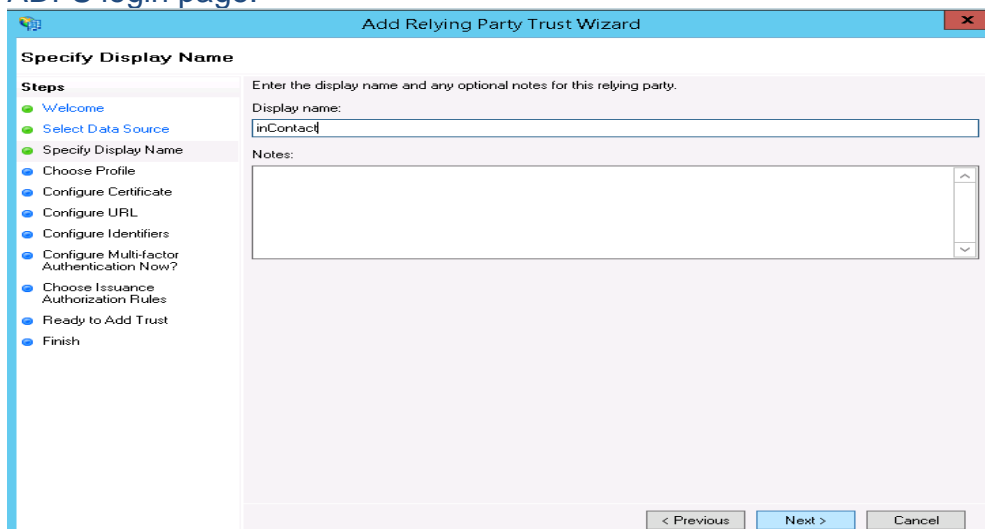
☐ Import data about the relying party published online or on a local network.
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:

☒ Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

- Provide a name for the Relying Party which will be displayed on the ADFS login page.



Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

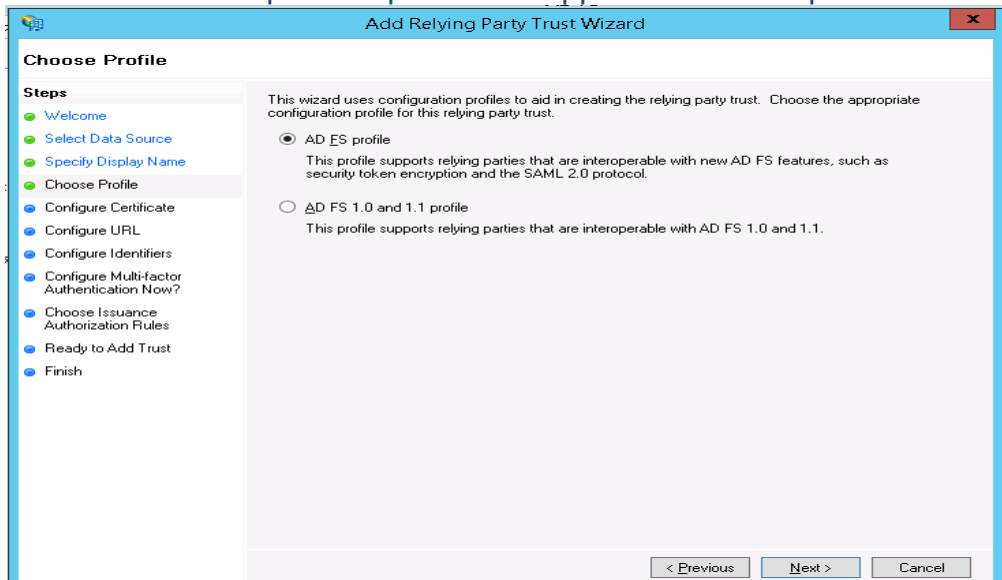
Enter the display name and any optional notes for this relying party.

