Microsoft Dynamics CRM 365

Security Hardening Guideline 2017

(Even though most of the material in this document was collected from official Microsoft material and channels, this document itself is **NOT OFFICIAL MICROSOFT documentation**.)

Innovation Pack 2017

Includes Unified Service Desktop Security 2.3

Includes Security Integration Technical Guideline (STIG) Recommendations

March 2017
Version 1.3

Roman S. Montagueo II
Microsoft Dynamics CRM/ERP Solutions Architect

Table of Contents

Preface

This guide covers Microsoft Dynamics CRM Security Hardening implementation and administration.

This guide is intended for system administrators, database administrators, developers, security groups, and IT staff involved in securing environments for Microsoft Dynamics CRM Business Applications.

Related Documents

This guide has references to material from Microsoft.

For more information, see the following documents on Microsoft Dynamics CRM Network:

Microsoft Dynamics CRM Scalable Security Guide

Microsoft Dynamics CRM System Administration Guide

Microsoft Dynamics CRM Installation Guide for the operating system you are using

Conventions

The following text conventions are used in this document:

Convention

italic

Italic type indicates book titles, emphasis, a defined term, or placeholder variables for which you supply particular values.

`monospace`

Monospace type indicates text, documentation, and wording specific to federal and public government systems.

Section 1. OPERATING SYSTEM AND PLATFORM TECHNOLOGY SECURITY CONSIDERATIONS FOR MICROSOFT DYNAMICS 365

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

In the broadest sense, security involves planning and considering tradeoffs between threats and access. For example, a computer can be locked in a vault and available only to one system administrator. This computer may be secure, but it's not very usable because it's not connected to any other computer. If your business users need access to the Internet and your corporate intranet, you must consider how to make the network both secure and usable.

In this topic you'll find helpful information and links to many resources you can use to make your computing environment more secure. Because ultimately, Microsoft Dynamics 365 data security largely depends on how well you first secure the operating system and software components.

1.1 In this topic

Securing Windows Server

Securing SQL Server

Securing Exchange Server and Outlook

Securing mobile devices

1.2 Securing Windows Server

Windows Server, the foundation of Microsoft Dynamics 365, provides sophisticated network security. The Kerberos version 5 authentication protocol that is integrated into Active Directory and Active Directory Federation Services (AD FS) lets you federate Active Directory domains by using claims-based authentication. Both give you powerful standards-based authentication. These authentication standards let users enter a single user name and password sign-in combination for resource access across the network. Windows Server also includes several features that help make the network even more secure.

Follow these links to learn more about these features and how to make your Windows Server deployment more secure:

- Windows Server 2012
  - Secure Windows Server 2012 R2 and Windows Server 2012

    - Windows Server 2012 Security Baseline

1.2.1 Windows error reporting

Microsoft Dynamics 365 requires the Windows Error Reporting (WER) service, which Setup will install if it is missing. The WER service collects information, such as IP addresses. These IP addresses are not used to identify users. The WER service does not intentionally collect names, addresses, email addresses, computer names, or any other form of personally identifiable information (PII). It is possible that such information may be captured in memory or in the data collected from open files, but Microsoft does not use it to identify users. In addition, some information that is transmitted between the Microsoft Dynamics 365 application and Microsoft may not be secure. For more information about the type of information that is transmitted, see Privacy statement for the Microsoft Error Reporting Service.

1.2.2 Virus, malware, and identity protection

To better protect your identity and your system against malware or viruses, check out these resources:

- Microsoft Security. This page is an entry point for tips, training, and guidance about how to keep your computer up to date and prevent it from being susceptible to exploitation, spyware, and viruses.
- Security TechCenter. This page has links to technical bulletins, advisories, updates, tools, and guidance designed to make computers and applications up to date and more secure.

1.2.3 Update management

Microsoft Dynamics 365 updates include security, performance, and functional improvements. Making sure your Microsoft Dynamics 365 applications have the latest updates helps make sure your system runs as efficiently and reliably as it can. You can find more information about how to manage updates here:

- Windows Server Update Services
- Software Updates in Configuration Manager
- Update Management in Windows Server 2012: Revealing Cluster-Aware Updating and the New Generation of WSUS

1.3 Securing SQL Server

Because Microsoft Dynamics 365 relies on SQL Server, make sure you take the following measures to improve the security of your SQL Server database:

- Apply the latest operating system, SQL Server service packs (SPs), and updates. Check the Microsoft Security website for the latest details.
- Install all SQL Server data and system files on NTFS partitions for file system-level security. You should make the files available only to administrative or system-level users

through NTFS permissions. This helps safeguard against users who access those files when the MSSQLSERVER service is not running.

- Use a low-privilege domain account. Or, specify the Network Service or Local System Account for SQL Server services. However, we do not recommend that you use these accounts because Domain User accounts can be configured with fewer permissions to run the SQL Server services. Domain User accounts should have minimal rights in the domain, which should help contain (but will not stop) an attack on the server if there is a compromise. In other words, Domain User accounts should have only local user-level permissions in the domain. If SQL Server is installed using a Domain Administrator account to run the services, a compromise of SQL Server will lead to a compromise of the entire domain. If you have to change this setting, use SQL Server Management Studio to make the change, because the access control lists (ACLs) on files, the registry, and user rights will be changed automatically.
- Because SQL Server authenticates users who have either Windows Authentication or SQL Server credentials, we suggest you use Windows Authentication for single sign-on convenience and the most secure authentication.
- At a minimum, enable auditing of failed sign-ins. By default, SQL Server system auditing is disabled, and no conditions are audited. This makes intrusion detection difficult and helps attackers cover their tracks.
- Report Server administrators should enable RDL Sandboxing to restrict access to the Report Server. More information: Enabling and Disabling RDL Sandboxing
- Configure each SQL logon to use the master database as the default database. Although users shouldn't have rights to the master database, as a best practice, you should change the default for every SQL logon (except those with the SYSADMIN role) to use *OrganizationName*_MSCRM as the default database. More information: Securing SQL Server

1.4 Securing Exchange Server and Outlook

The following considerations are for Microsoft Exchange Server or Exchange Server in a Microsoft Dynamics 365 environment:

- Exchange Server contains a rich series of mechanisms for precise administrative control of its infrastructure. In particular, you can use administrative groups to collect Exchange Server objects like servers, connectors, or policies, and then modify the ACLs on those administrative groups to make sure only certain users can access them. You may, for example, want to give Microsoft Dynamics 365 administrators control over servers that directly affect their applications. When you implement administrative groups efficiently, you know you are giving Microsoft Dynamics 365 administrators exactly the rights they need to do their jobs.
- Frequently, you may find it convenient to create a separate organizational unit (OU) for Microsoft Dynamics 365 users, and give Microsoft Dynamics 365 administrators limited administrative rights over that OU. Administrators can make changes for any user in that OU, but not for any user outside it.
- Always be sure you adequately protect against unauthorized email relay. Email relay lets an SMTP client use an SMTP server to forward email messages to a remote domain. By

default, Microsoft Exchange Server is configured to prevent email relay. The settings you configure will depend on your message flow and how your Internet service provider's (ISP) email server is configured. However, the best approach here is to lock down your email relay settings and then gradually open them to let email flow successfully. For more information, see the Exchange Server Help.

- If you use forward mailbox monitoring, the Email Router requires an Exchange Server or POP3-compliant mailbox. We recommend you set the permissions on this mailbox to prevent other users from adding server-side rules. For more information about Exchange Server mailboxes, see Recipients Permissions.
- The Microsoft Dynamics 365Email Router service operates under the Local System Account. This enables the Email Router to access a specified user's mailbox and process email in that mailbox.

For more information about how to make Exchange Server more secure, see Deployment Security Checklist.

1.5 Securing mobile devices

As organizations move to support an increasingly mobile workforce, strong security remains essential. Here are some resources to help you implement best practices for mobile devices, such as smartphones and tablets:

- How to Manage Mobile Devices by Using Configuration Manager and Windows Intune
- Windows for business
- Security Considerations (Microsoft Surface)
- iOS in Business (iPad and iPhone)

Section 2. NETWORK PORTS FOR MICROSOFT DYNAMICS 365

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

This section describes the ports that are used for Microsoft Dynamics 365. This information is helpful as you configure the network when users connect through a firewall.

2.1 In This Topic

Network ports for the Microsoft Dynamics 365 web application

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

Network ports for the Organization Web Service server role

Network ports that are used by the SQL Server that runs the SQL Server and Microsoft Dynamics 365 Reporting Extensions server roles

2.2 Network ports for the Microsoft Dynamics 365 web application

The following table lists the ports used for a server that is running a Full Server installation of Microsoft Dynamics 365. Moreover, except for the Microsoft SQL Server role, and the Microsoft Dynamics 365 Reporting Extensions server role, all server roles are installed on the same computer.

Protocol	Port	Description	Explanation
TCP	80	HTTP	Default web application port. This port may be different as it can be changed during Microsoft Dynamics 365 Server 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. Although this port is not required to run Microsoft Dynamics 365, we strongly recommend it. For information about how to configure HTTPS for Dynamics 365, see Make Dynamics 365 client-to-server network communications more secure.

TCP	445	Microsoft-DS	Active 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 service required for Active Directory access and authentication.
UDP	1025	Blackjack	DCOM, used as an RPC listener.

Important

Depending on your domain trust configuration, additional network ports may need to be available for Microsoft Dynamics 365 to work correctly. More information: Active Directory and Active Directory Domain Services Port Requirements

2.3 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	Dynamics 365 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\.

2.4 Network ports for the Organization Web Service server role

The following table lists the additional port that is used by the Organization Web Service server role.

Protocol	Port	Description	Explanation
TCP	808	Used for Fetch-based reports	Microsoft SQL Server Reporting Services servers that run Fetch-based reports initiated by Dynamics 365 clients communicate with the Organization Web Service server role (a Front End Server role) over this port.

