RuffaloCODY™

EnrollmentManager™
Make Your Class.

Enrollment Manager™

Server, Application and User Security

Enrollment Manager is built on the Microsoft Dynamics CRM 2011 platform and has been subjected to rigorous testing in all areas, including security. RuffaloCODY follows Microsoft's best practices related to encryption practices (see below) and has implemented all recommended IIS and Active Directory security protocols to protect the application.

As a Microsoft Certified Partner, RuffaloCODY is able to leverage existing Microsoft testing and technology to ensure that Enrollment Manager meets industry standards for security, performance and accessibility. Key components of this strategy include Microsoft Windows Server 2008, Microsoft SQL Server 2008 and a set of private Microsoft Dynamics CRM 2011 encryption keys.

Additional information about Microsoft security standards, testing methodology and best practices required for Partner Certification are available through the Microsoft TechNet Library (technet.microsoft.com/en-us/library/default.aspx) and the Microsoft Dynamics Developer Center (msdn.microsoft.com/en-us/dynamics/default.aspx).

Windows Server 2008 Security

RuffaloCODY utilizes Windows Server 2008, with Internet Information Services (IIS) 7.0, to provide a security-enhanced, easy-to-manage platform for developing and reliably hosting Enrollment Manager. This approach protects our web servers from malicious requests and unauthorized access with new URL authorization rules and built-in request filtering:

- *URL Authorization*: IIS 7.0 stores URL authorization rules in an application's web.config file, so that the authorization rules which protect against unauthorized access follow the content, even if/when content is moved to a different server or even a new domain. IIS 7.0 also supports ASP.NET URL authorization for all types of Web content requests in the integrated pipeline.

- *Built-in Request Filtering*: IIS 7.0's Request Filtering allows RuffaloCODY administrators to implement URL acceptance polices both globally and per URL. Filtering requests helps secure Enrollment Manager servers by ensuring that only valid requests are processed. By providing multiple filtering options, RuffaloCODY administrators can prevent malicious or incorrect URLs

from being processed. (For example, using Request Filtering, an administrator can set a rule that prevents the display of files with certain file extensions, like .ini.)

- *URL Rewriting*: RuffaloCODY administrators also use URL Rewriter for IIS 7.0, which enables dynamic modification of URLs based on rules defined by the network engineers, to protect applications on the Web server. Using rule templates, rewrite maps and other functionality integrated into IIS Manager, administrators can easily set up rules to define URL rewriting behavior based on HTTP headers and server variables.

IIS 7.0 also incorporates a modular architecture that enables RuffaloCODY administrators to customize web servers by selectively installing or removing modules. Administrators can install only the features that address the needs of Enrollment Manager clients while eliminating the server performance reductions and security risks that come with running unused server functionality. Administrators can easily minimize the attack and servicing surface, as well as shrink the process memory footprint.

To further limit security exposure, RuffaloCODY administrators utilize the "Server Core Installation" option of Windows Server 2008. Server Core omits graphical services and most libraries in favor of a stripped-down, command-line driven system. Because Server Core has a select number of roles, it can improve security and reduce the footprint of the operating system. With fewer files installed and running on the server, there are fewer attack vectors exposed to the network; therefore, there is less of an attack surface.

SQL Server 2008 Security

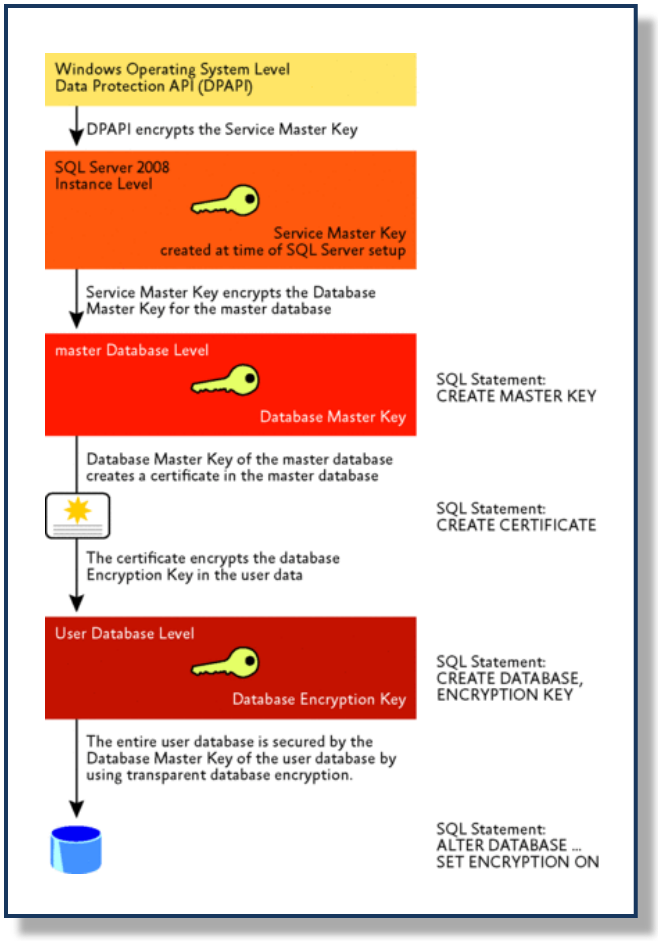
RuffaloCODY utilizes Microsoft SQL Server 2008 as the underlying database for Enrollment Manager. SQL Server 2008 delivers many enhancements and features specifically designed to improve the overall security of the Enrollment Manager environment. For example, it adds key encryption and authentication capabilities to those available through the application (see below) and provides an auditing system to help RuffaloCODY administrators report on Enrollment Manager user behavior.

