

MICROSOFT

How to configure an Internet-Facing Deployment for Microsoft Dynamics CRM 4.0

5/22/2009

This document is intended to cover how to set up the Microsoft Dynamics CRM 4.0 Web site to make it available from the Internet. This document will cover the following Internet-Facing Deployment (IFD) scenarios for Microsoft Dynamics CRM 4.0.

- Install or Upgrade Microsoft Dynamics CRM 4.0 through the user interface (UI) setup
- Install or Upgrade Microsoft Dynamics CRM 4.0 with a configuration file

Table of Contents

Overview	3
Using a configuration file or the “CRM40IFDTool”	3
Setup test DNS record.....	4
Microsoft Dynamics CRM Data Connector for SQL Server Reporting Services	5
Scenario 1: Install or Upgrade Microsoft Dynamics CRM 4.0 through the user interface (UI) setup.....	5
Scenario 2: Install or Upgrade Microsoft Dynamics CRM 4.0 with a configuration file.....	6
How to use the CRM40IFDTool.....	9
Steps to run the tool	9
More Information	12
ISA Server	12
Turn off IFD	12
Log File	12
Installing CRM with IFD enabled against an existing website with Host headers or a Certificate enabled on the website.	13
Splitting Out Server Roles	14
Troubleshooting Information.....	16
FAQ.....	18
Send Feedback on the article.....	24

How to configure an Internet-Facing Deployment for Microsoft Dynamics CRM 4.0

This document will cover the following Internet-Facing Deployment (IFD) scenarios for Microsoft Dynamics CRM 4.0.

- Install or Upgrade Microsoft Dynamics CRM 4.0 through the user interface (UI) setup
- Install or Upgrade Microsoft Dynamics CRM 4.0 with a configuration file

This document is intended to cover how to set up Microsoft Dynamics CRM 4.0 to make it ready to be accessed from the Internet. This document will not cover the steps that you must complete to make a server available from the Internet. There will be additional steps depending on if you are using ISA server, firewalls or anything else in your environment that may need to be configured to get your server accessible from the internet.

Overview

Using a configuration file or the “CRM40IFDTool”

To successfully set up a Microsoft Dynamics CRM 4.0 IFD environment, there are several items that must be set for authentication to work correctly. These options are set when you install Microsoft Dynamics CRM 4.0 by using a configuration file or by using the “CRM40IFDTool” after Microsoft Dynamics CRM is installed to enable IFD.

Enabling IFD does the following:

- The web.config file contains an authentication strategy parameter. This parameter will be updated to “ServiceProviderLicenseAgreement”
For example, you would see the following parameter in the web.config file:
<authentication strategy =”ServiceProviderLicenseAgreement”/>
- The **Enable anonymous access** authentication method on the Microsoft Dynamics CRM 4.0 Web site is marked.
Note: The **Integrated Windows authentication** method must remain marked for internal users who do not access the Microsoft Dynamics CRM Web site by using the IFD deployment.
- The **DeploymentProperties** table in the MSCRM_Config SQL database has three values that are updated.
 - IfdRootDomainScheme
 - http or https
 - IfdSdkRootDomain

- *Domain.com*
 - IfdWebApplicationRootDomain
 - *Domain.com*
- The **IfdInternalNetworkAddress** registry key on the Microsoft Dynamics CRM server is updated. This registry key determines whether the user is logging into the Microsoft Dynamics CRM Web site from the Internet or Intranet. This registry value then determines whether the user uses CRM ticket authentication (Internet) or Integrated Windows authentication (Intranet).
 - The **IfdInternalNetworkAddress** registry key is located here:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM
 - This key holds an example of an ip address and the subnet of the domain. For example, the key may hold the following ip address and subnet value:
 - 192.220.100.96-255.255.255.0
 - If you have more than 1 subnet, you can add multiple values to the registry key.
Note: The values must be separated by a comma.
 - 192.220.100.1-255.255.255.0, 192.220.64.1-255.255.252.0
- Key encryption will be enabled.
 - For a user to log on to the Microsoft Dynamics CRM Web site with the CRM Ticket Authentication, the CRMTicketKey must to be enabled. Without a ticket the authentication will fail.
 - The key encryption is enabled by setting the <ifdsettings enabled="true"> option in the configuration file when you install or upgrade to Microsoft Dynamics CRM 4.0. You can also use the “CRM40IFDTool” to enable the key encryption after the install or upgrade.

Setup test DNS record

After you have completed the installation or upgrade by using a configuration file or the “CRM40IFDTool,” you must set up a DNS record for each organization that will be accessed externally from the Internet. Setting up the DNS record enables the Web site to correctly resolve externally.

- When Microsoft Dynamics CRM 4.0 is installed, or when you create a new organization, you provide a **Display Name** and a **Name** for each organization. The Name field is a unique name that must be less than 30 characters and cannot contain spaces or other special characters. This **Name** is used in the URL address when you open the Microsoft Dynamics CRM Web site. The DNS host record that needs to be setup is for the Name of each organization you need to access through IFD.
 - For example, assume the **Display Name** value is Microsoft CRM and the **Name** value is Microsoft. To open the Microsoft Dynamics CRM Web site for an IDF deployment, the URL address would be <https://microsoft.domain.com>. You would need to create a DNS host record called Microsoft.
Note: This example assumes the DNS records are set up to correctly resolve this URL address externally.

Microsoft Dynamics CRM Data Connector for SQL Server Reporting Services

You must install the Microsoft Dynamics CRM Data Connector for SQL Server Reporting Services on the Microsoft SQL Server Report Server if users will run Microsoft Dynamics CRM reports when accessing Microsoft Dynamics CRM over IDF.

Note: Microsoft SQL 2005 Workgroup Edition does not support custom data extensions for SQL Server Reporting Services. Therefore, the Microsoft Dynamics CRM Data Connector for SQL Server Reporting Services will not work when installed on the Microsoft SQL 2005 Workgroup Edition.

