MITRATECH

CMO Compliance

Technical Overview

CMO Compliance 15.02 Technical Overview

Document ID: CMO_Technical_Overview, published on 1/22/2018

Disclaimer of Warranty

Mitratech Holdings, Inc. (Mitratech) makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Mitratech reserves the right to not support non-standard or non-default functionality and extended functionality available in third-party software, unless specifically documented as supported or certified in the Mitratech product documentation. For further information regarding third-party non-standard or non-default functionality, please contact Mitratech Support.

This document, along with the software that it describes, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Mitratech.

The following document is for the CMO™ release only. Though every effort was made to ensure that the information in this document is correct and reliable, Mitratech does not assume any liability for any errors encountered in this document.

If you need support for CMO, please contact the Mitratech support team by sending an email to: support@mitratech.com. For more information about Mitratech, visit our web site: http://www.mitratech.com.

CONTACT US:
Mitratech Holdings, Inc.
5001 Plaza on the Lake Suite 111, Austin, TX 78746
Phone: (512) 382-7322

NOTE: Throughout Mitratech product publications, in addition to using full product names where necessary, we also use familiar and shorter terms to increase your ease of reading. You may find the following aliases for our product names:

CMO
CMO Software
CMO Compliance
CMO Global
EasyAudit

Table of Contents

1 Technical Overview

1.1 Introduction

History has shown that every so often, incremental advances in technology and changes in business models create major paradigm shifts in the way software applications are designed, built, and delivered to end users. The invention of personal computers (PCs), computer networking and graphical user interfaces (UIs) gave rise to the adoption of client/server applications over expensive, inflexible, characterd mode mainframe applications. And today, reliable broadband Internet access, serviced-oriented architectures (SOAs), and the cost inefficiencies of managing dedicated on premise applications are driving a transition toward the delivery of decomposable, managed, shared, Web-based services called software as a service (SaaS).

This Technical Overview Guide provides an overview of the technical architecture of CMO Compliance. It details information about the software and deployment architecture (including system requirements), and how the applications interact with IT environments.