The encryption keys used in SQL Server 2008 are stored on an external third-party hardware security module and encrypts data in a method that is transparent to applications like Enrollment Manager that connect to the SQL database. This means RuffaloCODY database administrators can easily encrypt all of the data stored in an entire database without having to modify existing application code.

Another SQL 2008 feature, transparent data encryption, allows RuffaloCODY to encrypt database files without having to alter each client's Enrollment Manager environment. Transparent data encryption performs real-time I/O encryption and decryption of the data and log files. As illustrated below, this encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is secured with a certificate stored in the master database of the server.

While software providers like RuffaloCODY can take several precautions to help secure a database, such as encrypting confidential assets and placing a firewall around the database servers, the physical media on which the database is stored (even backup tapes) offers a different vulnerability. Transparent data

encryption, however, allows software developers to encrypt data using Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) encryption algorithms. Encryption of the database file is performed at the page level, with pages being encrypted before they are written to disk and then later decrypted when read into memory. Backup files of databases that have transparent data encryption enabled are also encrypted by using the database encryption key.



To restore a database that is encrypted, you must have access to the certificate or asymmetric key that was used to encrypt the database. Without the certificate or asymmetric key, the database can't be restored.

Dynamics CRM 2011 Encryption

In addition to the SQL Server 2008 encryption described above, the Microsoft Dynamics CRM platform upon which the Enrollment Manager application is built uses three additional types of private encryption keys:

- *CRM-ticket key*: This key creates CRM tickets, which are generated each time an Enrollment Manager user logs on to the system. In addition, the CRM-ticket key decrypts the CRM ticket each time a request is made to the Enrollment Manager server, to validate users without forcing the user to reenter credentials.

- *Web Remote Procedure Call (WRPC)-token key*: This is used to generate a security token, which helps make sure that the request originated from the user who made the request. This security token decreases the likelihood of certain attacks, such as a cross-site request forgery (one-click) attack.

- *CRM e-mail credentials key*: This key encrypts the credentials for the E-mail Router, an optional component of Microsoft Dynamics CRM.

Authentication

Kerberos is a network authentication protocol that is used to provide a highly secure means to mutually authenticate client and server entities (or security principals) on a network. Kerberos helps users

mitigate security vulnerabilities, such as luring and man-in-the-middle attacks.

To authenticate a connection mutually using Kerberos, the Service Principal Names (SPN) of a SQL Server instance must be registered in the Active Directory®, and a client driver must provide a registered SPN when connecting. In SQL Server 2008, Kerberos authentication is applied to all network protocols, including TCP, Named Pipe, Shared Memory, and Virtual Interface Adapter (VIA). By default, the client driver automatically infers a correct SPN for a SQL Server instance to which it connects.

Security Auditing

SQL Server Audit allows RuffaloCODY administrators to create customized security audits of database engine events. This feature uses extended events to record information for audits, and it provides the tools and processes to enable, store, and view audits on various server and database objects.

Database audit specifications can also specify groups of audit action events collected into database-level audit action groups. In addition to the audit action groups, database audit specification can include individual audit action events to audit data manipulation language statements. These events can be configured to monitor the entire database or just specific database objects. The SELECT audit action, for instance, can be used to audit SELECT queries for a single table or an entire schema. These events can also be configured to monitor actions by specific users or roles.

