Microsoft Dynamics CRM

Connectivity and Firewall Port Requirements for Microsoft Dynamics CRM 2013

Microsoft Corporation

Published: September 2013 **Updated**: October 2013

Abstract

This document is designed to provide guidance on the connectivity requirements between Microsoft Dynamics CRM 2013 and other systems to assist readers with proper firewall configuration in customer environments.

Microsoft

Contents

Connectivity and Firewall Port Requirements for Microsoft Dynamics CRM 2013

Contributors: Venkat Sathyamurthy; Murali Vadakke Puthanveetil, Mahesh Hariharan, Peter Simons

Published: September 2013 **Updated**: October 2013

This document is designed to provide guidance on the connectivity requirements between Microsoft Dynamics CRM 2013 and other systems to assist readers with proper firewall configuration in customer environments.

Applies To

- Microsoft Dynamics CRM 2013

In this white paper

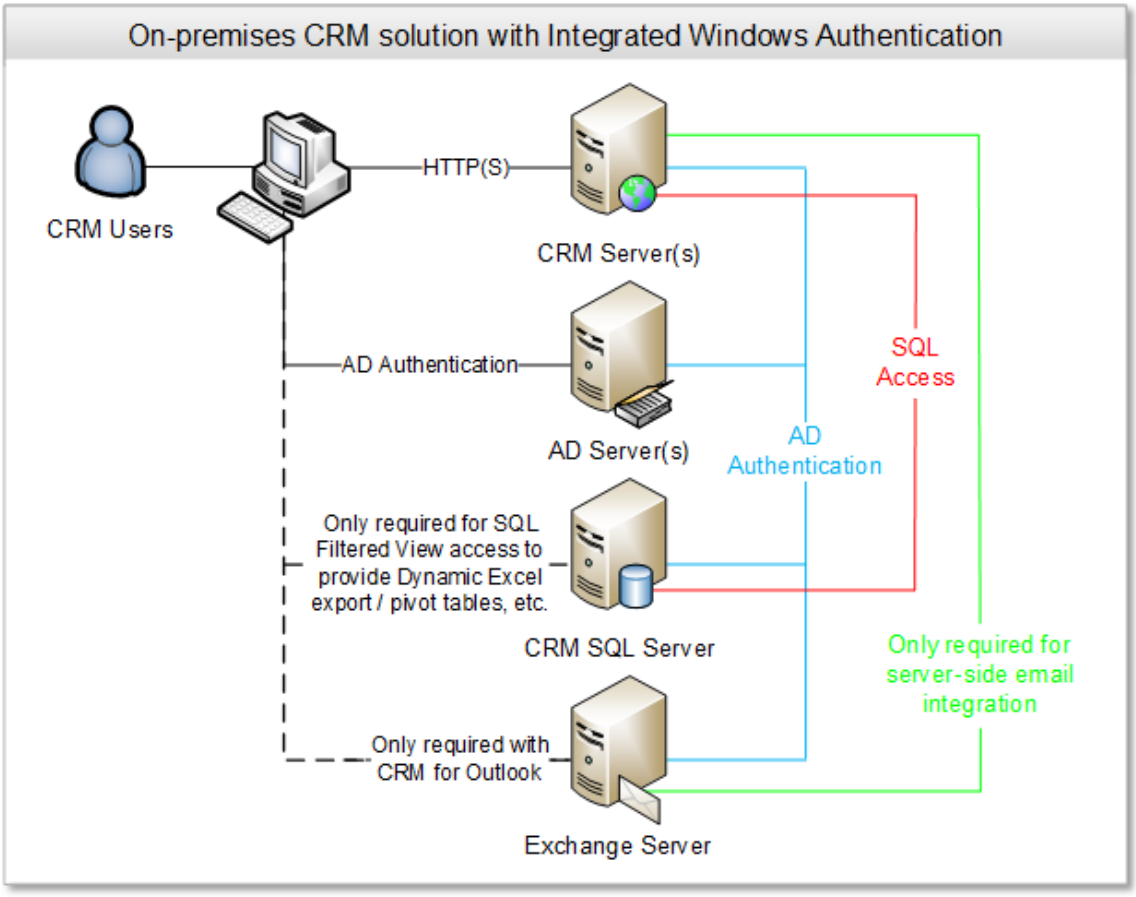
Many data centers include firewalls between the end users and the servers and other integrated systems that support an implementation of Microsoft Dynamics CRM 2013. This document is designed to provide guidance on the connectivity requirements between Microsoft Dynamics CRM 2013 and other systems to assist readers with proper firewall configuration in customer environments.