Display name:

Notes:

< Previous Next > Cancel

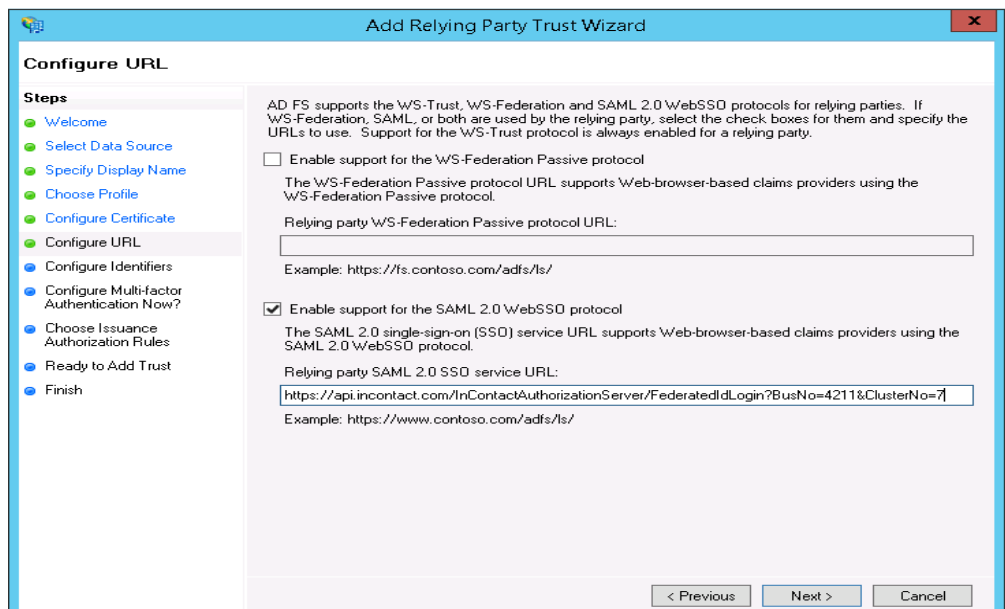
5. Select the 'AD FS profile' option that supports SAML 2.0 protocol



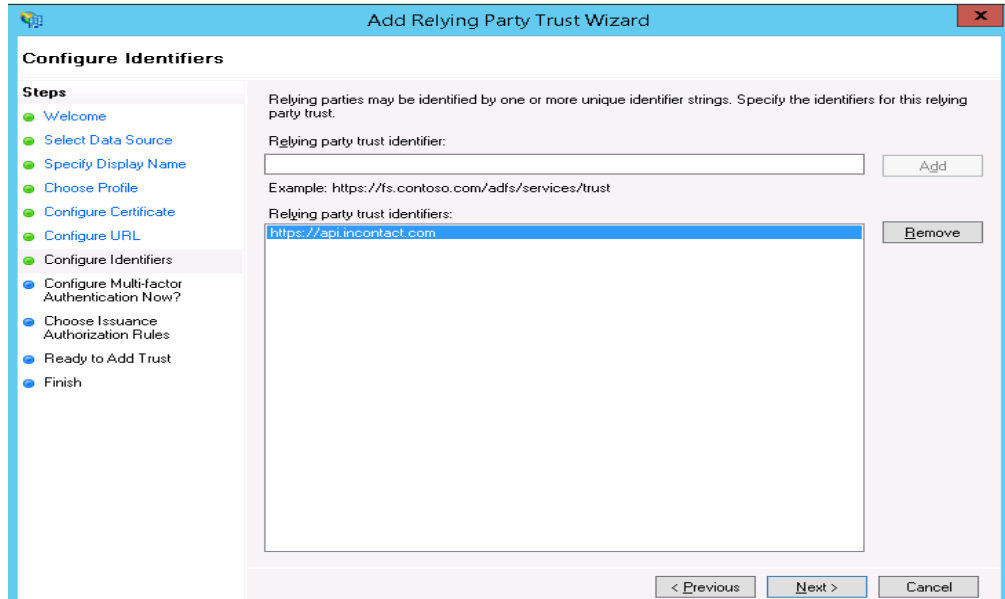
6. Skip the 'Configure Certificate' section and select Next.

