Architecture

Connectivity and Firewall Port Requirements for Microsoft Dynamics CRM 2011

White Paper

Published: October 2012

Updated: September 2013

Microsoft Dynamics

Feedback

To send comments or suggestions about this document, please click the following link and type your feedback in the message body:
http://go.microsoft.com/fwlink/?LinkID=267480

Important: 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.

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989
Worldwide +1-701-281-6500
www.microsoft.com/dynamics

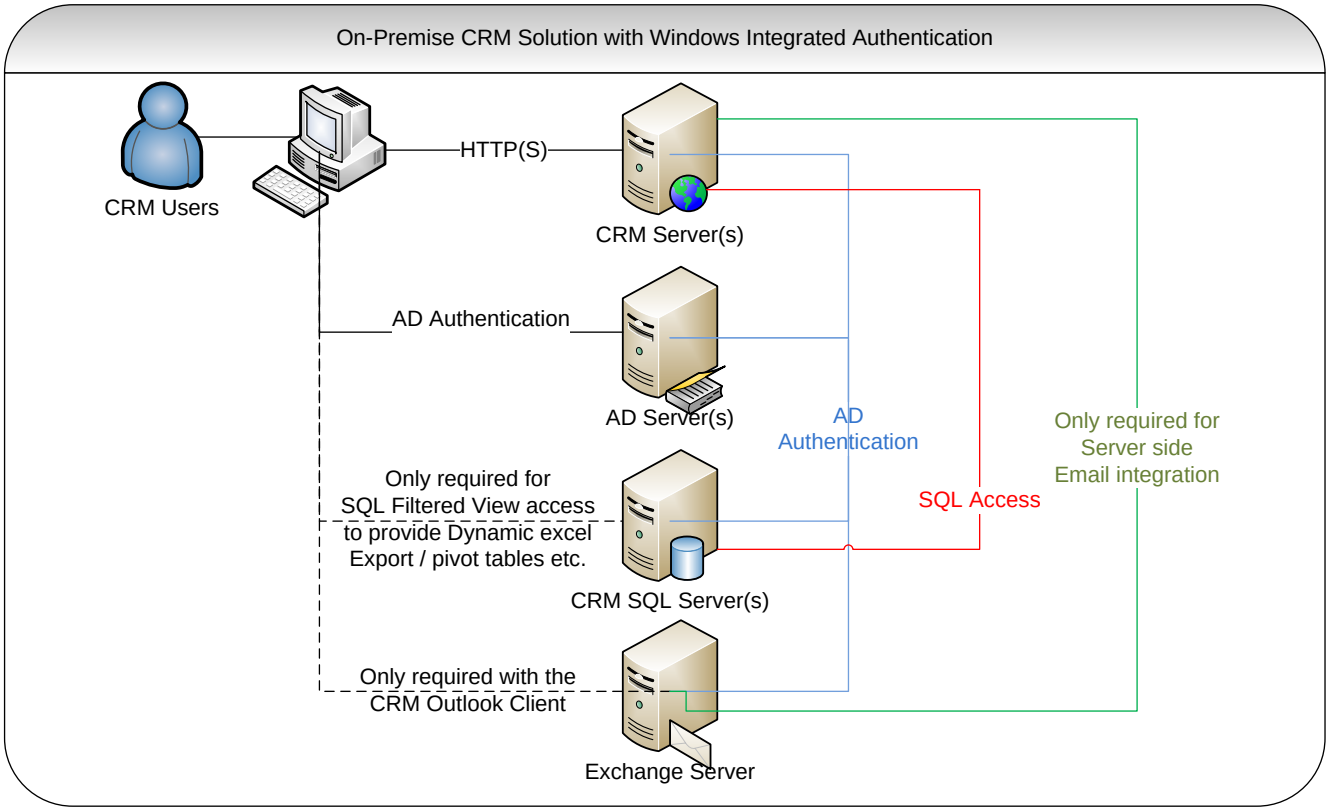
Table of Contents

Overview

Many data centers include firewalls between the end users and the servers and other integrated systems that support an implementation of Microsoft Dynamics CRM 2011. This document is designed to provide guidance on the connectivity requirements between Microsoft Dynamics CRM 2011 and other systems to assist readers with proper firewall configuration in customer environments.