Download

This paper can be downloaded from the Microsoft Download Center: Connectivity and Firewall Port Requirements for Microsoft Dynamics CRM 2013

On-premises with Integrated Windows Authentication

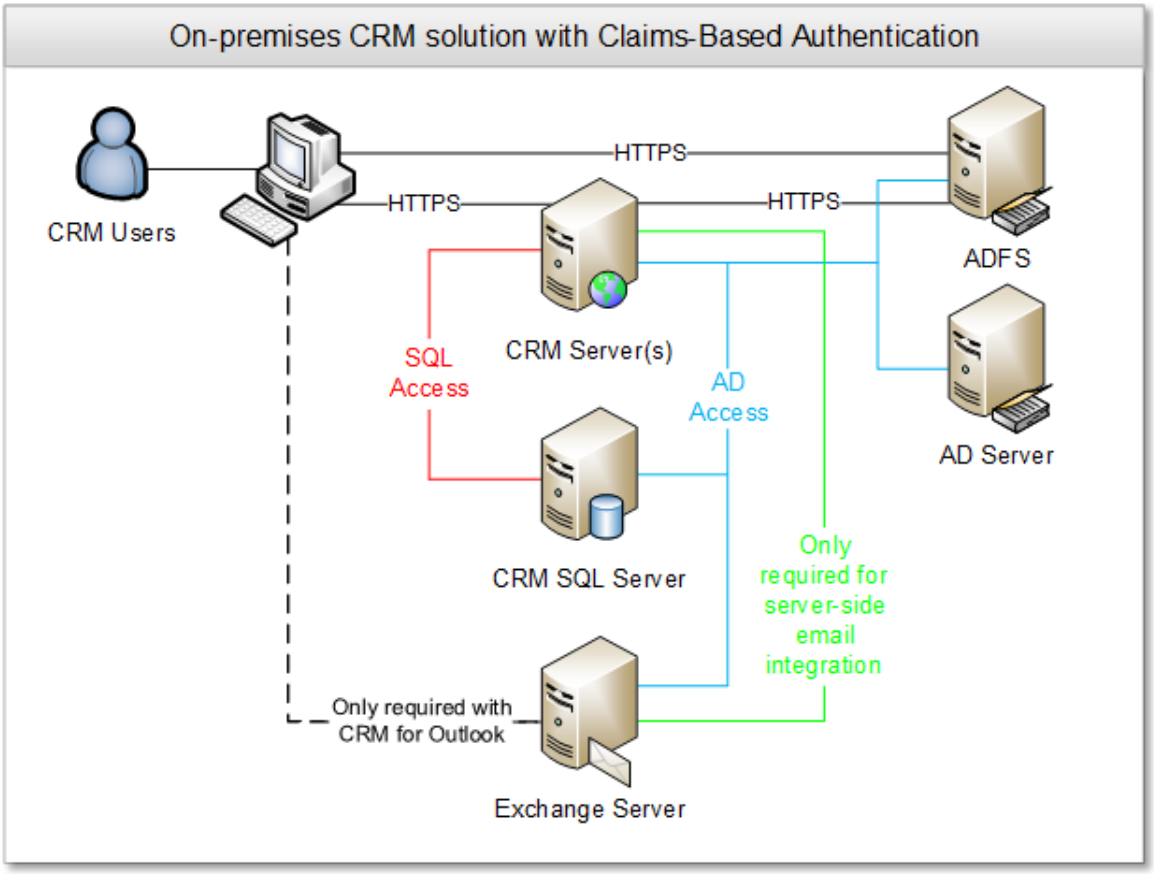
An overview of an on-premises implementation that uses Integrated Windows Authentication (IWA) is shown in the following diagram.