2.5 Network ports that are used by the SQL Server that runs the SQL Server and Microsoft Dynamics 365 Reporting Extensions server roles

The following table lists the ports that are used for a computer that is running SQL Server and has only SQL Server and the Microsoft Dynamics 365 Reporting Extensions (SRS Data Connector) 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 service required for Active Directory access and authentication.
TCP	1433	ms-sql-s	SQL Server sockets service. This port is required for access to SQL Server. This number may be different if you have configured your default instance of SQL Server to use a different port number or you are using a named instance.
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 service required for Active Directory access and authentication.
UDP	1025	Blackjack	DCOM, used as an RPC listener.

◆**Important**

In addition to the ports listed previously, UDP port 1434 (SQL Server Browser Service) on the SQL Server is required by Microsoft Dynamics 365 Server Setup to return a list of the computers that are running SQL Server during the installation of Microsoft Dynamics 365 Server. To work around this, specify the *SQLServer\InstanceName* during Setup.

Section 3. KNOWN RISKS AND VULNERABILITIES

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

This topic describes the risks and vulnerabilities that may exist when you use Microsoft Dynamics 365. Mitigations and workarounds are also described when applicable.

3.1 In This Topic

- Risks when users connect to Dynamics 365 over an unsecured network
- Security recommendations on server role deployments
- Anonymous authentication
- Isolate the HelpServer role for Internet-facing deployments
- Claims-based authentication issues and limitations
- Secure the web.config file
- Outbound Internet calls from custom code executed by the Sandbox Processing Service are enabled
- Secure server-to-server communication
- DNS rebinding attacks
- JavaScript allowed for Power BI URLs on personal dashboards

3.2 Risks when users connect to Dynamics 365 over an unsecured network

Here are some issues that can occur when you run Microsoft Dynamics 365 without using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) (HTTPS):

- Microsoft Dynamics 365 user-provided data, including Visual chart definitions, can be altered over an unsecured HTTP connection by using "man in the middle" type attacks. To mitigate this vulnerability, configure Microsoft Dynamics 365 to only use TLS/SSL. For more information about how to configure Microsoft Dynamics 365 Server to use TLS/SSL, see Make Dynamics 365 client-to-server network communications more secure.

3.3 Security recommendations on server role deployments

The following recommendations can help make your Microsoft Dynamics 365 deployment more reliable and secure.

Server role	Recommendation

Sandbox Processing Service	Install this role on a dedicated server on a separate virtual LAN (VLAN) from other computers that are running Microsoft Dynamics 365 Server roles. Then, if there is a malicious plug-in running in the sandbox that exploits the computer, the network isolation from a separate VLAN can help protect other Dynamics 365 resources from being compromised.
Help Server	Install this role on a separate computer for both IFD and internally-facing deployments. For more information, see Isolate the HelpServer role for Internet-facing deployments later in this topic.

3.4 Anonymous authentication

Microsoft Dynamics 365Internet-facing deployment (IFD) requires anonymous authentication enabled on IIS for claims-based authentication. The claims-based authentication token doesn't contain raw credentials or the connection string to Microsoft Dynamics 365 Server. However, the web.config file does contain configuration information about the authentication mode. For more information, see Secure the web.config file later in this topic. To secure the Microsoft Dynamics 365 website, use TLS/SSL.

3.5 Isolate the HelpServer role for Internet-facing deployments

Microsoft Dynamics 365Internet-facing deployment (IFD) requires anonymous authentication. Because anonymous website authentication is used, the virtual directory used by the Microsoft Dynamics 365 Help site can be targeted for denial of service (DoS) attacks.

To isolate the Microsoft Dynamics 365 Help pages, and help protect the other Microsoft Dynamics 365 Server roles from potential DoS attacks, consider installing the Help Server role on a separate computer.

For more information about the options for installing Microsoft Dynamics 365 roles on separate computers, see Microsoft Dynamics 365 server roles.

For more information about reducing the risk of DoS attacks, see MSDN: Improving Web Application Security: Threats and Counter-measures.

3.6 Claims-based authentication issues and limitations

This topic describes issues and limitations when you use claims-based authentication with Microsoft Dynamics 365.

3.6.1 Verify that the identity provider uses a strong password policy

When you use claims-based authentication, you should verify that the identity provider is trusted by the security token service (STS) and, in turn, Microsoft Dynamics 365, enforces strong password policies. Microsoft Dynamics 365 doesn't enforce strong passwords. By default, when it is used as an identity provider, Active Directory enforces a strong password policy.

3.6.2 ADFS federation server sessions are valid up to 8 hours even for deactivated or deleted users

By default, Active Directory Federation Services (AD FS) server tokens allocate a web single sign-on (SSO) cookie expiration of 8 hours. So even when a user is deactivated or deleted from an authentication provider, as long as the user session is still active, the user can continue to be authenticated to secure resources.

Use any of these options to work around this issue:

- Disable the user in Microsoft Dynamics 365 and in Active Directory. For information about how to disable a user in Microsoft Dynamics 365, see Manage users. For information about how to disable a user in Active Directory, see the Active Directory Users and Computers Help.
- Reduce the web SSO lifetime. To do this, see the Active Directory Federation Services (AD FS) Management Help.

3.7 Secure the web.config file

The web.config file that is created by Microsoft Dynamics 365 does not contain connection strings or encryption keys. However, the file does contain configuration information about the authentication mode and strategy, ASP.NET view state information, and debug error message display. If this file is modified with malicious intent it can threaten the server where Microsoft Dynamics 365 is running. To help secure the web.config file, we recommend you do these things:

- Give permissions to the folder where the web.config file is located to only those user accounts that require it, such as administrators. By default, the web.config file is located in the <drive:>Program Files\Microsoft Dynamics CRM\CRMWeb folder.
- Limit the number of users who have interactive access to Dynamics 365 servers, such as console logon permission.
- Disable directory browsing on the Dynamics 365 website. By default, this is disabled. For more information about how to disable directory browsing, see Internet Information Services (IIS) Manager Help.

3.8 Outbound Internet calls from custom code executed by the Sandbox Processing Service are enabled

By default, outbound calls from custom code executed by the Microsoft Dynamics 365Sandbox Processing Service that access services on the Internet are enabled. For high-security deployments of Microsoft Dynamics 365, this can pose a security risk. If you don’t want to allow outbound calls from custom code, such as Dynamics 365 plug-ins or custom workflow activities, you can disable outbound connections from custom code executed by the Sandbox Processing Service by following the procedure here.

Instead of blocking all outbound calls, you can enforce web access restrictions on sandboxed plug-ins. More information: MSDN: Plug-in isolation, trusts, and statistics

Disabling outbound connections for custom code includes disabling calls to cloud services such as Microsoft Azure and Microsoft Azure SQL Database.

3.8.1 Disable outbound connections for custom code on the computer that is running the sandbox processing service

1. On the Windows Server computer where the Microsoft Dynamics 365Sandbox Processing Service server role is installed, start Registry Editor and locate the following subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\MSCRM**
2. Right-click **MSCRM**, point to **New**, click **DWORD Value**, type **SandboxWorkerDisableOutboundCalls**, and then press ENTER.
3. Right-click **SandboxWorkerDisableOutboundCalls**, click **Modify**, type 1, and then press ENTER.
4. Close Registry Editor.
5. Restart the Sandbox Processing Service. To do this, click **Start**, type **services.msc**, and then press ENTER.
6. Right-click **Microsoft Dynamics 365 Sandbox Processing Service**, and then click **Restart**.
7. Close the Microsoft Management Console (MMC) Services snap-in.

3.9 Secure server-to-server communication

By default, Microsoft Dynamics 365 server-to-server communication, such as communication between the Web Application Server role and the server that is running Microsoft SQL Server, isn’t executed over a secure channel. Therefore, information that is transmitted between servers may be susceptible to certain attacks, like man-in-the-middle attacks.

We recommend you implement secure networking, such as Windows Firewall, to help protect information that is transmitted between servers in your organization. More information: Windows Firewall with Advanced Security Overview

3.10 DNS rebinding attacks

Like many web-based applications, Microsoft Dynamics 365 may be vulnerable to DNS rebinding attacks. This exploit involves misleading a web browser into retrieving pages from two different servers, trusting that the servers are from the same domain, and subsequently breaking the Same Origin Policy. Using this technique, an attacker can tamper with Dynamics 365 data using the victim’s identity through cross-site scripting attacks on Dynamics 365 pages.

For more information about how to help protect against such attacks, see Protecting Browsers from DNS Rebinding Attacks.

3.11 JavaScript allowed for Power BI URLs on personal dashboards

Because JavaScript can be used so that personal dashboards can use Power BIURLs, be aware of the following risks of script injection attacks from malicious sources:

- Arbitrary redirection to an unexpected website, such as a phishing website.
- The creation of multiple large JavaScript objects in an attempt to crash the web browser.

To reduce the risk, consider implementing the following best practices:

- Only allow approved SharePoint sites to host Microsoft Office Excel documents used for embedding Power BI reports in dashboards. More information: Introduction to Power BI for Office 365 Admin Center
- Secure the SharePoint site that hosts the Power BI components so that only trusted sources can add documents that will be added to dashboards. Read about SharePoint permission levels
- Ask Microsoft Dynamics 365 users to avoid adding unapproved components to their dashboards. This is similar to educating users to not open attachments or click hyperlinks found in email messages from unknown sources.

Section 4. SECURITY IN UNIFIED SERVICE DESK

Unified Service Desk 2.0

Applies To: Dynamics 365 (online), Dynamics 365 (on-premises), Dynamics CRM 2013, Dynamics CRM 2015, Dynamics CRM 2016

Unified Service Desk configuration entities and the underlying User Interface Integration (UII) entities are stored in Microsoft Dynamics 365, and you can use the Dynamics 365 security model to govern access to both of these entities. Dynamics 365 has a robust security model that combines role-based, record-level, and field-level security to define the overall security rights that users have. More information: Security concepts for Microsoft Dynamics CRM

Unified Service Desk users can be broadly classified into two categories:

- Administrators: People who configure the Unified Service Desk and UII entities to define an agent application.
- Agents: People who use the Unified Service Desk client application to read the configuration in the Unified Service Desk and UII entities to perform their day-to-day work in a call center.

