

CRM OnPremise External Access for Hosted Applications



CRM Innovation LLC 8527 Bluejacket Street Lenexa, KS 66214

crminnovation.com

Contents

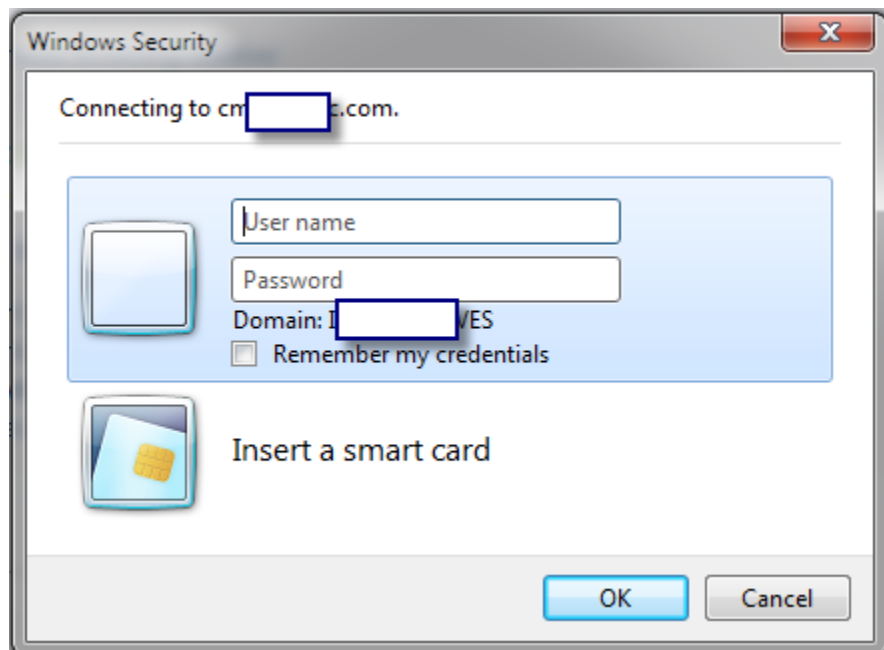
Overview	3
Process to Allow Secured Application Access	4
Locking Down Access IIS 6.....	4
Locking Down Access IIS7	4

Overview

Our cloud hosted applications – [Web2CRM](#), [Event2CRM](#) and [Email2CRM](#) – all require access to the CRM Organization Website to function. If you are using CRM Online or CRM Partner Hosted you are ready to go. In both these implementations the CRM site is available externally via IFD mode credentialed access. However, if you have a CRM OnPremise implementation it may or may not be accessible outside of your corporate firewall.

In an OnPremise implementation you would have to implement either IFD (Internet Facing Deployment) for CRM 4 or Claims Based Authentication IFD Mode for CRM 2011. This doesn't happen by default. If you have not implemented IFD mode and have no business requirement to allow your CRM users to connect to the CRM organization via the Web then you can still use our hosted applications without having to implement IFD mode. Note: If you are providing access to the CRM organization via VPN this will not work for our hosted applications, they need direct, credential access.

Basically what will need to be done is to allow an opening through the company firewall that redirects the incoming request to the CRM website/server. Ideally the 'user' would type in an address like the following: <http://crm.yourcompanydomain.com>. This would present them with a Windows Login Prompt that would be similar to:



However, since you don't want/need to provide access to 'real people' outside the firewall it will be necessary to lockdown access to only our hosted application server IP address and then all access attempts from other addresses will summarily be rejected without even receiving the prompt screen.

Process to Allow Secured Application Access

1. Create a DNS A record with a name like 'crm' pointed to the firewall IP address.
2. Open up the port on your firewall for the port that CRM runs on (typically 5555 or 80).
3. On the firewall have it forward the URL to the internal IP address of the CRM server.
4. The final configuration would like this: <https://crm.yourcompanydomain.com:5555>
(presuming that CRM is running on port 5555 for the purposes of this example and it is in SSL, if not drop the S and replace the port #)
5. Lockdown external access via IIS using the IP addresses we provide to you where our hosted applications run. This allows only our application to see the prompt. Everyone or anyone else will be ignored.
 - Hosted Application IP Address: 198.190.219.73, 198.190.219.60
 - Support Application IP Address: 63.76.54.18

Locking Down Access IIS 6

The following are instructions for locking down web site access from a selected IP address(es) if you are running IIS 6. They are taken from the following Microsoft support link:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/7586f163-2098-4719-a40b-065b2217d7ba.mspx?mfr=true>

1. Log on to the Web server computer as an administrator.
2. Click Start, point to Settings, and then click Control Panel.
3. Double-click Administrative Tools, and then double click Internet Services Manager.
4. If you want to limit access for the whole site, select the Web site from the list of different served sites in the left pane.
5. If you want to limit access to a specific set of sites but deny access to all other sites, click Denied Access.
6. To add a single computer to the list, click Single computer, type the IP address(es) in the appropriate box, and then click OK.