1.1.1 Software Architecture

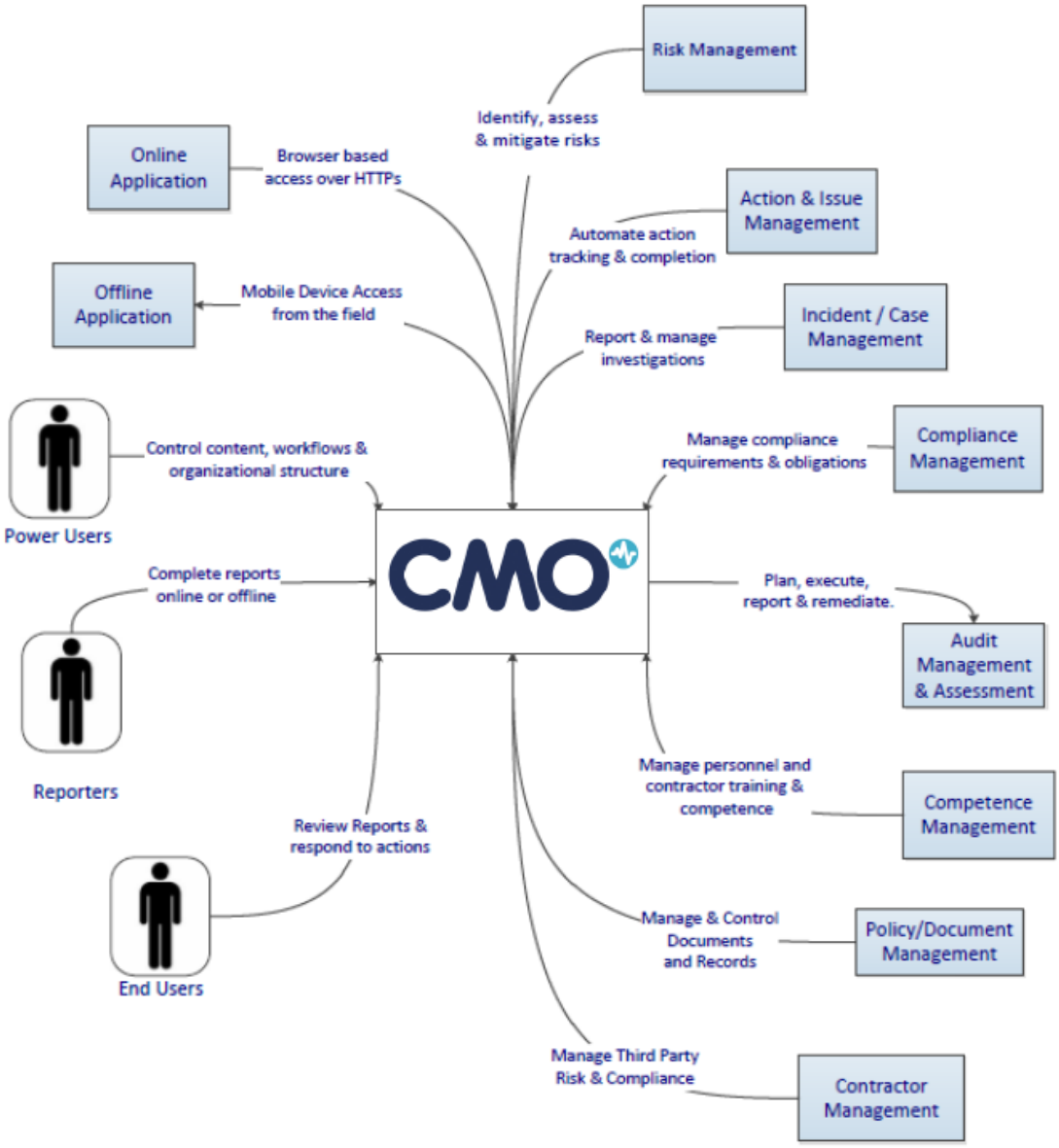
CMO Compliance is a process-driven, data management and analysis engine. Its fundamental structure is fully configurable, and so can fit any GRC and HSE data or process requirement. Users interact directly with the system using web browsers, email and mobile interfaces.

The CMO Compliance web application differs from other web applications, as it is not designed and implemented with specific processes and data objects in mind. In such applications, changes to processes and data structures often require re-implementation by software engineers or other qualified staff. However, using simple graphical interfaces, the processes and data structures within the CMO Compliance web application can be remodeled at any time by non-technical users who understand the processes being modeled rather than the technical issues.

The dynamic nature of the data structures and processes encompassed by CMO Compliance presents many challenges to the underlying software. We solve these challenges by reducing the requirements down to a simple premise: everything is an "object". What is stored depends on the type of object, and how the system behaves depends on the relationships between those objects. This abstract model is then fleshed out by the various layers and services in the software to allow the real world data model and processes to be presented.

CMO Compliance is built in an object- and service-oriented model, based on strict separation of objects to provide security, reliability and extensibility in all areas.

1.1.1.1 System Context Diagram



1.1.2 Multi Tenacy

To decrease the cost of delivering the same application to many different sets of users, an increasing number of applications are multi-tenant rather than single-tenant. With CMO Compliance's unique EHS Software as a Service Model (SaaS), a service can be offered to clients via a Cloud Edition. In addition, a Private Cloud Edition is provided allowing the application to run on a visualized cloud data center inside client's firewall, or from a private space dedicated to a client within a data centre if client's requirements dictate this. Whereas a traditional single-tenant application requires a dedicated set of resources to fulfill the needs of just one organization, a multi-tenant application can satisfy the needs of multiple tenants (companies or departments within a company, etc.) using the hardware resources and staff needed to manage just a single software instance. Tenants using a