For more information, see the following Microsoft Knowledgebase (KB) article:

<http://support.microsoft.com/kb/946753>

Scenario 1: Install or Upgrade Microsoft Dynamics CRM 4.0 through the user interface (UI) setup

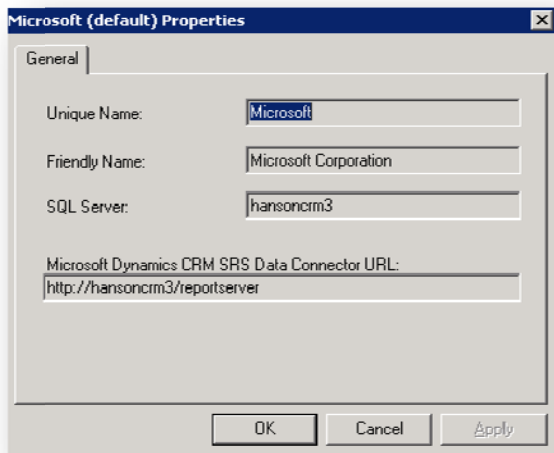
There are no options to enable the Microsoft Dynamics CRM 4.0 IDF deployment in the Setup Wizard. Therefore the CRM40IFDTool must be used to enable IFD after Microsoft Dynamics CRM 4.0 is installed. In this example CRM has been installed or upgraded to CRM 4.0 and our unique Organization Name is called Microsoft

Post Installation Tasks for Scenario 1:

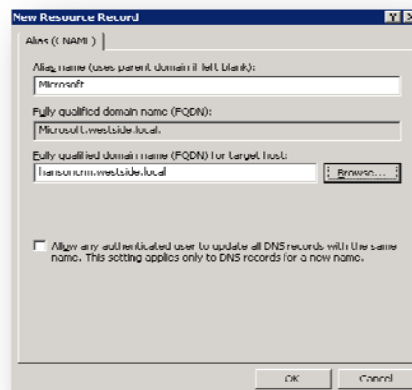
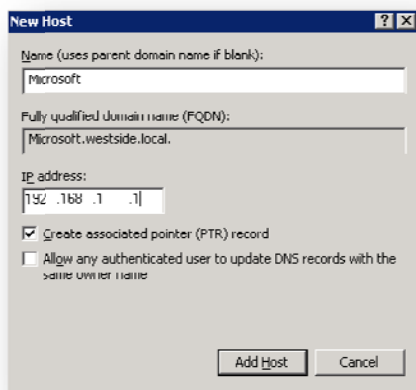
1. Run the 'CRM40IFDTool' to enable the IFD environment. This tool is available for download in the following Microsoft KB article: <http://support.microsoft.com/kb/948779> For information on how to run the 'CRM40IFDTool' see the '*How to use the Microsoft Dynamics CRM Internet Facing Deployment Configuration Tool*' section in this document.
2. Create a Host or Alias record in DNS for each Microsoft Dynamics CRM organization that will be accessed externally on the Internet. For the URL address to resolve correctly, you must create a DNS Host or Alias record for the for the unique organization name in Microsoft Dynamics CRM. For example: <https:// Microsoft.domain.com> would need a DNS host or alias record called Microsoft.
 - a. To create a DNS host or alias record follow these steps:
 - b. On your DNS server click **Start**, click **Run** and type in **dnsmgmt.msc**
 - c. Expand **Forward Lookup Zones** and right click your domain.com folder and choose **New Host (A)** or **New Alias (CNAME)**
 - d. In the Name field or Alias name field type the unique organization name you specified when setting up CRM.

Note: If you do not know the unique name you can check this in Deployment Manager on the Microsoft Dynamics CRM Server by selecting the Organizations node and then

right click on your Organization name and choose properties.



- e. Then type in the IP address of the CRM Server if you are creating a host record and click **Add Host**, then click **OK** and click **Done**. If you are adding an Alias click **Browse** and add the Microsoft Dynamics CRM server and click **OK**.



Scenario 2: Install or Upgrade Microsoft Dynamics CRM 4.0 with a configuration file

You can create IFD settings in the configuration file. Then, you can use the configuration file during the Microsoft Dynamics CRM installation or upgrade to enable IFD.

The following options are available in the configuration file:

- **<ifdsettings enabled="true"/>**

This option should only be used for Internet-facing deployments. Set enabled = "true" to notify Microsoft Dynamics CRM Server Setup to configure the deployment for Internet access. If the <ifdsettings> element is not specified, the enabled attribute value is set to false.

- `<internalnetworkaddress>`IP Network Address-Subject Mask`</internalnetworkaddress>`
IP address and subnet mask, such as 157.56.137.105-255.255.255.0. This is the internal IP address and the associated subnet mask of the subnet where your internal users reside. The subnets you enter here will be for the computers that you want to be considered as internal and you do not want the users to login through the IFD environment when they are on these subnets. To enter multiple subnets use a comma to separate the values in the configuration file
Note: If you leave this element blank, all communication to the Microsoft Dynamics CRM server will be considered as internal and users will default to windows authentication when hitting the Microsoft Dynamics CRM website.
- `<rootdomainscheme>https/http</rootdomainscheme>`
Must be https, which will use secure sockets layer (SSL), or http, which will use the nonsecure HTTP protocol.
Note: Setup does not require SSL on the Web site where Microsoft Dynamics CRM is installed. We strongly recommend that you specify the https value in the rootdomainscheme element. In addition, after Setup is complete, to help protect information that is transmitted between users and Microsoft Dynamics CRM Server, we recommend that you configure the Web site to require SSL. For more information about how to use SSL, see the Internet Information Services (IIS) Manager Help.
- `<sdkrootdomain>domain.com</sdkrootdomain>`
Specifies the domain name that will be used for applications that use the methods described in the Microsoft Dynamics CRM 4.0 Software Development Kit (SDK). The value that is set here will be prefixed by your unique organization name to form the URL so you only need to put in the domain.com
- `<webapplicationrootdomain>domain.com </webapplicationrootdomain>` *Specifies the domain name that will be used for the Microsoft Dynamics CRM Web application and Microsoft Dynamics CRM for Outlook. The value that is set here will be prefixed by your unique organization name to form the URL so you only need to put in the domain.com*

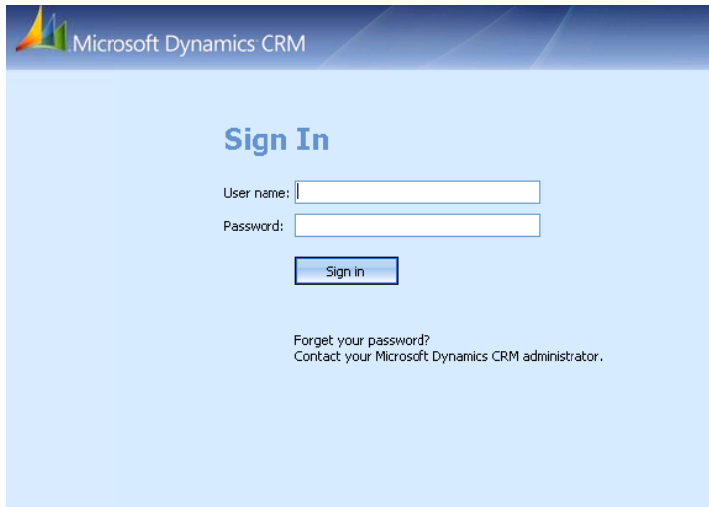
Note: If you are going to *split out* your server roles see the More Information section at the end of this document.

