

Security

Microsoft Dynamics CRM 4.0

Microsoft Dynamics CRM Online: Security Features

White Paper

Date: June 2010



Acknowledgements

Initiated by the Microsoft Dynamics CRM *Engineering for Enterprise* (MS CRM E²) Team, this document was developed with support from across the organization and in direct collaboration with the following:

Key Contributors

Michael Ott (*Microsoft*)
Stephanie Dart (*Microsoft*)

Technical Reviewers

Don Flaherty (*Microsoft*)
Bryan Cooke (*Microsoft*)
Andy Bergen (*Microsoft*)

The MS CRM E² Team recognizes their efforts in helping to ensure delivery of an accurate and comprehensive technical resource in support of the broader CRM community.

MS CRM E² Contributors

Amir Jafri, Program Manager

Jim Toland, Content Project Manager

Feedback

Please send comments or suggestions about this document to the MS CRM E² Team feedback alias (entfeed@microsoft.com).

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

Legal Notice

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Microsoft Dynamics, Microsoft Dynamics Logo, Active Directory, Internet Explorer, MSDN, Microsoft Office Outlook, Windows Live, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Table of Contents

- Introduction..... 4
- Inherent Risks to an Online Service and its Environment 4
- Security for Users and Administrators..... 5
 - Managing Identity and Trust 5
 - Applications Maintenance..... 5
 - Security for Data Exchange..... 5
 - Security for Client Applications 6
 - Developer Tools and Services..... 6
 - Role- and Object-based Security in Microsoft Dynamics CRM Online..... 7
 - Privacy 7
- Security for the Service Software..... 8
 - Security for Hosted Products 8
 - A Hardened Hosting Platform 8
 - Maintaining Accountability 8
- Security for the Hosting Environment 9
 - Back-end Infrastructure and Network Features 9
 - Physical Security 9
 - Maintaining the Service 10
 - Availability Processes 10
 - Back-up Process..... 10
 - Service Restoration Process 10
- Conclusion..... 11
- Appendix A: Additional Resources 12
 - Microsoft Dynamics CRM Online..... 12
 - Security and Operations 12
 - Privacy 12

Introduction

Businesses often express concerns about security when they consider the cloud services model for key communications and collaboration applications. Security when accessing, storing, and retrieving an organization's data is of paramount importance, as is the privacy of that data within the online service environment.

Microsoft takes a holistic approach to providing a highly secure environment for Microsoft Dynamics CRM Online. After an overview of the inherent risks to three key areas of the service, the remaining sections of this paper describe how Trustworthy Computing, Microsoft's core commitment to build software and services that better help protect customers and the industry, is reflected in the design and operation of Microsoft Dynamics CRM Online.

Inherent Risks to an Online Service and its Environment

When considering the inherent risks of operating an online service and maintaining the environment in which it runs, it is often helpful to segregate them according to the affected area of the service:

- Users and administrators
- The software that drives the service
- The hardware and software that make up the service hosting environment itself

Users and administrators. The most publicized threats to users and administrators of the service involve the transmission of data between the business premises and the online server. These "man in the middle" attacks enable eavesdropping, data substitution, and data replay scenarios. Users must have confidence that their sessions are secure, without a requirement for complex or intrusive security efforts on their part.

The software driving the service. Applications may also be subject to risk, especially if they haven't been specifically designed or configured for use in a Microsoft Dynamics CRM Online environment. Applications and services must be designed and engineered with security as a fundamental operating principal.

The hardware and software hosting environment. The service platform must reduce security risk by having security designed into network components, redundancy and failover systems, directory and Web hosting services, and data storage operations. Another key concern in the hosting environment is the physical security of the vendor's facilities, and the quality, reliability, and training of its administrative / operations staff.

Security for Users and Administrators

While it is important to provide end users and service administrators with features to help secure their interactions with Microsoft Dynamics CRM Online, it is also imperative to remember that the less user intervention that is required, the more likely it is that you can maintain the overall security of the organization.

Managing Identity and Trust

The Windows Live ID service is designed to manage identity and trust within the Windows Live ecosystem. Windows Live ID provides a single-sign on experience that allows businesses and customers to use a single set of credentials (logon name and password) for accessing various Web sites or Web applications. With Windows Live ID authentication, CRM Online users that navigate to <http://crm.dynamics.com> and choose to log on are prompted to provide their Windows Live ID credentials.

Important: It is a best practice to create a Windows Live ID identity solely for the purpose of accessing the Microsoft Dynamics CRM service. Using a Windows Live ID identity that is shared among a variety of services creates additional potential attack vectors that can compromise the identity.

Note: For more information about Windows Live ID Authentication, on MSDN[®], see the article *Introduction to Windows Live ID* at: <http://msdn.microsoft.com/en-us/library/bb288408.aspx>

Applications Maintenance

Periodic security checks on the client side are important, and for this process to be effective, all associated tools and applications must be up-to-date. The Microsoft Office Outlook Client for CRM Online has an auto-update mechanism that is designed to allow non-administrative users to apply updates.