In this scenario the user must have a certain level of connectivity to the CRM Server(s), the Active Directory Server(s) and the SQL Server for SQL Filtered View access (if Export to Excel functionality is required). The remainder of this document focuses primarily on this scenario and details the required level of connectivity between these various components as well as further options for integration, Citrix implication, and so on.

On-premises with claims-based authentication

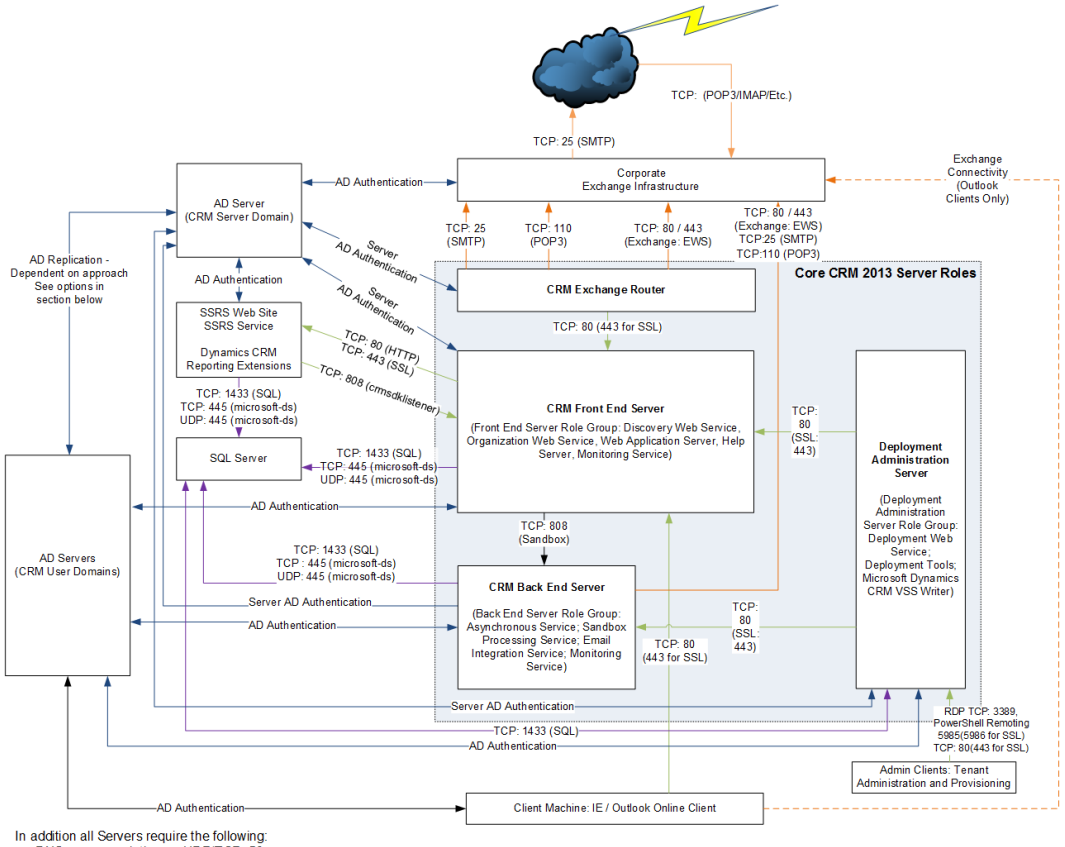
An overview of an on-premises implementation that uses claims-based authentication using Active Directory Federation Service (ADFS) as the Security Token Service (STS) is shown in the following diagram.



With claims-based authentication, the Microsoft Dynamics CRM site is accessed anonymously and is then redirected to ADFS. Users enter their credentials, which are validated by ADFS by contacting Active Directory Directory Services (AD-DS) or alternative Identity Provider. Finally, AFDS issues a SAML token containing the necessary claims for accessing Microsoft Dynamics CRM.

Default CRM connectivity requirements

An overview of the default connectivity requirements for an on-premises deployment of Microsoft Dynamics CRM 2013 is shown in the following diagram.