The following configuration file example contains an IFD section:

```
<ifdsettings enabled="true">
    <internalnetworkaddress>192.200.47.1-255.255.255.0</internalnetworkaddress>
    <rootdomainscheme>https</rootdomainscheme>
    <sdkrootdomain>domain.com</sdkrootdomain>
    <webapplicationrootdomain>domain.com</webapplicationrootdomain>
</ifdsettings>
```

NOTE: For more information about configuration file installations, see the Microsoft Dynamics CRM 4.0 Implementation Guide.

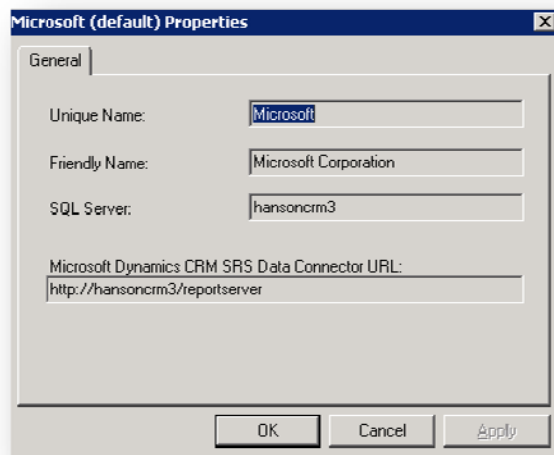
After the installation is complete, when you log on to the Microsoft Dynamics CRM Web site from a computer that is outside the subnet zone(s) you specified in the **IFDInternalNetworkAddress** registry key, you will get redirected to the sign in page like in the screen shot below.



Post Installation Tasks for Scenario 2:

1. Create a Host or Alias record in DNS for each Microsoft Dynamics CRM organization that will be accessed externally on the Internet. For the URL address to resolve correctly, you must create a DNS Host or Alias record for the unique organization name in Microsoft Dynamics CRM. For example: [https:// Microsoft.domain.com](https://Microsoft.domain.com) would need a DNS host or alias record called Microsoft.
 - a. To create a DNS host or alias record follow these steps:
 - b. On your DNS server click **Start**, click **Run** and type in **dnsmgmt.msc**
 - c. Expand **Forward Lookup Zones** and right click your domain.com folder and choose **New Host (A)** or **New Alias (CNAME)**
 - d. In the Name field or Alias name field type the unique organization name you specified when setting up CRM.

Note: If you do not know the unique name you can check this in Deployment Manager on the Microsoft Dynamics CRM Server by selecting the Organizations node and then right click on your Organization name and choose properties.



- e. Then if you are creating a host record type in the IP address of the Microsoft Dynamics CRM Server and click **Add Host**, then click **OK** and click **Done**. If you are adding an Alias click **Browse** and add the Microsoft Dynamics CRM server and click **OK**.

New Host

Name (uses parent domain name if blank):
Microsoft

Fully qualified domain name (FQDN):
Microsoft.westside.local

IP address:
192.168.1.11

Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):
Microsoft

Fully qualified domain name (FQDN):
Microsoft.westside.local

Fully qualified domain name (FQDN) for target host:
hms000rm.westside.local Browse...

Allow any authenticated user to update DNS records with the same name. This setting applies only to DNS records for a new name.

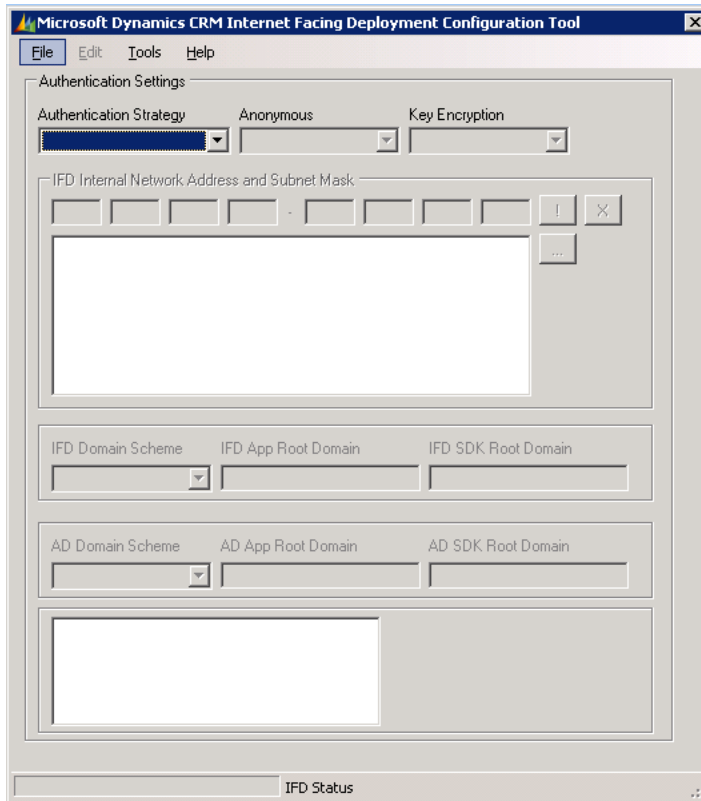
OK Cancel

How to use the CRM40IFDTool

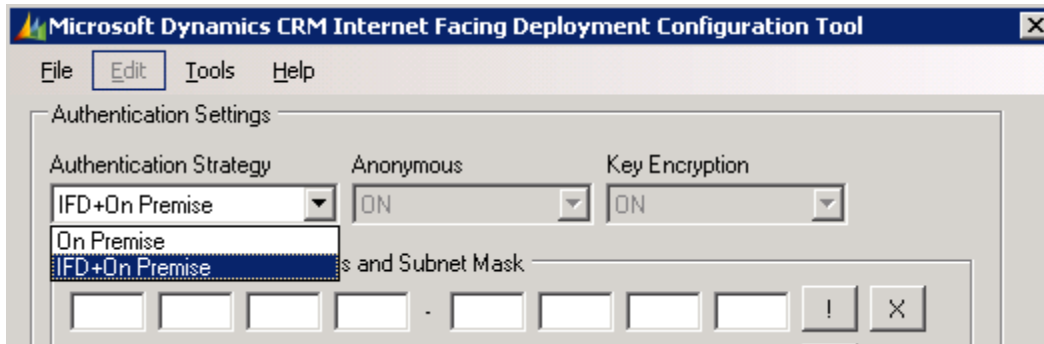
Steps to run the tool

1. Download the CRM4IFDTool from the following Microsoft KB article:
<http://support.microsoft.com/kb/948779>
2. On the computer that is running the server installation of Microsoft Dynamics CRM 4.0, extract the CRM4IFDTool to the following directory:
drive :\Program Files\Microsoft Dynamics CRM\Tools