4.1 Using Unified Service Desk security roles

When you deploy Unified Service Desk to a Dynamics 365 instance, four security roles are created:

- **UIIAdministrator** and **UIIAgent** roles define access to the UII and required Dynamics 365 entities.
- **USD Administrator** and **USD Agent** roles define access to the Unified Service Desk entities, the underlying UII entities, and required Dynamics 365 entities. You must assign one of these two roles to users in your organization depending on their job role (administrator or agent).

More information: Manage access using Unified Service Desk security roles

4.2 Using Unified Service Desk configuration

Another approach to filtering access to Unified Service Desk data is through the use of configurations. A configuration is the logical grouping of various components in the Unified Service Desk agent application such as action calls, agent scripts, entity searches, events, and hosted controls. The configuration can be assigned to a user so that when the user starts the Unified Service Desk agent application, only the components included in the configuration are displayed. This is a great way to filter things that you want to be displayed to your agents without having to manage their security roles. However, please keep the following things in mind:

- A configuration can only be assigned to a user, and not to a team in Microsoft Dynamics 365.
- A configuration only filters the components when you access Unified Service Desk information through the client application. If you access Microsoft Dynamics 365 or Microsoft Dynamics 365 for Outlook directly, you can access data as per your Dynamics 365 security role.

Section 5. MANAGE ACCESS USING UNIFIED SERVICE DESK SECURITY ROLES

Unified Service Desk 2.0

Applies To: Dynamics 365 (online), Dynamics 365 (on-premises), Dynamics CRM 2013, Dynamics CRM 2015, Dynamics CRM 2016

You must assign the two Unified Service Desk security roles to appropriate users or teams. The **USD Administrator** role must be assigned to the users who will be configuring the application using Dynamics 365 to define an agent application. The **USD Agent** role must be assigned to the end users (agents) who will be using the client application to connect to the Dynamics 365 instance with the configured Unified Service Desk entities.

You must also assign the appropriate Dynamics 365 security role to the Unified Service Desk administrators and agents along with the Unified Service Desk security role to facilitate appropriate access on the Dynamics 365 entities along with the custom Unified Service Desk and UII entities. For example, you should assign the **Customer Service Representative** role along with the **USD Agent** role to the agents.

For information about assigning a security role to a user or team in Dynamics 365, see Manage users or Manage teams.

Section 6. MANAGE ACCESS USING UNIFIED SERVICE DESK CONFIGURATION

Unified Service Desk 2.0

Applies To: Dynamics 365 (online), Dynamics 365 (on-premises), Dynamics CRM 2013, Dynamics CRM 2015, Dynamics CRM 2016

Unified Service Desk configuration is a great way to filter things that you want your agents to see without having to manage their security roles. Agents can see only those Unified Service Desk components in the Unified Service Desk client application that are added in a configuration assigned to them.

You can add the following Unified Service Desk components in a configuration:

- Action calls
- Agent scripts
- Entity searches
- Events
- Forms
- Hosted controls
- Options
- Scriptlets
- Session information
- Toolbar
- Window navigation rule

6.1 In This Topic

Create a Unified Service Desk configuration

Set a configuration as the default

Associate auditing and diagnostics with a configuration

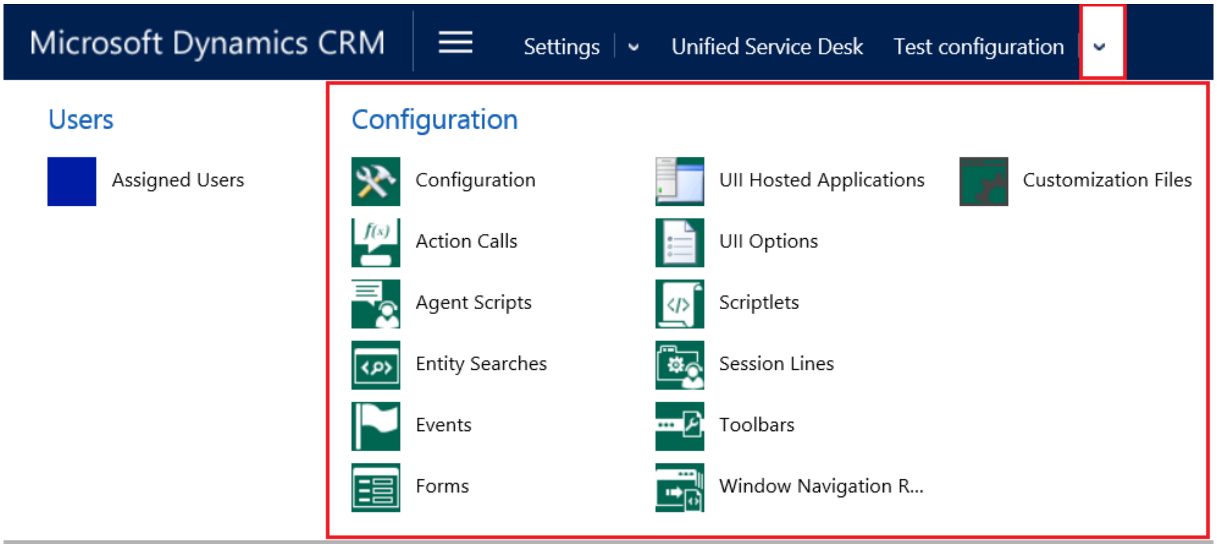
Assign users to a Unified Service Desk configuration

Clone a Configuration

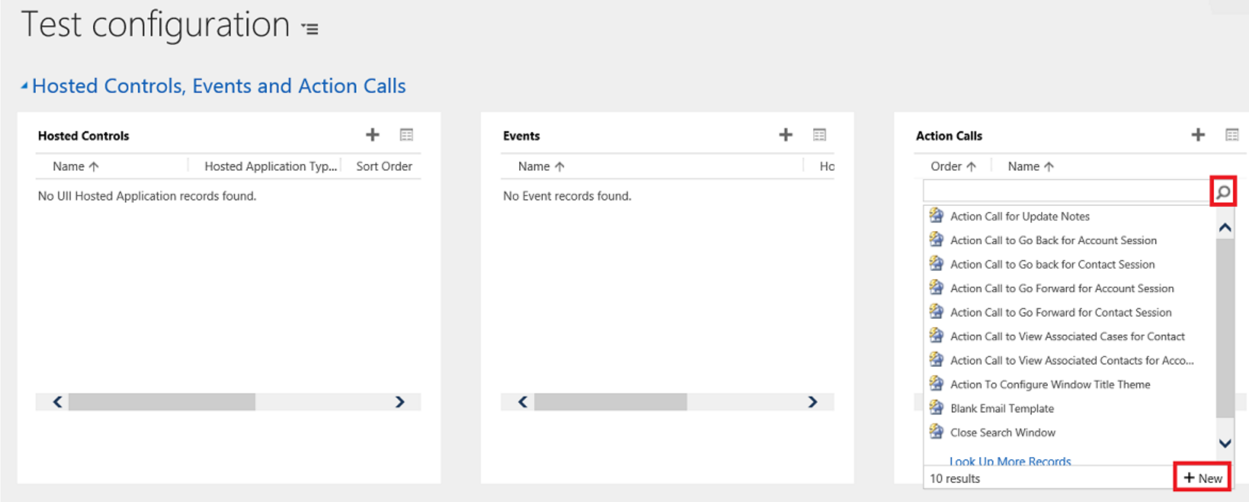
6.2 Create a Unified Service Desk configuration

1. Sign in to Microsoft Dynamics 365.
2. On the nav bar, click **Microsoft Dynamics 365**, and then select **Settings**.
3. Click **Settings** > **Unified Service Desk** > **Configuration**.

4. On the configuration page, click **New**.
5. On the **New Configuration** page, type the name of the configuration, and then click **Save**.
6. After the new configuration is saved, on the nav bar, click the down arrow next to the configuration name. This shows the components that can be added to a configuration.



7. Click a component to add it. The entity search page for the corresponding component appears. Click **Add Existing > <Component Name>** to search for the existing records. For example, if you selected **Action Calls**, click **Add Existing Action Call** on the entity search page.
8. Type the name of the component in the search box, and then press ENTER or click the search button. If a record doesn't exist, click **New** in the search results box to create an instance of the component you want to add.



No UII Hosted Application records found.

No Event records found.

Action Call for Update Notes
Action Call to Go Back for Account Session
Action Call to Go back for Contact Session
Action Call to Go Forward for Account Session
Action Call to Go Forward for Contact Session
Action Call to View Associated Cases for Contact
Action Call to View Associated Contacts for Acco...
Action To Configure Window Title Theme
Blank Email Template
Close Search Window
Look Up More Records
10 results

9. Repeat this with other components you want to add to the configuration.
10. After you have added the components, click the **Save** button 💾to save the configuration.

◆**Important**

If no hosted controls are added to a configuration, or if certain hosted controls are not added, such as the Panel Layout, Global Manager, and Connection Manager hosted controls, assigned users may see a blank Unified Service Desk client application window. For more information about how to create a sample configuration, see MSDN: Walkthrough 1: Build a simple agent application.

6.3 Set a configuration as the default

You can set a Configuration as the default configuration by using the Is Default attribute of the Configuration record. Then, any user not assigned to a Configuration will have only the Unified Service Desk components associated with the default configuration cached when they sign in to the Unified Service Desk client.

6.3.1 Set a configuration as the default

1. Sign in to Microsoft Dynamics 365.
2. On the nav bar, click **Main** > **Settings** > **Unified Service Desk**.
3. Click **Configuration**.
4. In the Active Configuration list, select for the configuration record you want to make the default.
5. Choose **Set As Default** from the actions menu.

