CaseLoad

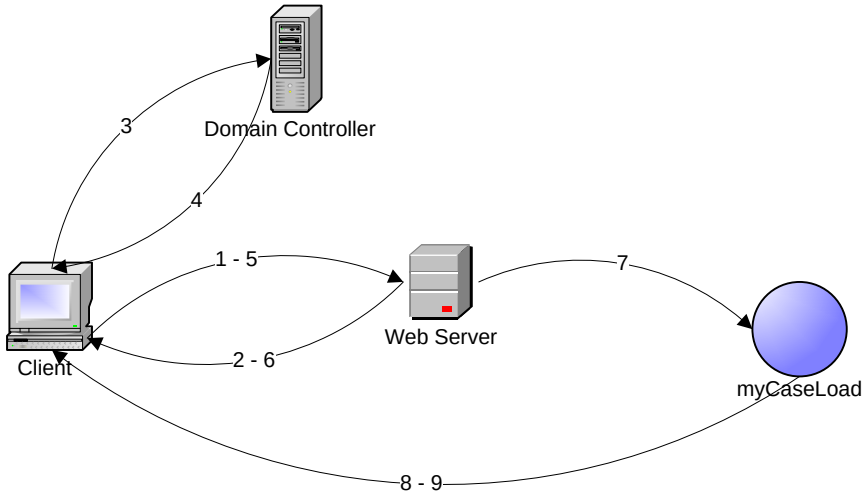
myCaseLoad Security Features

myCaseLoad includes many security features that satisfies or exceeds the industry standards. The following gives an overview of these features and highlights the main mechanisms used by myCaseLoad to ensure the privacy and security of the data and restricts the access to authorized users only.

Server Security

myCaseLoad is an ASP.NET application hosted on a Microsoft web platform architecture using Internet Information Services (IIS). The access to the application is controlled by Windows Authentication using Negotiate and/or NTLM providers.

myCaseLoad grants access to the application by comparing the login coming from a successful authentication and the content of a user code column in the user table. The following diagram presents the authentication and authorization process:



The client makes an HTTP request to the web server
The server denies the request with a 401 Authorization Required
The client requests a Service Ticket from the Key Distribution Center (KDC) hosted on the Domain Controller
The Domain Controller returns the Service Ticket to the client
The client generates the Authenticator composed of an encrypted client ID and a timestamp and sends the Service Ticket and the Authenticator in a new HTTP request to the web server
The web server determines the identity of the client, checks the ACL on the web application and permits or denies access to it
If the web server permits access to the web application, myCaseLoad maps the login information from the client to the content of the user code column in the user table
If mapping is successful, myCaseLoad verifies the application rights for the user and authorizes him/her to use the application and perform the actions for which he/she has the rights.

All communications between the client and the server or between two servers is secured using the Secure Sockets Layer (SSL) 3.2 and Transport Layer Security (TLS) 1.2.

The application is usually installed behind a firewall which opens only the required ports. It's also running with least privileges using a service account with minimum practical privileges on the server.

User inputs are validated against html or sql injection and no sensitive information is stored in places accessible by the browser.

Finally, myCaseLoad uses error handling and custom errors that display only limited information to the users and store the details in a database table for further review preventing exposure of sensitive information to the user.

Application Security

Within the myCaseLoad application, there are 5 security levels that are applied in the following order once the user has been successfully authenticated and mapped to a user login:

1. Allowed applications -> the right to use an application (myCaseLoad, Workflow Designer) is specified for each user. A user without this right can't access the application
2. User type -> Standard or Query. Query users can only see information and all the creation/modification/deletion actions are disabled for this user type
3. Application rights -> the application rights are top level actions such as perform administrative tasks, change case location or allow resource overbooking. Every user belongs to one or more security role for which the application rights can be configured. For example, an Administrator role could have the right to perform administrative tasks, but may not have the right to manually dispose a case depending on how the application rights are configured for his role
4. Entity Actions -> every standard action (new/edit/delete) is secured individually and specifies which groups of users can perform the action
5. Per page security -> every view page in the application can be configured to restrict the access to only specified groups of users for an even more fine grained level of security.

Data Security

Encryption in transit

Data transmitted between the web application and the database server can be encrypted using Secure Sockets Layer (SSL). By default, the connection string information stored in the web application configuration file is also encrypted preventing an unauthorized use of this sensitive information.

Encryption at Rest

The myCaseLoad database can be configured to use Microsoft SQL Server's Transparent Data Encryption (TDE) which performs real-time I/O encryption and

decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an Extensible Key Management (EKM) module. TDE protects data "at rest", meaning the contents of the data and log files is protected from unauthorized access. The data can’t be restored or moved to a different server without the encryption key preventing data theft. It provides the ability to comply with many laws, regulations, and guidelines established in various industries.