Ebix OneOffice

OneOffice Security Architecture

Introduction

This document outlines the Security Architecture used by the OneOffice application running under the .NET technology stack.

OneOffice Security

Authorised Access

OneOffice is designed to be secure by using industry standard authentication and authorisation methodology. OneOffice security model is built with ASP.Net Identity and OAuth.

The OneOffice login function securely authenticates a user through use of a username and password. There is a limit to invalid login attempts to prevent system hacks. If the user exceeded the limit, the account will be locked out. Of course, OneOffice system administrators can unlock these accounts.

Secure Socket Layer (SSL)

Host servers will issue security certificates with in and out traffic to the websites encrypted.

The URL of the hosted sites will start with https://.

Token System

A token will be generated once a username and password are validated by the authorisation server. This highly encrypted token will live within a time limit and any expired token will flag an unauthorised access.

All tokens generated by the authorisation server cannot be forged, and having a token protects both content and data access.

Password and Encryption

Passwords are encrypted with recovery of forgotten passwords performed via email. Each password created must adhere to password strength rules which are configurable (such as length, combination of characters and case-sensitivity).

Passwords can be expired and there is a rule preventing reuse of old passwords.

Single Signon

OneOffice Authenticate User APIs can be used to request a token for user access from an external system such as a CRM. Site policies can be applied to the authentication e.g. token timeout duration.

Access Protocols

HTTP - Ideal for public websites when no authentication required.

HTTPS - Best for websites with authentication so traffic and sensitive data is encrypted.

Third-Party Services

SendGrid (email service) - OneOffice uses this service for sending emails, as well as for password recovery. All emails are tracked for events such as; delivered, bounced or blocked. There is a security setup in place between the OneOffice API and the SendGrid API.

MasterSoft (address validation service) – The OneOffice API securely connects to the MasterSoft API for address validation. Single-line address validation provides the best user experience as valid addresses are displayed for user selection after entry of a minimal number of characters. Use of this service also minimises the entry of invalid addresses and consequently returned mail.

Underwriting Rules Engine – OneOffice can install the external system security certificate and communicate with the rules engine via API calls.

User Management

Every user of the system will be required to have a unique username and a password, with each username having defined roles. The roles grant the user access to the secured pages and menu within the application.

In addition to roles, a user is required to have permission associated to their roles. The permissions grant each user access to the actions within a page; such as read, write, edit, and delete.

Session Management

There is a time limit (measured in minutes and set via configuration) where the security token is valid. Once the security token is expired, the user will receive a notification that they need to login again.

There are two factors that will cause a security token to expire. These are:

- Time limit
- Duration of inactivity

Roles Management

OneOffice uses roles defined in the system to grant access to the menu and pages within the application. Standard OneOffice roles are:

- System Administrator
- Adviser
- Sales
- Policy Administrator
- External Users

Additional roles can be defined if required.