6.4 Associate auditing and diagnostics with a configuration

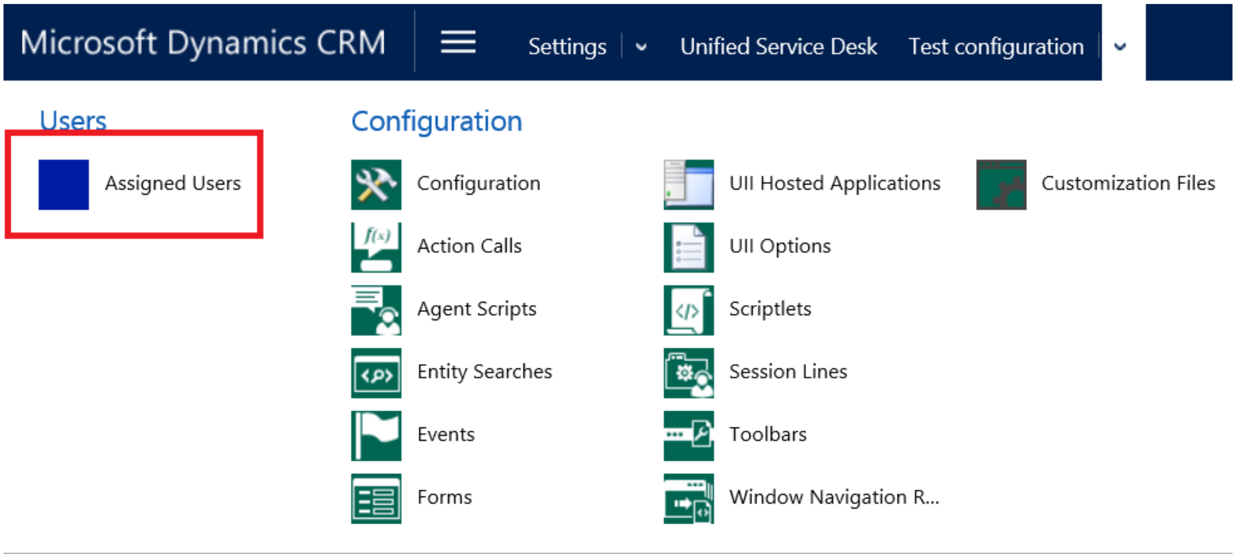
When you associate an Audit & Diagnostics record with a configuration, only the auditing and diagnostics events specified in the Audit & Diagnostics record are logged, and only for users who are assigned to the configuration. The following procedure describes how to associate an existing Audit & Diagnostics record with a configuration. For information about how to create an Audit & Diagnostics record, see Configure auditing and diagnostics in Unified Service Desk.

1. Sign in to Microsoft Dynamics 365.
2. On the nav bar, click **Main** > **Settings** > **Unified Service Desk**.
3. Click **Configuration**.
4. In the configuration list, select the configuration record you want to add an Audit & Diagnostic record for.
5. Next to **Audit & Diagnostic Settings**, type the name of the Audit & Diagnostic record in the search box, and then press ENTER or click the search button.
6. After you add the Audit & Diagnostics record, click the **Save** button 💾to save the configuration.

6.5 Assign users to a Unified Service Desk configuration

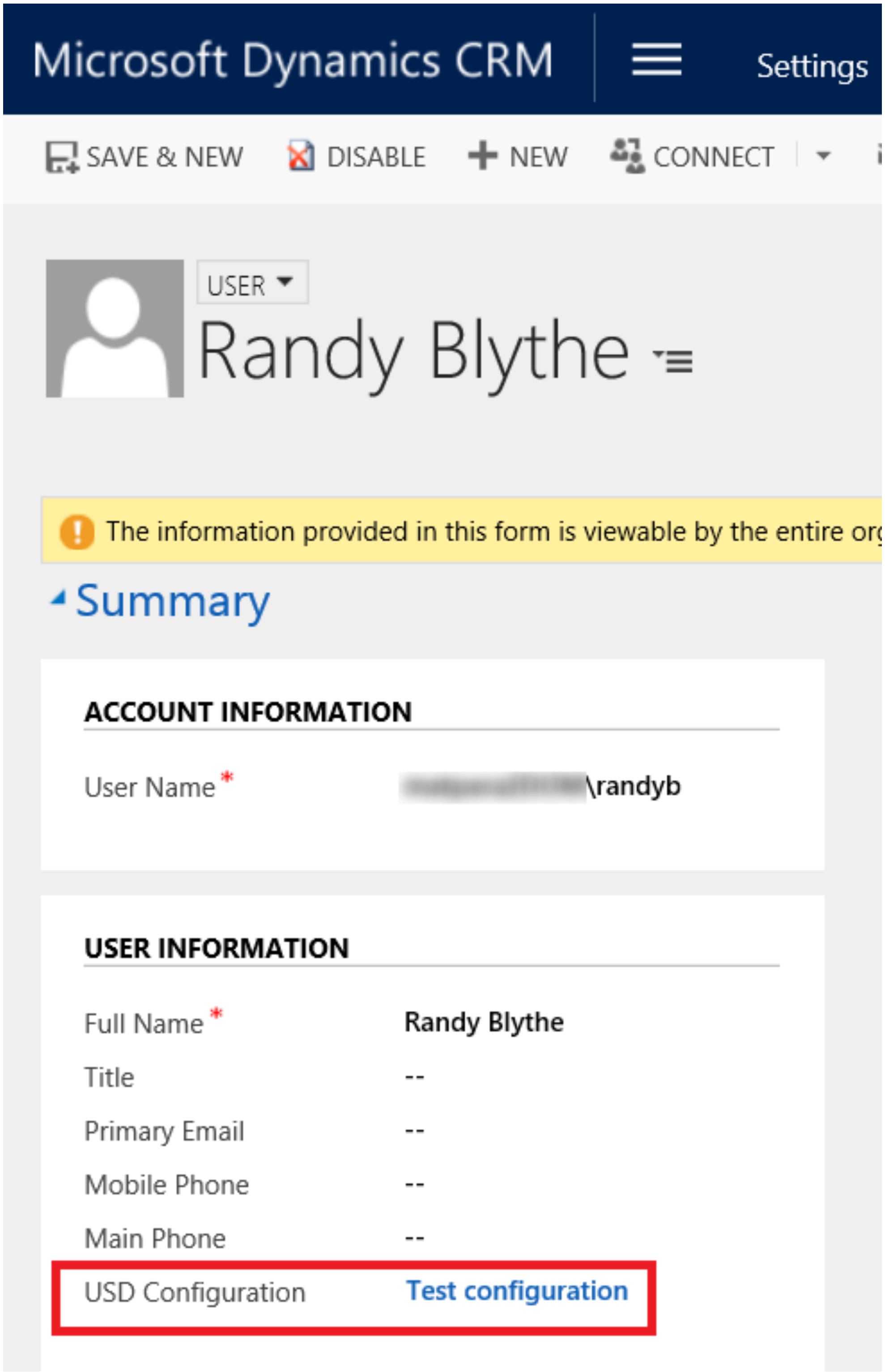
After you create a Unified Service Desk configuration, you can assign users to it. The users assigned to a configuration can only access components in the Unified Service Desk client application that are added to the configuration.

1. Sign in to Microsoft Dynamics 365.
2. On the nav bar, click **Microsoft Dynamics 365**, and then select **Settings**.
3. Click **Settings** > **Unified Service Desk** > **Configuration**.
4. On the configuration page, search for the required configuration record.
5. To open a configuration definition, either click the configuration name, or select the record, and then click **Edit**. This opens the configuration definition.
6. On the nav bar, click the down arrow next to the configuration name, and then click **Assigned Users**.



7. On the next page, you can either assign the configuration to an existing user, or create a new user and assign the configuration to it.
8. Type the name of the required user in the search box, and then press ENTER or click the search button.
9. Click the names of the required users to add them to the configuration. Click the **Save** button 💾to save your changes.

   If you click the user name under the **Name** column, the user record opens, and you can see that the Unified Service Desk configuration is assigned to the user in the **USD Configuration** field.



Randy Blythe

The information provided in this form is viewable by the entire org

Summary

ACCOUNT INFORMATION

User Name *	[redacted]\randyb

USER INFORMATION

Full Name *	Randy Blythe
Title	--
Primary Email	--
Mobile Phone	--
Main Phone	--
USD Configuration	Test configuration

A user can only be assigned to one Configuration. To assign a user to a different Configuration, you must first remove the existing Configuration.

6.5.1 Remove a user from a Configuration

1. Open the User form for the agent who you want to remove from a Configuration. One way you can do this is through **Settings** > **Security** > **Users**.
2. On the user form, click the **USD Configuration**.
3. Press the Delete key to remove the Configuration, and then save the form.

6.6 Clone a Configuration

You can copy a Configuration by cloning it. This lets you quickly copy an existing configuration and corresponding relationships to use for a different Configuration. Because a user can only belong to a single configuration, any users associated with configuration will not be associated with the cloned configuration.

6.6.1 Clone a configuration

1. Sign in to Microsoft Dynamics 365.
2. On the nav bar, click **Microsoft Dynamics 365**, and then select **Settings**.
3. Click **Settings** > **Unified Service Desk** > **Configuration**.
4. In the configuration list, select for the configuration record you want to clone.
5. Choose **Clone** on the actions menu, and when prompted, click **Clone**.

Section 7. SECURITY BEST PRACTICES FOR MICROSOFT DYNAMICS 365

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

Internet Information Services (IIS) is a mature web service that is included with Windows Server. Microsoft Dynamics 365 depends on an efficient and secure IIS web service. Consider the following:

- In the **machine.config** and **web.config** configuration files you can determine whether debugging is enabled, and also if detailed error messages are sent to the client. You should make sure that debugging is disabled on all production servers, and that a generic error message is sent to the client if a problem occurs. This avoids unnecessary information about the web server configuration being sent to the client.
- Make sure that the latest operating system and IIS service packs and updates are applied. For the latest information, see the Microsoft Security website.
- Microsoft Dynamics 365 Server Setup creates application pools called **CRMAppPool** and **CRMDeploymentServiceAppPool** that operate under user credentials that you specify during Setup. To facilitate a least-privileged model, we recommend that you specify separate domain user accounts for these application pools instead of using the Network Service account. Additionally, we recommend that no other ASP.NET-connected application be installed under these application pools. For information about the minimum permissions required for these components, see Minimum permissions required for Microsoft Dynamics 365 Setup and services.