3. Run the CRM4IFDTool.exe tool.



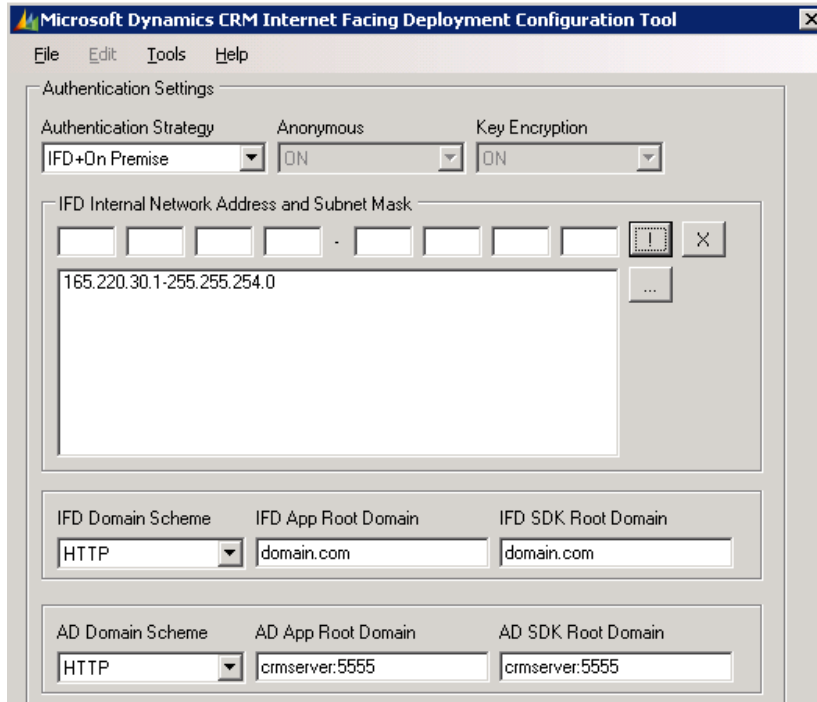
4. Click the **Authentication Strategy** list and click **IFD+On Premise**.



5. Type the IP Address and the subnet.

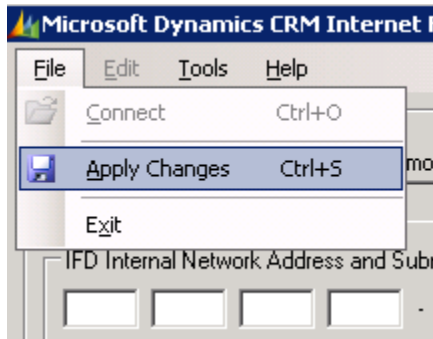
Note: The IP address is just an example of a valid IP address on the specific subnet. It does not have to be the IP address for the Microsoft Dynamics server. You can enter more than one subnet. The subnets you enter here will be for the computers that are internal and you do not

want the users to login through the IFD environment when they are on these subnets.



6. Click the **IFD Domain Scheme** list, and then click either **HTTP** or **HTTPS**.
7. Type the **IFD App Root Domain** and **IFD SDK Root Domain**. This will only be the domain name. For example, type domain.com or subdomain.domain.com
Note: The IFD settings will be how the client computers will access the Microsoft Dynamics CRM 4.0 Website when not logged on the local Intranet. The domain name entered here will be prefixed by the unique organization name to form the full URL of the IFD environment when the user is logging in.
8. The **AD Domain Scheme** should already be filled in from when you installed CRM.
9. The **AD App Root Domain** and **AD SDK Root Domain** will also already be filled in from when you installed CRM. However, you can use this tool to change them if needed.
Note: Do not type http or https as that is already selected in the **AD Domain Scheme** list.
Note: The AD settings will be how the client computers will access the Microsoft Dynamics CRM 4.0 Website when logged on the local Intranet and not logging on through IFD.

10. Click **File**, and then click **Apply Changes**.



More Information

The CRM4IFDTool will enable IFD for Microsoft Dynamics CRM 4.0. However, you must create the DNS record and verify the server and Microsoft Dynamics CRM 4.0 website are accessible from the Internet. The CRM40IFDTool will only change the settings needed to get Microsoft Dynamics CRM 4.0 ready to be accessed externally.

ISA Server

If you are configuring IFD in an environment where an ISA Server 2006 is being used please refer to this blog post for more information.

<http://blogs.technet.com/isablog/archive/2008/07/23/publishing-microsoft-crm-4-0-through-isa-server-2006.aspx>

Turn off IFD

You can also turn off IFD by selecting the **On Premise** option in the **Authentication Strategy** list, and then click **Apply Changes**.

IMPORTANT: Before making any changes to the **On Premise** option, you must verify the values in the **AD Domain Scheme**, **AD App Root Domain** and **AD SDK Root Domain** are correctly set.

Otherwise if the settings are left blank and you click **Apply Changes**, those settings will be updated with a null value in the MSCRM_Config database. This will result in users not being able to login to the Microsoft Dynamics CRM 4.0 Website.

