Front Office Security

Security controls, risks, response and remediation policy

Contents

1.0 Introduction

Front Office provides Service Catalog and Request fulfillment functionality to enterprises and managed service providers. The solution allows services to be intuitively managed, presented and requested. Approval and fulfillment workflow ensure requests are fulfilled to standard repeatable processes in the most optimal and automated way. Process measurements and notification ensure effective management of in-flight processes to meet customer expectations and commitments.

The solution can be regarded as a flexible content management system for services and their associated processes. The risk profile of Front Office therefore varies significantly dependent on the type of services and requests configured. Typical examples of service request processes include:

- Software installation/access to business application
- Hardware/accessories
- Virtual environments
- Employee on/off boarding
- Employee role change
- Backup restoration
- IT change requests

Front Office consists of a web application, database and application service components. These can be deployed for private network access only or exposed to the internet for easier off-premise access. Clearly how Front Office is deployed has a bearing on the security risk profile.

2.0 Front Office Security Controls

2.1 Security Features

User Authentication:

Front Office authenticates a user session either natively (enter user name/password), via integrated Windows (Active Directory) authentication, or via a custom single sign on (SSO) from integrated external portal. Any passwords held by Front Office are salted and hashed (SHA-256).

Password Policies:

The password policies enforced in Front Office are configurable. Options include:

- Enforce passwords of mixed numbers and characters
- Enforce passwords of a minimum length
- The number of incorrect password entry retries allowed
- Expiring passwords after a configurable time period

Access Control:

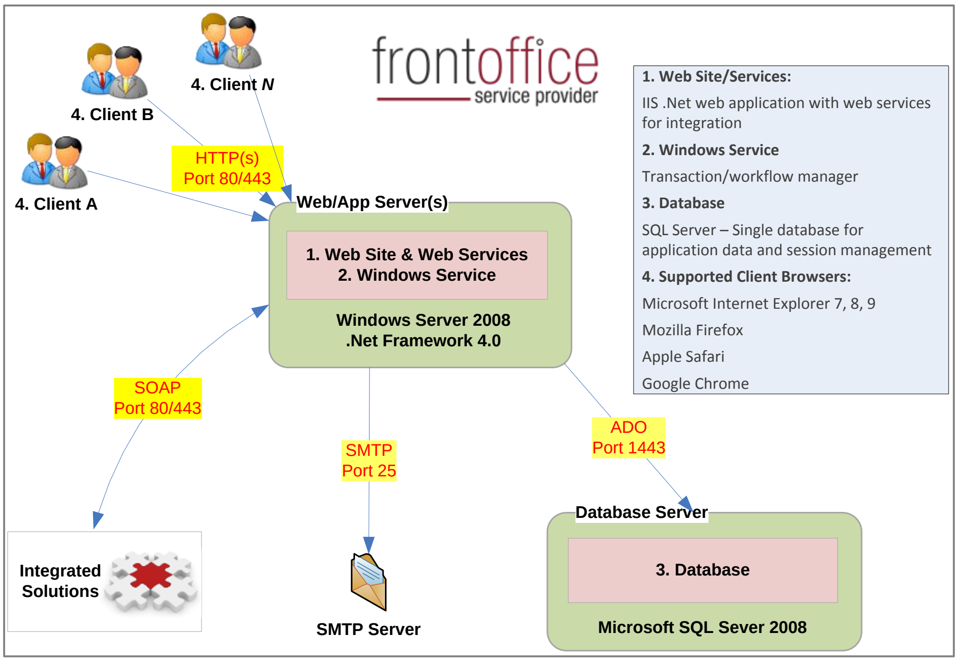
Front Office uses role based security and resource based security. The role based security controls dictate what functions are available to a user e.g. menu options, action buttons. Resource based security controls are available on key data resources allowing restricted access to specific users e.g. a Service Catalog category can be made visible/invisible to selected user groups.

Access control is checked at all levels throughout the application, preventing security bypass via direct access to application pages.

Communications:

Front Office can be configured to use HTTPS (SSL) to safeguard the transfer for information between the client and server. Additionally public / private keys can be used to further enhance communications and messaging security between Front Office and third party systems using X.509 certificates.

2.2 Multi-Client Security



1. Web Site/Services:
IIS .Net web application with web services for integration
2. Windows Service
Transaction/workflow manager
3. Database
SQL Server – Single database for application data and session management
4. Supported Client Browsers:
Microsoft Internet Explorer 7, 8, 9
Mozilla Firefox
Apple Safari
Google Chrome

Front Office Service Provider enables a single instance to be used by multiple clients, all with their own view of service offerings, request forms and associated workflow.

All client specific data is strictly visible only by authenticated users belonging to the same client organization. An extension in the resource based security controls is used to ensure all shared resources can be restricted to either one or more clients (e.g. a Service Provider can publish services to one or more clients).