♦**Important**

- Make sure all websites that are running on the same computer as the Microsoft Dynamics 365 website also have access to the Dynamics 365 database.
- If you use a domain user account, before you run Microsoft Dynamics 365 Server Setup, you may need to verify that the service principal name (SPN) is set correctly for that account, and if necessary, set the correct SPN. For more information about SPNs and how to set them, see How to use SPNs when you configure Web applications that are hosted on IIS.

7.1 Service principal name management in Microsoft Dynamics 365

The service principal name (SPN) attribute is a multivalued, nonlinked attribute that is built from the DNS host name. The SPN is used during mutual authentication between the client and the server hosting a particular service. The client finds a computer account based on the SPN of the service that it’s trying to connect to.

The Microsoft Dynamics 365 Server installer deploys role-specific services and web application pools that operate under user credentials specified during Setup. To review the complete list of these roles and their permission requirements, see Minimum permissions required for Microsoft Dynamics 365 Setup and services.

When you deploy a hosted Microsoft Dynamics 365 infrastructure, two of these roles may require additional consideration:

- Deployment Web Service
- Application Service

In web farm scenarios, as is the case for a hosted offering, the recommendation is to leave kernel-mode authentication enabled. In addition, you should closely consider using separate domain user accounts to run these services because:

- Having separate service accounts for these server roles facilitates being able to implement hardware load balancing.
- The Deployment Web Service server role requires elevated permissions to provision organizations in the Dynamics 365 database. If you want to adhere to a least-privileged model, the safest approach for implementing SPNs in a hosted Microsoft Dynamics 365 infrastructure involves having the Deployment Web Service run under a different domain user account than the Application Service.

If you follow this suggestion to use separate domain accounts for these server roles, you should check to make sure that the SPN is correct for each account before you start Microsoft Dynamics 365 Server Setup. This will make it easier for you to set the correct SPN when necessary.

If kernel-mode authentication is enabled, the SPNs will be defined for the machine account, regardless of the specified service account. When you implement a web farm, enable kernel-mode authentication and change the local **ApplicationHost.config** file.

If application and deployment web services are running on the same system, and kernel-mode authentication is disabled, you could configure both services to run under the same domain user account to prevent duplicate SPN issues. If you can’t enable kernel-mode authentication, install the Application and Deployment web services on separate systems. The SPNs may still need to be created manually since kernel-mode authentication is disabled.

For more information about SPNs and how to set them, see Service Principal Name (SPN) checklist for Kerberos authentication with IIS 7.0/7.5

Section 8. MICROSOFT DYNAMICS 365 SERVER ROLES

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

With Microsoft Dynamics 365 Server, you can install specific server functionality, components, and services on different computers. These components and services correspond to specific server roles. For example, customers who have larger user bases can install the Front End Server role on two or more servers that run Internet Information Services (IIS) to increase throughput performance for users. Or, a Full Server role can be installed on one computer and Microsoft Dynamics 365 Reporting Extensions on another. If a server role is missing, Deployment Manager displays a message in the **Messages** area.

Use one of the following options to install server roles:

- Run the Microsoft Dynamics 365 Server Setup Wizard to select one or more server role groups or one or more individual server roles. If Microsoft Dynamics 365 Server is already installed, you can use Programs and Features in Control Panel to add or remove server roles.
- Configure an XML Setup configuration file and then run Setup at the command prompt to specify a server role group or one or more individual server roles. You cannot explicitly select the SQL Server "role" for installation during Microsoft Dynamics 365 Server Setup. This is a logical role that SQL Server sets when you specify a particular instance of SQL Server, either local or on another computer (recommended) for use in the Microsoft Dynamics 365 deployment. For more information, see Microsoft Dynamics 365 Server XML configuration file.

Note

At any time after the initial installation of server roles, you can add or remove server roles in Control Panel. For more information, see Uninstall, change, or repair Microsoft Dynamics 365 Server.

Important

If you have a Microsoft Dynamics 365 deployment that includes one or more Front End Server and Back End Server roles, the Language Pack must be installed on the computer that has the Front End Server role. If you have deployed individual server roles, the Language Packs must be installed on the computers that are running the Web Application Server and the Help Server roles.

8.1 In This Topic

- Available group server roles
- Available individual server roles
- Scope definition

- Installation method definition
- Install the Microsoft Dynamics 365 Asynchronous Service to process only asynchronous events or email
- Microsoft Dynamics 365 Server role requirements

8.2 Available group server roles

Although these server role groups are recommended for most deployments, any individual server role may be installed during Setup.

All server roles must be running in your organization's network to provide a fully functioning system.

Server Role Group	Description	Scope	Installation Method
Full Server	Contains all roles from Front End Server, Back End Server, and Deployment Administration Server. By default, Microsoft Dynamics 365 Server Setup deploys the system as Full Server. In a Full Server deployment, server roles are not listed separately in Control Panel. To view the installed roles or make changes, right-click **Microsoft Dynamics 365 Server** , click **Uninstall/Change**, and then click **Configure**.	Deployment	Full
Front End Server	Enables the server roles for running client applications and applications developed with the Microsoft Dynamics 365 SDK.	Deployment	Group or Full
Back End Server	Includes the server roles that handle processing asynchronous events, such as workflows and custom plug-ins, database maintenance, and email routing. These roles are usually not exposed to the Internet. For a list of server roles that are included in this group, see the following table.	Deployment	Group or Full
Deployment Administration Server	Enables the server roles for components that are used to manage the Microsoft Dynamics 365 deployment either by using the methods described in the Microsoft Dynamics 365 SDK or the deployment tools. Also includes the interface for database disaster recovery support. For a list of server roles that are included in this group, see the following table.	Deployment	Group or Full

8.3 Available individual server roles

Server Role	Description	Server Group	Scope	Installation Method
Discovery Web Service	Finds the organization that a user belongs to in a multi-tenant deployment.	Front End Server	Deployment	Individual, Group, or Full
Organization Web Service	Supports running applications that use the methods described in the Microsoft Dynamics 365 SDK.	Front End Server	Deployment	Individual, Group, or Full
Web Application Server	Runs the Web Application Server that is used to connect users to Microsoft Dynamics 365 data. The Web Application Server role requires the Organization Web Service role.	Front End Server	Deployment	Individual, Group, or Full
Help Server	Makes Microsoft Dynamics 365 Help available to users.	Front End Server	Deployment	Individual, Group, or Full
Asynchronous Service	Processes queued asynchronous events, such as workflows, bulk e-mail, or data import.	Back End Server	Deployment	Individual, Group, or Full
Sandbox Processing Service	Enables an isolated environment to allow for the execution of custom code, such as plug-ins. This isolated environment reduces the possibility of custom code affecting the operation of the organizations.	Back End Server	Deployment	Individual, Group, or Full
Email Integration Service	Handles sending and receiving of email messages by	Back End Server	Deployment	Individual, Group, or Full

	connecting to an external email server.			
Deployment Web Service	Publishes the web service that provides the deployment interface described in the Microsoft Dynamics CRM SDK, such as those used to create an organization or manage the list of Deployment Administrators for the Microsoft Dynamics 365 deployment.	Deployment Administration	Deployment	Individual, Group, or Full Server
Deployment Tools	Consists of the Deployment Manager and Windows PowerShell cmdlets. Microsoft Dynamics 365 administrators can use the Windows PowerShell cmdlets to automate Deployment Manager tasks. Deployment Manager is a Microsoft Management Console (MMC) snap-in that deployment administrators can use to manage organizations, servers, and licenses for deployments of Microsoft Dynamics 365.	Deployment Administration	Deployment	Individual, Group, or Full Server
Microsoft Dynamics 365 VSS Writer	The Microsoft Dynamics 365 VSS Writer service provides an interface to backup and restore Dynamics 365 data	Deployment Administration	Deployment	Individual, Group, or Full Server

	by using the Windows Server Volume Shadow Copy Service (VSS) infrastructure.			
Microsoft Dynamics 365 Reporting Extensions	Provides reporting functionality by interfacing with the Microsoft Dynamics 365 system and Microsoft SQL Server Reporting Services.	N/A	Deployment	Individual by using srsDataConnectorSetup.exe.
SQL Server	Installs the MSCRM_CONFIG database on the SQL Server.	N/A	Deployment	Individual during Microsoft Dynamics 365 Server Setup or from Deployment Manager**Edit Organization Wizard**.

8.4 Scope definition

- **Deployment**. Each instance of the server role services the entire deployment.
- **Organization**. Each instance of the server role services an organization. Therefore, you can use a different server role instance for a given organization.

8.5 Installation method definition

- **Individual , Group, or Full**. During Microsoft Dynamics 365 Server Setup, you can install a server role individually, install one of the three predefined groups of server roles, or perform a Full Server installation that includes all roles. Or, you can select multiple individual server roles.
- **Microsoft Dynamics 365 Reporting Extensions**. Install this role using srsDataConnectorSetup.exe on the computer where Microsoft SQL Server Reporting Services is running.

For more information about Microsoft Dynamics 365 server roles and multiple server deployment, see Install Microsoft Dynamics 365 Server on multiple computers.

8.6 Install the Microsoft Dynamics 365 Asynchronous Service to process only asynchronous events or email

The Microsoft Dynamics 365 Asynchronous Processing Service (NT style service) can be used to process asynchronous events and email, accounts, contacts, and tasks using server-side synchronization. Depending on what server roles you select during Microsoft Dynamics 365 Server Setup, you can configure the Asynchronous Service to have the following features.

- Selecting both Asynchronous Service and Email Integration Service server roles installs the Asynchronous Processing Service that will be configured to process both asynchronous events and email, accounts, contacts, and tasks using server-side synchronization.
- Selecting only the Asynchronous Service server role installs the Asynchronous Processing Service that will be configured to process only asynchronous events.
- Selecting only the Email Integration Service server role, installs the Asynchronous Processing Service that will be configured to only process email, accounts, contacts, and tasks by using server-side synchronization.