In addition all Servers require the following:

- DNS name resolution on UDP/TCP: 53
- NetBIOS name resolution on TCP: 139, UDP: 137/138
- NTP time synchronisation: 123 – *this is a requirement for Kerberos Authentication*
- DCOM and RPC: TCP 135, UDP 1025

***Note**. Arrow direction depicts source and target of initiating request rather than direction of data flow*

Important

Because this diagram is focused on Microsoft Dynamics CRM connectivity requirements, full details about the specific port requirements for Microsoft Exchange Server and the Microsoft Windows Active Directory service are not shown. Additional information and links to related articles about these technologies and their specific requirements are provided in the following sections of this document.

The default connectivity requirements for components of an on-premises deployment of Microsoft Dynamics CRM 2013 are shown in the following table.

Component	Default connectivity requirements
ALL	• AD Connectivity • RDP Connection from Administrator Users • DNS name resolution (where applicable) on UDP/TCP: 53 • NetBIOS name resolution (where applicable) on TCP: 139, UDP: 137/138 • NTP: Required on all Servers to Sync Network Time. UDP: 123 – *this is a requirement for Kerberos Authentication* • DCOM and RPC: Required on all Servers. TCP 135, UDP 1025
CRM Front End Servers	• AD Connectivity • RDP Connection from Administrator Users • DNS name resolution (where applicable) on UDP/TCP: 53 • NetBIOS name resolution (where applicable) on TCP: 139, UDP: 137/138 • NTP: Required on all Servers to Sync Network Time. UDP: 123 – *this is a requirement for Kerberos Authentication* • DCOM and RPC: Required on all Servers. TCP 135, UDP 1025
CRM Back End Servers	• Connectivity to Exchange or other email services for server-side email integration • Connectivity from CRM Front End Servers • SQL Server access
CRM Deployment Servers	• Remote PowerShell access from Administrator users' client computers • Access to all CRM Servers / network load balancer • SQL Server access
Exchange Router	• Exchange Server Connectivity (EWS / SMTP / POP3) • Other Mail Server Connectivity (POP3/SMTP) • Optional Connectivity to a Microsoft Dynamics CRM Sink Mailbox • HTTP / HTTPS access to CRM Servers / Network Load Balancer
SSRS Servers	• Connectivity to CRM Front End Server SDK listener to run FetchXML • Connectivity from CRM Front End Server to execute, publish, and delete reports. • SQL Server access

Component	Default connectivity requirements
Client	• Outlook Connectivity to Exchange • HTTP / HTTPS access to CRM Servers / Network Load Balancer • Optional access to SQL Server for direct access to SQL Views*

* It is recommended that the solution be designed to work using the FetchXML access (via the Web services) rather than by granting users access to SQL Views directly. Using this approach simplifies any future migration to CRM Online, with which SQL access is not available.

Important
In each case, the port numbers can be configured to run under alternative (non-default) values, so environments will vary.

Port recommendations

Network ports for the Microsoft Dynamics CRM web application

The following table lists the ports used for a server that is running a Full Server installation of Microsoft Dynamics CRM. Moreover, except for the Microsoft SQL Server role and the Microsoft Dynamics CRM Connector for SQL Server Reporting Services server role, all server roles are installed on the same computer.

Protocol	Port	Description	Explanation
TCP	80	HTTP	Default web application port; may be different as it can be changed during Microsoft Dynamics CRM setup. For new websites, the default port number is 5555.
TCP	135	MSRPC	RPC endpoint resolution
TCP	139	NETBIOS-SSN	NETBIOS session service
TCP	443	HTTPS	Default secure HTTP port. The port number may differ from the default port. This secure network transport must be manually configured. Though this port is not required to run Microsoft Dynamics CRM, it is strongly recommend that it be used. For information about how to configure HTTPS for Microsoft Dynamics CRM, in the Installing Guide, in topic Microsoft Dynamics CRM 2013 Post-Installation and Configuration Guidelines, see the section **Make Microsoft Dynamics CRM client-to-server network communications more secure**.
TCP	808	crmsdklistener	CRM SDK Listener
TCP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication.