Log File

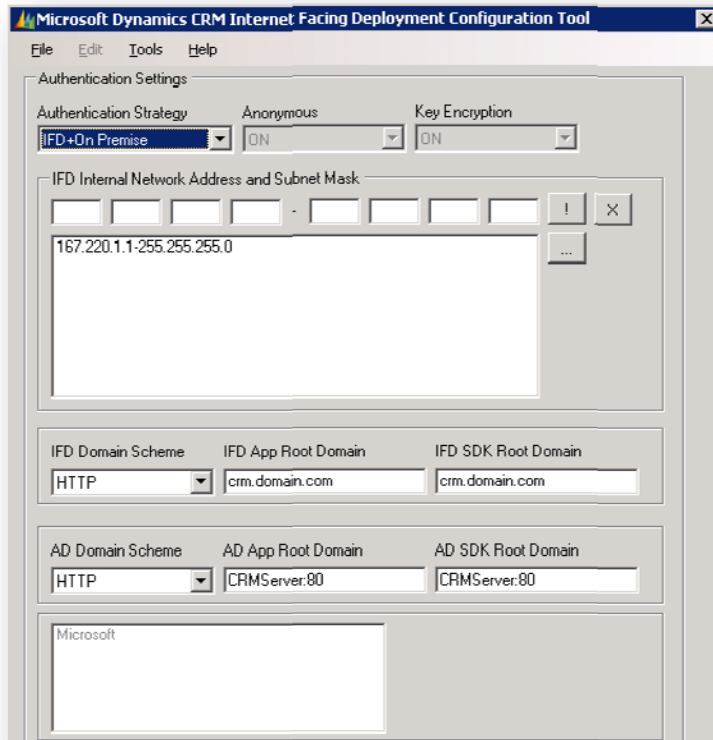
To look at the log file created when you run the CRM4IFDTool follow these steps:

1. Click **Start**, click **Run**, type `%appdata%\Microsoft\MSCRM\Log`s, and then click **OK**. The file is called **CRM40IFDTool.log**

Installing CRM with IFD enabled against an existing website with Host headers or a Certificate enabled on the website.

If you have an existing website with host headers or a Certificate enabled and you chose to install Microsoft Dynamics CRM against the website and enable IFD the following changes needs to be made.

1. DNS Changes needed:
 - a. On your DNS server click **Start**, click **Run** and type in **dnsmgmt.msc**
 - b. Expand **Forward Lookup Zones** and expand your **domain.com**. Find your current alias for the website you installed Microsoft Dynamics CRM to and delete it.
 - c. Right click your **domain.com** folder and choose **New Host (A)**
 - d. Type in the unique organization name and the host header name.
Example: if your unique organization name is **Microsoft** and your host header or certificate on the website is **crm.domain.com** then you would enter **Microsoft.crm** for the Host record
 - e. Enter the IP Address of the CRM Server and click **Add Host** then click **OK** and click **Done**.
2. IIS changes needed for host headers
 - a. On your Microsoft Dynamics CRM server click **Start**, click **Run** and type in **inetmgr**
 - b. Expand **Web Sites** and right click the Microsoft Dynamics CRM website and click **properties**.
 - c. Click on the **Web site** tab and then click on the **Advanced** button
 - d. If your unique organization is called **Microsoft** and your alias is **crm** and your domain is **domain.com** enter a host header using the following format **Microsoft.crm.domain.com**
Note: If you have multiple IP's assigned to the CRM server make sure to point host header to the IP specified in step 1.e
3. IIS changes needed for certificates
If your current certificate is **crm.domain.com** you would need to get a new certificate that would be called **Microsoft.crm.domain.com** or a wildcard certificate for ***.crm.domain.com**
Note: Wildcard certificates will be needed if you plan to have more than one organization enabled for IFD.
4. Run the 'CRM40IFDTool' to enable the IFD environment. This tool is available for download in the following Microsoft KB article: <http://support.microsoft.com/kb/948779> For information on how to run the 'CRM40IFDTool' see the '*How to use the Microsoft Dynamics CRM Internet Facing Deployment Configuration Tool*' section in this document.
5. The values you will specify in the CRM40IFDTool will be
IFD App Root Domain – crm.domain.com
IFD SDK Root Domain – crm.domain.com
AD App Root Domain – crmserver:80
AD SDK Root Domain – crmserver:80



Splitting Out Server Roles

The App Root Domain and SDK Root Domain values need to be different if you have split out the server roles. The App Root Domain is the Application Server Role. SKD Root Domain is the Platform Server Role. If you have two servers one for the Application Role called AppServer and one for the Platform Role called Platserver then you would set the values to something like the following

iFD App Root Domain – app.domain.com

iFD SDK Root Domain – platform.domain.com

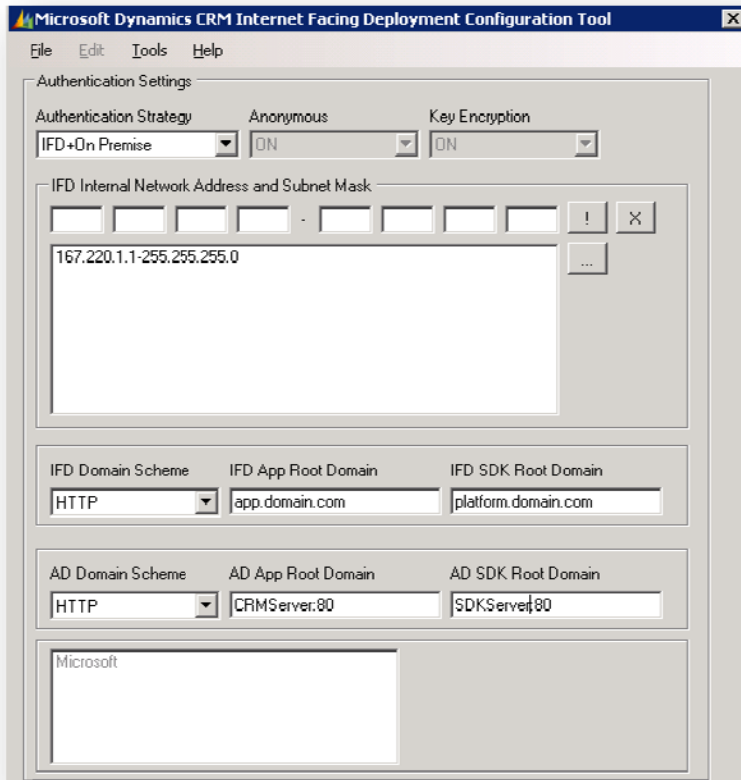
Note: host header will be a value that will be added in DNS along with the unique org name to differentiate the App Root Domain from the SDK Root Domain. For example if my host header name was app and my unique organization name was Microsoft then in DNS I would create a host record called Microsoft.app