Given these options, you can separate asynchronous events from server-side synchronization to help improve Dynamics 365 system performance and simplify monitoring.

8.7 Microsoft Dynamics 365 Server role requirements

The following table describes the components necessary for each Microsoft Dynamics 365 Server role. An "X" indicates the component is required for the Microsoft Dynamics 365 Server role to install and function. Notice that, in most cases if a component is not already installed, Microsoft Dynamics 365 Server Setup will install it.

8.7.1 Microsoft Dynamics 365 Server Role Prerequisites

Component	Back End Server	Front End Server	Deployment Administration Server
Microsoft SQL Server Reporting Services ReportViewer control		X	
SQL Server Native Client	X	X	X
Microsoft Application Error Reporting Tool	X	X	X
Microsoft Visual C++ Runtime Library	X	X	X
Windows Server Web Server Role		X	X
Indexing Service		X	
Microsoft .NET Framework 4	X	X	X
Microsoft Chart Controls for Microsoft .NET Framework		X	
Microsoft Azure platform SDK	X	X	X
Windows PowerShell			X
Microsoft URL Rewrite Module for IIS		X	
File Server Resource Manager		X	

The following table describes the group membership for the Active Directory that is used by Microsoft Dynamics 365. An “X” indicates the group membership required for the service to function.

8.7.2 Group Membership Requirements

Service	PrivUserGroup	SQLAccessGroup	PrivReportingGroup	ReportingGroup
Deployment Web Service service account	X	X		
Web Application Service*	X	X		
Asynchronous Service service account	X	X		
Sandbox Processing Service service account**				
SQL Server service account		X		
Microsoft SQL Server Reporting Services server account	X		X	
Email Router service account	X			
Installing User/Service account				X
Individual user accounts in Microsoft Dynamics 365				X
Unzip Service service account	X			
Microsoft Dynamics 365 VSS Writer service account	X	X		

* The Web Application Service identity is applied to the CRMAppPool application pool. Subsequently, this identity is used by the Organization Service, Web Application, and Microsoft Dynamics CRM platform.

** The Sandbox Service does not need any Microsoft Dynamics 365 group membership.

Note

Email Router runs as a local system.

Important

- The Installing user should be a separate service account, but it should not be used to run any services.
- If any of the service accounts are created as users in Microsoft Dynamics 365, you may encounter various problems, some of which are potential security issues.

Section 9. ADMINISTRATION BEST PRACTICES FOR ON-PREMISES DEPLOYMENTS OF MICROSOFT DYNAMICS 365

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

By following some simple rules of administration, you can significantly improve the security of your Microsoft Dynamics 365 on-premises deployment.

- Typically, there is no need for Dynamics 365 users to have administrative privileges over the domain. Therefore, all Dynamics 365 user accounts should be restricted to Domain Users membership. Also, following the principle of least-privilege, anyone who uses the Dynamics 365 system should have minimal rights. This starts at the domain level. A domain user account should be created and used to run Dynamics 365. Domain Administrator accounts should never be used to run Dynamics 365.
- Limit the number of Microsoft Dynamics 365Deployment Administrator and System Administrator roles to a few people who are responsible for rule changes. Others who are SQL Server, Microsoft Exchange Server, or Active Directory administrators do not have to be members of the Dynamics 365 users group.
- Make sure that at least two or three trusted people have the Deployment Administrator role. This avoids system lockout if the primary Deployment Administrator is unavailable.
- In some organizations it is a common practice to reuse passwords across systems and domains. For example, an administrator responsible for two domains may create Domain Administrator accounts in each domain that use the same password, and even set local administrator passwords on domain computers that are the same across the domain. In such a case, a compromise of a single account or computer could lead to a compromise of the entire domain. Passwords should never be reused in this manner.
- It is also common practice to use Domain Administrator accounts as service accounts for common services such as back-up systems. However, it is a security risk to use Domain Administrator accounts as service accounts. The password can easily be retrieved by anyone who has administrative rights over the computer. In such a case, the compromise could affect the entire domain. Service accounts should never be Domain Administrator accounts, and they should be limited in privilege as much as possible.
- A domain user account that is specified to run a Microsoft Dynamics 365 service must not also be configured as a Dynamics 365 user. This can cause unexpected behavior in the application.

Section 10. SECURITY CONSIDERATIONS FOR MICROSOFT DYNAMICS 365

Dynamics CRM 2016

Applies To: Dynamics 365 (on-premises), Dynamics CRM 2016

Microsoft Dynamics 365 is designed in a way that helps make your deployment more secure. This section provides information and best practices for the Microsoft Dynamics 365 application. More information: Security concepts for Microsoft Dynamics 365

10.1 In This Topic

- What kind of service account should I choose?
- Minimum permissions required for Microsoft Dynamics CRM Setup and services
- Microsoft Dynamics CRM installation files

10.2 What kind of service account should I choose?

When you specify an identity to run a Microsoft Dynamics 365 service, you can choose either a domain user account or the Network Service account.

If the service interacts with network services, accesses domain resources like file shares or if it uses linked server connections to other computers, you can use a minimally-privileged domain account. Many server-to-server activities can be performed only with a domain user account and can provide the most secure option. This account should be pre-created by domain administration in your environment.

Note

When you configure a service to use a domain account, you can isolate the privileges for the application, but must manually manage passwords or create a custom solution for managing these passwords. Many server applications use this strategy to enhance security, but this strategy requires additional administration and complexity. In these deployments, service administrators spend a considerable amount of time on maintenance tasks such as managing service passwords and service principal names (SPNs), which are required for Kerberos authentication. In addition, these maintenance tasks can disrupt service.

The Network Service account is a built-in account that has more access to resources and objects than members of the Domain Users group. Services that run as the Network Service account access network resources by using the credentials of the computer account in the format <domain_name>\<computer_name>$. The actual name of the account is NT AUTHORITY\NETWORK SERVICE.

10.3 Minimum permissions required for Microsoft Dynamics CRM Setup and services

Microsoft Dynamics 365 is designed so that its features can run under separate identities. By specifying a domain user account that is granted only the permissions necessary to enable a particular feature to function, you help secure the system and reduce the likelihood of exploitation.

This topic describes the minimum permissions that are required by the user account for Microsoft Dynamics 365 services and features.

10.3.1 Microsoft Dynamics CRM Server 2016 Setup

The user account used to run Microsoft Dynamics CRM Server 2016 Setup that includes the creation of databases requires the following minimum permissions:

- Be a member of the Active Directory Domain Users group. By default, Active Directory Users and Computers adds new users to the Domain Users group.
- Be a member of the Administrators group on the local computer where Setup is running.
- Have Local Program Files folder read and write permission.
- Be a member of the Administrators group on the local computer where the instance of SQL Server is located that will be used to store the Microsoft Dynamics 365 databases.
- Have sysadmin membership on the instance of SQL Server that will be used to store the Microsoft Dynamics 365 databases.
- Have organizational unit and security group creation and add membership permission to those groups in Active Directory. Alternatively, you can use a Setup XML configuration file to install Microsoft Dynamics CRM Server 2016 when security groups have already been created. For more information, see Use the command prompt to install Microsoft Dynamics Server 365.
- If Microsoft SQL Server Reporting Services is installed on a different server, you must add the Content Manager role at the root level for the installing user account. You must also add the System Administrator Role at the site-wide level for the installing user account.

10.3.2 Microsoft Dynamics 365 services and IIS application pool identity permissions

This section lists the minimum permissions that domain user accounts require for the services and the IIS application pools that Microsoft Dynamics 365 uses.

Important

- Microsoft Dynamics 365 services and application pool (CRMAppPool) identity accounts must not be configured as a Microsoft Dynamics 365 user. Doing so can cause authentication issues and unexpected behavior in the application for all Microsoft

Dynamics 365 users. More information: Problems in CRM when the CRMAppPool user account is a CRM user

- Managed service accounts (group-managed service accounts (gMSA) or single-managed service accounts) and virtual accounts (NT SERVICE\,<SERVICENAME>) aren't supported for running Microsoft Dynamics 365 services.

The following subsections describe the domain user account permissions required for each service or application pool identity:

- Microsoft Dynamics 365 Sandbox Processing Service
- Microsoft Dynamics 365 Asynchronous Processing Service and Microsoft Dynamics 365 Asynchronous Processing Service (maintenance) services
- Microsoft Dynamics 365 Monitoring Service
- Microsoft Dynamics 365 VSS Writer service
- Deployment Web Service (CRMDeploymentServiceAppPool Application Pool identity)
- Application Service (CRMAppPool IIS Application Pool identity)

10.3.2.1 Microsoft Dynamics 365 Sandbox Processing Service

- Domain Users membership.
- That account must be granted the **Logon as service** permission in the Local Security Policy.
- Folder read and write permission on the **Trace**, by default located under \Program Files\Microsoft Dynamics 365\Trace, and user account **%AppData%** folders on the local computer.
- Read permission to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM** subkey in the Windows registry.
- The service account may need an SPN for the URL used to access the website that is associated with it. To set the SPN for the Sandbox Processing Service account, run the following command at a command prompt on the computer where the service is running.

  ```
  SETSPN –a MSCRMSandboxService/<ComputerName> <service account>
  ```

10.3.2.2 Microsoft Dynamics 365 Asynchronous Processing Service and Microsoft Dynamics 365 Asynchronous Processing Service (maintenance) services

- Domain Users membership.
- PrivUserGroup and SQLAccessGroup membership. By default, these groups are created and appropriate membership is granted during Microsoft Dynamics CRM Server Setup.
- Built-in local group Performance Log Users membership.
- That account must be granted the **Logon as service** permission in the Local Security Policy.
- Read and write permission on the following folders.