Protocol	Port	Description	Explanation
UDP	123	NTP	Network Time Protocol
UDP	137	NETBIOS-NS	NETBIOS name service
UDP	138	NETBIOS-dgm	NETBIOS datagram service
UDP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication
UDP	1025	Blackjack	DCOM, used as an RPC listener

Important

Depending on the domain trust configuration, additional network ports may be required for Microsoft Dynamics CRM to work correctly. For more detail, see Knowledge Base article ID 179442, How to configure a firewall for domains and trusts.

Network ports for the Asynchronous Service, Web Application Server, and Sandbox Processing Service server roles

The following table lists the additional port that is used for a deployment in which the Sandbox Processing Service is running on a separate computer.

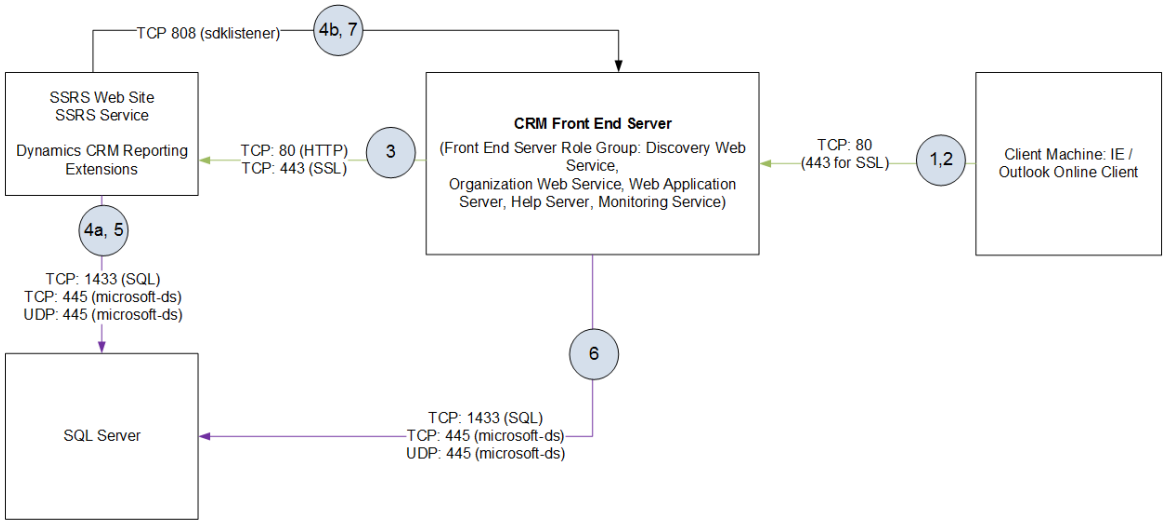
Port	Protocol	Description	Explanation
TCP	808	CRM server role communication	The Asynchronous Service and Web Application Server services communicate to the Sandbox Processing Service through this channel. The default port is 808, but can be changed in the Windows registry by adding the DWORD registry value TcpPort in the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM\.

Network ports for CRM Reporting Extensions

The following table lists the additional port that is required for CRM Reporting Extensions connectivity.

Protocol	Port	Description	Explanation
TCP	808	Use for Fetch-based reports	The CRM Reporting Extensions that are running Fetch-based reports communicate over this port when communicating with the computer that is running the Front End Server Role using the crmsdklistener to query the CRM database over FetchXML.

The following diagram shows the connectivity for CRM Reporting Extensions.



Report Execution Process

The following steps are involved in the report execution process.

1. Client connects and authenticates (as the user using AD or ADFS/Cookie) with CRM Front Ender Server over HTTP/HTTPS.

2. Client hits a page in CRM that includes the report viewer control to view a report.

3. The reporting control in CRM makes a requests to SSRS (Sandboxed), connecting using the CRM Service Account (i.e. not the user) but passing the user context over HTTP/HTTPS.

4a. SSRS uses the Dynamic CRM SQL Reporting Extension to query the data via the CRM security views (for SQL queries) on the standard SQL Port (default TCP:1433), obtains dataset for report.

4b. SSRS uses the Dynamics CRM Fetch Reporting Extensions to connect to the crmsdklistener on the Front End CRM Server to run the FetchXML (TCP:808).