multi tenant service operate in virtual isolation from one another: Organizations can use and customize an application as though they each have a separate instance, yet their data and customizations remain secure and insulated from the activity of all other tenants. The single application instance effectively morphs at run-time for any particular tenant at any given time. Multi tenancy is an architectural approach that pays dividends to both application providers and users. Operating just one application instance for multiple organizations yields tremendous economy of scale for the provider. Only one set of hardware resources is necessary to meet the needs of all users, a relatively small, experienced administrative staff can efficiently manage only one stack of software and hardware, and developers can build and support a single code base on just one platform (operating system, database, etc.) rather than many. The economics afforded by multi tenancy allow the application provider to, in turn, offer the service at a lower cost to customers. Some interesting side benefits of multi tenancy are improved quality, user satisfaction, and customer retention. Unlike single-tenant applications, which are isolated silos deployed outside the reach of the application provider, a multi tenant application is one large community that is typically hosted by the provider itself. This design shift lets the provider gather operational information from the collective user population (which queries respond slowly, what errors happen, etc.) and make frequent, incremental improvements to the service that benefit the entire user community at once. Two additional benefits of a multi tenant platform-based approach are collaboration and integration. Because all users run all applications in one space, it is easy to allow any user of any application varied access to specific sets of data. This capability greatly simplifies the effort necessary to integrate related applications and the data they manage.

1.1.3 Challenges, Choices and Benefits

With every paradigm shift comes a new set of technical challenges, and SaaS is no different. Further, CMO Compliance is truly dynamic and flexible, allowing any business objects and processes to be modeled and implemented within the system.

1.1.3.1 Challenges

Key architectural areas that deal with the complexities of such a dynamic and flexible system are:

Database query builder:	Can query different database types to match user requirements.
Mapping engine:	Maps relational database structures to the generic objects used within the system, and manages changes to object structures dynamically rather than relying on fixed build-time mappings.
Framework:	Allows management, localisation, audit and security of the generic business objects and actions.
Referencing:	Allows for the creation of relationships between objects.

1.1.3.2 Choices and Benefits

Key architectural choices provided by CMO Compliance and their advantages are:

Configuration: One key aspect of the architecture is the highly configurable nature of CMO based on business rules configurable by the end user. One of the goals was to remove the imposition of structures and behavior as much as possible, allowing users to configure environments to their own requirements, or indeed provide prepackaged configurations for solutions to specific GRC problems. The advantages of this are:

- Flexible
- End User Configurable
- Pre-configurable

Integration: XML is the primary mechanism for passing information between CMO and third party system elements. The advantages of this are:

- Widely understood format within IT community
- Many tools available for manipulation
- Used for definition of web based standards
- Easily machine-readable

1.2 Deployment Architecture

Most users only need access to the browser-based web application. Power Users, Field Users and End Users typically access different modules, which are configurable on a role by role basis from the Business Rules engine.

User Profiles and Access

User Type	Function	Access
End Users	Viewing and reporting on information, as well as responding to and closing out actions and issues	Browser
Field Users	Entering data into forms (assessments, audits, inspections and other data collection forms but excluding incident forms and actions)	Browser
Power Users	Maintenance and management of content and solution including reporting & analysis.	Browser

1.2.1 Deployment Requirements

If you are planning on deploying CMO Compliance on a private cloud, the following requirements are the minimum that we recommend for private cloud deployment. These are guidelines only. Please contact CMO Support for advice on requirements to suit your organization's specific deployment needs.

Note: *CMO recommends that you apply all Windows updates and security patches as they are released.*

1.2.1.1 Client Computer Requirements

CMO Compliance should run on most computers without any alteration. The section below details 16.0 recommendations for client devices and computers:

Server and Hardware Requirements

- For a 100-1000 user environment:
  - 16 GB RAM / 4 CPU (Dedicated Database Server)
  - 8 GB RAM / 4 CPU (Dedicated Application Server)
- For higher concurrency systems it may be recommended to use two or more load balanced application servers to accommodate peak loads.

Supported Databases

- Microsoft SQL Server 2008 R2 or later
- Microsoft SQL Server 2012 or later is required for Data Warehouse

Application and Web Servers

- Internet Information Services (IIS) 7.5 or later

Web Browsers

- Internet Explorer 11
- Microsoft Edge (Latest)
- Google Chrome (Latest)
- Safari (Latest)

View the online Tech Specs sheet for further information about version-specific hardware and software requirements for both Web and Mobile platforms.