    - The **Trace** folder. By default located under \Program Files\Microsoft Dynamics CRM\, and user account **%AppData%** folder on the local computer.
    - The **CustomizationImport** folder. By default located under \Program Files\Microsoft Dynamics CRM\. This may be required for solution import when you use the Microsoft Dynamics 365 SDK.
- All access permissions except Full Control and Write DAC to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM** and **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSCRMSandboxService** subkeys in the Windows registry.
- The service account may need an SPN for the URL used to access the website that is associated with it. To set the SPN for the Asynchronous Service account, run the following command at a command prompt on the computer where the service is running.

  ```
  SETSPN –a MSCRMAsyncService/<ComputerName> <service account>
  ```

10.3.2.3 Microsoft Dynamics 365 Monitoring Service

- Domain Users membership.
- That account must be granted the **Logon as service** permission in the Local Security Policy.
- If the Microsoft Dynamics 365 Monitoring Service is installed with a Front End Server server role, local administrator group membership on the computer where the service is running is required to monitor the web site and application pools. More information: Available individual server roles
- Read permission to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM**
- SQLAccessGroup membership. By default, this group is created and appropriate membership is granted during Microsoft Dynamics CRM Server Setup.
- The service account may need an SPN for the URL used to access the website that is associated with it.

10.3.2.4 Microsoft Dynamics 365 VSS Writer service

- Domain Users membership.
- That account must be granted the **Logon as service** permission in the Local Security Policy.
- Read permission to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM**
- PrivUserGroup and SQLAccessGroup membership. By default, these groups are created and appropriate membership is granted during Microsoft Dynamics CRM Server Setup.

10.3.2.5 Deployment Web Service (CRMDeploymentServiceAppPool Application Pool identity)

- Domain Users membership.

- That account must be granted the **Logon as service** permission in the Local Security Policy.
- Local administrator group membership on the computer where SQL Server is running is required to perform organization database operations (such as create new or import organization).
- Local administrator group membership on the computer where the Deployment Web Service is running.
- Sysadmin permission on the instance of SQL Server to be used for the configuration and organization databases.
- Folder read and write permission on the **Trace** and **CRMWeb** folders, by default located under \Program Files\Microsoft Dynamics CRM\, and user account **%AppData%** folder on the local computer.
- All access permissions except Full Control and Write DAC to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM** and **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSCRMSandboxService** subkeys in the Windows registry.
- PrivUserGroup and SQLAccessGroup membership. By default, these groups are created and appropriate membership is granted during Microsoft Dynamics CRM Server Setup.
- CRM_WPG group membership. This group is used for IIS worker processes. The group is created and the membership is added during Microsoft Dynamics CRM Server Setup.
- The service account may need an SPN for the URL used to access the website that is associated with it.

10.3.2.6 Application Service (CRMAppPool IIS Application Pool identity)

- Domain Users group membership.
- Built-in local group Performance Log Users membership.
- Folder read and write permission on the **Trace** and **CRMWeb** folders, by default located under \Program Files\Microsoft Dynamics CRM\, and user account **%AppData%** folder on the local computer.
- All access permissions except Full Control and Write DAC to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSCRM** and **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSCRMSandboxService** subkeys in the Windows registry.
- CRM_WPG group membership. This group is used for IIS worker processes. The group is created and the membership is added during Microsoft Dynamics CRM Server Setup.
- The service account may need an SPN for the URL used to access the website that is associated with it.

10.3.2.7 IIS Application Pool identities running under Kernel-Mode authentication and SPNs

By default, IIS websites are configured to use Kernel-Mode authentication. When you run the Microsoft Dynamics 365 website by using Kernel-Mode authentication, you might not need to configure additional service principal names (SPNs) for the CRMAppPool identities.

To determine whether your IIS deployment requires SPNs, see Service Principal Name (SPN) checklist for Kerberos authentication with IIS 7.0/7.5.

10.4 Microsoft Dynamics CRM installation files

If you plan to install Microsoft Dynamics CRM 2016 from a location on the network, such as a network share, you must make sure that the correct permissions are applied to the folder, preferably on an NTFS volume, where the installation files are located. For example, you may want to allow only members of the Domain Admins group permissions for the folder. This practice can help to reduce the risk of attacks on the installation files that may compromise or alter them. For more information about how to set permissions on files and folders on the Windows operating system, see Windows Help.

Excerpt from:

Scalable Security Modeling with Microsoft Dynamics CRM

VERSION: 1.1 AUTHOR: Roger Gilchrist

COMPANY: Microsoft Corporation

RELEASED: September 2015 Updated: March 2016 Applies to: Microsoft Dynamics CRM 2015 and Microsoft Dynamics CRM 2016

Microsoft Dynamics CRM

Copyright

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.

Feedback

To send comments or suggestions about this document, please click the following link and type your feedback in the message body: Send Feedback

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.

Introduction

Microsoft Dynamics CRM 2015 and Microsoft Dynamics CRM 2016 offer a wide range of security modeling features, and it is important to choose the most appropriate approach to implementing a particular solution. Each feature offers a combination of characteristics that provide a balance between granularity of access control, administrative ease, and impact on scalability. Having an understanding of the underlying mechanisms supporting each security modeling feature can be useful when selecting the best approach to solving a particular challenge, especially when planning to develop a large volume system.

Granting access for a user to the system can be broken out into: ▪ Authentication: Determining who the user is and confirming that they are who they say they are ▪ Authorization: Determining whether the authenticated user is entitled to access the system and what

they're permitted to see or do in the system

Authentication in Dynamics CRM is handled using platform features such as Integrated Windows Authentication or claims-based authentication with an identity provider such as Active Directory Federation Services. These all determine the identity of the user who is requesting access to the system. The deployment and scalability of the technologies supporting authentication is best described by resources focused specifically on those technologies and, therefore, is out of the scope of this document.

After a user has been identified, information recorded about the user in the Dynamics CRM system, such as their security roles and team memberships, is used to determine whether they are allowed to use the system and what they are allowed to see and do in the system, or in other words, what they are authorized to do.

This paper describes how these security modeling features in Microsoft Dynamics CRM for authorization work at scale, the implications associated with these features functioning at high volumes, and guidance on common and recommended usage patterns for modeling Dynamics CRM security at scale, incorporating teams as appropriate.

Important: For additional information about scalable security modeling in

Microsoft Dynamics CRM 2016, see Security concepts for Microsoft Dynamics CRM.

Common business scenarios

In most CRM implementations, access to information is either provided openly within the organization or it's limited by a combination of the role and the business area or group in which a user works or operates. In many organizations, people perform multiple roles concurrently. Sometimes, there are also requirements for exceptional circumstances in which individuals require access to information that is outside of their normal job demands and perhaps information that wouldn't normally be exposed to them.

While there is no one-size-fits-all model and different businesses and industries follow varying approaches, common user access patterns do emerge, particularly regarding alternative perspectives on relationship management. The reason these common patterns occur is that often the approach to interact with a client and the way that client expects to be treated by the organization are the same particularly when the importance of that interaction to the business is equivalent, even though the actual content of the conversations are very different.

Typically encountered user access patterns are described in the following table.

Usage pattern	Description
Active involvement	▪ Regular, significant involvement directly with the customer/deal ▪ Informed, with existing knowledge of the customer/deal and current related activity, and personal actions based on a direct relationship with the people involved
Secondary involvement	▪ ·Informed involvement, maintaining active knowledge of activity but not directly participating or acting on the deal or with the customer, such as providing cover for

	absence of actively involved staff ▪ ·Support others who have a personal relationship with customer such as providing advice or support to the people actively involved, providing specialist knowledge to a specific deal or customer
Transactional interaction	▪ Specific activity oriented involvement, for example, receiving and acting on a request to update a customer's address ▪ No personal or on-going engagement, such as in a contact center
Management oversight	▪ Managerial or governance responsibility across a business or geographical area ▪ Viewing and directing involvement of others rather than specific involvement
Reporting	▪ Aggregated business reporting ▪ Data organized to preserve anonymity rather providing direct access to customers/deals
Compliance	▪ Oversight read-only access to all records for a business area

In a CRM system, an important concept to understand and model is the nature of the active relationship to individual customers, including aspects such as:

▪ How often the organization and customer interact ▪ Who initiates each interaction ▪ Whether or not there is interaction even when no active business is taking place at that moment ▪ Who within the organization may be involved in an interaction with the customer

How each of these interaction characteristics is exhibited for an organization can vary depending on the type of service the organization delivers and the size and type of customer base they work with to be able to deliver an effective working model. This interaction in a relationship often can be viewed based on the value of the relationship with a customer; the higher the value, the more personalized and actively managed the relationship becomes. In this context, value can be measured from a variety of perspectives, including financial, influence, sensitivity, or risk, depending on the specific business in question.

Characteristics of the different values of customer interactions are shown in the following table.

Value of interaction	Characteristics
Low	▪ Minimal investment of time ▪ Transactional relationship ▪ No personal relationship ▪ Wide access
Medium	▪ Proactive management ▪ Perception of personalized approach ▪ Group relationship/access
High	▪ Large investment of time ▪ Personalized approach ▪ Personal relationship ▪ Privacy/controlled Access

In some industries, particularly in financial services and professional services, users typically work more on the basis of individual opportunities or cases. With higher value services, such as investment banking and legal services in which large sums of money are involved, a common requirement is to provide access to information only when a person needs to work on individual deals or cases. This requirement may arise for a number of reasons, such as legal restrictions, privacy, competitive detail, or data sensitivity.

In these scenarios, people from different parts of the business work together in teams on each opportunity or case. Often, there isn't a specific pattern for allocating people particular work items, but instead work is allocated based on criteria such as specialist skills and availability. In these types of scenarios, it's important to only grant permissions to individual records or sets of records (such as a case and all the supporting activities related to the case) to the specific people who will be involved.

This determination of restricted access is important to define. In many cases, while there is a need to assign individual responsibility, there is no requirement to prevent other users from seeing the information. The preceding examples contain many cases in which it is important to control access, but the additional checks and controls that are required add complexity to the solution implementation and to the processing required of the system. It is therefore a valuable exercise to determine if the extra security controls are genuinely required to address the business need. For situations that don't require the extra controls, it makes sense to determine this early on, as broad access needs for secondary usage patterns may contradict an initial perception that tight controls to primary owners are required. This is particularly important for environments in which individual owners are supported by much broader call center support teams that need access to the same data to assist the customer.