5. SQL returns the data (for SQL reports) on open SQL connection (no new connection).

6. The front end CRM server (web server role) executes FetchXML for report against SQL Database over SQL port (default 1433), and obtains dataset for report.

7. The crmsdklistener returns FetchXML data on open TCP connection (no new connection).

Report Publishing and Deletion

3. Report publishing and deletion also uses the 2005 web service endpoint available on the SSRS report server.

The following table lists the ports that are used for a computer that is running SQL Server with only SQL Server and the CRM Reporting Extensions server roles installed.

Protocol	Port	Description	Explanation
TCP	135	MSRPC	RPC endpoint resolution
TCP	139	NETBIOS-SSN	NETBIOS session service
TCP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication
TCP	1433	ms-sql-s	SQL Server sockets service; required for access to SQL Server; may vary if you have configured your SQL Server to use a different port number
TCP	80/443	WebService	SSRS Web service end point
UDP	123	NTP	Network Time Protocol
UDP	137	NETBIOS-NS	NETBIOS name service
UDP	138	NETBIOS-dgm	NETBIOS datagram service
UDP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication
UDP	1025	Blackjack	DCOM, used as an RPC listener

Note

The NETBIOS ports (TCP 139, UDP 137 and 138) are an alternative to port 445 which is used by SQL named pipes. These ports are required only during setup to determine the

SQL port for named instances of SQL; NETBIOS ports are not required during normal operation.

Connectivity requirements for Windows services

Microsoft client, server, and server-based programs use a variety of network ports and protocols to communicate with client systems and with other server systems over the network. While beyond the scope of this article, details of the essential network ports, protocols and services that are used by Microsoft client and server operating systems, server-based programs, and their subcomponents in the Microsoft Windows server system are available on the Microsoft Support site in Article ID 832017, Service overview and network port requirements for Windows.

Connectivity requirements for Integrated Windows Authentication

The key service and port requirements for Integrated Windows Authentication (IWA) are shown in the following table.

Service Name	UDP	TCP
LDAP	389	389
LDAP SSL	n/a	636
RPC Endpoint Mapper	135	135
Global Catalog LDAP	n/a	3268
Global Catalog LDAP SSL	n/a	3269
Kerberos	88	88

However, in larger deployments, firewalls can present two challenges when deploying a distributed Active Directory (AD) directory service architecture:

- Initially promoting a server to a domain controller
- Replicating traffic between domain controllers

Active Directory relies on remote procedure call (RPC) for replication between domain controllers. Simple Mail Transfer Protocol [SMTP] can be used in certain situations—schema, configuration, and global catalog replication—but not for domain naming context, which limits its usefulness.

Configuring replication in environments in which a directory forest is distributed among internal, perimeter networks and external (that is, Internet-facing) networks can be challenging. In these scenarios, there are three possible approaches:

- Open the firewall wide to permit the native dynamic behavior of RPC
- Limit the use of TCP ports by RPC and open the firewall just a little bit

  Note
  For additional detail about this option, see the following resources:
  - Article ID 929851 - The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008
  - Article ID 154596 - How to configure RPC dynamic port allocation to work with firewalls
  - How to limit dynamic RPC ports used by DPM and protected servers
- Encapsulate domain controller (DC-to-DC) traffic inside IP Security Protocol (IPSec) and open the firewall for that

Each of these approaches has its pros and cons; in general, there are more cons than pros associated with the first option listed above and more pros than cons associated with the third option listed above.

Note
For more information about each option, including details of the configuration and port requirements for each, see the TechNet article Active Directory Replication Over Firewalls.

Mail Server connectivity requirements

Microsoft Dynamics CRM 2013 provides for integration with Exchange and other SMTP/POP3 servers. Mail system integration is typically achieved either through client-side integration via Outlook or server-side integration via Exchange or a third-party POP3/SMTP server.

Note
This document focuses on server-side integration via Exchange, but the same principles would apply to server-side integration via other POP3/SMTP servers.

Administrators can specify to use either client-side or server-side integration, which can be configured at a user level within the User properties in Microsoft Dynamics CRM. After the administrator specifies the level at which integration will occur, users on the client computers must agree to have email sent on their behalf by Microsoft Dynamics CRM by using their own user options configuration.