AD App Root Domain – AppServer:80

AD SDK Root Domain – PlatServer:80

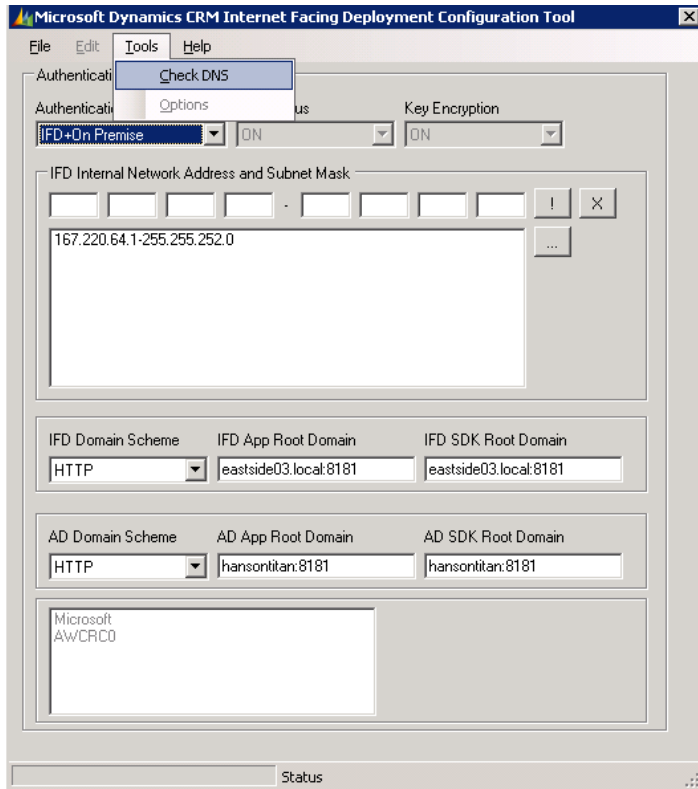
Note: When the server roles are split out you will need 2 certificates one for the AppServer and one for the PlatformServer. The AppServer would need a wildcard certificate if you plan to have more than one organization be accessed through IFD. For example *.app.domain.com. The

PlatformServer would just need a certificate for the url. For example platform.domain.com. The platform role contains the discovery service and that is needed for the Microsoft Dynamics CRM Clients for Outlook, Microsoft Dynamics CRM Email Router, Microsoft Dynamics CRM Data Migration Manager and any custom applications accessing Microsoft CRM through IFD.



DNS check

To verify the organization name in Microsoft Dynamics CRM 4.0 can be resolved in DNS, click **Tools** and then click **Check DNS**.



This will check all organizations that are listed in the text box in the CRM4IFDTool.

Troubleshooting Information

Issue: Unable to log on after entering credentials on the signin.aspx page

Resolution: Verify the Microsoft CRM Asynchronous Service is running. If this service is not running the CRMTicketKeys will not be generated and the Enable anonymous access authentication will fail for users who try to log on externally by using the Internet.

Issue: When opening Microsoft Dynamics CRM and being re-directed to the sign-in page, the page will not resolve. Additionally, the URL is <http://orgname.servername.domain.com>

Resolution: Check the DeploymentProperties table in the MSCRM_Config database. When you are redirected to the sign-in page, Microsoft Dynamics CRM uses the organization name and the value that is stored in the IfdWebapplicationRootDomain record to create the URL address. If the value in the DeploymentProperties table is incorrect, the sign-in page will not resolve correctly.

Issue: When you click **Apply Changes** or when you use the config file to enable IFD, Anonymous Access is getting set on the Microsoft Dynamics CRM 4.0 Website. If you have SQL Server Reporting Services under the same Website as Microsoft Dynamics CRM 4.0, Anonymous Access will be checked on the **Reports** and **ReportServer** virtual directories. You must manually remove Anonymous Access from the **Reports** and **ReportServer** virtual directories, and any other none CRM related virtual directories that you may have running under the Microsoft Dynamics CRM 4.0 Website.

Resolution: Verify Anonymous Access is not set on additional virtual directories:

1. Click **Start**, click **Run**, type **inetmgr** and then click **OK**.
2. Expand the server name, expand **web sites**, and then expand the Microsoft Dynamics CRM website.
3. Right click the virtual directory. For example, expand **Reports** or **ReportServer**, and then click **Properties**.
4. Click the **Directory Security** tab, click **Edit** on the **Authentication and access control** section
5. Unmark **Enable anonymous access**.

Tip: Download the Fiddler tool from <http://fiddlertool.com> to help troubleshoot authentication issues.

Tip: Create a simple test html page at the root of the Microsoft Dynamics CRM Web site to help with troubleshooting DNS issues. If you can access the test html page, DNS and IIS are set up correctly. Any additional issues may be related to the setup of Microsoft Dynamics CRM and values that are stored in the MSCRM_Config database.

Tip: Clear the DNS cache on the DNS server and flush the DNS cache on the local server when you troubleshoot any IFD issues.

On the DNS Server

1. Click **Start**, click **Administrative Tools**, and then click **DNS**.
2. Right-click the *DNSServerName*, and then click **Clear Cache**.

On the Microsoft Dynamics CRM Server and the client computer

1. Click **Start**, click **Run**, and then type **cmd**.
2. Type **ipconfig /flushdns**.

Tip: If you make any manual changes to the MSCRM_Config database, you must restart IIS.





1. Click **Start**, Click **Run**, and then type **iisreset**.

Issue: IFD Tool is not enabling IFD successfully and no error is being thrown. The status bar at the bottom will either not move at all or move half way thru and stop.



Resolution: When this happens the tool is not making the changes. This can be quickly verified by checking in the *IFDInternalNetworkAddress* registry key to see if it is created or changed the values. If it is not here are two things to resolve the issue.

1. The web site identifier match the website in the registry.
 - a) In the registry under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM

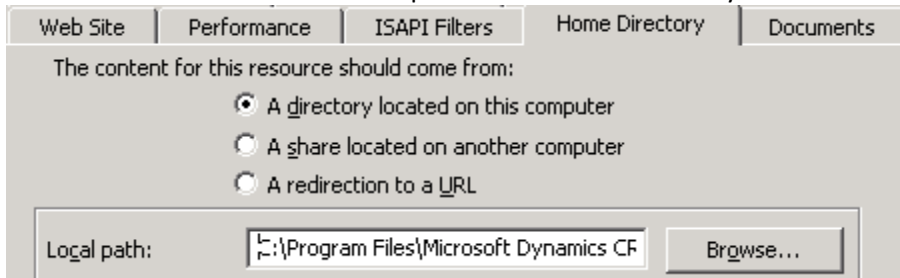
b) Check the website regkey and compare it with the Website Identifier.

	UninstallData	REG_SZ	<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" />
	website	REG_SZ	/LM/W3SVC/1
	WebSitePath	REG_SZ	C:\Program Files\Microsoft Dynamics CRM\CRMWeb
	WebStoreEnabled	REG_DWORD	0x00000000 (0)

c) Launch IIS and click on the website folder to see the list of websites check the Identifier tab and then update the website regkey found in step b to the correct value.