User Security

To control data access across your set of authorized users, you can set up an organizational structure that both protects sensitive data and enables collaboration where appropriate. Within Enrollment Manager, this is set up through the creation of security roles and, if needed, business units (e.g., undergraduate admissions, graduate admissions, continuing education).

The security role assigned to a user determines which tasks the user can perform and which parts of the user interface the user can view. All users must be assigned at least one security role in order to access the system. RuffaloCODY utilizes a set of standard security roles based on a best practices model that accounts for most enrollment management business unit configurations.

A business unit basically is a group of users (e.g., the admissions office). Large institutions with multiple constituent bases or more complex enrollment management structures may require multiple business units to control data access and define security roles so that users can access records only in their own business unit. This also lets the system administrator delegate tasks such as user management for a specific business unit.

Security Roles

A security role defines how different types of records can be accessed by one category of users, such as all admission counselors. To control access to data, you can modify existing security roles, create new security roles, or change which security roles are assigned to each user. Each user can have multiple security roles.

A user's rights to perform specific actions on specific record types or to perform tasks are referred to as user security role privileges. Privileges are assigned by system administrators to security roles. Users are then assigned security roles. Examples of privileges include Update Account and Execution of Workflow Rules.

Each security role consists of record-level privileges that are specific to one record type, such as Read, Create, and Write, and task-based privileges that apply to tasks that are not specific to one record type, such as Export to Excel and Go Offline. The access level for each privilege determines which records can be accessed:

- *None*: An access level that denies the user privileges at any level.
- *User*: An access level that lets the user work with record types they own, record types that are shared with the user, and record types that are shared with the team of which the user is a member. For example, if a user is assigned the User access level on the Read privilege for Organization records, the only organizations that can be read are those that are owned by or shared to the user.
- *Business Unit*: An access level that lets the user work with record types in the user's business unit. Users who have Business Unit access automatically have User access as well.

- *Parent-Child Business Units*: An access level that lets the user work with record types in the user's business unit, and all business units subordinate to the user's business unit. Users with Parent-Child Business Units access automatically have Business Unit and User access as well.
- *Organization*: An access level that lets the user work with all record types within the entire organization, regardless of the business unit hierarchical level to which the entity or user

belongs. Users who have Organization access automatically have Parent-Child Business Units, Business Unit, and User access as well.

Each type of record is either user-owned (records that are used by individuals or sub-groups, such as organizations, activities, and person) or organization-owned (records that everyone in the organization needs to access, such as program offerings or recruitment literature items). Record-level privileges define what tasks a user with access to the record can do, such as:

- *Read*: A privilege required to read a record. Which records can be read depends on the access level of the permission defined in your security role.
- *Create*: A privilege required to create a new record. Which records can be created depends on the access level of the permission defined in your security role.
- *Delete*: A privilege required to permanently remove a record. Which records can be deleted depends on the access level of the permission defined in your security role.
- *Write*: A privilege required to make changes to a record. Which records can be changed depends on the access level of the permission defined in your security role.
- *Assign*: A privilege required to give ownership of a record to another user. Which records can be assigned depends on the access level of the permission defined in your security role.
- *Share*: A privilege required to give access to a record to another user while keeping your own access. Which records can be shared depends on the access level of the permission defined in your security role.
- *Append*: A privilege required to associate a record with the current record. For example, if a user has Append rights on an opportunity, the user can add a note to an opportunity. Which records can be appended depends on the access level of the permission defined in your security role.
- *Append To*: A privilege required to associate the current record with another record. For example, a note can be attached to an enrollment opportunity if the user has “Append To” rights on the note. Which records can be appended-to depends on the access level of the permission defined in your security role.

Overriding Security Roles

The owner of a record or a person who has the Share privilege on a record can share a record with other users or *teams*. Sharing can add Read, Write, Delete, Append, Assign, and Share privileges for specific records.

Teams are used primarily for sharing records that team members ordinarily couldn't access. For example, if your financial aid functions are in different business units but you want members of a cross-functional team to be able to view all admitted student records, by creating a team all team members can be set up to view those records.

Password Policy

Passwords are an important aspect of computer security. Where the infrastructure helps secure unauthorized access, the passwords are the primary form of protection for authorized users. A poorly chosen password may result in the compromise of data. The password policy addresses two distinct populations: RuffaloCODY Staff and Enrollment Manager Users.

The RuffaloCODY Staff

All RuffaloCODY staff members (including contractors and vendors with access to RuffaloCODY systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any RuffaloCODY facility, has access to the RuffaloCODY network, or stores any non-public RuffaloCODY information.

