TORQUE SOFTWARE

FMCS TECHNICAL GUIDE

September 2015

FTG-MNL-v2.1

CONTENTS

INTRODUCTION

The Financial Management and Compliance System (FMCS) is a web based application used by Government agencies to manage financial governance and other administrative requirements.

This document provides technical information about the FMCS, including application schematics, architecture and security.

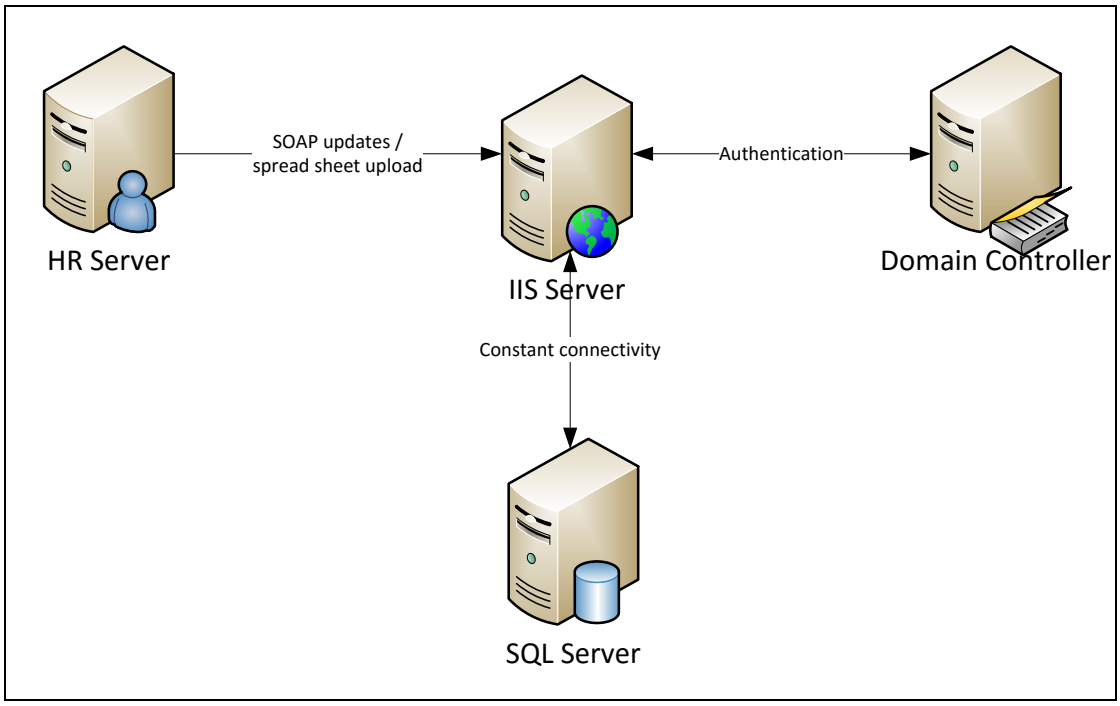
DEVELOPMENT PLATFORM

The FMCS development platform is Microsoft .NET 4.5 and Microsoft SQL Server. Third party controls have been used to develop the application (sourced from DevExpress), however these are all native .NET source code.

ARCHITECTURE

The FMCS is a two-tier application with the ASP.NET application component hosted on a Microsoft IIS8+ web server. The database is hosted on a Microsoft SQL Server 2008+ instance.

To enable single sign-on, the IIS server must be on the Active Directory domain.



Branch and user information can be updated routinely from existing HR software (or similar application) by way of a spread sheet export or development of an integration piece utilising SOAP web services built into the FMCS.

SECURITY

User Access Security

Integrated Authentication (locally-hosted instances only)

When hosted on a local domain, user identity is assured and access is provided through integrated authentication between the IIS server and Active Directory.

Username/Password Authentication

When hosted on a remote server, user identity is assured through standard login and password protocol; passwords are encrypted within the database using AES encryption.

Failed logon attempts are logged and available for viewing within the FMCS. The FMCS can be configured to lockout accounts after a set number of failed login attempts.

Single Sign-On Authentication

VANguard Federated Authentication Service

VANguard is provided by the Department of Industry and Science and is recommended for Federal Government agencies wishing to obtain authentication services for internet applications.

The VANguard Federated Authentication Service allows users logged on to their own Federal Government agency's network to authenticate and then use web applications such as the Financial Management Compliance System. Authentication occurs transparently without additional credentials or software being required on the user's computer.

Please see this page for more information about VANguard.

To check if your department is already using the VANguard service, please see this page or contact VANguard.

Torque Proprietary Single Sign-On

When hosted on a remote server and using Torque Software's SSO solution, the FMCS SSO authenticator obtains the local user's login account ("DOMAIN*Login*"), excluding the domain portion (unless this is required for multi-domain instances of the FMCS).

Note: The FMCS SSO tool does not gather or use any information from the local domain other than the user's login and, if required for multi-domain clients, domain name.

In addition, the SSO authenticator calculates an encrypted time-limited token to identify itself as a valid redirection algorithm based on a unique secure key (provided by Torque Software), the login itself and the time and date.

Database Security

The FMCS application connects to SQL Server via SQL Server Authentication (integrated authentication is available when the SQL Server is running on the same server as IIS).

The FMCS application uses the FMCS_users role to perform all database transactions. The FMCS Users role provides only SELECT, INSERT, DELETE and UPDATE permission on the FMCS tables, ensuring that the security context cannot be escalated by users of the FMCS.

FMCS uses proprietary 256-bit key Rijndael AES functionality to encrypt text fields where sensitive data may be entered. The encryption is performed via the application prior to storing in the database.

The encryption key is compiled into the application and so is contained in the source code. The source code is contained in Torque Software's private SVN (source control) repository and is restricted to authorised personnel via user id and password.

Encryption

Torque Software uses Microsoft's .NET Cryptography provider which provides standard Rijndael AES encryption for string data prior to storing in the database.

The Encryption key is generated by Torque Software and is contained in the FMCS source code and compiled into the application. The source code is contained in Torque Software's private SVN (source control) repository and is restricted to personnel authorised to work on the FMCS via user id and password. The encryption key can be recovered from the source code by authorised personnel. Encryption keys are revoked/destroyed by generating a new key and replacing the old key in the source code.

The encryption key would be considered to be compromised and require revoking if any unauthorised person gained access to the source code.

Browser Security

When hosted on Torque Software managed servers, the FMCS runs over TLS (commonly known as HTTPS), ensuring an encrypted communication channel between the client browser and the FMCS server.

FMCS uses cookies as standard to maintain authentication state (industry standard). Using cookie-based authentication over URL-based ensures that only the local machine containing the cookie is able to access the authenticated session.

To learn more about Torque Software, contact us on 1300 795 581 or visit www.torquesoftware.com.au.

TORQUE SOFTWARE