Description	Identifier	State	Home Directory
 Microsoft Dynamics CRM	1	Running	
 Virtual Server	3	Running	

2. The WebSitePath match the Local path of the Home Directory in IIS



FAQ

Q1: What is Internet Facing Deployment Configuration Tool?

A1: Internet Facing Deployment Configuration Tool configures Internet Facing Deployment (IFD) for Microsoft Dynamics CRM 4.0 after you have already installed or upgraded to Microsoft Dynamics CRM 4.0. This configuration allows administrators to configure Microsoft Dynamics CRM 4.0 to be accessed over the Internet. This tool is also used for changing the IFD settings.

Q2: Where can I obtain the Internet Facing Deployment Configuration Tool and how to configure it?

A2: The following article explains how to download the file from the Microsoft Download Center as well how to configure Internet Facing Deployment (IFD) for Microsoft Dynamics CRM 4.0:

948779 How to use the Microsoft Dynamics CRM Internet Facing Deployment Configuration tool

Q3: During IFD configuration, I've checked the DNS and the following warning message box was shown: 'DNS Could Not Resolve Microsoft.contoso.com' in 'Check DNS' option in the 'Tools' menu. What this message means?

A3: Internet Facing Deployment Configuration Tool checks DNS resolution for the Internet name that will be available for Internet users by appending the Organization name with the IFD App Root Domain name accordingly to the following example:

Organization name: Microsoft

IFD App Root Domain: domain.com

IFD Configuration Tool will check DNS resolution for 'Microsoft.contoso.com'

The IFD App Root Domain will be the DNS namespace used for Internet users accessing CRM through IFD. It is highly recommended to configure DNS resolution for both internal (AD App Root Domain) and external (IFD App Root Domain) DNS namespaces.

Q4: I would like to configure Internet Facing Deployment for all my CRM organizations in my Microsoft Dynamics CRM 4.0 Enterprise edition server. Do I have to configure IFD for each organization?

A4: No. Internet Facing Deployment configures the CRM Deployment for IFD which includes all the organization in the deployment. The only task required is to create the DNS Host or alias record for external DNS for each Organization accordingly to the following example:

Enabled organization names: Microsoft, AdventureWorks and Fabrikam.

IFD APP Root Domain: domain.com

Required Internet External DNS Hostnames: 'Microsoft.domain.com', 'AdventureWorks.domain.com', and 'Fabrikam.domain.com'.

Q5: What is the difference between IFD Domain Scheme options? Should I use HTTP or HTTPS?

A5: IFD Domain scheme option allows configuring the access to Microsoft Dynamics CRM 4.0 by means of a HTTP connection or a HTTPS connection. Data transmitted over a HTTP connection is insecure and data transmitted over a HTTPS connection is secured by an encryption established between client and server. It's highly recommended when publishing CRM through the Internet once corporate domain logon authentication data is transmitted.

Depending on the Web Publishing strategy and how SSL certificate is configured, a specific configuration has to be set for IFD Domain Scheme as follows:

a) HTTP: This option should be selected when:

- Microsoft Dynamics CRM 4.0 web site will NOT be accessed only by means of a HTTP connection.
- The ISA Server will handle the SSL certificate and respective session/negotiation instead the CRM Server.

b) HTTPS: This option should be selected when:

- A SSL certificate is configured in the Microsoft Dynamics CRM 4.0 web site and the IIS will handle the SSL certificate and respective session.

Q6: What modifications are changed in my Microsoft Dynamics CRM Server after running Internet Facing Deployment Configuration Tool?

A6: See the Overview Section on Page 3 of this documents.

Q7: I have users located in a different network subnet that should authenticate to Microsoft Dynamics CRM Web Site using Windows Integrated authentication. What will change for these users?

A7: All users logged into the domain that belong to different networks subnets from the CRM Server will be able to authenticate to Microsoft Dynamics CRM Web Site by means of a Integrated Windows Authentication, but the respective networks subnets have to be configured in the “IFD Internal Network Address and Subnet Mask” option in the “Internet Facing Deployment Configuration Tool”.

Q8: What does enabling IFD do for Microsoft Dynamics CRM Outlook client users?

A8: The mobility for Microsoft Dynamics CRM Outlook client users is now increased due to the fact Internet Facing Deployment permits both Laptop and Desktop versions to connect to Microsoft Dynamics CRM though Internet.

Q9: When publishing Microsoft Dynamics CRM 4.0 though ISA Server 2006 we have the option to select the Client Authentication Method in the ISA Web Listener, Authentication Delegation and Single Sign On settings. What I should select? What is the difference between a usual web publishing and a Microsoft Dynamics CRM Web publishing?

A9: Microsoft Dynamics CRM 4.0 configured with Internet Facing Deployment allows Internet users to access the application by authentication to a ASPX Form inserting their valid CRM user credentials and the authentication must be handled only by CRM Server. The user authentication has to be managed by the CRM Server instead of the ISA Server if you want the Microsoft Dynamics CRM Client for Outlook to be able to connect over IFD. ISA Server 2006 offers some features for authentication like Client Authentication Method, Authentication Delegation and Single Sign On and to proper configure them for Microsoft Dynamics CRM, the mentioned settings have to be set as follows:

a) Publishing rule:

- Authentication Delegation: No delegation, but client may authenticate directly

b) Web Listener:

- Client Authentication Method: No authentication.
- Single Sign On Settings: Disabled

For more information see <http://blogs.technet.com/isablog/archive/2008/07/23/publishing-microsoft-crm-4-0-through-isa-server-2006.aspx>

If you are not using the Microsoft Dynamics CRM Client for Outlook you can have ISA manage the authentication and CRM not setup for IFD. <http://blogs.msdn.com/crm/archive/2008/11/06/iag-sp2-securely-publishing-dynamics-crm-4-0.aspx>

Q10: How can I measure how many users are authenticating using Windows Integrated Authentication and how many are authenticating using the ASPX Form Authentication (IFD)?

A10: You can use “CRM Authentication” Performance Objects in Performance Monitor to measure how many users are authenticating to Microsoft Dynamics CRM. In example, to measure how many users are trying to authenticate to Microsoft Dynamics CRM though Internet Facing Deployment, we can use the “CrmPostAuthenticationAttemptsInTheLastminute” performance counter and to measure how many users are trying to authenticate to Microsoft Dynamics CRM using Windows Integrated Authentication, we can use the “WindowsAuthenticationAttemptsInTheLastminute” performance counter.

