Configuring Claims-based Authentication for Microsoft Dynamics CRM Server

Last updated: June 2014

Microsoft Dynamics CRM

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

The videos and eBooks are in English only. Also, if you click the links, you may be redirected to a U.S. website whose content is in English.

Contents

Configure Claims-based Authentication for Microsoft Dynamics CRM Server

Last updated: February 2014

This document applies to an on-premises deployment of Microsoft Dynamics CRM Server 2011 and Microsoft Dynamics CRM Server 2013.

About claims authentication

Microsoft Dynamics CRM Server 2011 and Microsoft Dynamics CRM Server 2013 use claims-based authentication to authenticate internal users and to enable Internet access for external users not using VPN.

Claims-based authentication is built on Windows Identity Foundation (WIF), a framework for building claims-aware applications and security token service (STS) that is standards-based and interoperable. Interoperability is provided through reliance on industry standard protocols such as WS-Federation, WS-Trust, and Security Assertion Markup Language 1.1 (SAML).This document uses Active Directory Federation Services (AD FS) as the identity provider.

In claims-based authentication, an identity provider that contains a security token service (STS) responds to authentication requests and issues SAML security tokens that include any number of claims about a user, such as a user name and groups the user belongs to. A relying party application receives the SAML token and uses the claims inside to decide whether to grant the client access to the requested resource. Claims-based authentication can be used to authenticate your organization's internal users, external users, and users from partner organizations.

For more information about claims authentication, see the Recommended reading section of this document.

Important
If you have deployed Microsoft Dynamics CRM 2013 on-premises, Internet Facing Deployment (IFD) is required for Microsoft Dynamics CRM for tablets users to access their CRM data. If you have your Microsoft Dynamics CRM website available over the internet but it is not using the Microsoft Dynamics CRM IFD configuration, **this is not supported**. For more information, see CRM for tablets and IFD.

This document has the following goals:

- Prepare you to configure AD FS.
- Prepare you to install and configure Microsoft Dynamics CRM Server claims-based authentication for internal access, external access (IFD), or both internal and external access.
- Provide information about federation trusts, Microsoft Office Outlook connections, and other configuration considerations.

This document does not cover integrating Microsoft Dynamics CRM with Microsoft Office 365. For more information, see: Introduction to the Office 365 Deployment Guide for Enterprises

Prerequisites

Before configuring Microsoft Dynamics CRM Server for claims-based authentication, you should have a solid understanding of the following:

1. The Microsoft Dynamics CRM Server installation process.
2. Security token-based authentication as used in claims-based authentication.
3. AD FS installation and configuration.
4. Public key infrastructure (PKI) administration and digital certificates.

Recommended reading

- Active Directory Federation Services
- Active Directory Federation Services Overview
- Claims-Based Identity for Windows (pdf)
- CRM 2011 Implementing ADFS Claims Based Authentication - Best Practices and Tips

MSDN content

- A Guide to Claims–based Identity and Access Control (2nd Edition)
- Using Active Directory Federation Services 2.0 in Identity Solutions

Video

Microsoft Dynamics CRM 2011: Implementing Claims and IFD:

- Part 1 (http://youtu.be/cR7ku934x8Q)

  Prepare for claims-based authentication
- Part 2 (http://youtu.be/sFncc5DgqkQ)

Install and configure the AD FS 2.0 server

- Part 3 (http://youtu.be/tmLS3gi0b14)

  Configure the CRM server for claims-based authentication
- Part 4 (http://youtu.be/CM_8ILPEI2Y)

  Configure the CRM server for IFD
- Part 5 (http://youtu.be/chOuKgIKIWY)

  How to pass through claims for an untrusted domain
- Part 6 (http://youtu.be/qoCzmDi8xi4)

  Troubleshooting

Certificates and public key infrastructure

- Application Security - Certificates
- Certificate Requirements for Federation Servers

Troubleshooting

- Troubleshoot AD FS 2.0

Terminology

Term	Definition
Active Directory Federation Services (AD FS)	A component of Microsoft Windows Server that supports identity federation and Web single sign-on (SSO) for Web browser–based applications.
Attribute store	A database that stores identities and their associated attributes. For this document, Active Directory Domain Services (AD DS) is the attribute store.
Claim	A statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims have a security token service that issues them (such as AD FS), and they are given one or more values.
Claim rule	A rule that is written in the claim rule language in AD FS that defines how to generate, transform, pass through, or filter claims.
Claims-aware application	A relying party software application that uses claims to manage identity and access for users.

Term	Definition
	In this document, Microsoft Dynamics CRM is the claims-aware application.
Claims provider	A Federation Service that issues claims for a particular transaction. In Microsoft Windows Server claims-based authentication, AD FS issues claims to its users for the relying party - the Microsoft Dynamics CRM server.
Federation server	A computer running Microsoft Windows Server that has been configured using the AD FS Federation Server Configuration Wizard to act in the federation server role. A federation server issues tokens and serves as part of a Federation Service.
Federation Service	A logical instance of a security token service such as AD FS.
Identity provider	A Web service that handles requests for trusted identity claims and issues SAML tokens. An identity provider uses a database called an attribute store to store and manage identities and their associated attributes. For this document, AD FS is the identity provider and Active Directory Domain Services (AD DS) is the attribute store.
Relying party	An application that consumes claims to make authentication and authorization decisions. For example, the Microsoft Dynamics CRM server receives claims that determine whether users in a partner organization can access your Microsoft Dynamics CRM data.
Relying party trust	A trust object, in the AD FS snap-in, that is created to maintain the relationship with a Federation Service or with an application that consumes claims from this Federation Service.

Authentication methods

The following authentication methods are supported by Microsoft Dynamics CRM Server:

- Windows Authentication

- Claims-based authentication: internal access
- Claims-based authentication: external access
- Claims-based authentication: internal and external access

Your choice of authentication method depends on your organization's design and deployment goals.

Authentication model	Scenario
Windows Authentication	You can use Windows Authentication in Microsoft Dynamics CRM Serverto authenticate clients using NTLM or Kerberos. Windows Authentication is used in an intranet environment where all users are members of your Active Directory domain.
Claims-based authentication: internal access	If you have a multiple domain environment where trust does not exist between the domains, or where some users exist in a different attribute store such as a partner organization, you can use claims-based authentication to handle internal user authentication.
Claims-based authentication: external access	Accessing Microsoft Dynamics CRM data over the Internet through an Internet-facing deployment (IFD) is done with claims-based authentication.

Important

- After deploying claims-based authentication, internal users can continue to use Windows Authentication to access Microsoft Dynamics CRM data (for example, using http://crmserver/orgname).
- Before deploying claims-based authentication in a production environment, first test your deployment settings in a test environment.

In This Section

Windows authentication

Claims-based authentication: internal access

Claims-based authentication: external access

See Also

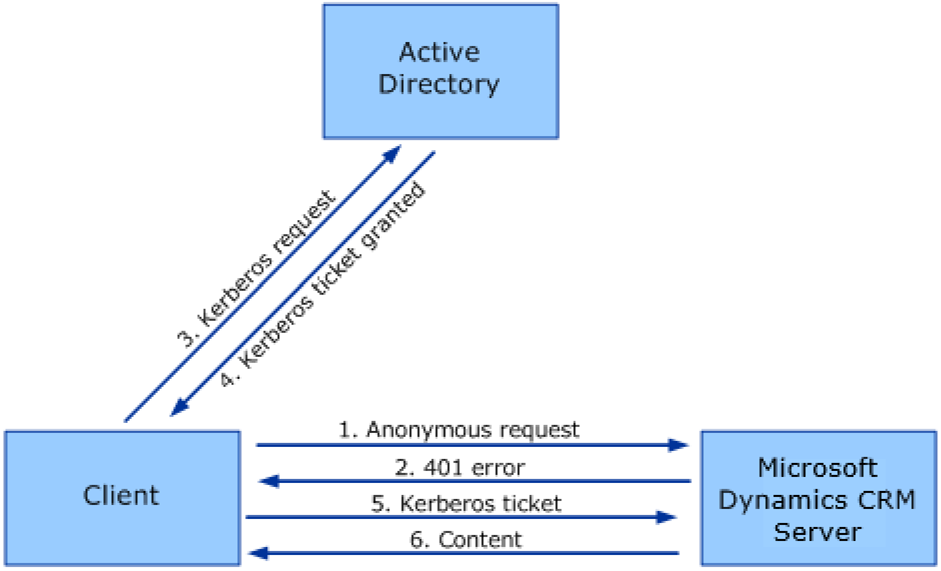
Terminology

Deployment scenarios in this document

Windows authentication

You can use Windows Authentication in Microsoft Dynamics CRM Server to authenticate clients using NTLM or Kerberos. Windows Authentication is used in an intranet environment where all users are members of your Active Directory domain.

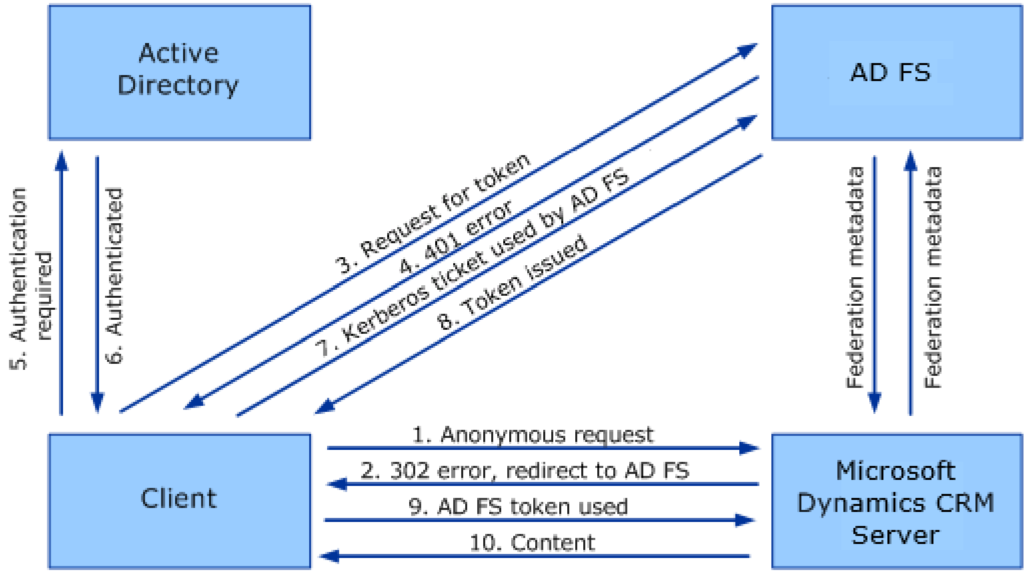
Windows Authentication using Kerberos flows as follows:



Claims-based authentication: internal access

If you have a multiple domain environment where trust does not exist between the domains, or where some users exist in a different attribute store such as a partner organization, you can use claims-based authentication to handle internal user authentication.

Claims authentication flows as follows:



1. The client sends a request to access the Microsoft Dynamics CRM website.
2. IIS refuses the connection with an HTTP 302 error message and redirects the user to the trusted claims provider (also known as the STS) for Microsoft Dynamics CRM (AD FS).
3. The client sends a request for a security token to AD FS.
4. AD FS returns an HTTP 401.1 error, indicating that the client must supply a Kerberos ticket.
5. The client sends a Kerberos authentication request to Active Directory.
6. Active Directory validates the client and sends a Kerberos ticket.
7. The client sends a request for a security token to AD FS and includes the Kerberos ticket.

   Note
   If the client already has a valid Kerberos ticket on the network, this ticket is sent to AD FS in step 3 and steps 4 through 7 are skipped.

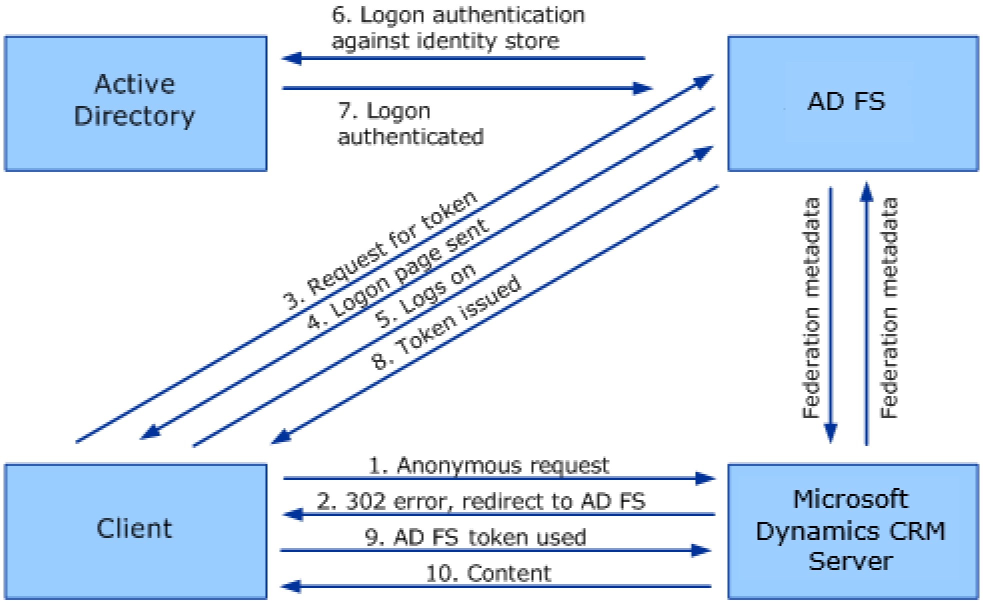
8. AD FS provides a security token containing claims for access to Microsoft Dynamics CRM data.
9. The client sends the security token containing claims obtained from AD FS to the Microsoft Dynamics CRM server.
10. The Microsoft Dynamics CRM server decrypts and validates the security token and presents the user with the requested information.

    Important
    Microsoft Dynamics CRM security roles and profiles are respected. The security token containing claims only replaces the Kerberos ticket used with Windows Authentication.

Claims-based authentication: external access

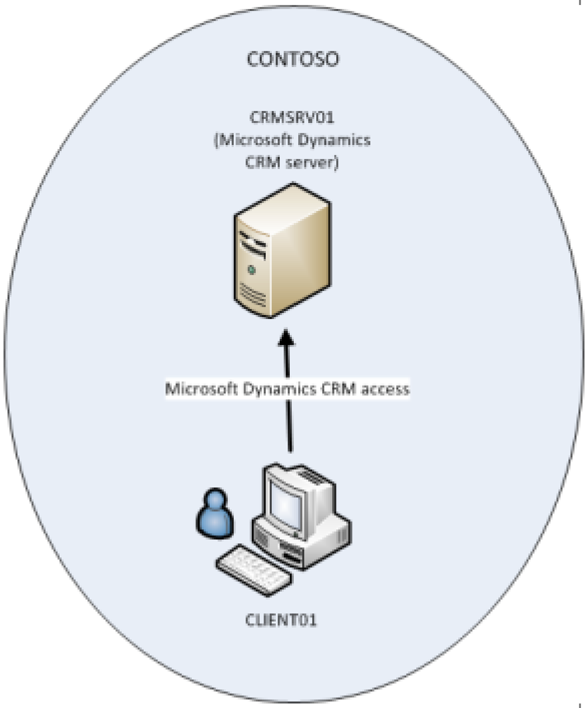
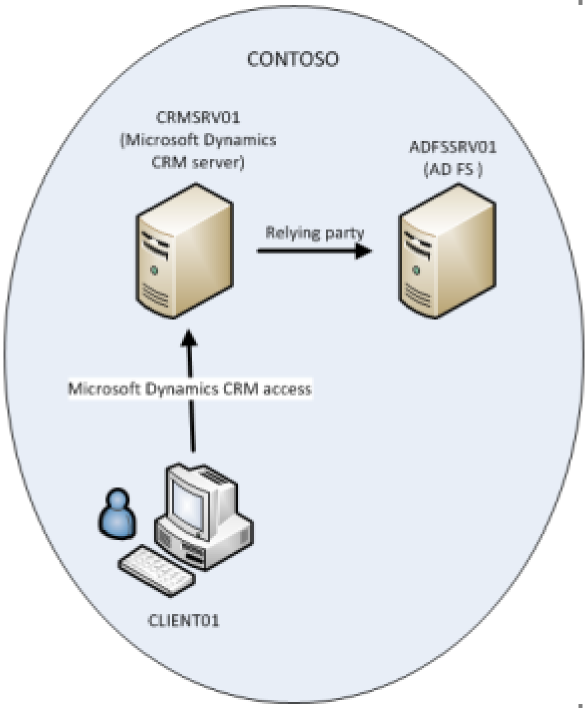
Accessing Microsoft Dynamics CRM data over the Internet through an Internet-facing deployment (IFD) is now done with claims-based authentication.