7. Select the 'Enable support for the SAML 2.0 WebSSO protocol' option and enter the SSO service URL and select Next

NOTE: The SSO service URL can be found on the Federated Identity configuration page for the Business Unit you have configured in inContact Central and should be of the format
"https://api.incontact.com/InContactAuthorizationServer/FederatedIdLogin?BusNo=<BusinessUnitId>&ClusterNo=<ClusterNumber>"



8. Add the URL <https://api.incontact.com> as a Relying party trust identifier and then select Next.



Add Relying Party Trust Wizard

Configure Identifiers

Steps:

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

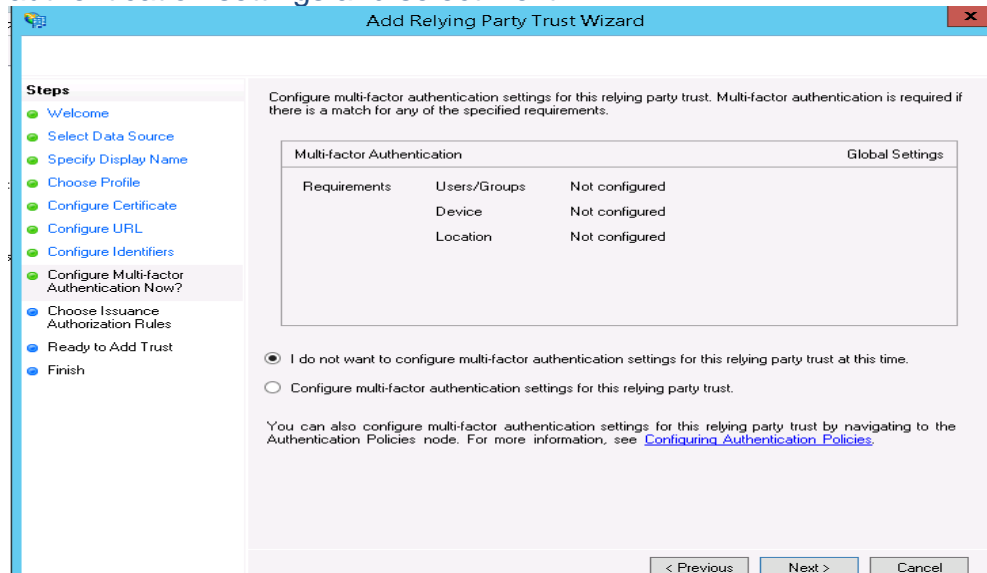
Example: <https://fs.contoso.com/adfs/services/trust>

Relying party trust identifiers:

<https://api.incontact.com>

< Previous Next > Cancel

9. Select the option that indicates you do NOT want to configure Multi-factor authentication settings and select Next.



Add Relying Party Trust Wizard

Steps:

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

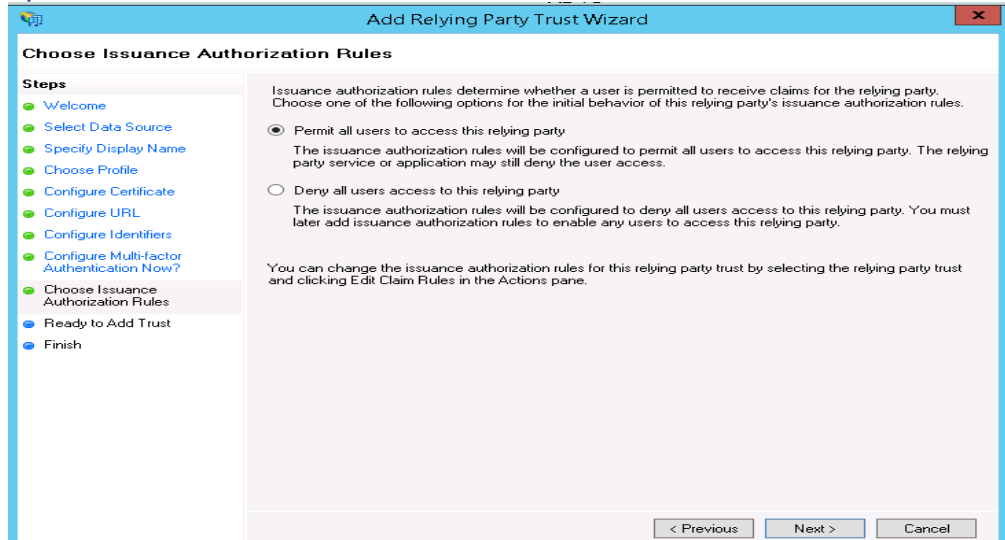
☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

10. Enable all users to access this relying party by selecting the appropriate option. Then select Next and finish the wizard.