“CRM Authentication” Performance Objects measure the following objects:

- ConfidDBWindowsAuthenticationAttemptsInTheLastminute
- ConfidDBWindowsAuthenticationFailuresInTheLastminute
- CrmPostAuthenticationAttemptsInTheLastminute
- CrmPostAuthenticationFailuresInTheLastminute
- PassportAuthenticationAttemptsInTheLastminute
- PassportAuthenticationFailuresInTheLastminute
- WindowsAuthenticationAttemptsInTheLastminute
- WindowsAuthenticationFailuresInTheLastminute

Q11: How can Internet Facing Deployment settings be part of my backup plan?

A11: The Internet Facing Deployment information settings are set on registry hives, MSCRM_Config database, web.config file for the Microsoft Dynamics CRM web site, and etc. Although, the registry can be exported and the database can be part of an existing backup plan, the recommendation is to re-run the Internet Facing Deployment Configuration tool after the server had been recovered from a disaster.

Q12: When configuring the Microsoft Dynamics CRM Client for Outlook to access CRM over IFD what option should I choose?

A12: If your Microsoft Dynamics CRM Client for Outlook users will be both Internal and External at times we recommend that you configure the Microsoft Dynamics CRM Client for Outlook with the My company option while they are within the subnet specified in the IFDInternalNetworkAddress regkey. That way you can specify both the Intranet address and the External IFD Web address while configuring the client.

If your Microsoft Dynamics CRM Client for Outlook users will only be External then you can configure the Microsoft Dynamics CRM Client for Outlook with the An online service provider option. Then you would only specify the External Web address when configuring the client.

When configuring the Microsoft Dynamics CRM Client to access CRM if the “An online service provider” option is selected, the client will access the discovery service with this URL `http://<ifdurl>/MSCRMServices/2007/SPLA/CrmDiscoveryService.asmx`. This web service will reject the access and return the "HTTP 401 Unauthorized" error if the client's IP address is inside the subnet specified in the IFDInternalNetworkAddress regkey when using the An online service provider option.

If the My Company option is selected the client will access the discovery service with this url `http://<CRMServer>/MSCRMServices/2007/AD/CrmDiscoveryService.asmx`. This web service will reject the access and return the "HTTP 401 Unauthorized" error if the client's IP address is outside the subnet specified in the IFDInternalNetworkAddress regkey when using the My Company option.

The IFDInternalNetworkAddress can be defined by the Microsoft Dynamics CRM Internet Facing Deployment (IFD) Configuration Tool or by updating the registry key manually at "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM\IfdInternalNetworkAddress" on the CRM server.

If IFD is enabled and you run the Microsoft Dynamics CRM Configuration Wizard, you must make sure the IP address of your client is not in the IFDInternalNetworkAddress regkey if the An online service provider option is used.

If you are using the My company option then you must make sure the IP address of your client is within in the IFDInternalNetworkAddress regkey.

Q13: We have an ISP that is hosing our DNS. How do we enable IFD in this scenario?

A13: If an organization is having their DNS servers hosted at their local Internet Service Provider(ISP).

The following example will give you an idea on how to enable Microsoft CRM 4.0 Internet Facing Deployment (IFD) where DNS is hosted with Internet Service Provider (ISP)

For example:

Environment Configurations:

CRM 4.0 is running on windows server 2003 with SQL 2005 and with organization name set to advworks.

Server Hostname: MSCRM01

Dual Network Cards:

Gigabit LAN:

IP Address : 10.10.16.2
Subnet Mask : 255.255.255.0
DNS Server : 10.10.16.2

Ethernet Adapter Internet:

IP Address : 192.168.1.101
Subnet Mask : 255.255.255.0
Default G/W : 192.168.1.1
DNS Server : 10.10.16.2
Internal Domain Name : advworks.local
External ISP : www.ispdomain.com
External registered domain name (ISP) : www.advworks.com , advworks.com
Static IP registered for the external domain : 202.45.101.243 (This is mapped to your server – MSCRM01)

Objective:

Users connecting from local intranet to CRM through the following URL :
http://MSCRM01:5555
Users connecting from Internet to CRM through the following URL :
http://advworks.advworks.com:5555

Instructions:

On the external ISP:

1. Contact your external ISP or login to your ISP page. (For example: www.ispdomain.com)
2. Ensure that under the WebForwarding session, these primary domains are forwarded to the IP address itself instead of http://202.45.101.243.
 - a. advworks.com --> 202.45.101.243
 - b. www.advworks.com --> 202.45.101.243
3. Under the Advanced DNS setting, create a C NAME(Alias) - advworks and map it to advworks.com.
 - a. advworks --> advworks.com

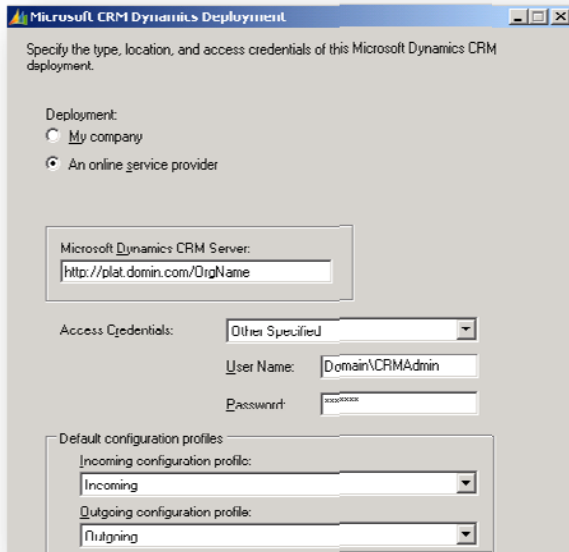
On Microsoft Dynamics CRM Internal Facing Deployment Configuration Tool:

1. Set the authentication strategy to 'IFD + On Premise'
2. Specify the IFD Internal Network Address and Subnet Mask to 192.168.1.1 – 255.255.255.0
3. Specify the IFD Root SDK domain to advworks.com:5555
4. Ensure the DNS can be resolved before applying the changes. (Tools | Resolve DNS)
5. Navigate to File | Apply Changes.

Note: Please ensure that the required port – 5555 is enabled or allowed for accepting connections from Internet.

Q14: What URL do I use when connecting the E-mail router over the IFD url.

A14: When connecting the E-mail router over IFD you will need to make sure you are choosing the An online service provider option in the Deployments tab of the E-mail Router configuration and then enter <https://<DiscoveryServerURL>/OrgName>
The Discovery service url will be the server that has the Platform Role installed on



[Send Feedback on the article](#)