Security for Data Exchange

Data exchanged with Microsoft Dynamics CRM Online uses the Microsoft implementation of the industry-standard Secure Sockets Layer (SSL) protocol. SSL helps secure data at several levels, providing server authentication, data encryption, and data integrity. Because SSL is implemented beneath the application layer, it is a passive security mechanism that does not rely on additional steps or procedures from the user. This allows client applications and their users to have little or no knowledge of secure communications and still be better protected from attackers. These features help secure data from incidental corruption and from malicious attack, and are intended to avoid common Web-based threats.

Client computers use familiar tried and tested applications such as Microsoft Outlook and Microsoft Internet Explorer to administer and use Microsoft Dynamics CRM Online. Security for these applications is supported with 40-bit to 256-bit negotiated SSL connections. Microsoft uses GTE Cyber Trust's Managed public key infrastructure (PKI) service for SSL keys managed by the Microsoft Dynamics CRM Online operations team.

Microsoft actively monitors its global network and uses custom traffic analysis tools to measure both normal and abnormal network traffic trends for early signs of potentially malicious activity.

Security for Client Applications

Secure practices for any Web service begin with the client applications that are used to access the service. Microsoft Dynamics CRM Online provides new methods and features that help to manage application and document security. The following security-related features in Microsoft Dynamics CRM Online help to establish a more secure client-side environment.

Microsoft Office Outlook. The Microsoft Dynamics CRM Outlook client ensures data protection by using security mechanisms that are built into the Microsoft stack. Specific security mechanisms include the following:

- The Server - Auth cookies are encrypted\decrypted by the server
- The channel – Secure Sockets Layer (SSL)
- Operating System - BitLocker, if enabled

E-mail Connector. The Microsoft Dynamics CRM E-mail Router is used for automatic e-mail processing that can connect to Exchange mailboxes and mailboxes that support POP3. The CRM E-mail Router retrieves and evaluates e-mail messages for relevance to CRM and accordingly creates corresponding e-mail activities in CRM. It uses WebDav or Exchange Web Services for processing incoming e-mail messages while connecting to Exchange mailboxes.

The CRM E-mail Router also supports POP3 for processing incoming e-mails from POP3 enabled servers. Outgoing e-mails are processed using SMTP protocol. The E-mail Router supports secure protocol if the same is supported by the mailbox server. The same can be done by enabling SSL in the e-mail router configuration for a POP3 or a SMTP enabled mailbox or by specifying a secure URL for an Exchange mailbox.

Note: Support for Exchange Web Services has been enabled in both Dynamics CRM 4.0 and Dynamics CRM Online for Exchange 2010 and Exchange Online.

Developer Tools and Services

Microsoft is committed to delivering secure software and to delivering tools and practices that enable our customers to build secure solutions on top of our software. This commitment extends from a combination of Microsoft's own internal policies and procedures in the developer community at large.

Developers build applications by using the common language runtime and the .NET Framework, which facilitate the use of cryptography and role-based security. They also provide classes and services that enable:

- Developers to easily write more secure code
- System administrators to customize that code's access to protected resources.

Role- and Object-based Security in Microsoft Dynamics CRM Online

In Microsoft Dynamics CRM Online, security is implemented at two levels.

Role-based security focuses on establishing security roles, each of which groups together a set of privileges that represent the responsibilities (or tasks that can be performed) by a user. For example, a user that has been assigned the System Administrator role can perform a wider set of tasks (and has a greater number of privileges) associated with viewing and modifying data and resources than can a user who has been assigned to the Salesperson role. A user assigned the System Administrator role can, for instance, assign an account to anyone in the system, while a user assigned the Salesperson role cannot.

Microsoft Dynamics CRM includes a set of predefined security roles, and when users are created in the system, they are assigned one or more security roles.

Object-based security in Microsoft Dynamics CRM focuses on access rights to entities such as accounts and leads. Access rights to an entity are often associated with the owner of that entity. If the owner of a contract does not have permission to delete contracts, the owner cannot delete that contract. In some cases, the permissions associated with an object are determined by the user who created it.

You combine role-based security and object-based security to define the overall security rights that users have within your Microsoft Dynamics CRM Online organization.

Privacy

Microsoft regards customer data as private and will take reasonable and customary measures to help protect the confidentiality of customer data.

The SSL protocol helps protect messages against tampering or unauthorized access while in transit. Also, when customer data is stored, access controls are applied to all stored data to help prevent unauthorized access.

In addition, hosted services benefit from privacy policies and procedures that are built into software development and deployment processes at Microsoft. Security Development Lifecycle (SDL) standards provide a set of guidelines for the development and deployment of Microsoft consumer software, enterprise software, and Web services.