On-Premises with Integrated Windows Authentication

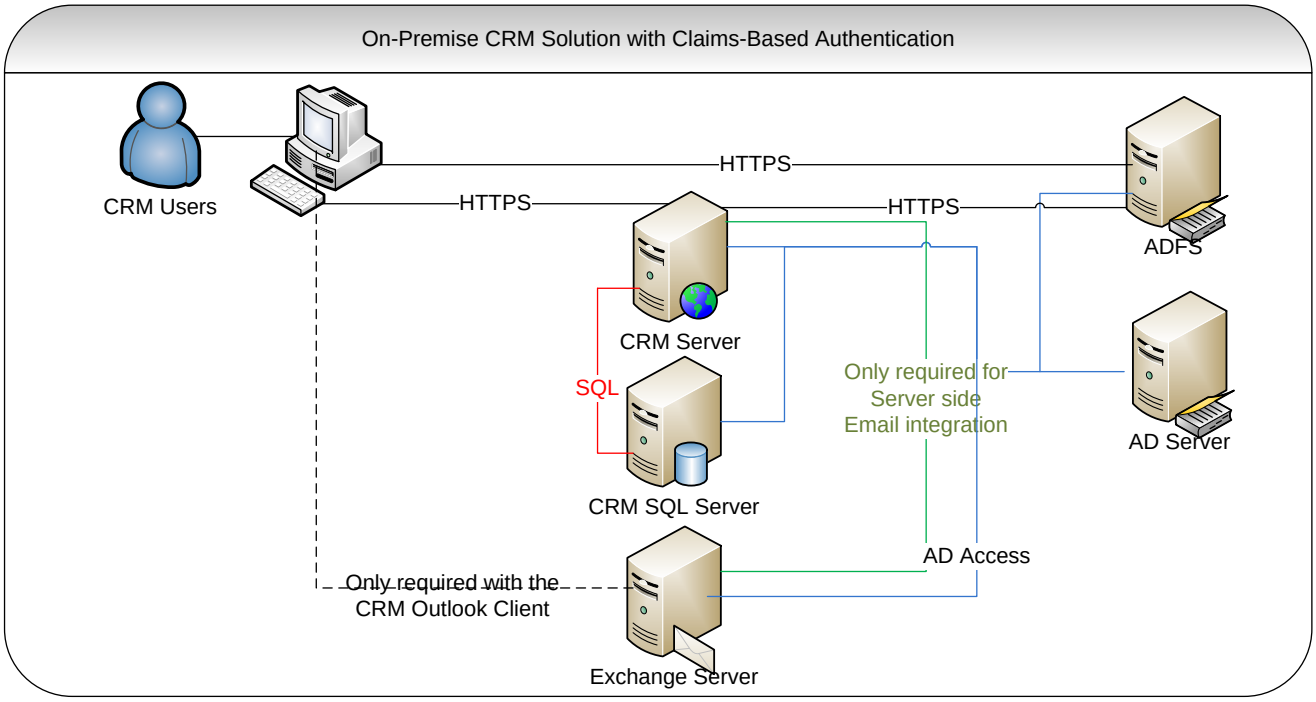
An overview of an on-premises implementation that uses Integrated Windows Authentication (IWA) is shown in the following diagram.