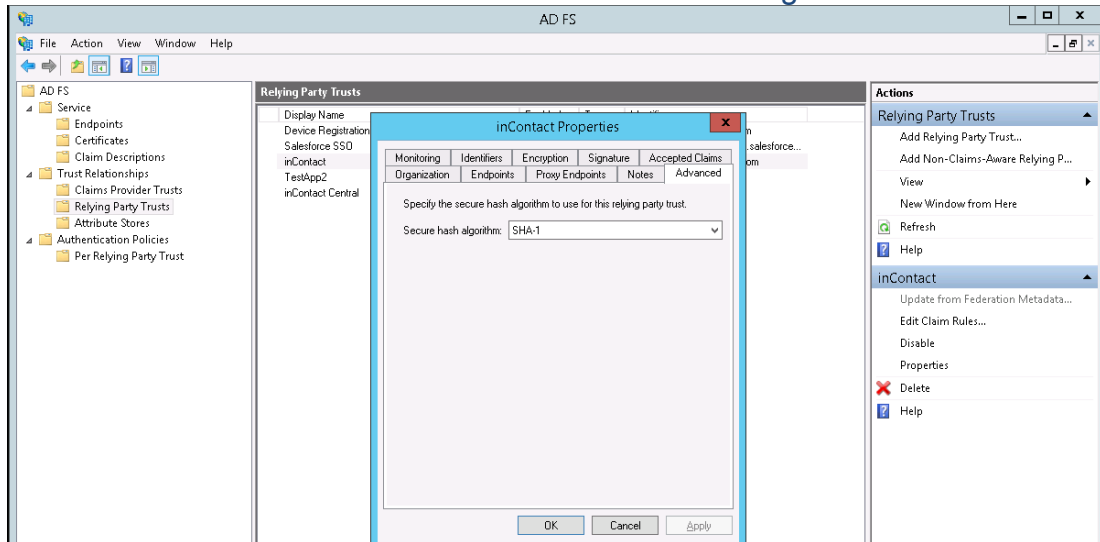


Configuring Claim Rules for a Trust in ADFS

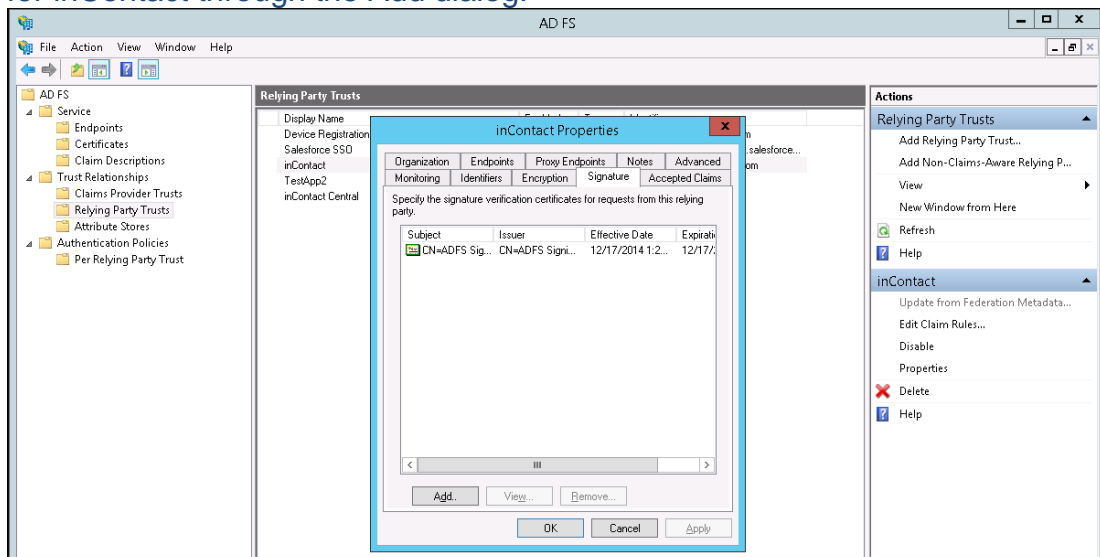
Once you have created a trust relationship between inContact and your ADFS system you must edit the Claim Rules before using it to login into inContact Central

1. Open the ADFS Management Console and navigate to Trust Relationships -> Relying Party Trusts and select the Trust you are using for inContact.

