Security

Microsoft Dynamics CRM Online: Security Features

White Paper

Date: September 2011

Microsoft Dynamics

Acknowledgements

Initiated by the Microsoft Dynamics CRM *Engineering for Enterprise* (MS CRM E^2) Team, this document was developed with support from across the organization and in direct collaboration with the following:

Key Contributor*
Carlo Gallazzi (*Microsoft*)

Technical Reviewer
Stephanie Dart (*Microsoft*)
Shamiq Islam (*Microsoft*)

*This paper leverages and updates content published in the white paper *Microsoft Dynamics CRM Online: Security Features*, which was released in conjunction with Dynamics CRM 4.0.

The MS CRM E^2 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 E^2 Contributors
Ahmed Bisht, Program Manager
Jim Toland, Content Project Manager

Feedback

To send comments or suggestions about this document, please click the following link and type your feedback in the message body:
http://go.microsoft.com/fwlink/?LinkId=225974.

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.

Table of Contents

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 the Microsoft Dynamics CRM Online service and within the application itself, which helps to guarantee that only users with the appropriate rights can access sensitive data and personally identifiable information (PII) within the implementation.

Microsoft Dynamics CRM Online has an end-to-end approach to security that begins with the development of the application through to the service's operations and management. Microsoft Dynamics CRM Online follows the Microsoft Security Development Lifecycle (SDL). This is the process by which we take services from the design through the build and implementation and release phases of its lifecycle, and consider security from all aspects.

Safeguards are applied on multiple fronts, including:

- Secure web application communication using SSL
- Customizable security roles governing user access and the actions they can perform
- Field-level security
- Full business data auditing
- Stringent physical security of Microsoft datacenters, including building and system/database access

Additionally, the application itself uses the standard security features of the Microsoft infrastructure on which Microsoft Dynamics CRM runs (for example: Windows Server, Microsoft SQL Server, and Microsoft Exchange Server).

After an overview of the inherent risks to four 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 the risks according to the areas of the service that are affected:

- Users and administrators
- Support
- 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.

Support. In the unfortunate event that an administrator needs to raise a call to Microsoft Support, Microsoft has spent a great deal of time and attention on limiting the customer data that a Microsoft technician can access to ensure as high a level of confidentiality as possible while providing the best support experience.

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. Microsoft Dynamics CRM Online has been developed with these concerns as a top priority.

The hardware and software hosting environment. The service platform must reduce security risks 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 and 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

Microsoft Dynamics CRM Online uses the Windows Live ID service to manage identity and trust within the Windows Live ecosystem, including Microsoft Dynamics CRM Online. Windows Live ID provides a single sign-in experience that allows businesses and customers to use a single set of credentials (logon name and password) for accessing various websites or web applications. Upon signing in, a user may elect to have his or her credentials preserved by Windows Live to facilitate direct access to the system without having to sign in again.

Important: A best practice is to create a Windows Live ID identity that is used solely for accessing the Microsoft Dynamics CRM service. Using a Windows Live ID identity that is shared among a variety of services creates potential attack opportunities.

Adding a new user is as simple as entering the user's name, email address, and role into the new user administration and inviting them to the system. Users can be removed from the system by disabling the user in Microsoft Dynamics CRM Online.

Microsoft Dynamics CRM Online is planning to offer support for different authentication providers in 2012 thereby allowing:

- Users to be authenticated against services managed by the customer.
- Password policies to be specified and enforced by the customer.

Note: For more information about Windows Live ID authentication, on MSDN, see the article *Windows Live Interactive SDK* at:
http://isdk.dev.live.com/

Data accessibility for Microsoft Dynamics CRM Online users

Microsoft Dynamics CRM Online includes key features that work together to ensure the security of the data, including:

- Role-, object-, and team-based security
- Field Level Security
- Auditing

Role-, Object-, and Team-based Security

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

- **Role-based security** focuses on establishing security roles, each of which groups together a set of privileges that represent the responsibilities of (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 must be 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.
- **Team-based security**. By using teams, Microsoft Dynamics CRM allows users to easily access records from more than one specific business unit without requiring organizational level permissions or continuous sharing for every record.