The flow for claims with IFD access is largely unchanged from the flow described above for internal access. The major difference is that user authentication does not include a Kerberos ticket. When accessing AD FS, users are prompted for credentials on an AD FS logon page. If more than one claims provider (by default Active Directory is the sole claims provider) is trusted by AD FS, users are prompted to select a claims provider (called the home realm discovery process). Users then enter their credentials and the AD FS server validates these logon credentials with the selected attribute store, such as AD DS.



Deployment scenarios in this document

The placement of the AD FS security token service is an important decision when planning your claims-based authentication. You can use a single or multiple server scenario as described below. **A multiple server scenario is recommended** and is what is used in this document.

AD FS and Microsoft Dynamics CRM on the same server	AD FS and Microsoft Dynamics CRM on separate servers
 CONTOSO CRMSRV01 (Microsoft Dynamics CRM server) Microsoft Dynamics CRM access CLIENT01	 CONTOSO CRMSRV01 (Microsoft Dynamics CRM server) ADFSSRV01 (AD FS) Relying party Microsoft Dynamics CRM access CLIENT01
A single-server deployment is suitable for small offices with a limited number of users. Because AD FS must be installed in the default website, the URL used for claims-based access to Microsoft Dynamics CRM will require a port number such as 444. **Note** For Windows Server 2012 R2, you do not need to create a separate website and use a new port.	Separating AD FS from Microsoft Dynamics CRM on separate servers is the recommended deployment scenario. You will especially want to use this scenario if you are deploying on Windows Server 2008 or Windows Server 2012 (not R2) to allow AD FS to be the default website on its own server. The second server for AD FS must have a public IP address and be an endpoint for external connections – unless you use an AD FS proxy server.

Note

This document assumes you are installing on Windows Server 2012 R2 using a separate AD FS server scenario – the recommended deployment. For Windows Server 2008 or Windows Server 2012, you must append a port number to the URL in a single server installation.

Plan for claims-based authentication

The following section covers considerations to be made and actions to be taken prior to a claims-based authentication deployment.

In This Section

Microsoft Dynamics CRM Server and AD FS conditions

Certificate selection and requirements

DNS configuration

Firewall configuration

See Also

Deployment scenarios in this document

Implement claims-based authentication: internal access

Microsoft Dynamics CRM Server and AD FS conditions

Before you configure claims-based authentication, note the following conditions for the web components:

1. If you are installing Microsoft Dynamics CRM Server in a single server configuration, be aware that AD FS installs on the default website. Therefore, you must create a new website for Microsoft Dynamics CRM Server.

   Note

   This does not apply to Windows Server 2012 R2 as AD FS in Windows Server 2012 R2 is no longer dependent on IIS.

2. Before you enable claims-based authentication, Microsoft Dynamics CRM Server must be running on a website that has been configured to use Secure Sockets Layer (SSL). Microsoft Dynamics CRM Server Setup will not configure the website for SSL.
3. Microsoft Dynamics CRM Server be running on a website that has a single binding. Multiple IIS bindings, such as a website with two HTTPS or two HTTP bindings, are not supported for running Microsoft Dynamics CRM Server.
4. When claims-based authentication is enabled, HTTPS must be used in your browser for both internal and external access to Microsoft Dynamics CRM Server.

Certificate selection and requirements

Certificate selection plays a critical role in securing communication between clients and Microsoft Dynamics CRM Server when using claims authentication. You should have a solid understanding of digital certificates before implementing claims-based authentication.

The following references provide an introduction to certificates and public key infrastructure (PKI) technologies:

- Application Security - Certificates
- Certificate Requirements for Federation Servers

Certificates are required for the following in Microsoft Dynamics CRM Server claims-based authentication.

- **Claims encryption**. Claims-based authentication requires a certificate to encrypt claims sent to the relying party. This certificate should be issued by a trusted certification authority (CA) and should be trusted by the computer where you are installing Microsoft Dynamics CRM Server so it must be located in the local Personal store where the Configure Claims-Based Authentication Wizard is running.
- **SSL (HTTPS) encryption**. The certificate for SSL encryption should be valid for host names similar to org.contoso.com, auth.contoso.com, and dev.contoso.com. To satisfy this requirement you can use a single wildcard certificate (*.contoso.com), or a certificate that supports Subject Alternative Names, or individual certificates for each name. Individual certificates for each host name are only valid if you use different servers for each web server role. Multiple IIS bindings, such as a website with two HTTPS or two HTTP bindings, are not supported for running Microsoft Dynamics CRM Server.

Consider the following when selecting a certificate for your configuration.

Wildcard certificate (recommended). A wildcard certificate supports internal and external access requirements for a single domain. For example, *.contoso.com certificate supports the externally accessed domains org1.contoso.com and org2.contoso.com as well as the internally accessed domain internalcrm.contoso.com. Because the external domain name must resolve for internal access, you cannot use the server name for internal access. If you wish, you can use separate Microsoft Dynamics CRM servers for internal and external claims access to allow the server name to be used for internal access.

Subject Alternative Name (SAN) certificate. Use a SAN certificate if you wish to use a different address for your internal domain that does not match your external domain. For example, your internal domain is org.contoso.local and your external domain is org.contoso.com. Be aware that third-party certificate providers typically do not provide certificates for .local domains.

Self-signed certificate. A self-signed certificate should only be used for testing purposes and not in a production deployment. If you use a self-signed certificate, it must be imported into the Trusted Root Certification Authorities store of all Microsoft Dynamics CRM servers and client computers accessing Microsoft Dynamics CRM Server. For information on how to import a certificate, see Help in the Certificates Microsoft Management Console (MMC). See “Creating a self-signed wildcard certificate for a test deployment” below for information on creating a self-signed wildcard certificate.

Certificate expiration Because there’s some pain and effort involved with updating a certificate, consider purchasing a certificate with an extended expiration period – three or more years.

Important

If you use a certificate that is created by using a custom certificate request, the template that was used must be the **Legacy key** template. Custom certificate requests created by using the **CNG key** template are incompatible with Microsoft Dynamics CRM. For more information about custom certificate request templates, see Create a Custom Certificate Request.

The default website certificate for Windows Server 2008 and Windows Server 2012.

Note

These steps apply to Windows Server 2008 and Windows Server 2012. They **do not** apply to Windows Server 2012 R2.

After you have obtained and installed a certificate, the certificate must be bound to the default website before you can use AD FS.

Bind an SSL certificate to the default website

1. Open IIS Manager.
2. In the **Connections** pane, expand the **Sites** node in the tree, and then click the **Default Web Site**.
3. In the **Actions** pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. Under **Type**, select **https**.
6. Under **SSL certificate**, select your SSL certificate and then click **OK**.
7. Click **Close**.

For more information about adding binding to a site, see Add or Edit Site Binding Dialog Box

The Microsoft Dynamics CRM Server website certificate

When enabling claims-based authentication, the Microsoft Dynamics CRM website must be accessible via HTTPS. You must bind your SSL certificate to the Microsoft Dynamics CRM website.

Bind an SSL certificate to the Microsoft Dynamics CRM Server website

1. Open IIS Manager.
2. In the **Connections** pane, expand the **Sites** node in the tree, and then click the Microsoft Dynamics CRM website.
3. In the **Actions** pane, click **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. Under **Type**, select **https**.
6. Under **SSL certificate**, select your SSL certificate.
7. Click **Close**.

See the section below DNS configuration to add a host record in DNS for internal access to Microsoft Dynamics CRM Server (for example, internalcrm.contoso.com).

Regarding the AD FS token-signing certificate

AD FS servers use a token-signing certificate created by the AD FS Configuration Wizard to digitally sign all security tokens that they produce. By default, Microsoft Dynamics CRM Server does not check for the presence or validity of this certificate and does not use AD FS token signing. To enable validation and use of the AD FS token-signing certificate, see Enable AD FS token signing in the Additional Considerations section at the end of this document.

Creating a self-signed wildcard certificate for a test deployment

You can create a self-signed wildcard certificate using one of the following programs. The certificate created is not publicly trusted and should only be used for testing.

Makecert.exe

You can use Makecert.exe (Certificate Creation Tool) to generate a self-signed wildcard certificate for testing purposes. Makecert.exe is available in the Microsoft Windows Software Development Kit for Windows Server 2008 and .NET Framework 3.5.

The following are the settings used for a wildcard certificate used to create test deployments for this document:

```
makecert.exe -r -pe -n "CN=*.contoso.com" -b 01/01/2010 -e 01/01/2050 -eku
1.3.6.1.5.5.7.3.1 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel
Cryptographic Provider" -sy 12
```

The self-signed certificate created with Makecert.exe is installed in the local computer's Personal store and is not trusted. To set certificate trust, copy the self-signed certificate (for example *.contoso.com) from the **Personal** store to the **Trusted Root Certification Authorities** store. For more information, see Help in the Certificates Microsoft Management Console (MMC).

Tip

Start a command prompt as an administrator before running makecert.exe.

For more information on Makecert.exe settings, see MakeCert.

SelfSSL

Download the IIS 6.0 Resource Kit and install the SelfSSL tool. For more information, see: Configuring CCF to Use HTTPS (SSL) on IIS 6.0

See Also

Changing the SSL certificate

DNS configuration

Before configuring Microsoft Dynamics CRM Server for claims-based authentication, you should configure your internal and public domain records so the various Microsoft Dynamics CRM Server and AD FS endpoints resolve correctly. If you are setting up Microsoft Dynamics CRM Server in a test lab, you can configure internal records in the hosts file instead of DNS. Hosts use is not recommended for a production environment.

You will create DNS records for the following domain names:

- **Internal URL used to access Microsoft Dynamics** (for example, internalcrm.contoso.local).
- **External URL used to access Microsoft Dynamics - Web Application Server domain** (for example, orgname.contoso.com).
- **Microsoft Dynamics CRM Organization Web Service domain**. Differs from the record used for external access if you have separate domains (for example, orgname.subdm.contoso.com).
- **Microsoft Dynamics CRM Discovery Web Service domain** (for example, dev.contoso.com).
- **AD FS server** (for example, sts1.contoso.com).
- **External IFD URL - Microsoft Dynamics CRM IFD federation endpoint** (for example, auth.contoso.com). This record will be used by the AD FS server when retrieving the Microsoft Dynamics CRM IFD federationmetadata.xml file.

Important

There are several names that cannot be used for host records, for example: support, help, and home. To view a complete list of reserved names, open the dbo.ReservedNames table in the MSCRM_CONFIG database on the Microsoft Dynamics CRM server and review the names in the ReservedName column.

Example DNS Settings – AD FS and Microsoft Dynamics CRM on separate servers

The following are example DNS settings for a two-server deployment. Two public IP addresses are required for external access to Microsoft Dynamics CRM – one for the Microsoft Dynamics CRM server and one for the AD FS server. Two internally hosted DNS zones are required: contoso.local and contoso.com.

Important

If you would rather not have a public connection for your AD FS server, you can use an AD FS proxy server. You can use federation server proxies to provide intermediary services between an Internet client and a federation server that is behind a firewall (not published on the Internet) on your corporate network.

Microsoft Dynamics CRM server always needs to talk to the AD FS server but the Internet client should talk to the AD FS proxy server. This can be achieved by pointing the sts.domain.com DNS record externally to the AD FS proxy server and internally to the AD FS server. The DNS records example table below covers the AD FS proxy scenario.

For more information, see Deploying Federation Server Proxies.

The following table contains records configured in the **Internal DNS Zone: contoso.local**.

Name	Type	Data	Comment
Internal DNS Zone: contoso.local			The following record is configured in DNS on your internal server.
crmserver	Host (A)	The IP address of the server where Microsoft Dynamics CRM is installed.	Configured in DNS on your internal server.

The following table contains records configured in the **Internal DNS Zone: contoso.com**.

Name	Type	Data	Comment
Internal DNS Zone: contoso.com			The following record is configured in DNS on your internal server.
sts1		IP address of your AD FS server.	This record is only needed if you use an AD FS proxy server.
internalcrm	Alias (CNAME)	crmserver.contoso.local	Configured in DNS on your internal server. Used in the internal URL to access Microsoft Dynamics CRM. Internal URL: https://internalcrm.contoso.com

The following table contains records that must be created with **your public host domain service.**

Name	Type	Data	Comment
Public DNS: contoso.com			The following records are created with your public host domain service. For performance and redundancy purposes you could also create these records in the contoso.com zone on your internal DNS server.

Name	Type	Data	Comment
orgname	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection.	Used in the external URL to access Microsoft Dynamics CRM. External URL: https://orgname.contoso.com
dev	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection.	The Microsoft Dynamics CRMDiscovery Web Service.
sts1	Host (A)	IP address of your AD FS server public-facing internet connection. If you use an AD FS proxy server, this would be the IP address of the public-facing internet connection of the proxy server.	The AD FS server or AD FS proxy server.
auth	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection.	The Microsoft Dynamics CRM IFD federation endpoint. This record will be used by the AD FS server when retrieving the Microsoft Dynamics CRM IFD federationmetadata.xml file.

Add a forward lookup zone in DNS

1. Open DNS Manager by clicking **Start**, pointing to **Administrative Tools**, and then clicking **DNS**.
2. In the console tree, right-click a DNS server, and then click **New Zone** to open the New Zone Wizard.
3. Follow the instructions in the wizard to create a forward lookup zone of type: primary zone, secondary zone, or stub zone.

Firewall configuration

You must set your firewall to allow inbound traffic on the ports used for Microsoft Dynamics CRM Server and AD FS. The default port for HTTPS (SSL) is 443.

Implement claims-based authentication: internal access

Enabling claims-based authentication for internal access to Microsoft Dynamics CRM Server data involves the following steps:

1. Deploy and configure AD FS.
2. Configure the Microsoft Dynamics CRM server for claims-based authentication.
3. Configure the AD FS server for claims-based authentication.
4. Test internal claims-based authentication.

Claims-based authentication is not a requirement for intranet Microsoft Dynamics CRM Server access. However, claims-based authentication is required for Microsoft Dynamics CRM IFD access.