While client-side integration does not require any additional server components, it works only with Microsoft Dynamics CRM for Outlook. The Microsoft Dynamics CRM for Outlook plug-in is then used to send email via Outlook and the users' preconfigured mail Server as well as to route inbound emails back into Microsoft Dynamics CRM. This integration happens on a regular polling basis (but is not immediate). Additional Microsoft Dynamics CRM-specific ports are not required

for this integration; standard Exchange connectivity is used. Emails are routed into Microsoft Dynamics CRM via the CRM Web Services; hence access to Port 80 (443 for SSL) from Microsoft Dynamics CRM for Outlook is the only requirement.

The CRM Exchange Router can be installed on an Exchange Server or on a dedicated CRM Exchange Router server. Using the CRM Exchange Router provides inbound and outbound email connectivity for both the Microsoft Dynamics CRM web client and Microsoft Dynamics CRM for Outlook. This CRM Exchange Router integrates with external mail systems via:

- POP3 (TCP:110) and SMTP (TCP:25)
- Exchange Web Service (EWS) (TCP:80)

The supported options for server-side synchronization with Microsoft Dynamics CRM 2013 are listed in the following table.

Email system	Email synchronization?	Appointment, contact, and task synchronization?	Protocol
• Exchange Server 2013 • Exchange Server 2013	Yes	Yes	Exchange Web Services
• Gmail • MSN • Outlook.com • Windows Live Mail • Yahoo! Mail	Yes	No	POP3/SMTP

Server-side synchronization doesn't support the following scenarios:

- Microsoft Dynamics CRM Online with Microsoft Exchange Online
- Hybrid deployments
    - Microsoft Dynamics CRM Online with Exchange (on-premises)
    - Microsoft Dynamics CRM 2013 (on-premises) with Exchange Online
- Mix of Exchange/SMTP and POP3/Exchange
- Creation of mass email marketing campaigns
- Extensibility scenarios like extending EWS/POP3/SMTP protocols and creating custom email provider
- Exchange Server 2003 and Exchange Server 2007

Appendix A: Additional resources

For additional information related to connectivity and firewall port requirements in Microsoft Dynamics CRM 2013, see the following additional resources.

- Microsoft Dynamics CRM 2013 Implementation Guide
  - Download
  - View online
- Article ID 832017 - Service overview and network port requirements for Windows
- Article ID 929851 - The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008
- Article ID 154596 - How to configure RPC dynamic port allocation to work with firewalls
- How to limit dynamic RPC ports used by DPM and protected servers
- Article ID 179442 - How to configure a firewall for domains and trusts
- Active Directory Replication Over Firewalls.
- Securing Your Application Server
- TCP/IP port numbers required to communicate to SQL over a firewall

Appendix B: Accessibility for Microsoft Dynamics CRM

Administrators and users who have administrative responsibilities typically use the Settings area of the Microsoft Dynamics CRM web application to manage Microsoft Dynamics CRM. A mouse and keyboard are the typical devices that administrators use to interact with the application.

Users who don't use a mouse can use a keyboard to navigate the user interface and complete actions. The ability to use the keyboard in this way is a result of support for keyboard interactions that a browser provides.

For more information, see the following Microsoft Dynamics CRM Web application accessibility topics:

- Keyboard shortcuts
- Accessibility for people with disabilities

Administrators and users who have administrative responsibilities for on-premises deployments of Microsoft Dynamics CRM 2013 also use Microsoft Dynamics CRM Deployment Manager, a Microsoft Management Console (MMC) application, to manage on-premises deployments of Microsoft Dynamics CRM Server 2013.

For more information, see the following Microsoft Management Console (MMC) accessibility topics:

- Navigation in MMC Using the Keyboard and Mouse
- MMC Keyboard Shortcuts

Accessibility features in browsers

Browser	Documentation
Internet Explorer	Microsoft Accessibility Language Support and Accessibility Features
Mozilla Firefox	Accessibility features in Firefox
Apple Safari	Safari
Google Chrome	Accessibility Technical Documentation

Note
For additional information, see the Microsoft Accessibility Resource Center.

Feedback

We appreciate hearing from you. To send your feedback, click the link below 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