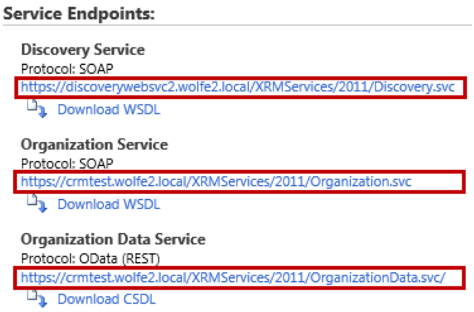
For situations in which it is important to control access to individuals directly involved in a deal or case, team ownership can become an effective way to model access to information. This approach is typically combined with access granted at a more general level for specialist roles or users who need access to a wide ranging set of information. This type of access can be required for roles such as Compliance Officer or General Manager that work across all the information in an area.

In addition to considering options for granting users access to data, it can be equally important to manage situations in which users should no longer have access to information, such as when an employee leaves a job changes roles. In these cases, their access must be revoked. As a result, be sure to carefully consider the lifetime of information access permissions.

Section 11. APPENDIX – REFERENCE MATERIAL

IBM Published document: CRM2011 Multi-Server Build – Robert Shurtleff is the contributor.

11.1 Test Access to the Service Endpoints

Test Access to the Service Endpoints • Login to CRM • Go to **Settings>Customizations** and click on **Developer Resources** • Click on each Service Endpoint to test access	 Service Endpoints: Discovery Service Protocol: SOAP https://discoverywebsvc2.wolfe2.local/XRMServices/2011/Discovery.svc Download WSDL Organization Service Protocol: SOAP https://crmtest.wolfe2.local/XRMServices/2011/Organization.svc Download WSDL Organization Data Service Protocol: OData (REST) https://crmtest.wolfe2.local/XRMServices/2011/OrganizationData.svc/ Download CSDL

Section 12. APPENDIX A - TROUBLESHOOTING PERMISSIONS

Note: The following permissions should have been applied to the Administrators group during the SQL install. Use these steps to troubleshoot if you're having issues.

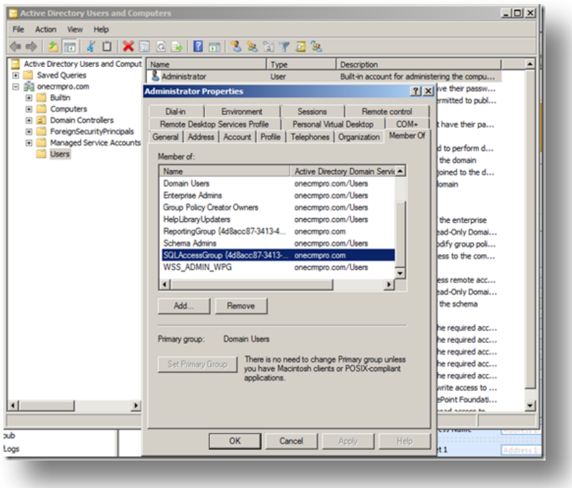
Trying to publish a CRM customization and exporting customizations will fail with a SQL error. This is because the administrator currently doesn't have adequate permissions. You can also fail simply trying to run a report. Go to:

Start -> Administrative Tools -> Active Directory Users and Computers

Add the Administrator user to the following groups:

SQL Admin group

Reboot the VM – and test again.



Name	Type	Description
Administrator	User	Built-in account for administering the compu...

Administrator Properties

Member of:

Name	Active Directory Domain Servi
Domain Users	onecrmpro.com/Users
Enterprise Admins	onecrmpro.com/Users
Group Policy Creator Owners	onecrmpro.com/Users
HelpLibraryUpdaters	onecrmpro.com/Users
ReportingGroup {4d8acc87-3413-4...	onecrmpro.com
Schema Admins	onecrmpro.com/Users
SQLAccessGroup {4d8acc87-3413-...	onecrmpro.com
WSS_ADMIN_WPG	onecrmpro.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Section 13. APPENDIX B - COMMON PERMISSION REQUIREMENTS FOR HARDENED ENVIRONMENTS

Note: The following section is for systems that have been hardened for security purposes. The permissions below are applied during the CRM 2013 install if the application has the access to do so. If your servers have been hardened using group policies or local policies and prevent permitting these permissions, you must ensure the appropriate minimum permissions are permitted to CRM for installation and execution by applying these permissions manually. Below is a short list of the areas that are more commonly locked down. For a complete list, please see Appendix B for a full list of minimum permissions necessary for CRM 2013.

i. Log on as a service
    - Using either Local Policy editor on the CRM server or through Group Policy apply the following permissions:
        a. Traverse to **Computer Configuration>Windows Settings>Security>Local Policies>User Right Assignments**
        b. Open the properties dialogue box for **Log on as a service**
        c. Add the following service accounts to this policy and click **OK**:
            i. Async Service account
            ii. CRM Monitoring Service account
            iii. CRM VSS Writer Service account
            iv. Deployment Web Service account
            v. Sandbox Processing Service account

ii. Add service accounts to the CRM_WPG group
    1. On the CRM server, open **Server Manager**
    2. Expand **Configuration>Local Users and Groups>Groups**
    3. Open the Properties dialogue box for the **CRM_WPG** group
    4. Add the following service accounts to the CRM_WPG group and click **OK**:
        a. Deployment Web Service account
        b. CRM Application Pool service account

Section 14. APPENDIX C - SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)

14.1.1 What is the terminology STIGs?

The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

Please contact DISA STIG Customer Support Desk:

disa.stig_spt@mail.mil

Go to the following link to download the STIG viewer:

http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

14.1.2 These are STIGs you must apply for a MS Dynamics CRM on premise implementation:

http://iase.disa.mil/stigs/Pages/a-z.aspx?&&p_Title=Microsoft%20Windows%20Vista%20STIG%20Benchmark%20-%20Ver%206%2c%20Rel%2044&&PageFirstRow=1&&View={25A09AF8-178B-447B-B42B-8839EBD71CAD}

(Note: You may have to include Windows, Exchange, and Mobile Device STIG's)

- Web Server Security Requirements Guide (SRG) - Version 2, Release 2

Microsoft SQL Server 2008 FAQ			Web link
Microsoft SQL Server 2012 STIG - Ver 1, Rel 13	1/27/2017	635 KB	ZIP
Microsoft SQL Server 2014 Database STIG - Ver 1, Rel 3	1/27/2017	359 KB	ZIP

Microsoft SQL Server 2014 Instance STIG - Ver 1, Rel 4	1/27/2017	387K B	ZIP
Microsoft SQL Server 2014 Overview - Ver 1, Rel 1	5/27/2016	90 KB	ZIP
Microsoft SQL Server 2016 FAQ			

Section 15. DATA ENCRYPTION

Applies To: Dynamics 365 (online), Dynamics 365 (on-premises), Dynamics CRM 2016, Dynamics CRM Online

Microsoft Dynamics 365 uses standard Microsoft SQL Server cell level encryption for a set of default entity attributes that contain sensitive information, such as user names and email passwords. This feature can help organizations meet FIPS 140-2 compliance.

For Microsoft Dynamics 365 (online) and Dynamics 365 (on-premises), all new and upgraded organizations use data encryption by default. Data encryption can't be turned off.

Microsoft Dynamics 365 users who have the system administrator security role can change the encryption key at any time. More information: Change an organization encryption key

◆**Important**

For on-premises versions of Microsoft Dynamics 365:

- Changing the encryption key requires TLS/SSL configured on the Microsoft Dynamics 365 website.
- It is a best practice is to change the encryption key once every year.
- The encryption key is required to activate data encryption when you import an organization database into a new deployment or a deployment that has had the configuration database (MSCRM_CONFIG) re-created after the organization was encrypted. You can copy the original encryption key to Notepad and paste it into the **Settings** > **Data Management** > **Data Encryption** dialog box after the organization import is completed.
- When you re-enter the data encryption key, we recommend that you run the Microsoft Dynamics 365 web application using Internet Explorer to paste the encryption key into the **Data Encryption** dialog box.

15.1 Change an organization encryption key

1. Go to **Settings** > **Data Management**.
2. Click **Data Encryption**.
3. In the **Change Encryption Key** box type the new encryption key and then select **Change**.
4. Select **OK** in the confirmation message and then click **Close** to exit the Data Encryption page.
5. We recommend that you copy the key to a safe place. Copy your organization data encryption key

15.2 Copy your organization data encryption key

We strongly recommend that you make a copy of your data encryption key. This is particularly important for on-premises deployments that may need to reactivate data encryption after a redeployment or failure recovery.

1. Sign in to Microsoft Dynamics 365 as a user with the system administrator security role.
2. Go to **Settings** > **Data Management**.
3. Click **Data Encryption**.
4. In the **Data Encryption** dialog box, select **Show Encryption Key**, in the **Current encryption key box** select the encryption key, and copy it to the clipboard.

   ⚠**Caution**

   When the Dynamics 365 (on-premises) website is not configured for HTTPS, the **Data Encryption** dialog box will not be displayed. For a more secure deployment, we recommend that you configure the website for HTTPS. However, if the website is not configured for HTTPS, use a tool that can be used to modify Dynamics 365 database tables, such as Microsoft SQL Server Management Studio or the Deployment Web Service, open the configuration database (MSCRM_CONFIG), and in the DeploymentProperties table, set DisableSSLCheckForEncryption to *1*.

5. Paste the encryption key in to a text editor, such as Notepad.

   ⚠**Warning**

   By default, Microsoft Dynamics 365 generates a passphrase that is a random collection of Unicode characters. Therefore, you must save the system-generated passphrase by using an application and file that supports Unicode characters. Some text editors, such as Notepad use ANSI coding by default. Before you save the passphrase using Notepad, select **Save As**, and then in the **Encoding** list, select **Unicode**.

6. As a best practice, save the text file that contains the encryption key on a computer in a secure location on an encrypted hard drive.