Client users can only be created with restricted access profiles to ensure only certain areas of the application can be accessed. Two fixed access profiles are provided, ‘client user’ and ‘client administrator’. Both these user account types enforce a strict filter within application on all content being viewed. Client administrators have limited ability to maintain other user accounts within the same organization.

Front Office Service Provider has been tested by an independent penetration testing company to ensure no escalation or transfer of privilege across user accounts.

2.3 Quality Assurance

Product enhancements are always assessed in terms of security risk by the Chief Architect and any recommendations built into the feature design from the start. Biomni uses an Agile approach to software development with developers always working in pairs to ensure optimal design and quality. Daily scrum meetings and peer reviews of progress ensure widespread appreciation of all enhancements and increased knowledge sharing.

Automated unit tests and builds are carried out as part of continuous integration processes and a dedicated QA team carries out feature, integration, and regression testing.

Biomni Front Office is also tested by an independent penetration testing company who carry out a wide reaching set of tests which aim to detect such security flaws as cross site scripting, broken authentication and session management, escalation of privileges, insecure object references, insecure storage of sensitive information, insufficient transport layer protection, and SQL injection. Any vulnerabilities detected are assessed and remediated in accordance with our response and remediation policy detailed below.

3.0 Security Risks & Mitigation

As a web application, many of the threats faced by Front Office have been documented by the well regarded Open Web Application Security Project (OWASP). The top ten security risks and how Front Office mitigates against those risks are detailed below.

3.1 Injection

> *"Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data."*

Front Office ensures:

- User input from the web interface is processed prior to be being passed to the database or APIs.
- The data access layer (API) blocks SQL injection attacks via the use of stored procedures with native parameters.

3.2 Cross Site Scripting (XSS)

> *"XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites."*

Front Office ensures:

- User entered data is treated as untrusted and never passed to a browser without analysis and processing.
- Display data is HTML escaped by default.

3.3 Broken Authentication and Session Management

> *"Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities."*

Front Office:

- Follows the well-established and proven ASP.net authentication and session management model.
- Stores user account passwords using a salted SHA-256 hash.
- Automatically time-outs session (configurable period).
- Supports a variety of password policies including forced renewal after configurable time period, configurable complexity and length.

3.4 Insecure Direct Object References

> *"A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data."*

Front Office ensures:

- Access control checks always carried out on application object references.

3.5 Cross Site Request Forgery (CSRF)

> *"A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim."*

Front Office ensures:

- A hash-based message authentication code (HMAC) with a random seed value is used on all URI query strings generated to ensure request authentication.

3.6 Security Misconfiguration

"Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application."

Front Office:

- Employs an automated installation and configuration tool to avoid error prone manual processes whilst ensuring best practice security settings.
- Is architected with a separate data access layer.
- Has a well-established patch process which ensures the latest fixes and third party components are available for customer application.

3.7 Insecure Cryptographic Storage

"Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes."

Front Office ensures:

- All passwords are stored with a salted SHA-256 hash.
- Other data requiring secure storage is encrypted using AES.

3.8 Failure to Restrict URL Access

"Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway."

Front Office ensures:

- Authentication and authorization to access application pages.
- Role based authorization to application pages is easily maintainable.
- By default access is denied.

3.9 Insufficient Transport Layer Protection

"Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly."

Front Office supports:

- SSL deployments (optionally enabled).
- WS-Security (OASIS standard) under a PKI model when integrating to external systems.

3.10 Unvalidated Redirects and Forwards

> *"Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages."*

Front Office ensures:

- That where redirects are used, they don't involve user parameters in calculating the destination.

4.0 Response and Remediation

Biomni work hard to ensure Front Office can be trusted by our customers and understand if that if we do not meet high security standards customers will not be able to deploy our software with confidence.

4.1 How to Report a Vulnerability

To report a security vulnerability, please contact the Biomni support desk and provide your product version and customer details.

Email: support.biomni.com
Online: community.biomni.com
Phone: +44 (0) 844 412 0919

4.2 Vulnerability Response and Remediation

Biomni will assess the vulnerability and classify its severity before deciding on a course of action. The table below lists the vulnerability classifications and their remediation actions.

Classification	Description	Remediation Actions
High	The vulnerability poses a significant security threat in either the ease or consequence of exploitation.	A patch will be issued for all affected versions within 30 working days.
Medium	The vulnerability poses a moderate	The vulnerability will be addressed in the

	security threat in isolated conditions.	next version release. A patch may additionally be issued at Biomni's discretion.
Low	The vulnerability poses a remote security threat or can be resolved via product / infrastructure configuration.	The vulnerability will be addressed in the next version release.

4.3 Customer Notification

Customers will be notified of any HIGH classified vulnerability on the issuance of the resolving patch.