In This Section

Deploy and configure AD FS

Configure the Microsoft Dynamics CRM Server for claims-based authentication

Configure the AD FS server for claims-based authentication

Add the AD FS website to the Local intranet security zone

Register the AD FS server as a service principal name (SPN)

Test internal claims-based authentication

See Also

Configure IFD for Microsoft Dynamics CRM 2013

Implement claims-based authentication: external access

Deploy and configure AD FS

A variety of identity providers can be used with Microsoft Dynamics CRM Server. This document uses Active Directory Federation Services (AD FS) for the security token service. For information on configuring identity federation deployment between AD FS and other identity providers, see: AD FS 2.0 Step-by-Step and How To Guides.

Important

If you are deploying on Windows Server 2008 or Windows Server 2012, and you are installing AD FS on the same server as Microsoft Dynamics CRM, AD FS installs on the default website. Before installing AD FS, you must create a new website for Microsoft Dynamics CRM Server.

This does not apply to Windows Server 2012 R2 as AD FS in Windows Server 2012 R2 does not depend on IIS.

Deploy a federation server

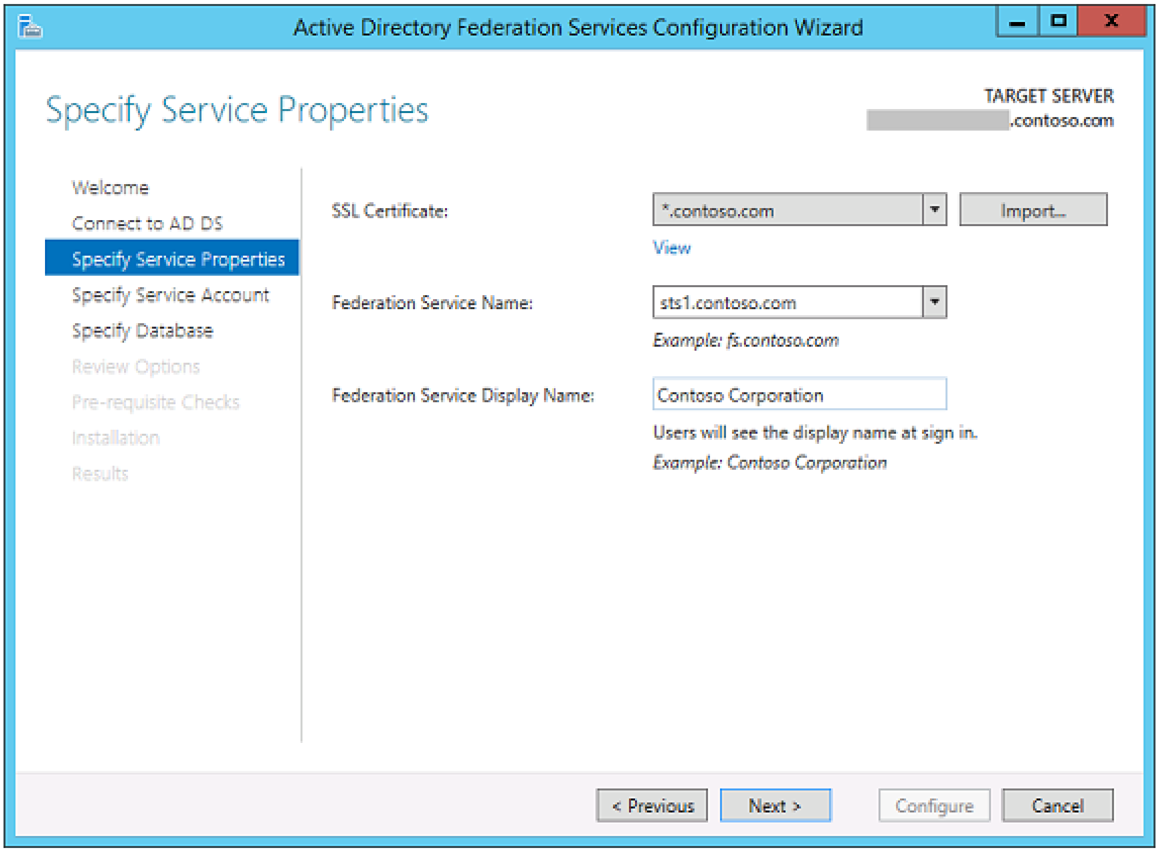
For information on deploying an AD FS server, see AD FS Deployment.

Configure AD FS for Windows Server 2012 R2

To configure AD FS as a stand-alone federation server for Microsoft Dynamics CRM Server claims authentication, do the following:

1. Open the Windows Server 2012 R2 **Add Roles and Features Wizard** and add the **Active Directory Federation Services** server role.
2. Proceed through the wizard. Click **Configure the federation service on this server**.
3. On the **Welcome** page in the Active Directory Federation Services Configuration Wizard, choose an option for a federation server, and then click **Next.**
4. Proceed through the wizard. On the **Specify Service Properties** page, select your SSL certificate, enter a **Federation Service Name**, and then enter a **Federation Service Display Name**.

> **Note**
>
> You only add the federation service name if you are using a wildcard certificate for the AD FS website.
>
> If you install AD FS and Microsoft Dynamics CRM Server on the same server, do not use the same URL for the Federation Service name and internal claims access to Microsoft Dynamics CRM Server. For example, if you use sts1.contoso.com for the Federation Service name, do not use https://sts1.contoso.com for internal Microsoft Dynamics CRM data access.



Specify Service Properties

TARGET SERVER
[redacted].contoso.com

SSL Certificate: *.contoso.com

Federation Service Name: sts1.contoso.com

Example: fs.contoso.com

Federation Service Display Name: Contoso Corporation

Users will see the display name at sign in.

Example: Contoso Corporation

5. Proceed through and complete the **Active Directory Federation Services Configuration Wizard**. Close the **Add Roles and Features Wizard**.
6. If you have not created a host record in DNS for the federation server name you specified in Step 4 previously, do so now.

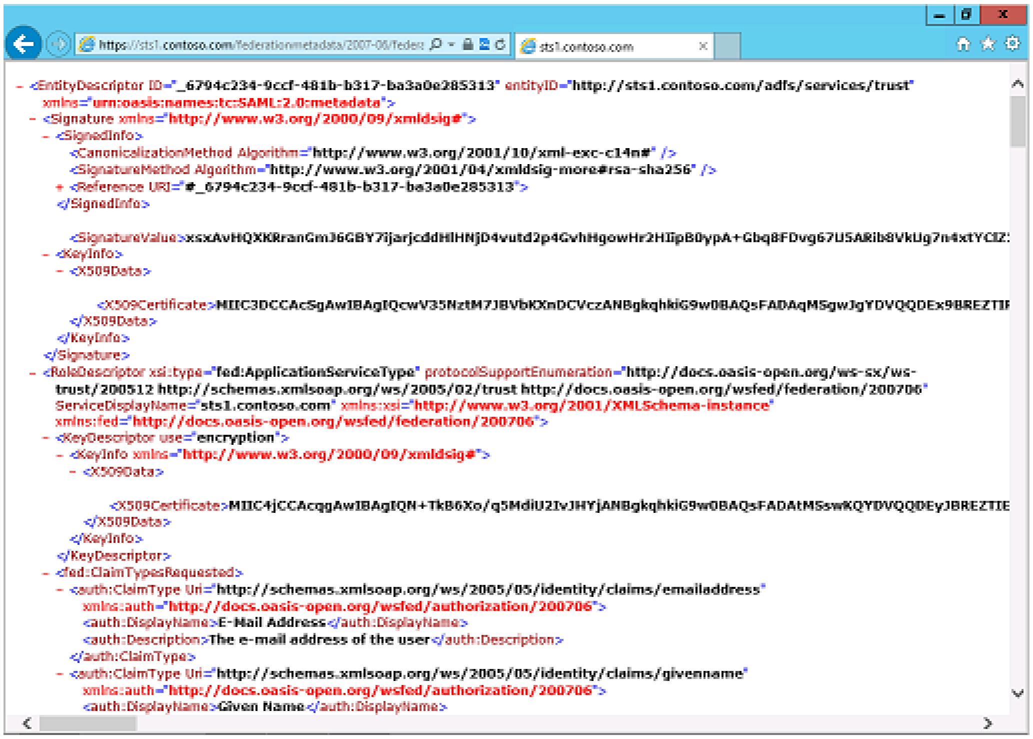
For more information, see Configure a Federation Server.

Verifying AD FS installation

Use the following steps to verify the AD FS installation:

1. On the AD FS server, open Internet Explorer.
2. Browse to the URL of the federation metadata. For example, https://sts1.contoso.com/federationmetadata/2007-06/federationmetadata.xml

   You may need to turn on **Compatibility View** in Internet Explorer.
3. Verify that no certificate-related warnings appear. If necessary, check your certificate and DNS settings.



```
- <EntityDescriptor ID="_6794c234-9ccf-481b-b317-ba3a0e285313" entityID="http://sts1.contoso.com/adfs/services/trust"
    xmlns="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/2001/04/xmldsig-more#rsa-sha256" />
      + <Reference URI="#_6794c234-9ccf-481b-b317-ba3a0e285313">
      </SignedInfo>

        <SignatureValue>xsxAvHQXKRranGm36GBY7ijarjcddHlHNjD4vutd2p4GvhHgowHr2HIipB0ypA+Gbq8FDvg67USARib8VkUg7n4xtYCIZ:
    - <KeyInfo>
      - <X509Data>

            <X509Certificate>MIIC3DCCAcSgAwIBAgIQcwV35NztM7JBVbKXnDCVczANBgkqhkiG9w0BAQsFADAqMSgwJgYDVQQDEx9BREZTIF
        </X509Data>
      </KeyInfo>
    </Signature>
  - <RoleDescriptor xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-
      trust/200512 http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706"
      ServiceDisplayName="sts1.contoso.com" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706">
    - <KeyDescriptor use="encryption">
      - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        - <X509Data>

              <X509Certificate>MIIC4jCCAcqgAwIBAgIQN+TkB6Xo/q5MdiU2IvJHYjANBgkqhkiG9w0BAQsFADAtMSswKQYDVQQDEyJBREZTIE
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
    - <fed:ClaimTypesRequested>
      - <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
          xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>E-Mail Address</auth:DisplayName>
          <auth:Description>The e-mail address of the user</auth:Description>
        </auth:ClaimType>
      - <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
          xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>Given Name</auth:DisplayName>
```

See Also

Implement claims-based authentication: internal access

Configure the Microsoft Dynamics CRM Server for claims-based authentication

After you have installed AD FS, you need to set the Microsoft Dynamics CRM Server binding type and root domains before you enable claims-based authentication.

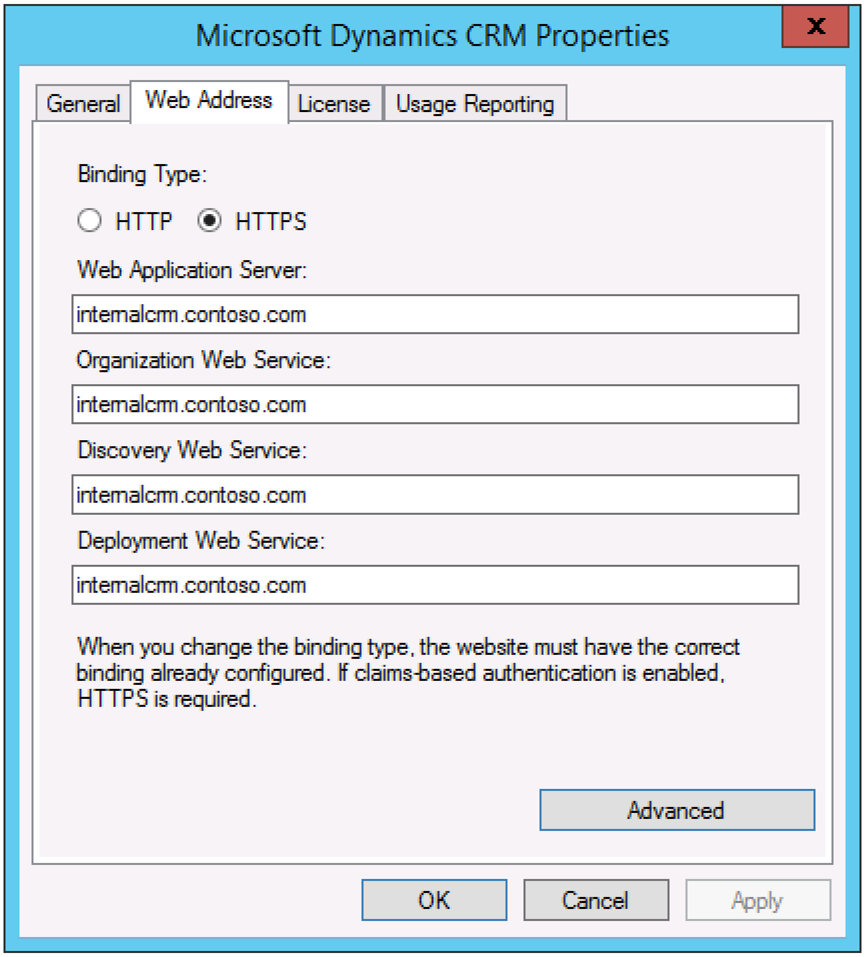
Set Microsoft Dynamics CRM Server binding to HTTPS and configure the root domain web addresses

▶

1. On the Microsoft Dynamics CRM server, start the Deployment Manager.
2. In the **Actions** pane, click **Properties**.
3. Click the **Web Address** tab.
4. Under **Binding Type**, select **HTTPS**.
5. Verify that the web addresses are valid for your SSL certificate and the SSL port bound to the Microsoft Dynamics CRM website. Because you are configuring Microsoft Dynamics CRM Server to use claims authentication for internal access, use the host name for the root domain web addresses.

For example, for a *.contoso.com wildcard certificate, you would use internalcrm.contoso.com for the web addresses.

If you install AD FS and Microsoft Dynamics CRM Server on separate servers, do not specify port 443 for the Web Application Server, Organization Web Service, or Discovery Web Service.



Binding Type:

○ HTTP ● HTTPS

Web Application Server: internalcrm.contoso.com

Organization Web Service: internalcrm.contoso.com

Discovery Web Service: internalcrm.contoso.com

Deployment Web Service: internalcrm.contoso.com

When you change the binding type, the website must have the correct binding already configured. If claims-based authentication is enabled, HTTPS is required.

6. Click **OK**.

> **Warning**
> If CRM for Outlook clients were configured using the old binding values, these clients will need to be configured with the new values.