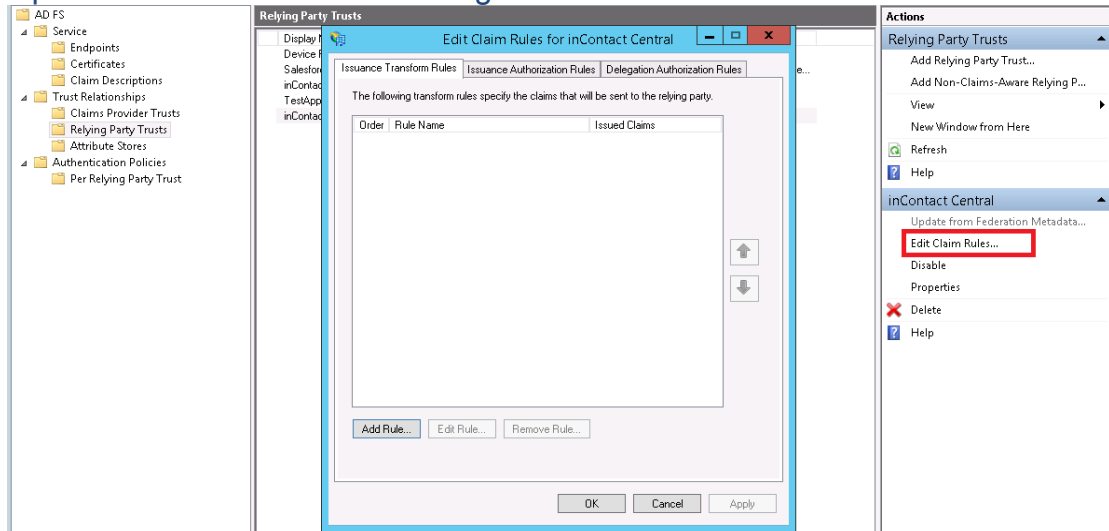
2. In the Advanced tab choose 'SHA-1' as secure hash algorithm



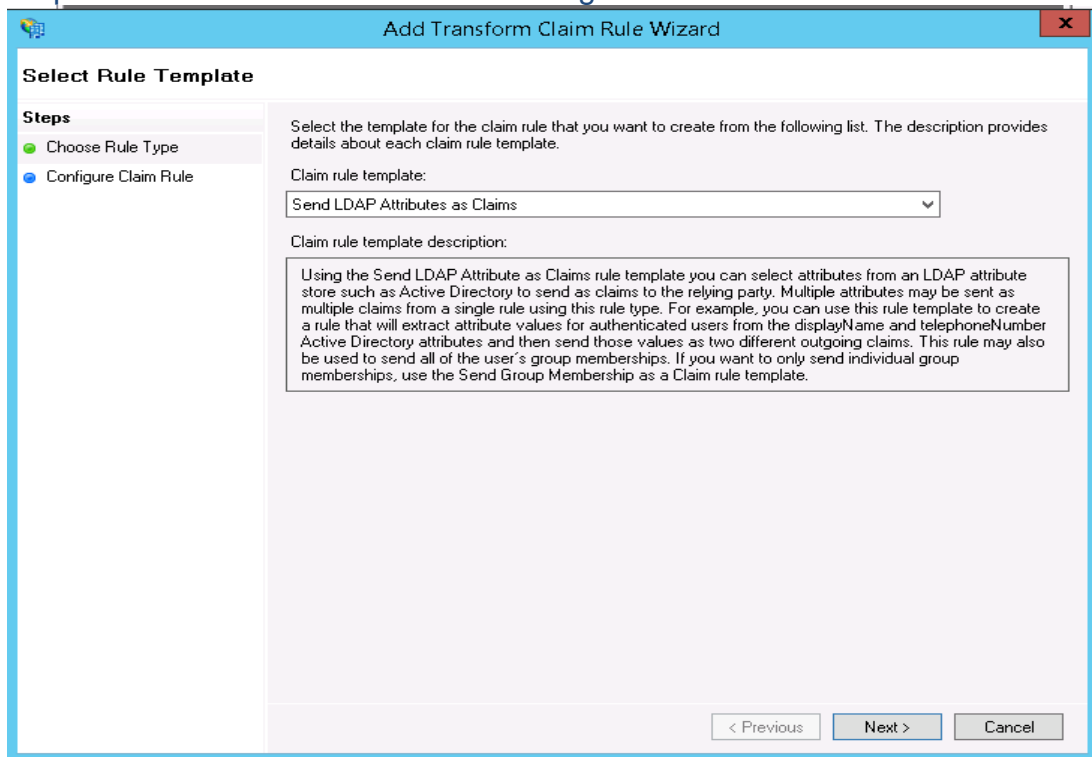
3. Select the Signature tab and upload the Security Certificate you have created for inContact through the Add dialog.