  Teams can be assigned a security role and can own Microsoft Dynamics CRM records. Microsoft Dynamics CRM does not require a specific user to be the record owner. This reduces the amount of record ownership housekeeping required from administrators when users change business units, teams or leave the company.

By combining role-based security, and object- and team-based security, you can define the overall security rights for users within your Microsoft Dynamics CRM Online organization.

Field Level Security

Field Level Security (FLS) allows administrators to set permissions on each field to allow a user to perform Update, Create, and/or Read actions on a specific field. To enable this, the Administrator needs to create one or more Field Security Profiles that define the permissions for different fields. After creating the Field Security Profiles, they are assigned to a user and/or team to provide the user with certain permissions to the fields that are marked as secured. This feature is only available on custom fields in Microsoft Dynamics CRM Online.

Field Security Profiles are independent of any security roles that a user may have. Field Security Profiles are defined and assigned to give certain users or teams access to secured fields. The process of adding a user or team to a Field Security Profile is similar to the process for adding a role to a user or team. By default, there is one Field Security Profile created called *System Administrator*, which grants system administrators full access to all secured fields. The system administrator will have the *System Administrator* profile automatically added. This profile cannot be edited as it is maintained by the system. If a new custom field is marked as secured, it will be automatically added to the System Administrator Profile.

Field Level Security is also available in Microsoft Dynamics CRM for Microsoft Office Outlook and in the web application.

Auditing

Organizations use auditing to track changes that are made to database records for a variety of purposes. These changes include maintaining security, examining the history of a particular record, documenting modifications for future analysis, and record keeping necessary for regulatory compliance. Further, auditing helps to limit change repudiation by a user by providing an accurate history of when something was changed, and by whom.

New auditing functionality has been introduced in Microsoft Dynamics CRM Online and can be enabled for all customizable entities. This functionality is available both for entities and for fields. Auditing tracks creation, deletion, and modification of records, but it does not track reads or changes in the metadata. Currently, auditing is not available to track users signing in or out.

Auditing is enabled at the organization level by selecting the *Start Auditing* flag. If the flag is not enabled, nothing will be audited even if specific entities or fields are enabled for auditing.

The auditing summary provides a central point of administration. Here administrators have the option to view the data that has been audited based on specific criteria. As this could be a large number of records, administrators have the option to enable or disable filters for each of the displayed columns. For example, it is possible to filter for any record that has been changed by a specific user on a specific date. Going further, administrators can narrow this search to an operation that was applied to the record, for example, delete.

Auditing cannot be used to recover records that have been accidentally deleted. The Audit Summary only shows the information that a certain user deleted the record at a certain point in time.

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 identity verification and data channel encryption. Because SSL is implemented beneath the application layer, it is a transparent security mechanism that does not rely on additional steps or procedures from the user. This allows users with little or no knowledge of secure communications to 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 communication attacks.

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 RSA 2048-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 Dynamics CRM for Outlook. Microsoft Dynamics CRM for Outlook ensures data protection by using security mechanisms that are built into the Microsoft stack. Specific security mechanisms include the following:

- The Server – Securely encrypts authentication cookies before transmission
- The channel – Secure Sockets Layer (SSL)
- Operating System - BitLocker, if enabled

Windows Update. Microsoft Dynamics CRM for Outlook is now part of the Windows Update platform as a single source for receiving Microsoft Dynamics CRM updates for managed and unmanaged systems. It performs non-administrative update install for important and recommended updates. If only one online organization is updated, the corresponding Microsoft Dynamics CRM for Outlook clients will need to be updated. too. In this case, updates will be marked as "Required" in Microsoft Update for these corresponding clients. In order to enforce these updates, Microsoft Dynamics CRM will use a blocking mechanism to block clients from communicating with the server, while providing a message to the clients similar to this "Your CRM Outlook Client version is too low, please visit http://URL..... to update" thus maintaining the Microsoft Dynamics CRM Online security standard.

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

The E-mail Router also supports POP3 for processing incoming emails from POP3 enabled servers. Outgoing emails 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 Microsoft Dynamics CRM 2011 and Microsoft Dynamics CRM Online for Exchange 2010 and Exchange Online.