General Policy

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Password Protection Standards

Staff members are discouraged from using the same password for RuffaloCODY accounts as for other non-RuffaloCODY access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, staff will not use the same password for various RuffaloCODY access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Passwords are not to be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential RuffaloCODY information.

All passwords are changed at least once every six months (except system-level passwords which must be changed quarterly). If an account or password is suspected to have been compromised, it is immediately reported to the Network Administrator and automatically changed.

Enrollment Manager Users

Enrollment Manager passwords are stored in encrypted form and can only be reset by RuffaloCODY staff or the user. The following requirements have been established for password management:

- Passwords must be at least eight alphanumeric characters in length
- Passwords must contain both upper and lower case letters (e.g., a-z, A-Z)
- Passwords must include at least one digit in addition to letters
- Passwords cannot contain more than 3 consecutive characters matching an email address or display name
- Passwords should not represent standard words in any language, slang, dialect, jargon, etc.
- Passwords should not be based on personal information, names of family, nicknames, birthdays, etc.

RuffaloCODY provides guidelines and suggestions for creating strong passwords though our user support website.

Security Breach

RuffaloCODY defines a security breach as an unauthorized acquisition of data that compromises the worth, confidentiality, or integrity of personal information maintained by RuffaloCODY. Good faith acquisition of personal information by an employee or agent of our company for business purposes is *not* defined as a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

If a breach or suspected breach of personal information is identified by RuffaloCODY network operations staff, technical support staff, or an RuffaloCODY partner, the RuffaloCODY Technical Operations Manager and Vice President, Products and Services, will be notified immediately so that an incident report can be created. The report will serve to (1) capture all relevant information about the breach or suspected breach that is available, and to (2) notify members of the RuffaloCODY client services and support teams.

The Vice President, Products and Services, in conjunction with the Technical Operations Manager, will determine whether any breach or suspected breach is serious enough to warrant activation of the RuffaloCODY security breach response process. If a formal response is warranted, the following steps will be taken as part of that process:

1. The Technical Operations Manager performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident.

2. The Technical Operations Manager, in conjunction with an Enrollment Manager Infrastructure Support Specialist, identifies the systems and type(s) of information affected and determines

whether the incident could be a breach, or suspected breach of personal information about an individual.

3. The Technical Operations Manager and Enrollment Manager Database Administrator will work with the appropriate parties to determine the extent of the potential breach. The data that has been compromised on all test, development and production servers will be identified, as will the number of individuals placed at risk.

4. The Vice President, Products and Services, will notify Enrollment Manager client(s) impacted by the potential breach and review the steps being taken to investigate the situation and secure all client data.

    a. Enrollment Manager client(s) impacted by the potential breach will be asked to assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by RuffaloCODY.

5. The Technical Operations Manager, in conjunction with an Enrollment Manager Infrastructure Support Specialist, will determine where and how the breach occurred via these steps:

    a. Identify the source of the compromise, and the timeframe involved.

    b. Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.

    c. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

6. The Enrollment Manager Database Administrator will determine the type of personal information that was at risk, including but not limited to: Name, Address, Social Security Number/Social Insurance Number, and Date of Birth. Furthermore, a determination will be made regarding whether this data has been exported and/or deleted.

    a. A list of affected persons will be provided to the Enrollment Manager client(s) impacted by the security breach.

7. The Technical Operations Manager, in conjunction with an Enrollment Manager Infrastructure Support Specialist, will secure all files and/or tables that have been the subject of unauthorized access or use.

8. The Technical Operations Manager, in conjunction with an Enrollment Manager Infrastructure Support Specialist, will take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls. If it is determined that an authorized user's account was compromised and used by the intruder, the account will be disabled.

9. An Enrollment Manager Infrastructure Support Specialist will continuously monitor access to Enrollment Manager database files for a period of time specified by the Vice President, Products and Services, in order to identify any subsequent attempts to gain unauthorized access.

10. An Enrollment Manager Infrastructure Support Specialist will preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Documentation on all actions taken, by whom, and the exact time and date of those actions will be logged and made available for review as needed.

Please note that Enrollment Manager clients are owners of their data and should play an active role in the discovery and reporting of any breach or suspected breach related to their data. This includes notification received from any third party service providers or other institutional partners with whom the client shares personal information on individuals. A breach can be reported through the RuffaloCODY Support website or email address (support@admissionslab.com) 24 hours a day, seven days a week.