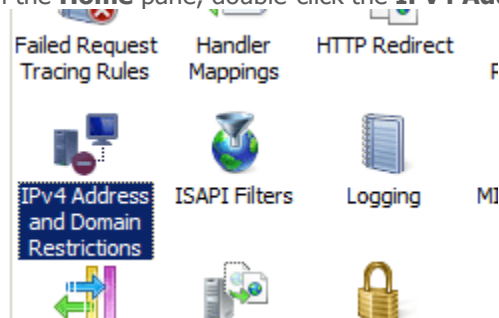
Locking Down Access IIS7

The following are instructions for locking down web site access from selected IP address(es) if you are running IIS 7. They are taken from the following Microsoft support link:

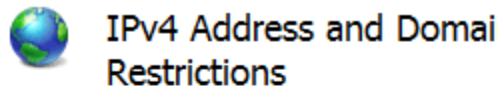
<http://www.iis.net/ConfigReference/system.webServer/security/ipSecurity>

How to add IP restrictions to deny access for a Web site

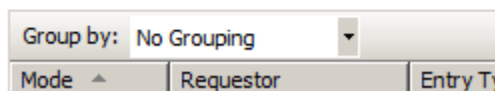
1. Open **Internet Information Services (IIS) Manager**:
 - If you are using Windows Server 2008 or Windows Server 2008 R2:
 - On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
 - If you are using Windows Vista or Windows 7:
 - On the taskbar, click **Start**, and then click **Control Panel**.
 - Double-click **Administrative Tools**, and then double-click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name, expand **Sites**, and then site, application or Web service for which you want to add IP restrictions.
3. In the **Home** pane, double-click the **IPv4 Address and Domain Restrictions** feature.



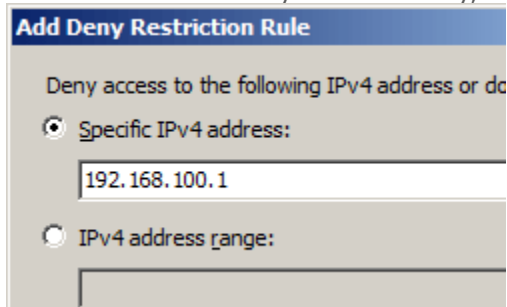
4. In the **IPv4 Address and Domain Restrictions** feature, click **Add Deny Entry...** in the **Actions** pane.



Use this feature to restrict or grant access to Web on IPv4 addresses or domain names. Set the restriction priority.



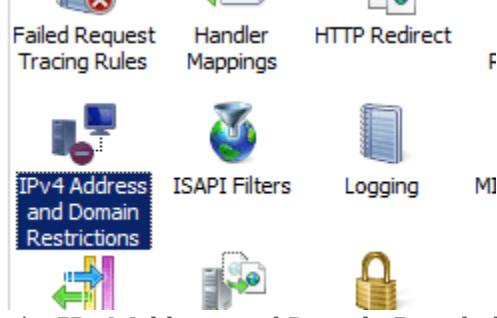
5. Enter the IP address that you wish to deny, and then click **OK**.



How to edit the IP restrictions feature settings for a Web site

1. Open **Internet Information Services (IIS) Manager**:
 - If you are using Windows Server 2008 or Windows Server 2008 R2:

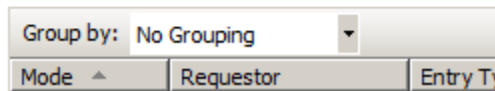
- On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
 - If you are using Windows Vista or Windows 7:
 - On the taskbar, click **Start**, and then click **Control Panel**.
 - Double-click **Administrative Tools**, and then double-click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name, expand **Sites**, and then site, application or Web service for which you want to add IP restrictions.
 3. In the **Home** pane, double-click the **IPv4 Address and Domain Restrictions** feature.



4. In the **IPv4 Address and Domain Restrictions** feature, click **Edit Feature Settings...** in the **Actions** pane.

IPv4 Address and Domain Restrictions

Use this feature to restrict or grant access to Web on IPv4 addresses or domain names. Set the restriction priority.



5. Choose the default access behavior for unspecified clients, specify whether to enable restrictions by domain name, and then click **OK**.