Note: For more information about privacy efforts, on the Microsoft Trustworthy Computing site, see the topic *Privacy Resources* at:

<http://www.microsoft.com/mscorp/twc/privacy/resources.mspx>

Security for the Service Software

A major challenge for all software vendors and systems integrators is to create a more secure deployment that offers administrators and users more efficient security management and fewer updates.

Security for Hosted Products

Product security, meaning the inherent security of applications at the foundation of the service, is sometimes overlooked. The Microsoft Trustworthy Computing Security Development Lifecycle (SDL) is a process that Microsoft has adopted for developing software capable of withstanding malicious attack. SDL adds a series of security-focused activities and deliverables to each of the phases of the Microsoft software development process. Consistent application of these practices ensures that the software driving CRM Online is more secure, more easily deployed in a secure manner, and requires fewer updates. SDL activities/deliverables include:

- Developing threat models during software design.
- Using static analysis code-scanning tools during implementation.
- Conducting code reviews and security testing during a focused pre-launch security push.

Before software subject to the SDL can be released, it must undergo a Final Security Review by a team independent from its development group.

Note: For an overview of SDL, on MSDN, see the topic *The Trustworthy Computing Security Development Lifecycle* at:

<http://msdn.microsoft.com/en-us/library/ms995349.aspx>

A Hardened Hosting Platform

The servers that comprise the hosting platform provide specialized services such as DNS, firewall, database, directory services, Microsoft Dynamics CRM Online services, and e-mail roles. Overall platform hardening includes removing or disabling unnecessary services on each computer, and also segmenting the network to ensure that each service is exposed only to the network traffic necessary for its function. Ongoing, comprehensive platform hardening entails:

- Determining which services must be active, which services need to run when required, and which services can be disabled.
- Limiting Internet Information Services (IIS) Web extensions on Web servers.
- Reducing protocol exposure to the server message block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Lightweight Directory Access Protocol (LDAP).
- Creating useful and efficient audit policies that capture the events of interest.
- Keeping the servers up-to-date with the latest security patches

Maintaining Accountability

Microsoft Dynamics CRM Online helps administrators to monitor and maintain security measures by using:

- *Third-party security audits*, helping to ensure effective and up-to-date security measures
- *Regular penetration testing*, providing administrators with a greater level of feedback
- *Proactive deployments of countermeasures for potential threats*, which act as a key part of CRM Online operations best-practices.

Security for the Hosting Environment

The hosting environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialized hardware, along with the administrative and operations staff required to run and maintain the environment. The environment also includes the physical operations centers that house the solution and which themselves must be secured against malicious and accidental damage.

Overlaying the solid foundation of the Windows Server 2003 or Windows Server 2008 operating systems, the architecture of Microsoft Dynamics CRM Online leverages the centralized security, management, and operations features in Microsoft Windows Server, both for the back-end services platform and for the networking features that help secure client communications.

Back-end Infrastructure and Network Features

Centralized security policy management is a mature technology that has been a longstanding feature of Microsoft hosting solutions, such as the Microsoft Solution for Windows-based Hosting. This is but one example of how the CRM Online platform benefits from the years of experience gained by Microsoft and its partners in designing, building, and deploying Web-based platforms for hosting services such as e-mail, messaging, Web-based meeting and collaboration services, SQL databases, and Web sites.

At the interface with the public network, Microsoft uses special-purpose security devices for firewall, NAT, and IP filtering functions. Functions at this layer include Denial of Service (DOS) blocking, Intrusion Detection Systems (IDS), SSL, and initial access/certificate validation. The edge of the service network houses those servers and services that provide first level authentication and load balancing.

The back-end network is made up of partitioned LANs for Web and applications servers, data storage, and centralized administration. These servers are grouped into private address segments behind the load balancers. Data centers themselves are interconnected by VPN, and all administrative access is secured by multiple-factor authentication.

Operations are monitored with the use of event correlation, which help administrators to proactively manage the large amount of information generated by the network, providing pertinent and timely monitoring for all servers in the data center.

Physical Security

Physical security goes hand-in-hand with virtual or software-based security measures, and similar risk assessment and mitigation procedures apply to each. Microsoft Dynamics CRM Online is delivered through a data center designed to run 24 hours a day, 7 days a week. The data center uses various measures to help protect operations from power failure, physical intrusion, and network outages, and it complies with industry standards for physical security and reliability and is managed, monitored, and administered by Microsoft operations staff.

Microsoft uses highly secured access mechanisms limited to a very small number of operations personnel who must regularly change their administrator access passwords. Data center access, and authority to open data center access tickets, is controlled by the network operations director in conjunction with data center security practices.

In addition, third-party security assessments are performed to validate Microsoft security processes and to ensure that all security policies and practices are current.