The CRMAppPool account and the Microsoft Dynamics CRM encryption certificate

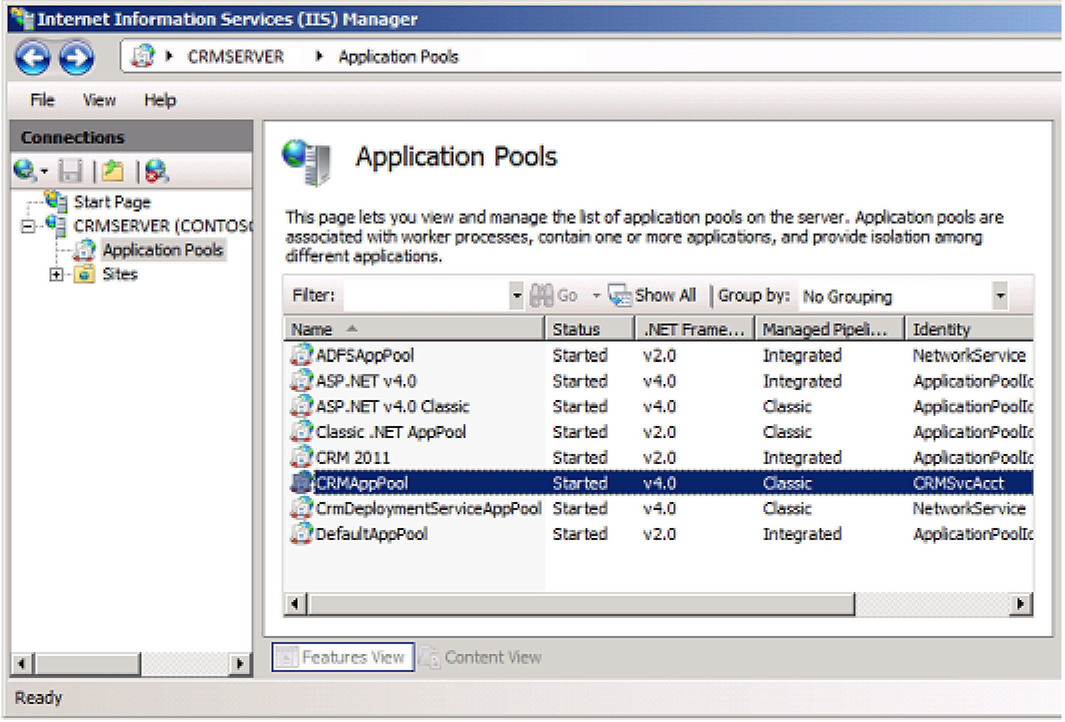
The certificate you specify in the Configure Claims-Based Authentication Wizard is used by AD FS to encrypt security tokens issued to the Microsoft Dynamics CRM Server client. The

CRMAppPool account of each Microsoft Dynamics CRM web application must have read permission to the private key of the encryption certificate.

1. On the Microsoft Dynamics CRM server, create a Microsoft Management Console (MMC) with the **Certificates** snap-in console that targets the **Local computer** certificate store.
2. In the console tree, expand the **Certificates (Local Computer)** node, expand the **Personal** store, and then click **Certificates**.
3. In the details pane, right-click the encryption certificate specified in the Configure Claims-Based Authentication Wizard, point to **All Tasks**, and then click **Manage Private Keys**.
4. Click **Add**, (or select the Network Service account if that is the account you used during Setup) add the **CRMAppPool** account, and then grant **Read** permissions.

Note

You can use IIS Manager to determine what account was used during setup for the CRMAppPool account. In the Connections pane, click Application Pools, and then check the Identity value for CRMAppPool.



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...	Identity
ADFSAppPool	Started	v2.0	Integrated	NetworkService
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIc
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIc
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIc
CRM 2011	Started	v2.0	Integrated	ApplicationPoolIc
CRMAppPool	Started	v4.0	Classic	CRMSvcAcct
CrmDeploymentServiceAppPool	Started	v4.0	Classic	NetworkService
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIc

5. Click **OK**.

Configuring claims-based authentication using the Configure Claims-Based Authentication Wizard

Run the Configure Claims-Based Authentication Wizard to enable claims authentication on your Microsoft Dynamics CRM Server.

1. On the Microsoft Dynamics CRM server, start the Deployment Manager.
2. In the **Deployment Manager** console tree, right-click **Microsoft Dynamics CRM**, and then click **Configure Claims-Based Authentication**.
3. Review the contents of the page, and then click **Next**.
4. On the **Specify the security token service** page, enter the federation metadata URL, such as https://sts1.contoso.com/federationmetadata/2007-06/federationmetadata.xml.

   This data is typically located on the website where Active Directory Federation Services is running. To verify the correct URL, open an Internet browser and view the federation metadata URL. Verify that no certificate-related warnings appear.
5. Click **Next**.
6. On the **Specify the encryption certificate** page, specify the encryption certificate in one of two ways:
   - In the **Certificate** box, type the complete common name (CN) of the certificate by using the format CN=certificate_subject_name.
   - Under **Certificate**, click **Select**, and then select a certificate.

   This certificate is used by AD FS to encrypt authentication security tokens that are issued to the Microsoft Dynamics CRM client.

   > **Note**
   > The Microsoft Dynamics CRM service account must have Read permissions for the private key of the encryption certificate. For more information, see “The CRMAppPool account and the Microsoft Dynamics CRM encryption certificate” above.
7. Click **Next**.

   The Configure Claims-Based Authentication Wizard verifies the token and certificate that you specified.
8. On the **System Checks** page, review the results, perform any steps required to fix problems, and then click **Next**.
9. On the **Review your selections and then click Apply** page, verify your selections, and then click **Apply**.
10. Note the URL you must use to add the relying party to the security token service. View and save the log file for later reference.
11. Click **Finish**.

Configuring claims-based authentication using Windows PowerShell

1. On the Microsoft Dynamics CRM server, open a Windows PowerShell prompt.
2. Add the Microsoft Dynamics CRM Windows PowerShell snap-in:

```
PS > Add-PSSnapin Microsoft.Crm.PowerShell
```

3. Get the claims-based authentication settings:

   ```
   PS > $claims = Get-CrmSetting -SettingType "ClaimsSettings"
   ```

4. Configure the claims-based authentication object:

   ```
   PS > $claims.Enabled = 1 (or $true) PS >
   $claims.EncryptionCertificate = certificate_namePS >
   $claims.FederationMetadataUrl = federation_metadata_URL
   ```

   Where:

   - 1 = "true".
   - **certificate_name** is the name of the encryption certificate.
   - **federation_metadata_URL** is the federation metadata URL for the security token service. (For example, https://sts1.contoso.com/federationmetadata/2007-06/federationmetadata.xml.)

5. Set the claims-based authentication values:

   ```
   PS > Set-CrmSetting $claims
   ```

Set Read permissions for the ADFSAppPool account

If you are installing AD FS on a separate server, verify the account used for the ADFSAppPool application pool has **Read** permissions. See the preceding topic “The CRMAppPool account and the Microsoft Dynamics CRM encryption certificate” for the process steps.

See Also

Implement claims-based authentication: internal access

Configure the AD FS server for claims-based authentication

After enabling claims-based authentication, the next step is to add and configure the claims provider and relying party trusts in AD FS.

Configure the claims provider trust

You need to add a claims rule to retrieve the user principal name (UPN) attribute from Active Directory and send it to Microsoft Dynamics CRM as a UPN.

Configure AD FS to send the UPN LDAP attribute as a claim to a relying party

1. On the server running AD FS, start AD FS Management.
2. In the **Navigation Pane**, expand **Trust Relationships**, and then click **Claims Provider Trusts**.
3. Under **Claims Provider Trusts**, right-click **Active Directory**, and then click **Edit Claims**

Rules.

4. In the Rules Editor, click **Add Rule**.
5. In the **Claim rule template** list, select the **Send LDAP Attributes as Claims** template, and then click **Next**.
6. Create the following rule:
   - Claim rule name: *UPN Claim Rule* (or something descriptive)
   - Add the following mapping:
     i. Attribute store: **Active Directory**
     ii. LDAP Attribute: **User Principal Name**
     iii. Outgoing Claim Type: **UPN**
7. Click **Finish**, and then click **OK** to close the Rules Editor.

Configure a relying party trust

After you enable claims-based authentication, you must configure Microsoft Dynamics CRM Server as a relying party to consume claims from AD FS for authenticating internal claims access.

▶

1. On the server running AD FS, start AD FS Management.
2. In the **Navigation Pane**, expand **Trust Relationships**, and then click **Relying Party Trusts**.
3. On the **Actions** menu located in the right column, click **Add Relying Party Trust**.
4. In the **Add Relying Party Trust Wizard**, click **Start**.
5. On the **Select Data Source** page, click **Import data about the relying party published online or on a local network**, and then type the URL to locate the federationmetadata.xml file.

   This federation metadata is created during claims setup. Use the URL listed on the last page of the Configure Claims-Based Authentication Wizard (before you click **Finish**), for example, https://internalcrm.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml. Verify that no certificate-related warnings appear.
6. Click **Next**.
7. On the **Specify Display Name** page, type a display name, such as CRM Claims Relying Party, and then click **Next**.
8. On the **Configure Multi-factor Authentication Now** page, make your selection and click **Next**.
9. On the **Choose Issuance Authorization Rules** page, click **Permit all users to access this relying party**, and then click **Next**.
10. On the **Ready to Add Trust** page, on the **Identifiers** tab, verify that **Relying party identifiers** has a single identifier such as the following:
    - https://internalcrm.contoso.com

    If your identifier differs from the above example, click **Previous** in the **Add Relying Party**

Trust Wizard and check the Federation metadata address.

11. Click **Next**, and then click **Close**.
12. If the Rules Editor appears, click **Add Rule**. Otherwise, in the **Relying Party Trusts** list, right-click the relying party object that you created, click **Edit Claims Rules**, and then click **Add Rule**.

    Important

    Be sure the **Issuance Transform Rules** tab is selected.
13. In the **Claim rule template** list, select the **Pass Through or Filter an Incoming Claim** template, and then click **Next**.
14. Create the following rule:
    - Claim rule name: *Pass Through UPN* (or something descriptive)
    - Add the following mapping:

      i. Incoming claim type: **UPN**

      ii. **Pass through all claim values**
15. Click **Finish**.
16. In the **Rules Editor**, click **Add Rule**, in the **Claim rule template** list, select the **Pass Through or Filter an Incoming Claim** template, and then click **Next**.
17. Create the following rule:
    - Claim rule name: *Pass Through Primary SID* (or something descriptive)
    - Add the following mapping:

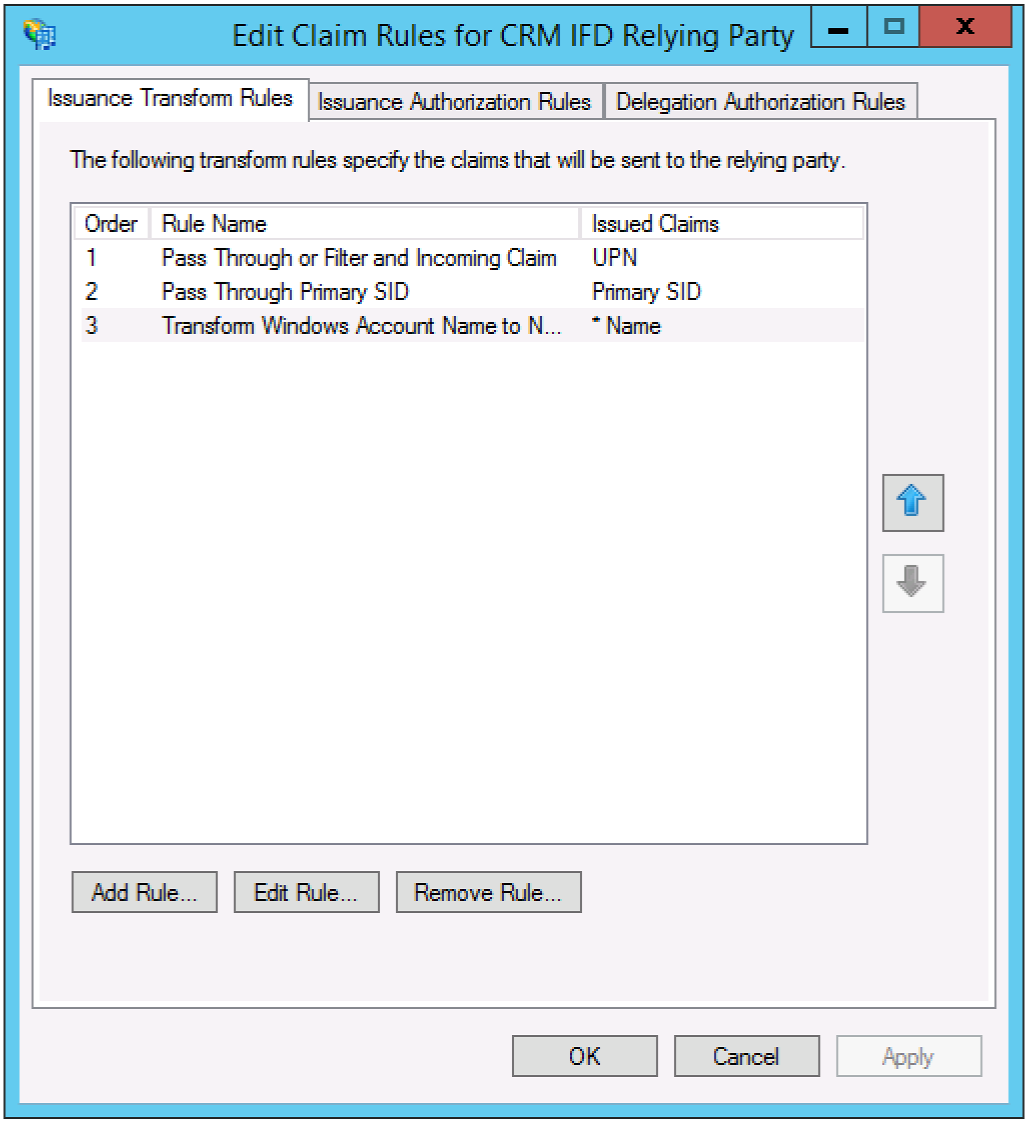
      i. Incoming claim type: **Primary SID**

      ii. **Pass through all claim values**
18. Click **Finish**.
19. In the **Rules Editor**, click **Add Rule**.
20. In the **Claim rule template** list, select the **Transform an Incoming Claim** template, and then click **Next**.
21. Create the following rule:
    - Claim rule name: *Transform Windows Account Name to Name* (or something descriptive)
    - Add the following mapping:

      i. Incoming claiming type: **Windows account name**

      ii. Outgoing claim type: **Name** or *** Name**

      iii. **Pass through all claim values**
22. Click **Finish**, and when you have created all three rules, click **OK** to close the Rules Editor.


Edit Claim Rules for CRM IFD Relying Party
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Pass Through or Filter and Incoming Claim	UPN
2	Pass Through Primary SID	Primary SID
3	Transform Windows Account Name to N...	* Name

This illustration shows the three relying party trust rules you create.

The relying party trust you created defines how AD FS Federation Service recognizes the Microsoft Dynamics CRM relying party and issues claims to it.