4. Open the 'Edit Claim Rules' dialog from the Actions window

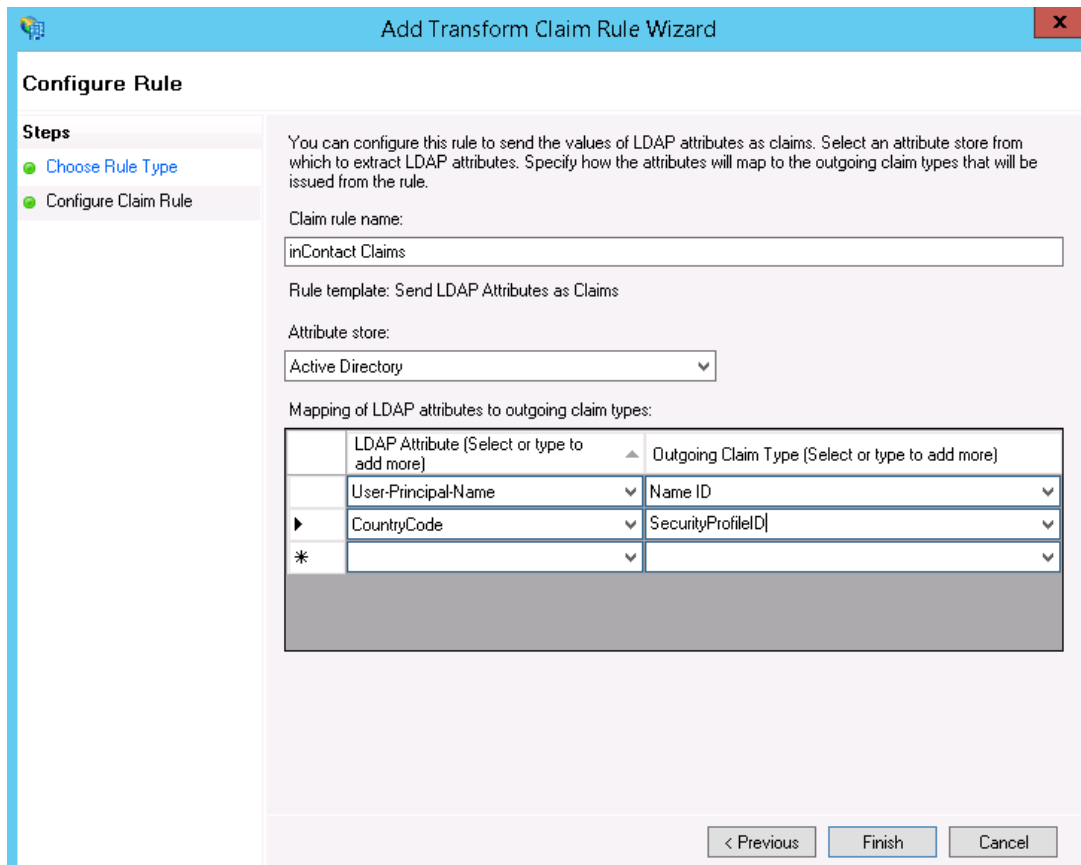


5. Select the 'Tab Issuance Transform Rules' and choose Add Rule. Select the Claim Rule Template labeled 'Send LDAP Attributes as Claims' from the dropdown menu and select Next to configure the Claim Rule.



6. Provide the name of the rule and specify that it use the Active Directory as the Attribute Store and map the LDAP attributes with the claims required by inContact then select Finish.

NOTE: You can use any unique value in ADFS as the Name ID, in the example below we use User-Principal-Name. This value must match the Federated Identity value configured for this user in inContact Central. The SecurityProfileID must contain a valid security profile ID from your inContact Central Business Unit. In our example this is stored in CountryCode but this could be stored in any accessible field in ADFS.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- **Configure Claim Rule**

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	Name ID
▶	CountryCode	SecurityProfileID
*		

< Previous Finish Cancel