Maintaining the Service

To maintain a high-level of availability for Microsoft Dynamics CRM Online, Microsoft has put the applicable environment, process, applications, and people in place, including:

- A state-of-the-art datacenter
- Many aspects of the Microsoft Dynamics CRM Online system are configured in an N+M redundant configuration, where N is the number of components of a given type needed for the service to operate, and +M is the redundancy
- The latest power systems—including on-site diesel generators for backup power and backups for the cooling systems and water supplies
- Carrier-class bandwidth dedicated to Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online offers an industry-leading service-level agreement that provides a 99.9 percent uptime service level agreement to all customers. This SLA gives businesses a high level of trust and confidence in Microsoft that its operations will have access to mission-critical systems, or it will receive a service credit.

Note: The full text of the Microsoft Dynamics CRM Online Service Level Agreement (“SLA”) can be found at <https://signin.crm.dynamics.com/portal/sla.htm>

Availability Processes

The Microsoft Dynamics CRM Online Operation Team maintains a Systems Operations Manual which thoroughly documents the technical aspects of numerous processes related to the availability of the Microsoft Dynamics CRM Online service. The detailed steps of these processes will not be made available to the public; however they do include the following in the case of a failure in the datacenter:

- Recovery and restore of operating systems to previous state
- Recovery and restore of SQL database binaries to previous state
- Recovery and restore of SQL data files containing customer data
- Rebuild applications and web servers

Back-up Process

The Microsoft Dynamics CRM Online Operation Team maintains a Systems Operations Manual which thoroughly documents the technical aspects of our backup process. This process is not available for public knowledge; however this process does include the following:

- Daily backup of customer data
- Backup of data to tape
- Offsite data storage with a 3rd party that meets Microsoft security requirements

Service Restoration Process

Microsoft Dynamics CRM Online has invested significant capital in designing and implementing the system to include redundancy with the goal of minimizing the impact of any failure that might occur. An equal amount of effort has been placed on operational best practices to help promote continuous service availability. In addition to built-in redundancy, potential failure vectors have been defined and operational recovery processes for them are tested with each release.

Conclusion

The benefits of cloud services are often weighed against perceived costs in terms of security risks and the potential for interrupted access to mission-critical business data.

Microsoft brings world-class experience in software design, development, deployment, and operations to its Microsoft Dynamics CRM Online offering, enabling businesses to gain considerable cost advantages while helping to avoid many of the security risks that are associated with Web-based software services.

Increased security in the CRM Online solution is derived from:

- Simplified access using single sign-on.
- Reduced user intervention for security-related tasks.
- Automated software and service updates.
- Comprehensive implementation of leading-edge, industry-standard network security and encryption protocols.
- Mature applications designed, built, tested, and deployed according to Microsoft-established software development disciplines.
- Field-proven service hosting platforms.
- Best practices for data center design and operations.

CRM Online is designed to provide a cloud services environment that features enhanced security and continuous access to applications and data. Increased security at each stage of the cloud services transaction – user and administrator access, network connectivity, service hosting platform and physical datacenter -- helps you gain the established benefits of cloud services while minimizing your risk.

Appendix A: Additional Resources

For additional information related to security features in Microsoft Dynamics CRM Online, see the following resources.

Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online Product Fact Sheet

http://crm.dynamics.com/docs/Microsoft_Dynamics_CRM_Online_Datasheet_HiRes.pdf

Microsoft Dynamics CRM Online Service Agreement

<https://signin.crm.dynamics.com/portal/tos.htm>

Microsoft Dynamics CRM Online "Uptime" Service Level Agreement

<https://signin.crm.dynamics.com/portal/sla.htm>

Microsoft Dynamics CRM Online Resource Center

http://rc.crm.dynamics.com/rc/regcont/en_us/onlinedefault.aspx

Security and Operations

Microsoft® System Center Operations Manager 2007

<http://download.microsoft.com/download/5/E/F/5EF5C723-A451-471A-B06D-7249B99DC52A/Whitepaper%20-%20Systems%20Center%20Operations%20Manager%202007%20Overview.doc>

System Center Operations Manager 2007 R2 SDK

<http://msdn.microsoft.com/en-us/library/cc268402.aspx>

Security and Authentication in Microsoft Dynamics CRM: The Dynamics CRM Security Model

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=fb4bb16b-586f-4aae-aa4b-790023e95b61>

Microsoft Trustworthy Computing Security Development Lifecycle

<http://msdn2.microsoft.com/en-us/library/ms995349.aspx>

Microsoft Security Central

<http://www.microsoft.com/security/default.msp>

Privacy

Microsoft Dynamics CRM Online Service Policy

<https://signin.crm.dynamics.com/portal/tos.htm>

The Microsoft Trustworthy Computing Privacy Overview

<http://www.microsoft.com/mscorp/twc/privacy/default.msp>