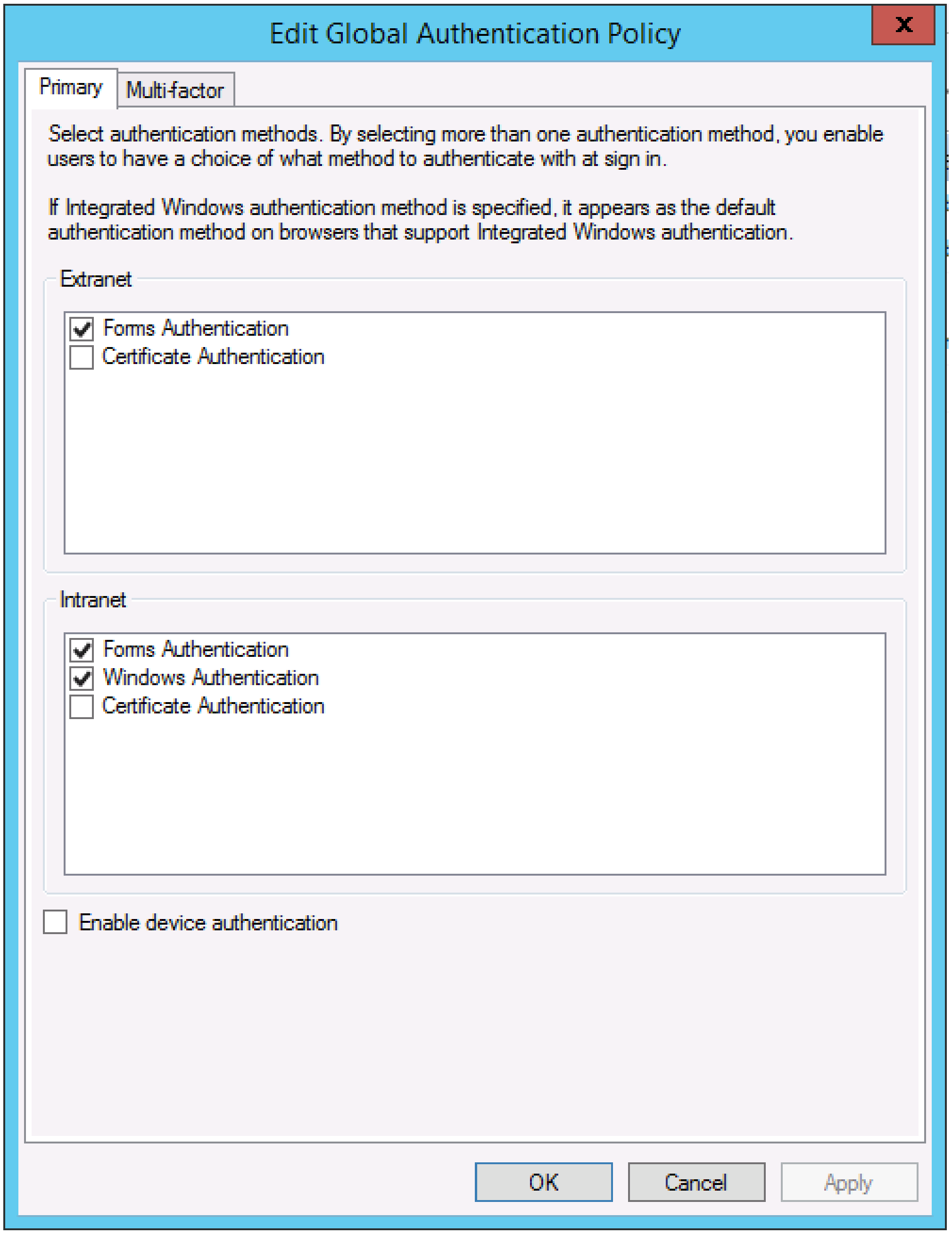
Enable Forms Authentication

In AD FS in Windows Server 2012 R2, forms authentication is not enabled by default.

▶

1. Log on to the AD FS server as an administrator.
2. Open the AD FS management console and click **Authentication Policies**.
3. Under **Primary Authentication**, **Global Settings**, **Authentication Methods**, click **Edit**.

4. Under **Intranet**, enable (check) **Forms Authentication**.



Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.

If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.

Extranet

☑ Forms Authentication
□ Certificate Authentication

Intranet

☑ Forms Authentication
☑ Windows Authentication
□ Certificate Authentication

□ Enable device authentication

See Also

Implement claims-based authentication: internal access

Add the AD FS website to the Local intranet security zone

Because the AD FS website is loaded as a FQDN, Internet Explorer places it in the **Internet** zone. By default, Internet Explorer clients do not pass Kerberos tickets to websites in the **Internet** zone. You must add the AD FS website to the **Intranet** zone in Internet Explorer on each client computer accessing Microsoft Dynamics CRM data internally.

▶ Add the AD FS server to the Local intranet zone

1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. Click the **Security** tab, click the **Local intranet** zone, and then click **Sites**.
3. Click **Advanced**.
4. In **Add this website to the zone**, type the URL for your AD FS server, for example, https://sts1.contoso.com.
5. Click **Add**, click **Close**, and then click **OK**.
6. Select the **Advanced** tab. Scroll down and verify that under Security **Enable Integrated Windows Authentication** is checked.
7. Click **OK** to close the Internet Options dialog box.

You will need to update the Local intranet zone on each client computer accessing Microsoft Dynamics CRM data internally. To use Group Policy to push this setting to all domain-joined internal client computers do the following.

▶ To use Group Policy to update the Local intranet zone

1. Use Internet Explorer to add the AD FS server to the Local intranet zone following the preceding steps. You will import these settings in your Group Policy Object (GPO).
2. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
3. Right-click the Group Policy Object (GPO) you use to publish changes to client computers in your domain and then click **Edit**.
4. Under **User Configuration**, expand **Policies**, expand **Windows Settings**, expand **Internet Explorer Maintenance**, click **Security**, and then double-click **Security Zones and Content Ratings**.
5. Under **Security Zones and Privacy** select **Import the current security zones and privacy settings**.

   Read the information about enhanced security configuration carefully. If the local intranet zone is considered a trusted zone without enhanced security configuration, click **Continue**. If the local intranet zone requires enhanced security, follow the directions on this screen and click **Cancel.**
6. Click **OK**.
7. Group Policy setting will refresh after 90 minutes. Clients can refresh immediately by running **gpudate /force**.

See Also

Implement claims-based authentication: internal access

Register the AD FS server as a service principal name (SPN)

A service principal name, also known as an SPN, is a name that uniquely identifies an instance of a service. Ensuring that the correct SPNs are set becomes important when applications such as Microsoft Dynamics CRM, Microsoft SQL Server Reporting Services, and Microsoft SQL Server are split onto multiple servers. When these applications are split across servers, the users' credentials must be passed from one server to another. This process, known as Kerberos delegation, allows a service to impersonate your credentials to another server.

For more information on SPNs, see: Configuring service principal names (SPNs)

Register the AD FS server as a service principal name (SPN)

1. Rerun the Configure Claims-Based Authentication Wizard and advance to the **Specify the security token service** page. Note the AD FS server in the **Federation metadata URL** (for example, sts1.contoso.com).
2. Open a command prompt.
3. Type the following commands: (replace your data in the example command below)
   - **c:\>setspn -s http/sts1.contoso.com contoso\crmserver$**

     Important
     If you’ve deployed AD FS on a second server, replace **crmserver$** with **adfsserver$** in the above sample command. **Adfsserver** is the name of the server running AD FS.
   - **c:\>iisreset**

See Also

Implement claims-based authentication: internal access

Test internal claims-based authentication

You should now be able to access Microsoft Dynamics CRM Server internally using claims authentication. Browse to the internal Microsoft Dynamics CRM webpage (for example, https://internalcrm.contoso.com).

You will be required to log on several times to the Microsoft Dynamics CRM webpage. Subsequent visits to the Microsoft Dynamics CRM website will only require one log on. In the browser, notice that the AD FS URL is loaded and then directed back to the Microsoft Dynamics CRM server.

Troubleshooting

If the Microsoft Dynamics CRM website does not display, at a command prompt, run the **iisreset** command, and then try browsing to the Microsoft Dynamics CRM website again.

Try adding the following sites to your Trusted sites in your browser:

- https://sts1.contoso.com – change to what use in DNS
- https://internalcrm.contoso.com – change to what you use in DNS

See Also

Implement claims-based authentication: internal access

Implement claims-based authentication: external access

To enable claims-based authentication for external access to Microsoft Dynamics CRM Server data, do the following:

1. Complete the steps in the previous section, Implementing Claims-based Authentication - Internal Access.
2. Configure the Microsoft Dynamics CRM Server server for IFD.
3. Configure the AD FS for IFD.
4. Test external claims-based authentication.

In This Section

Configure the Microsoft Dynamics CRM Server for IFD

Configure the AD FS server for IFD

Test external claims-based authentication

See Also

Implement claims-based authentication: internal access

CRM for tablets and IFD

Configure the Microsoft Dynamics CRM Server for IFD

With internal claims authentication access enabled on Microsoft Dynamics CRM Server, you can now enable external claims access through IFD.

Configure an Internet-facing deployment using the Configure Internet-Facing Deployment Wizard

1. Start the Deployment Manager.
2. In the Deployment Manager console tree, right-click **Microsoft Dynamics CRM**, and then click **Configure Internet-Facing Deployment**.
3. Click **Next**.
4. On the **Make Microsoft Dynamics CRM available to users who connect through the Internet** page, type the domains for the specified Microsoft Dynamics CRM Server roles, and then click **Next**.

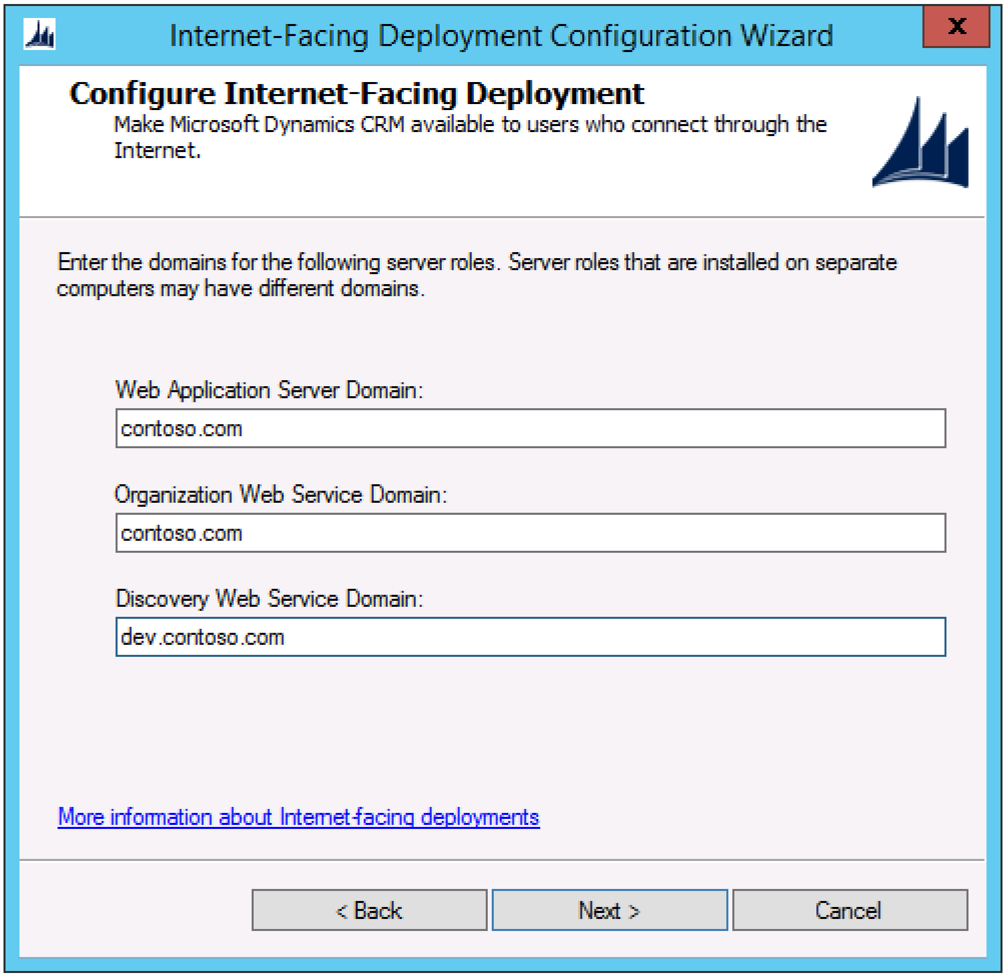
   Important

   - Specify domains, not servers.
   - If your deployment is on a single server or on servers that are in the same domain, the Web Application Server domain and Organization Web Service domain will be identical.
   - The Discovery Web Service domain must be a resolvable host name and not a root domain. For example: dev.contoso.com.
   - The Discovery Web Service domain must not match an organization's Fully Qualified Domain Name (FQDN). For example, the Discovery Web Service domain should not be: orgname.contoso.com.
   - The domains must be valid for the SSL certificate's common name or names.
   - The domains must be set to resolve correctly in DNS to your Microsoft Dynamics CRM servers holding the server roles.
   - The domains can be in a different domain than the domain which the Microsoft Dynamics CRM servers reside.

     Example domains:

   - Web Application Server domain: **contoso.com**
   - Organization Web Service domain: **contoso.com**
   - Discovery Web Service domain: **dev.contoso.com**

   With the example settings above, if your organization name was "orgname", clients would access your Microsoft Dynamics CRM website with the following URL: **https://orgname.contoso.com**.



Configure Internet-Facing Deployment

Make Microsoft Dynamics CRM available to users who connect through the Internet.

Enter the domains for the following server roles. Server roles that are installed on separate computers may have different domains.

Web Application Server Domain: contoso.com

Organization Web Service Domain: contoso.com

Discovery Web Service Domain: dev.contoso.com

For more information about web addresses on multiple servers, see Install Microsoft Dynamics CRM Server 2013 on multiple computers in the Microsoft Dynamics CRM Installing Guide.

5. In the **Enter the external domain where your Internet-facing servers are located** box, type the external domain information where your Internet-facing Microsoft Dynamics CRM Server servers are located, and then click **Next**.

   The domain you specify must be a sub-domain of the Web Application Server domain specified in the previous step. By default, "auth." is pre-pended to the Web Application Server domain.

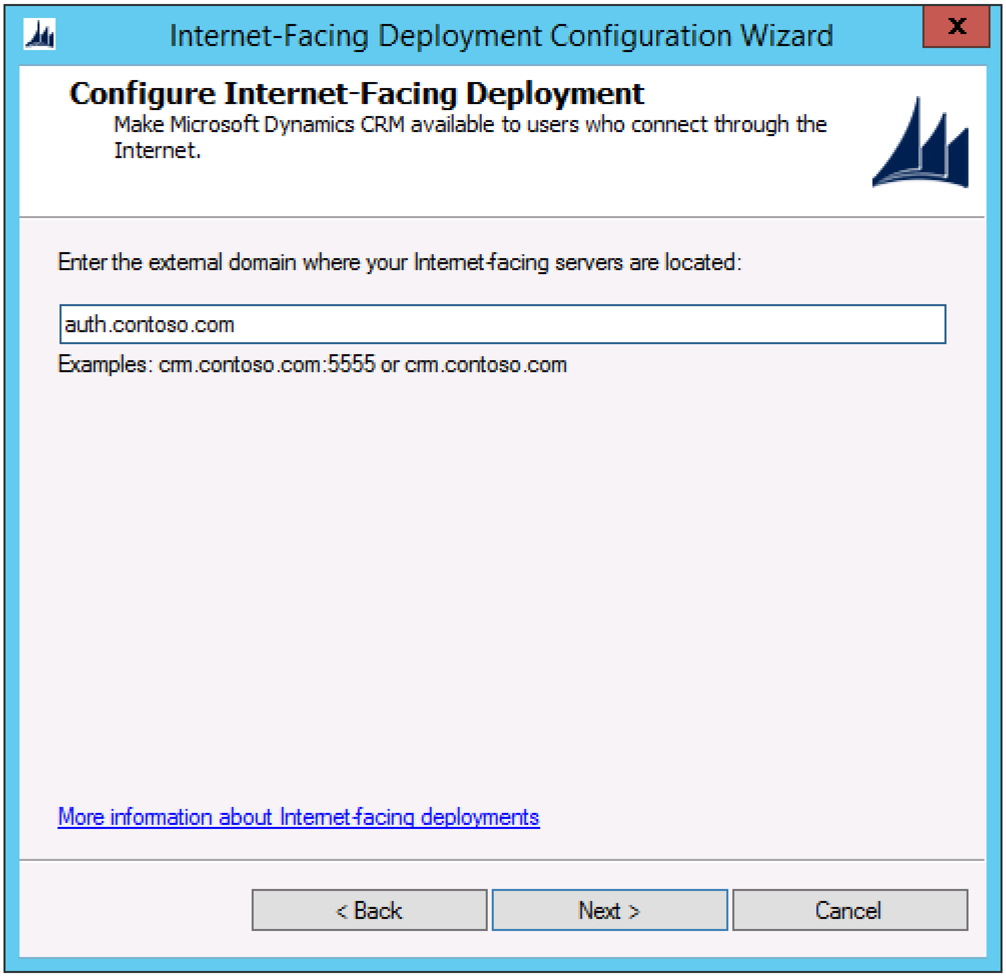
Important

- The external domain is used by the AD FS server when retrieving the Microsoft Dynamics CRM IFD federationmetadata.xml file.
- The external domain must not contain an organization name.
- The external domain must not contain an underscore character ("_").
- The external domain must be valid for the SSL certificate's common name or names.