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. Microsoft Office Outlook for Microsoft Dynamics CRM Online has an auto-update mechanism that is designed to allow non-administrative users to apply updates.

Developer Tools and Services

Microsoft is committed to delivering secure software and to delivering tools and practices that enable 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, as well as provide classes and services that enable:

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

Privacy

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

SSL 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 mitigate unauthorized access. Microsoft uses highly secure offsite storage for data back-up stored on tape media. Tapes are protected against any threat, from natural disasters to man-made threats.

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.

Support engineers at any level (including escalation engineers) cannot view customer data.

Note: For more information about how Microsoft protects the confidentiality of customer data, on the Malware Protection Center site, see the Privacy statement at: http://www.microsoft.com/security/portal/Shared/Privacy.aspx

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 Microsoft Dynamics CRM Online is more secure, more easily deployed in a secure manner, and requires fewer updates. SDL activities and 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 the SDL, on the Microsoft Security Development Lifecycle site, see the topic *Microsoft Security Development Lifecycle Process* at:
http://www.microsoft.com/security/sdl/discover/default.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 email roles. Overall platform hardening includes removing or disabling unnecessary services on each server, 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 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*, to ensure effective and up-to-date security measures.
- *Regular penetration testing*, for both the Microsoft Dynamics CRM Online application and internal network topography.

- *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 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 Microsoft Dynamics 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 email, messaging, web-based meeting and collaboration services, SQL databases, and websites.

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) prevention, 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 protection 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

Microsoft Dynamics CRM Online has a well-defined change control process to provide applicable patches and upgrades. This includes deployment and verification of patches in a pre-production environment, scheduled maintenance windows for production deployment, and a defined notification processes to help minimize interruption of the service. Microsoft Dynamics CRM Online notifies customers (administrators, and in some cases, users) through various methods including the website, application, and email of scheduled or unscheduled updates and changes to the service. For planned service interrupting events (such as service maintenance), customers are notified five days in advance.

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:

- State-of-the-art datacenters distributed around the world to provide for global coverage.
- 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 for 99.9 percent uptime to all customers. This SLA gives businesses a high level of trust and confidence in Microsoft that their operations will have access to mission-critical systems. Microsoft Dynamics CRM Online is one of the quickest and easiest ways for businesses to take advantage of the cloud and cloud economies, including reducing systems management and maintenance costs as well as paying only for the capacity needed.

Note: The full text of the *Microsoft Dynamics CRM Online Service Level Agreement (SLA)* can be found at:
http://go.microsoft.com/fwlink/?LinkID=196557&clcid=0x409

Availability Processes

The Microsoft Dynamics CRM Online Operation Team maintains a Systems Operations Manual that 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 that 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

Customer data is backed up daily to tape and taken offsite. Data is retained on tape for 90 days. The data exists for disaster recovery purposes; we do not offer "point-in-time recovery" as part of the service.

After the 90 day window the tape media is sanitized prior to reuse or destruction.

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 software development disciplines.
- Field-proven service hosting platforms.
- Best practices for data center design and operations.

Microsoft Dynamics 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://crmdynamics.blob.core.windows.net/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 Service Level Agreement
http://signin.crm.dynamics.com/portal/static/1033/sla.htm

Microsoft Dynamics CRM Online Solution Center
http://support.microsoft.com/gp/dynamics-crm-online#tab2

Microsoft Dynamics CRM Online Resource Center
http://rc.crm.dynamics.com/rc/2011/en-us/online/default.aspx

Security and Operations

Microsoft® System Center Operations Manager 2007
http://www.microsoft.com/download/en/details.aspx?id=2353

System Center Operations Manager 2007 R2 SDK
http://msdn.microsoft.com/en-us/library/cc268402.aspx

The Security Model of Microsoft Dynamics CRM
http://msdn.microsoft.com/en-us/library/gg309524.aspx

Microsoft Trustworthy Computing Security Development Lifecycle
http://msdn2.microsoft.com/en-us/library/ms995349.aspx

Microsoft Safety and Security Center
http://www.microsoft.com/security/default.mspx

Privacy

The Microsoft Trustworthy Computing Privacy Overview
http://www.microsoft.com/mscorp/twc/privacy/default.mspx