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

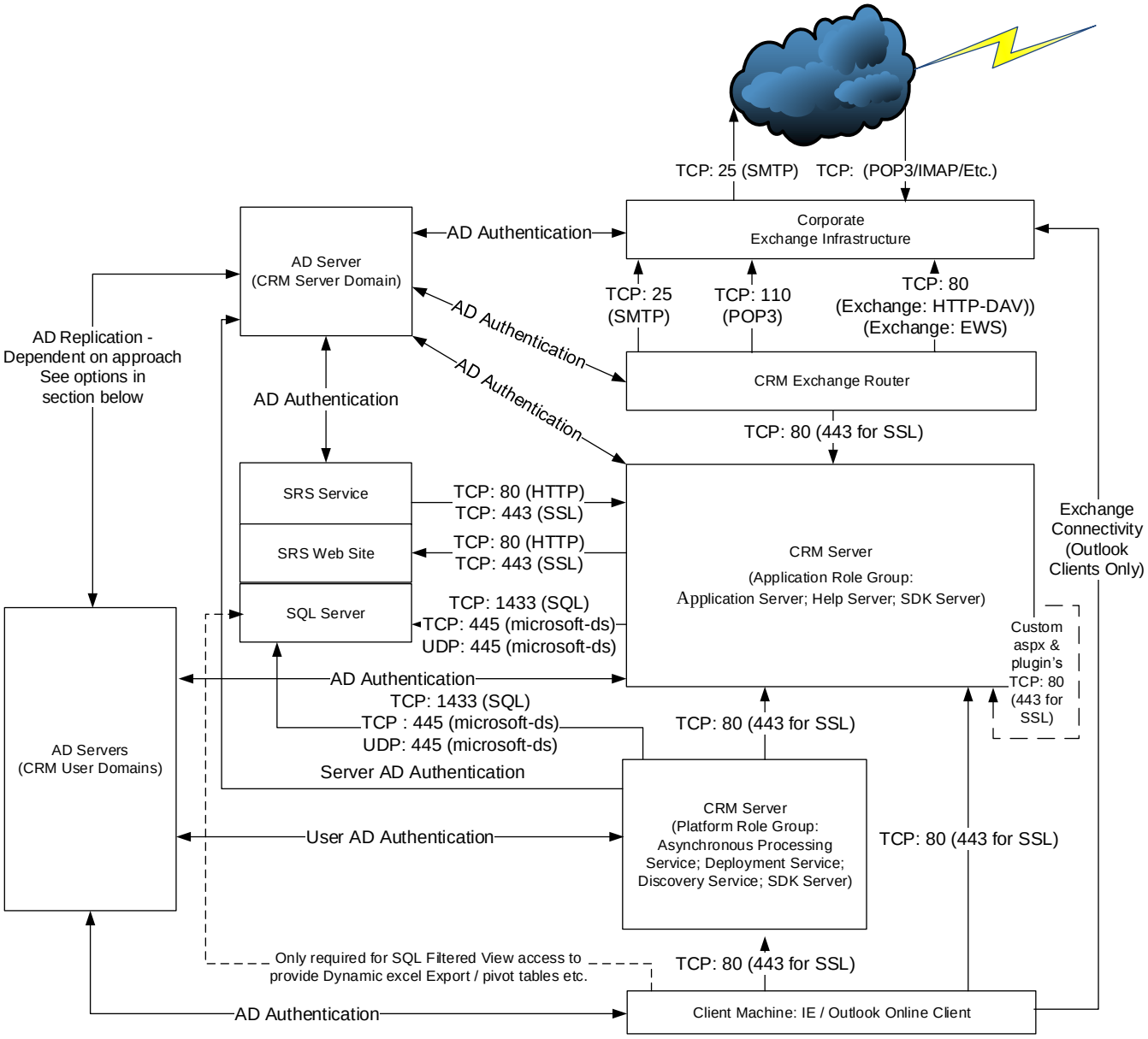
An overview of an on-premises implementation that uses claims-based authentication is shown in the following diagram using Active Directory Federation Service (ADFS) as the Security Token Service (STS).



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). 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 2011 is shown in the following graphic:



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 2011 are shown in the following table.

Component	Default Connectivity Requirements
CRM Server	▪ AD Connectivity from Microsoft Dynamics CRM Servers ▪ RDP Connection to all Servers recommended ▪ SQL Server access ▪ SQL Reporting Services access
Exchange Router	▪ Exchange Server Connectivity (HTTP DAV / EWS / SMTP) ▪ Other Mail Server Connectivity (POP3/SMTP) ▪ Optional Connectivity to a Microsoft Dynamics CRM Sink Mailbox ▪ HTTP / HTTPS access to CRM Servers / Network Load Balancer ▪ AD Authentication
Client	▪ Outlook Connectivity to Exchange ▪ Optional Connectivity to SQL Server for views ▪ HTTP / HTTPS access to CRM Servers / Network Load Balancer ▪ AD Authentication
ALL	▪ 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

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, we strongly recommend it. For information about how to configure HTTPS for Microsoft Dynamics CRM, see "Make Microsoft Dynamics CRM client-to-server network communications more secure" in **Post-Installation and Configuration Guidelines** in the Installing Guide.
TCP	445	Microsoft-DS	Active Directory directory service required for Active Directory access and authentication.
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 ports that are used for a deployment where the Sandbox Processing Service is running on a separate computer.

Protocol	Port	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 that are used by the SQL Server that runs the Microsoft Dynamics CRM Reporting Extensions server roles

The following table lists the ports that are used for a computer that is running SQL Server with only SQL Server and the Microsoft Dynamics 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; this number may vary if you have configured your SQL Server to use a different port number.
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; the 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	UPD	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. Note that while Simple Mail Transfer Protocol [SMTP] can be used in certain situations—schema, configuration, and global catalog replication—but not 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 behaviour 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 2011 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)
- HTTP-DAV (TCP:80) for the CRM Sink account or direct to users mail account
- Exchange Web Service (EWS) (TCP:80)

Appendix A: Resources

For additional information related to connectivity and firewall port requirements in Microsoft Dynamics CRM 2011, see the following additional resources:

- *Microsoft Dynamics CRM 2011 Implementation Guide*
  - Download
  - View Online
- 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
- Active Directory Replication Over Firewalls
- Securing Your Application Server