- The external domain must be set to resolve correctly in DNS to your Microsoft Dynamics CRM server holding the Web Application Server role.

Example domain:

- External domain: **auth.contoso.com**


Internet-Facing Deployment Configuration Wizard
X

Configure Internet-Facing Deployment

Make Microsoft Dynamics CRM available to users who connect through the Internet.

Enter the external domain where your Internet-facing servers are located:

auth.contoso.com

Examples: crm.contoso.com:5555 or crm.contoso.com

More information about Internet-facing deployments
< Back
Next >
Cancel

6. On the **System Checks** page, review the results, fix any problems, and then click **Next**.
7. On the **Review your selections and then click Apply** page, verify your selections, and then click **Apply**.
8. Click **Finish**.
9. Run the following command at a command prompt: *iisreset*
10. If you have not already done so, add host records in DNS for the IFD endpoints (for example: orgname.contoso.com, auth.contoso.com, dev.contoso.com)

To Configure an Internet-facing deployment using Windows PowerShell

1. Open a Windows PowerShell prompt.
2. Add the Microsoft Dynamics CRM Windows PowerShell snap-in:

```
PS > Add-PSSnapin Microsoft.Crm.PowerShell
```

3. Get the IFD settings:

   ```
   PS > $ifd = Get-CrmSetting -SettingType "IfdSettings"
   ```

4. Configure the IFD object:

   ```
   PS > $ifd.Enabled = 1 (or $true) PS >
   $ifd.DiscoveryWebServiceRootDomain =
   Discovery_Web_Service_DomainPS > $ifd.ExternalDomain =
   External_Server_DomainPS >
   $ifd.OrganizationWebServiceRootDomain=
   Organization_Web_Service_DomainPS >
   $ifd.WebApplicationRootDomain = Web_Application_Server_Domain
   ```

   where:

   - 1 = "true".
   - Discovery_Web_Service_Domain is the Discovery Web Service domain.
   - External_Server_Domain is the external server domain.
   - Organization_Web_Service_Domain is the Organization Web Service domain.
   - Web_Application_Server_Domain is the Web Application Server domain.

   For the domain paths, the values for the paths must be in the form:

   server:port

   or

   server.domain.tld:port,

   where:

   - *server* is the computer name
   - *domain* is the complete sub domain path where the computer is located
   - *tld* is the top level domain, such as com or org
   - The *:port* designation is required if you are not using the standard http port (80) or https port (443).

   Typically, in a Full Server or Front-end Server role deployment, the path values are the same. However, if you deploy Microsoft Dynamics CRM on multiple servers with separate server roles, that is, where the Web Application Server, Organization Web Service, or Discovery Web Service server roles are located on different servers, these path values will be different:

   - Web Application Server. WebApplicationServerName.domain.tld:port
   - Organization Web Service. OrganizationWebServiceServerName.domain.tld:port
   - Discovery Web Service. DiscoveryWebServiceServerName.domain.tld:port

5. Set the Internet-facing deployment object.

   ```
   PS > Set-CrmSetting $ifd
   ```

See Also

Implement claims-based authentication: external access

Configure the AD FS server for IFD

After you have enabled IFD on the Microsoft Dynamics CRM Server you will need to create a relying party for the IFD endpoint on the AD FS server.

Configure relying party trusts

1. On the computer that is running Windows Server where the AD FS federation server is installed, start AD FS Management.
2. In the **Navigation Pane**, expand **Trust Relationships**, and then click **Relying Party Trusts**.
3. On the **Actions** menu located in the right column, click **Add Relying Party Trust**.
4. In the **Add Relying Party Trust Wizard**, click **Start**.
5. On the **Select Data Source** page, **click Import data about the relying party published online or on a local network**, and then type the URL to locate the federationmetadata.xml file.

   This federation metadata is created during IFD Setup, for example, https://auth.contoso.com/FederationMetadata/2007-06/FederationMetadata.xml.

   Type this URL in your browser and verify that no certificate-related warnings appear.
6. Click **Next**.
7. On the **Specify Display Name** page, type a display name, such as **CRM IFD Relying Party**, and then click **Next**.
8. On the **Configure Multi-factor Authentication Now** page, make your selection and click **Next**.
9. On the **Choose Issuance Authorization Rules** page, click **Permit all users to access this relying party**, and then click **Next**.
10. On the **Ready to Add Trust** page, on the **Identifiers** tab, verify that **Relying party identifiers** has three identifiers such as the following:
    - https://auth.contoso.com
    - https://orgname.contoso.com
    - https://dev.contoso.com

    If your identifiers differ from the above example, click **Previous** in the **Add Relying Party Trust Wizard** and check the Federation metadata address.
11. Click **Next**, and then click **Close**.
12. If the Rules Editor appears, click **Add Rule**. Otherwise, in the **Relying Party Trusts** list, right-click the relying party object that you created, click **Edit Claims Rules**, and then click **Add Rule**.

Important
Be sure the **Issuance Transform Rules** tab is selected.

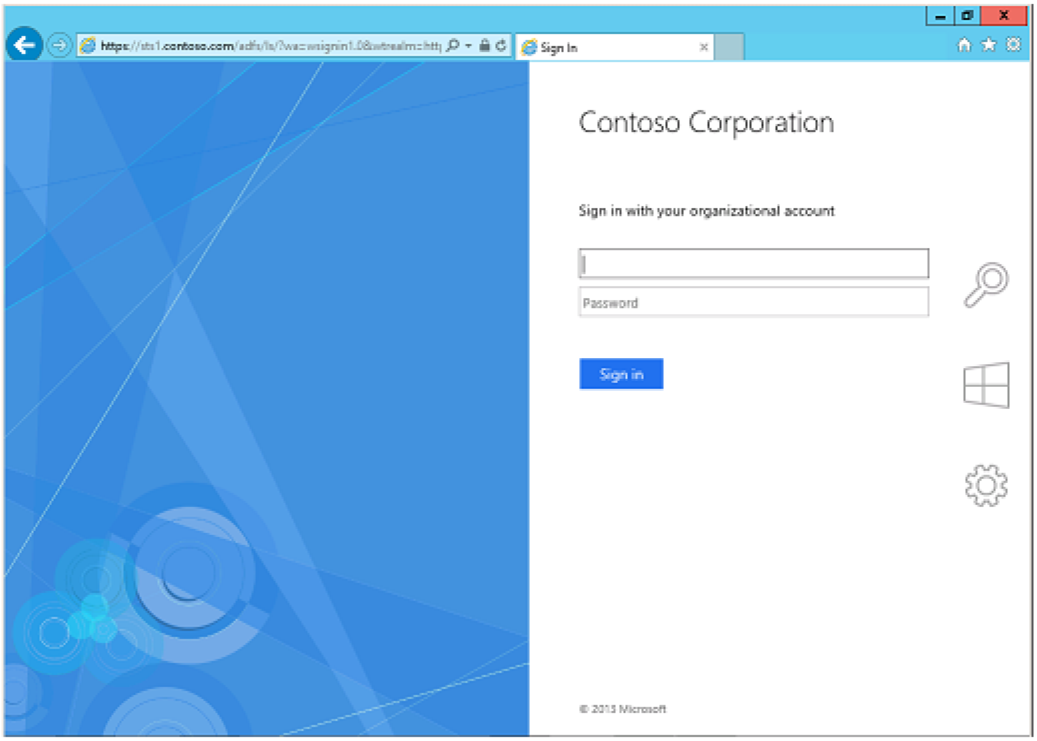
13. In the **Claim rule template** list, select the **Pass Through or Filter an Incoming Claim** template, and then click **Next**.
14. Create the following rule:
    - Claim rule name: **Pass Through UPN** (or something descriptive)
    - Add the following mapping:
        i. Incoming claim type: **UPN**
        ii. **Pass through all claim values**
15. Click **Finish**.
16. In the **Rules Editor**, click **Add Rule**, and in the **Claim rule template** list, select the **Pass Through or Filter an Incoming Claim** template, and then click **Next**.
    - Claim rule name: **Pass Through Primary SID** (or something descriptive)
    - Add the following mapping:
        i. Incoming claim type: **Primary SID**
        ii. **Pass through all claim values**
17. Click **Finish**.
18. In the **Rules Editor**, click **Add Rule**,
19. In the **Claim rule template** list, select the **Transform an Incoming Claim** template, and then click **Next**.
20. Create the following rule:
    - Claim rule name: **Transform Windows Account Name to Name** (or something descriptive)
    - Add the following mapping:
        i. Incoming claim type: **Windows account name**
        ii. Outgoing claim type: **Name** or *** Name**
        iii. **Pass through all claim values**
21. Click **Finish**, and, when you have created all three rules, click **OK** to close the Rules Editor.

See Also

Implement claims-based authentication: external access

Test external claims-based authentication

You should now be able to access Microsoft Dynamics CRM Server externally using claims authentication. Browse to your Microsoft Dynamics CRM website's external address (for example: https://orgname.contoso.com). You should see a screen like the following:



Contoso Corporation

Sign in with your organizational account

Sign in and verify that you have external access to Microsoft Dynamics CRM Server.

Note

You might need to add the external access website as a trusted site. Use the wild card designator (for example: https://*.contoso.com).

See Also

Implement claims-based authentication: external access

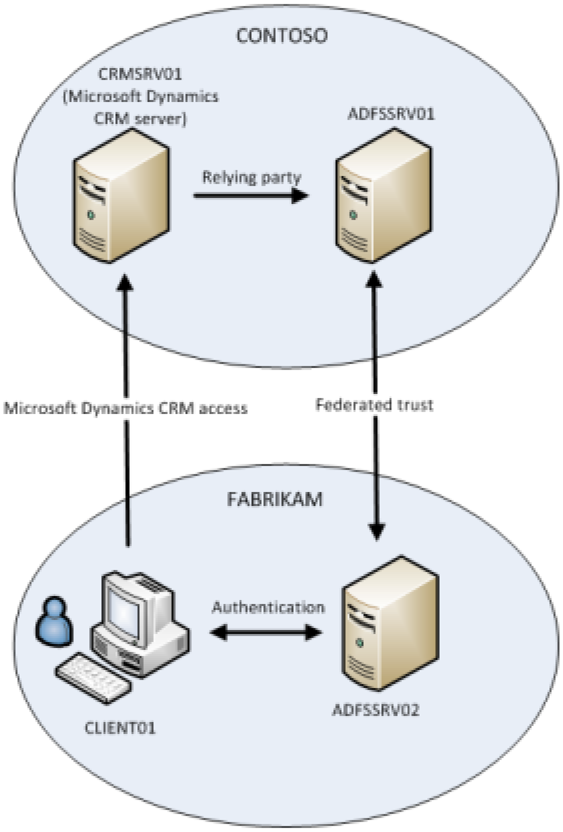
Claims access and partner companies

To provide access to an additional federation server, for example, if you want a partner company to have access to your Microsoft Dynamics CRM Server data, the partner company's federation server needs to have a trust relationship with your AD FS federation server. For more information about federation trusts, see Provide Users in Another Organization Access to Your Claims-Aware Applications and Services.

Note

For users from the federated domain to have access to your domain's CRM data, you'll need to create CRM user accounts using their domain; for example: username@fabrikam.com.

When creating a user for a federated domain, the user record fields are not populated from Active Directory. You will need to manually enter data such as user name, email, and phone number.



To set up a federation trust

1. On the AD FS server used with Microsoft Dynamics CRM Server, create a claims provider trust for the partner company's federation server. Add a claims rule to pass through UPN claims. Use the following settings:
   - Data Source: the path to the partner company's federation data.
   - Claim rule template: **Pass Through or Filter an Incoming Claim**
   - Claim rule name: *Pass through UPN* (or something descriptive)
   - Incoming claim type: **UPN**
   - **Pass through all claim values**
2. On the partner company's federation server, create a relying party trust for the AD FS server used with Microsoft Dynamics CRM Server. Use the following settings:
   - Data Source: the path to the AD FS server used with Microsoft Dynamics CRM Server federation data.
   - Rule type: **Issuance Transform Rules**
   - Claim rule template: **Send LDAP Attributes as Claims**

- Claim rule name: *LDAP UPN --> Claim UPN* (or something descriptive)
- LDAP Attribute: **User-Principal-Name**
- Outgoing Claim Type: **UPN**

Configure Microsoft Dynamics CRM for Outlook to use claims-based authentication

In an environment that supports claims-based authentication, a client (such as CRM for Outlook) can use federated AD FS to connect to the Microsoft Dynamics CRM Server. The client obtains credentials through federated AD FS and uses these credentials to be authenticated on the same or a different Active Directory domain to connect to the Microsoft Dynamics CRM Server.

You can connect CRM for Outlook on one Active Directory domain to a Microsoft Dynamics CRM server in a different Active Directory domain. You can do this when the credentials that CRM for Outlook uses on its own domain are authenticated by a server on the other domain. To make this work, use AD FS.

After federation is established, the client can use either its current domain credentials or different domain credentials when attempting to connect to the Microsoft Dynamics CRM Server. You specify which domain and which Active Directory to use through the home realm - an identity provider that authenticates the user.

Note
For external claims-based authentication deployments, use the Microsoft Dynamics CRM Server website's external address (for example: https://orgname.contoso.com) for the **Server URL** connection setting.

Set up a client for claims-based authentication

In the following procedure, you create a registry key on a single client computer. You may also want to consider using group policy so that you can make this registry change on multiple client computers.

▶

1. Make sure that a web browser on the client can reach the Microsoft Dynamics CRM Server URL with no certificate errors. If you use a self-signed certificate, you will need to import it to avoid certificate errors. After you import any needed certificates, you should be able to connect to the organization by using non-federated credentials.
2. To use federated credentials, specify HomeRealmUrl in the Windows registry, as shown here:

   Note
   This registry key is only needed if the claims provider server is different from the claims provider server used by Microsoft Dynamics CRM Server; for example,

the Microsoft Dynamics CRM client authenticates across realms to a different domain.

a. With Administrator privileges, open the Registry Editor.

b. Open the registry key **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MSCRMClient**.

c. Create the registry string **HomeRealmUrl**.

d. Enter the value data of the federated AD FS. This URL will end in /adfs/services/trust/mex. For example, https://adfs.contoso.com/adfs/services/trust/mex.

e. Close the Registry Editor.

f. Configure CRM for Outlook. For more information, see Task 2: Configure Microsoft Dynamics CRM for Outlook in the Microsoft Dynamics CRM Installing Guide.

You should now be able to connect CRM for Outlook to Microsoft Dynamics CRM Server by using claims-based authentication.

Use an administrative template (.adm) file

Modify the following sample data to create an .adm file to use group policy to publish the HomeRealmUrl registry setting.

```
CLASS MACHINECATEGORY "Microsoft Dynamics CRM"    KEYNAME
"Software\Policies\Microsoft\MSCRMClient"   POLICY "Home Realm URL"      EXPLAIN "Allow
Administrator to specify the Home Realm URL for federated domains."      PART "Specify
Home Realm URL (example: https://adfs.contoso.com/adfs/services/trust/mex" EDITTEXT
REQUIREDVALUENAME "HomeRealmUrl"      END PART   END POLICYEND CATEGORY
```

For more information, see Administrative Template File Format.

See Also

Install CRM for Outlook for Microsoft Dynamics CRM 2013 and Dynamics CRM Online

Configure IFD for Microsoft Dynamics CRM 2013

Additional considerations

The following section covers additional considerations for your claims-based authentication deployment.

In This Section

Manually updating a claims provider

Claims-based authentication and security token expiration

System time synchronization and claims-based authentication

Enable AD FS token signing

Changing the SSL certificate

Two-way domain trusts required

Access multiple organizations

CRM for tablets and IFD

AD FS port conflict

Manually updating a claims provider

By default, AD FS updates a relying party trust from federation metadata every 24 hours. You should manually update the relying party trust metadata if you make any of the following changes:

- You change the encryption certificate used for claims-based authentication.
- You change the root domain web addresses. To view these settings:
    a. Start the Deployment Manager.
    b. In the **Actions** pane, click **Properties**.
    c. Click the **Web Address** tab.
- You create a new organization. Create a DNS record for the organization before updating the metadata.
- You change the domains for the server roles for Microsoft Dynamics CRM Server entered in the IFD Configuration Wizard. To view these settings:
    a. Start the Deployment Manager.
    b. In the Deployment Managerconsole tree, right-click **Microsoft Dynamics CRM**, and then click **Configure Internet-Facing Deployment**.
    c. Click **Next**.
- You change the external domain.
- You change the certificate common name. To view these settings:
    a. Start the Deployment Manager.
    b. In the **Deployment Manager** console tree, right-click **Microsoft Dynamics CRM**, and then click **Configure Claims-based authentication**.
    c. Click **Next** twice.

To manually update a relying party trust from federation metadata

1. On the AD FS server, open AD FS Management.
2. Open the **Trust Relationships** folder, and then click either **Claims Provider Trusts** or **Relying Party Trusts**, depending on which trust you want to update.
3. In the details pane, right-click the claims provider trust or relying party trust that you want to update from federation metadata.
4. Click **Update from Federation Metadata**, and then click **Update**.

You can specify how often the Federation Service will monitor the federation metadata of relying parties and claims providers that are enabled for federation metadata monitoring.

To set the interval for monitoring metadata for trust partners using Windows PowerShell

1. Open a Windows PowerShell prompt.
2. Set the monitoring interval:

   ```
   PS > Set-ADFSProperties -MonitoringInterval <int>
   ```

   where:

   - *<int>* is the interval in minutes

Claims-based authentication and security token expiration

The lifetime of a default security token for a claims-based authentication deployment using AD FS is 60 minutes. By default, Microsoft Dynamics CRM Server is configured to display the **Authentication is Required** dialog box 20 minutes before the token expires.

In the **Authentication is Required** dialog box, if you click **Cancel**, the token expires as indicated. When the security token expires, you will need to start a new browser session to Microsoft Dynamics CRM to access your data. Any unsaved changes will be lost.

In the **Authentication is Required** dialog box, if you click **Sign In**, the **Sign-Out** page appears. When you close the Sign-Out page, one of the following occurs:

- If you have not deployed an Internet-facing deployment (IFD), you will automatically re-authenticate with domain credentials and a new security token will be issued.
- If you have an IFD deployment, you will be required to re-authenticate by entering your credentials on the login page.

By using Windows PowerShell, you can change the **TokenLifetime** property for the relying party objects that you created from 60 minutes to a longer period, such as 480 minutes (8 hours):

1. Open a Windows PowerShell prompt.
2. Add the AD FS snap-in to the Windows PowerShell session:

   ```
   PS > Add-PSSnapin Microsoft.Adfs.PowerShell
   ```

3. Configure the relying party token lifetime:

   ```
   PS > Get-ADFSRelyingPartyTrust -Name "relying_party"PS > Set-
   ADFSRelyingPartyTrust -Targetname "relying_party" -TokenLifetime
   480
   ```

   where:

   - *relying_party* is the name of the relying party that you created.

For more information, see: Setting the ADFS Timeout for CRM 2011 Internet Facing Deployments (IFD)

System time synchronization and claims-based authentication

The system time on the computer running the security token service (STS) must be synchronized with the computer running Microsoft Dynamics CRM. Servers on the same domain are normally synchronized automatically through the Windows Time service. If your STS server and Microsoft Dynamics CRM Server are on separate domains, you should periodically monitor the system time on the two servers to ensure that the time difference is not greater than 5 minutes.

Enable AD FS token signing

By default, Microsoft Dynamics CRM Server does not check for the presence or validity of the AD FS token signing certificate and does not use AD FS token signing. To enable validation and use of the AD FS token-signing certificate, create the TrustedIssuerCertificateValidation registry entry on all Front End Servers.

To create the TrustedIssuerCertificateValidation registry

1. Run regedit and locate and click the following registry subkey:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM

2. Create the following registry entry:

   Value name: **TrustedIssuerCertificateValidation**

   Value type: **String**

   Value data: (one of the following)

Value Data	Description
None	No validation of the certificate is done.
PeerTrust	The certificate is valid if it is in the trusted people store.
PeerOrChainTrust	The certificate is valid if the chain builds to a certification authority in the trusted root store.
PeerOrChainTrust	The certificate is valid if it is in the trusted people store, or if the chain builds to a certification authority in the trusted root store.

   Note
   The **Custom** value is not supported in Microsoft Dynamics CRM Server.

3. Close the Registry Editor.

For more information, see X509CertificateValidationMode Enumeration.

Note the following information regarding enabling AD FS token signing:

- By default, AD FS creates a self-signed certificate for signing tokens.

  Note
  If token signing is enabled, when the signing certificate expires AD FS creates a new signing certificate. The new signing certificate will need to be moved to the Trusted Root Certification Authorities store of all Microsoft Dynamics CRM servers.

- To use the self-signed certificate, do the following:

Export the signing certificate.

1. On the AD FS server, open AD FS Management, expand **Service**, and then expand **Certificates**.
2. Double-click the token-signing certificate, click the **Details** tab, and then click **Copy to File**.
3. Proceed through the Certificate Export Wizard using default values and save the certificate.

Import the signing certificate.

1. On the Microsoft Dynamics CRM server, create a Microsoft Management Console (MMC) with the **Certificates** snap-in console that targets the **Local computer** certificate store.
2. Import the token-signing certificate into the **Trusted Root Certification Authorities** store.

- You can use a signed certificate from a trusted CA instead of the self-signed certificate generated by AD FS.

For more information, see Certificate Requirements for Federation Servers.

Changing the SSL certificate

If you change the certificates used by Microsoft Dynamics CRM and AD FS, follow these steps.

Updating the SSL certificate

1. Add the new certificate to the AD FS server.
   a. Import the new certificate to the AD FS server.
   b. Grant the ADFSAppPool account **Read** permission to the new certificate
   c. Bind the new certificate to the AD FS website.
2. Add the new certificate to the Microsoft Dynamics CRM server.

   a. Import the new certificate to the Microsoft Dynamics CRM server.
   b. Grant the CRMAppPool account **Read** permission to the new certificate
   c. Bind the new certificate to the Microsoft Dynamics CRM website.

3. Start the **Deployment Manager** and run the **Configure Claims-Based Authentication Wizard** to use the new certificate.
4. On the AD FS server, update all the relying party trusts used by Microsoft Dynamics CRM.
5. If the certificate subject name changes, update the root domain web addresses to match the new subject name. For more information, see: Configure the Microsoft Dynamics CRM Server for claims-based authentication in this document.
6. Run the **iisreset** command on the AD FS and Microsoft Dynamics CRM servers.

Tip

Consider removing and unbinding the old certificate on the AD FS and Microsoft Dynamics CRM servers.

Two-way domain trusts required

Claims-based authentication between trusted domains requires two-way domain trust. A one way domain trust will result in the following error message:

For more information, see the following KB article An error message occurs in Microsoft Dynamics CRM 2011 when trying to access the CRM URL using a One-way Domain Trust

Access multiple organizations

If you have multiple Microsoft Dynamics CRM organizations on the same domain configured for IFD, you can access more than one organization by opening separate browser sessions.

In Internet Explorer:

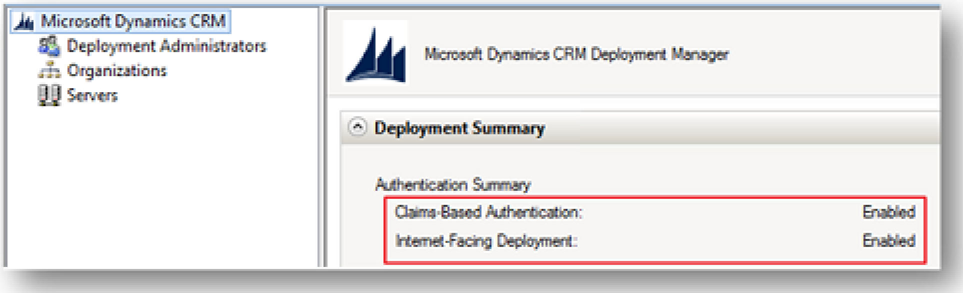
- **Safety** > **InPrivate Browsing**

or

- **File** > **New session**

CRM for tablets and IFD

Microsoft Dynamics CRM 2013 on-premises deployments require Internet Facing Deployment (IFD) for users to access their data on their tablets. If you have your Microsoft Dynamics CRM website available over the internet but it is not using the Microsoft Dynamics CRM IFD configuration, **it is not supported**. To verify that your on-premises deployment is configured for IFD, open Microsoft Dynamics CRM Deployment Manager on your Microsoft Dynamics CRM Server. The Authentication Summary section should show that both Claims-Based Authentication and Internet-Facing Deployment are enabled.



Microsoft Dynamics CRM
Deployment Administrators
Organizations
Servers
Microsoft Dynamics CRM Deployment Manager
Deployment Summary

Authentication Summary

Claims-Based Authentication: Enabled

Internet-Facing Deployment: Enabled

Important

For Microsoft Dynamics CRM for tablets to successfully connect to a new deployment of Microsoft Dynamics CRM Server 2013, you must run a Repair of Microsoft Dynamics CRM Server 2013 on the server running IIS where the Web Application Server role is installed *after* the Internet-Facing Deployment Configuration Wizard is successfully completed. More information: Uninstall, change, or repair Microsoft Dynamics CRM Server 2013.

See Also

Set up CRM for tablets

Configure IFD for Microsoft Dynamics CRM 2013

AD FS port conflict

When installing Microsoft Dynamics CRM on the same server as Windows Server 2012 R2 AD FS (not a recommended scenario), you may need to change the port used by AD FS to a port other than TCP 808. Sandbox Processing Service listens on Port 808, Microsoft Dynamics CRM Asynchronous Service and Web Application Server services communicates with the Sandbox Processing Service on Port 808. A port conflict could also cause issues for Microsoft Dynamics CRM Email Router, Microsoft Dynamics CRM for Outlook, and the Plug-in Registration Tool.

Check your AD FS event log for EventID 102 and the following in Exception details:

“System.ServiceModel.AddressAlreadyInUseException: There is already a listener on IP endpoint 0.0.0.0:808.”

If this exists, you need to change your AD FS port.

To change the port used by AD FS to another port such as 809, use the following PowerShell command: `Set-ADFSProperties -nettcpport 809`

For more information, see:

- Dynamics CRM IFD on Windows server 2012 R2 ADFS (aka ADFS 3.0) – CRM Addin for Outlook
- Network ports for Microsoft Dynamics CRM

- AD FS 2.0: How to Change the net.tcp Ports for Services and Administration

Troubleshoot Microsoft Dynamics CRM Server IFD

A quick checklist

Did you…	Reference
Configure DNS records?	See “DNS configuration” in the downloadable document
Install and bind your certificate on the Microsoft Dynamics CRM website?	See “Certificate selection and requirements” in the downloadable document
Add an AD FS signing certificate as a trusted certificate under the CRMAppPool account profile?	See “Enable AD FS token signing” in the downloadable document
Change the binding type for Microsoft Dynamics CRM websites to HTTPS and use the correct web addresses in Deployment Manager?	Configure the Microsoft Dynamics CRM Server for IFD
Give the CRMAppPool account the rights to use an existing certificate used by Microsoft Dynamics CRM as signing certificate? This could be the wildcard certificate installed on the Microsoft Dynamics CRM server.	Configure the Microsoft Dynamics CRM Server for claims-based authentication
Run the Configure Claims-Based Authentication Wizard from Microsoft Dynamics CRM Deployment Manager? Have you specified the correct URL in this wizard? Have you selected the appropriate encryption certificate?	Configure the Microsoft Dynamics CRM Server for claims-based authentication
Configure relying party trust in AD FS for Microsoft Dynamics CRM internal claims endpoint? Have you provided the correct URL for the Microsoft Dynamics CRM IFD claims endpoint? Have you setup the correct rules for the relying party trusts?	Configure the AD FS server for claims-based authentication Configure the AD FS server for IFD

AD FS

Use the following to verify your AD FS settings.

Review AD FS events

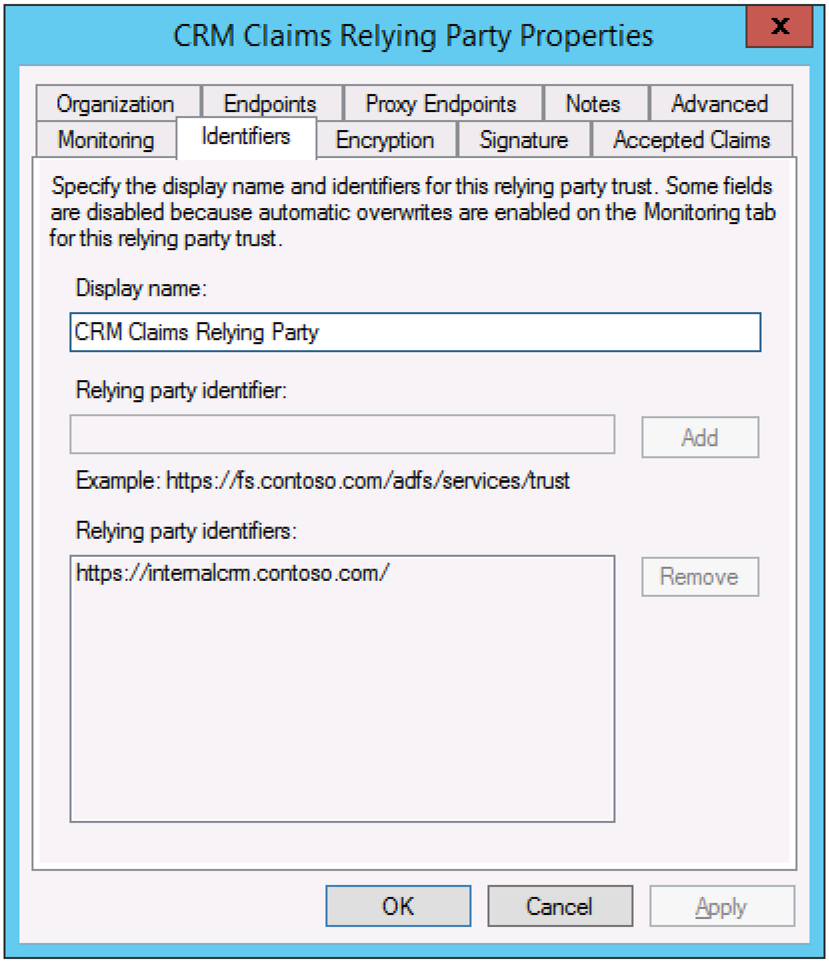
1. Open Event Viewer.
2. Expand **Applications and Services Logs**. Expand **AD FS**. Click **Admin**.
3. Review the events looking for errors.

   Events such as Event ID 184 describing an unknown relying party trust could indicate missing host records in DNS or incorrect path configuration for the relying party's federation metadata URL.

Verify relying party trust identifiers

1. Open the AD FS Management console.
2. Under **Trust Relationships**, click **Relying Party Trusts**. Verify the relying party trusts are enabled and not displaying an alert.
3. Right-click the relying party trust and click **Properties**. Click the **Identifiers** tab. You should see identifiers like the following.

   Relying party trust for claims: internalcrm.contoso.com



Specify the display name and identifiers for this relying party trust. Some fields are disabled because automatic overwrites are enabled on the Monitoring tab for this relying party trust.

Display name:

CRM Claims Relying Party

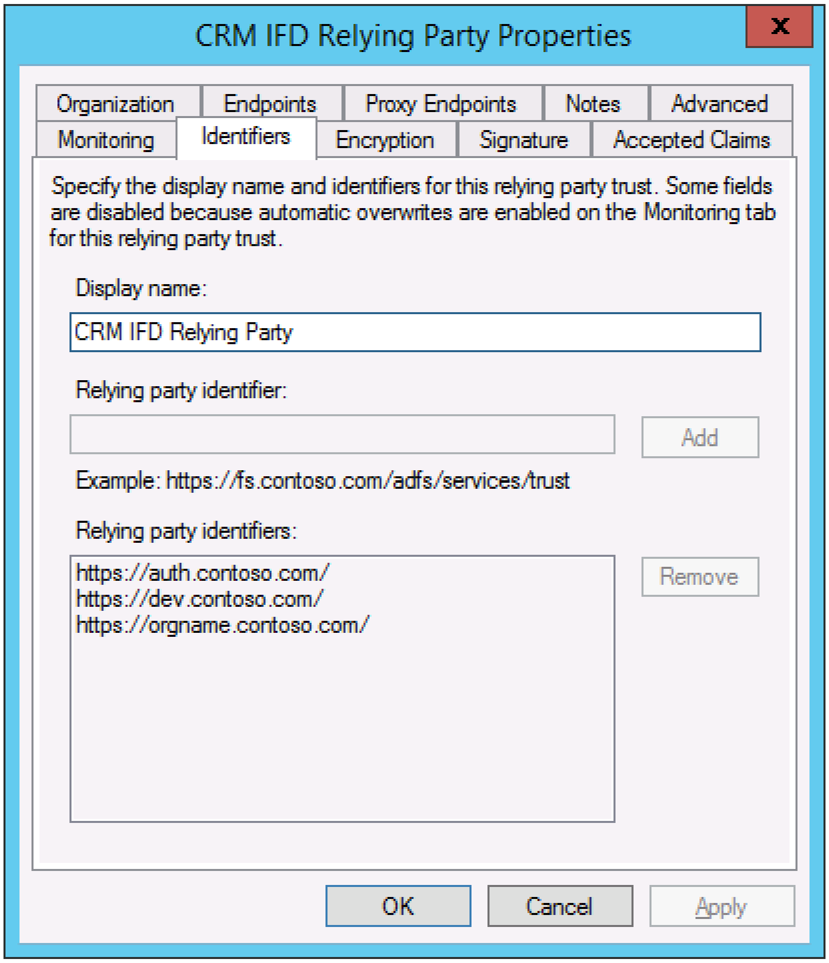
Relying party identifier:

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

Relying party identifiers:

https://internalcrm.contoso.com/

Relying party trust for IFD: auth.contoso.com



Specify the display name and identifiers for this relying party trust. Some fields are disabled because automatic overwrites are enabled on the Monitoring tab for this relying party trust.

Display name:

CRM IFD Relying Party

Relying party identifier:

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

Relying party identifiers:

https://auth.contoso.com/
https://dev.contoso.com/
https://orgname.contoso.com/

If your identifiers aren't similar to the above examples, check the path entered for the relying party's federation metadata URL on the **Monitoring** tab and check your DNS records.

When attempting an internal claims-based authentication connection, you might receive prompt for your credentials. Try the following steps.

Resolve prompt for credentials

1. Add the add website address for the AD FS server (for example, https://sts1.contoso.com) to the Trusted Intranet Zone in Internet Explorer.
2. Turn off Extended Protection. On the server running IIS for the Microsoft Dynamics CRM website:

   Turn off extended protection on the Microsoft Dynamics CRM website.

   a. Open IIS.
   b. Select the Microsoft Dynamics CRM website.
   c. Under IIS, double-click **Authentication**.

d. Right-click **Windows Authentication**, and then click **Advanced Settings**.

e. Set **Extended Protection** to **Off**.

For more AD FS troubleshooting information

1. See the following: Troubleshoot AD FS 2.0

HTTP Error 401.1 - Unauthorized: Access is denied

If the Microsoft Dynamics CRM website fails to display or produces the following error: HTTP Error 401.1 - Unauthorized: Access is denied, there are two steps to try to resolve this issue:

1. You might need to update the Federation metadata URLs and do an IIs reset. See KB2686840.
2. You might need to register the AD FS server as a service principal name (SPN). See “Register the AD FS server as a service principal name (SPN)” in the downloadable document.

Time differs between two servers

An authentication error can occur if the time between the AD FS and the Microsoft Dynamics CRM server differs by more than 5 minutes. See Windows Time Service Technical Reference for information on how to configure time synchronization on your servers.

See Also

Configure IFD for Microsoft Dynamics CRM 2013

Configure AD FS on the same server as Microsoft Dynamics CRM

Example DNS Settings – AD FS and Microsoft Dynamics CRM on the same server

The following are example DNS settings for a single-server deployment. A single domain – contoso.local – is used for internal access. A publicly registered domain – contoso.com – is used for external Microsoft Dynamics CRM access. Contoso.com can also be used for internal access. A single public IP address is required for external access to Microsoft Dynamics CRM.

The following table contains records configured in the **Internal DNS Zone: contoso.local**.

Name	Type	Data	Comment
Internal DNS Zone: contoso.local			The following record is configured in DNS on

Name	Type	Data	Comment
			your internal server.
crmserver	Host (A)	The IP address of the server where Microsoft Dynamics CRM and AD FS are installed.	Configured in DNS on your internal server.

The following table contains records configured in the **Internal DNS Zone: contoso.com**.

Name	Type	Data	Comment
Internal DNS Zone: contoso.com			The following record is configured in DNS on your internal server.
internalcrm	Alias (CNAME)	crmserver.contoso.local	Configured in DNS on your internal server. Used in the internal URL to access Microsoft Dynamics CRM. Internal URL: https://internalcrm.contoso.com:444

The following table contains records that must be created with **your public host domain service.**

Name	Type	Data	Comment
Public DNS: contoso.com			The following records must be created with your public host domain service. For performance and redundancy purposes you could also create these records in the contoso.com zone on your internal DNS server.
orgname	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection	Used in the external URL to access Microsoft Dynamics CRM. External URL: https://orgname.contoso.com:444

Name	Type	Data	Comment
dev	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection	The Microsoft Dynamics CRMDiscovery Web Service.
sts1	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection	The AD FS server.
auth	Host (A)	IP address of your Microsoft Dynamics CRM public-facing internet connection	The Microsoft Dynamics CRM IFD federation endpoint. This record will be used by the AD FS server when retrieving the Microsoft Dynamics CRM IFD federationmetadata.xml file.

For Windows Server 2008 or Windows Server 2012, you must append a port number to the URL in a single server installation. Appending a port number is required on a single server installation where Microsoft Dynamics CRM uses a non-default website with binding to a port other than the standard 443 port.

Set Microsoft Dynamics CRM Server binding to HTTPS and configure the root domain web addresses

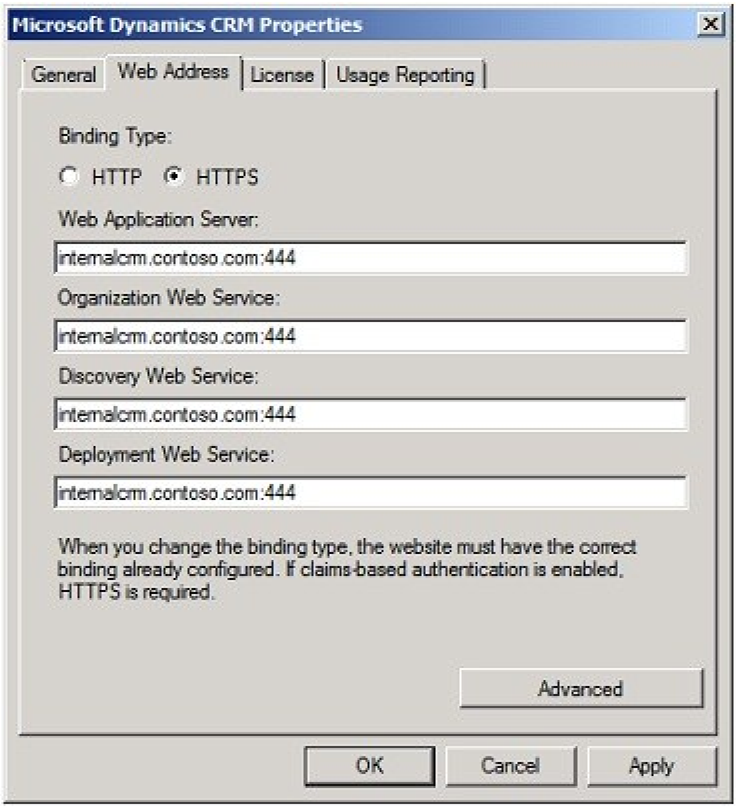
▶

1. On the Microsoft Dynamics CRM server, start the Deployment Manager.
2. In the **Actions** pane, click **Properties**.
3. Click the **Web Address** tab.
4. Under **Binding Type**, select **HTTPS**.
5. Verify that the web addresses are valid for your SSL certificate and the SSL port bound to the Microsoft Dynamics CRM website. Because you are configuring Microsoft Dynamics CRM Server to use claims authentication for internal access, use the host name for the root domain web addresses. The port number should match the settings for the Microsoft Dynamics CRM website in IIS.

   For example, for a *.contoso.com wildcard certificate, you would use internalcrm.contoso.com:444 for the web addresses.

   If you install AD FS and Microsoft Dynamics CRM Server on separate servers, do not specify port 443 for the Web Application Server, Organization Web Service, or Discovery

Web Service.



Binding Type:

○ HTTP ● HTTPS

Web Application Server: internalcrm.contoso.com:444

Organization Web Service: internalcrm.contoso.com:444

Discovery Web Service: internalcrm.contoso.com:444

Deployment Web Service: internalcrm.contoso.com:444

When you change the binding type, the website must have the correct binding already configured. If claims-based authentication is enabled, HTTPS is required.

6. Click **OK**.

   ⚠ **Warning**
   If CRM for Outlook clients were configured using the old binding values, these clients will need to be configured with the new values.

Configure AD FS on Windows Server 2012

This topic provides information that is unique to Active Directory Federation Services (AD FS) in Windows Server 2012 (not R2). First configure IFD and claims as described in this article, and then follow the instructions below to complete the AD FS configuration. In addition, your Microsoft Dynamics CRM 2011 server must be running Microsoft Dynamics CRM 2011 Update Rollup 13 or later.

Configure a Microsoft Dynamics CRM 2011 Advanced Setting

At the time of this writing, AD FS has a known issue publishing metadata for MEX endpoints. After configuring claims, MEX endpoints are no longer reachable which an administrator sees as an invalid URL. This problem applies to AD FS in Windows Server 2012 only. AD FS 2.0

(Windows Server 2008), and AD FS in Windows Server 2012 R2 will continue to automatically configure the MEX endpoints correctly.

When using AD FS in Windows Server 2012, it is necessary to update an advanced setting on a Microsoft Dynamics CRM 2011 (on-premises) server deployment. The following procedure describes how to configure the server setting.

How to Configure the ActiveMexEndpoint Advanced Setting

1. Log on as administrator to a Microsoft Dynamics CRM 2011 server that has the Deployment Manager installed.

   If you have more than one server with Deployment Manager installed, perform these steps on only one deployment server in your deployment.
2. Create a PowerShell script file named UpdateMEXEndpoint.ps1 using the PowerShell ISE or your favorite editor.
3. Copy the following PowerShell code, paste it into the file you just created, and save the file.

```
Param
(
    #optional params
    [string]$ConfigurationEntityName="FederationProvider",
    [string]$SettingName="ActiveMexEndpoint",
    [object]$SettingValue,
    [Guid]$Id
)
$RemoveSnapInWhenDone = $False

if (-not (Get-PSSnapin -Name Microsoft.Crm.PowerShell -
ErrorAction SilentlyContinue))
{
    Add-PSSnapin Microsoft.Crm.PowerShell
    $RemoveSnapInWhenDone = $True
}
//For AD FS 2.1, use the following:
$Id=(Get-CrmAdvancedSetting -ConfigurationEntityName
FederationProvider -Id 26332692-CD1E-4DD6-BD5B-07326C43302E -
Setting ActiveMexEndpoint).Attributes[0].Value
```

```
//For AD FS 2.0 or AD FS 2.2, use the following:
$Id=(Get-CrmAdvancedSetting -ConfigurationEntityName
FederationProvider -Setting
ActiveMexEndpoint).Attributes[0].Value

$setting = New-Object
"Microsoft.Xrm.Sdk.Deployment.ConfigurationEntity"
$setting.LogicalName = $ConfigurationEntityName
if($Id) { $setting.Id = $Id }

$setting.Attributes = New-Object
"Microsoft.Xrm.Sdk.Deployment.AttributeCollection"
$keypair = New-Object
"System.Collections.Generic.KeyValuePair[String, Object]"
($SettingName, $SettingValue)
$setting.Attributes.Add($keypair)

Set-CrmAdvancedSetting -Entity $setting

if($RemoveSnapInWhenDone)
{
    Remove-PSSnapin Microsoft.Crm.PowerShell
}
```

4. Run the preceding shell script from within a PowerShell window using the following command. Substitute the name of your configured AD FS host for <ADFS STSHOST> in the command.

   UpdateMEXEndpoint.ps1 –SettingValue "https://<ADFS STSHOST>/adfs/services/trust/mex"

   For example, if your STS is using sts.contoso.com, the command would be:
   UpdateMEXEndpoint.ps1 –SettingValue "https://sts.contoso.com/adfs/services/trust/mex"

   Running this command will update your Microsoft Dynamics CRM 2011 deployment to connect to AD FS using the endpoint provided in the *SettingValue* parameter.

For more information about the **Set-CrmAdvancedSetting** cmdlet, see the "Read and Update Advanced Settings with PowerShell" section of Use Advanced Configuration Settings (ConfigDB).

See Also

Configure IFD for Microsoft Dynamics CRM 2013

Send us your feedback about this document

We appreciate hearing from you. To send your feedback, click the following link and type your comments in the message body.

Note

The subject-line information is used to route your feedback. If you remove or modify the subject line, we may be unable to process your feedback.

Send feedback