1.2.1.2 Offline Tablet PC/Itra Moblie PC/Laptop Minimum Requirements

CMO Compliance can also run offline on Tablet PCs, iPads, Ultra Mobile PCs (UMPCs), PCs and Laptops.

Supported Mobile Devices

The list below contains the supported mobile devices that CMO Compliance will run on:

- **iPad**: Any supported Apple devices receiving updates (from official Apple Support)
- **iPhone**: Any supported Apple devices receiving updates (from official Apple Support)
- **Android Devices**: Devices running Marshmallow (version 23) or later
- **Windows mobile devices**: Devices running Windows 7 or later

Offline PC Tablet Operating System Requirements

The list below contains the recommended minimum Mobile system requirements:

- Windows 7 or above
- iOS 9 or above
- Marshmallow (version 23) or later (Android OS)
- Microsoft .NET 4.7 Framework
- Minimum Memory Requirement: 2Gb RAM

1.2.1.3 Servers

CMO Compliance is a Microsoft.NET application, running on standard Microsoft Windows infrastructure including with virtualized infrastructure recommended. The recommended minimum server specification for CMO is detailed below.

Note it can be shared with other applications, and is not particularly resource intensive however depending upon the level of concurrent usage expected, the below specification may need to be revised:

1.2.1.3.1 General Requirements

General Requirements	Description
SQL Authentication:	CMO Compliance requires an SQL Authenticated User to be available for access during the configuration of the application.
Remote Desktop Protocol:	CMO Compliance requires Remote Desktop access to the web server for maintenance and updates, as well as SQL Server updates via Management Studio for Custom Report Building and Database Management

General Requirements	Description
Hypervisor Support:	CMO Compliance supports running on a virtual infrastructure, preferably VMWare VSphere
Email Account Configuration:	In order for CMO Compliance to send and receive emails a SMTP and POP3 account are required within the email server. This account can operate with Microsoft Exchange via POP3 using SSL and authentication. POP3 is required so that CMO Compliance can receive responses from users and take actions based on those responses. SMTP is required to send email notifications from within the system. We also now support IMAP to fetch and read emails into the management system.
Scheduled Task:	CMO Compliance requires a scheduled task to be setup in Windows Task scheduler that will be run approximately every 10 minutes. This task calls a number of web services within the application but the main task is to send and receive pending emails, for example new audit notifications. This is typically setup by the CMO Installation Engineer.
Scheduled Task:	CMO Compliance recommends a weekly index rebuild and statistics update to be carried by an SQL Agent job.
SSRS Considerations, Firewall, Email Subscriptions:	If you are using SQL Server Reporting Services and have purchased the module from Mitratech, the installation of SSRS must be considered. It is similar to the web application in that it requires database access, as well as appropriate firewall rules for incoming connection from users. CMO will also need to access the server with SSRS installed on to configure the instance. If your IT policies state that database servers (as this is typically where SSRS is installed) cannot have public facing connections, SSRS would need to be provisioned on another machine. If you are using email subscriptions feature with SSRS, please note this does NOT support SMTP authentication directly. If SMTP authentication is required then an intermediary SMTP service on IIS is required. IIS SMTP can be configured as a middle man to forward on using authentication.
Storage Requirements:	The CMO Compliance database will often be no larger than 5 GB however this can vary depending on your configuration and workload. Typically it is just uploaded documents/images/attachments in the application servers /Upload directory that are the source of most of the storage usage. CMO recommend restricting SQL Server memory to 75% of the total available memory in the machine. **Please note:** By default, any uploaded files are stored on the web server, however this can be modified to use symbolic links to redirect to another folder or point the upload path directly to a file share on the network.
Monitoring:	CMO recommends that monitoring of the application is carried out using internal application monitoring tools, or a third party tool such as

General Requirements	Description
	Newrelic. We also recommend the use of software such as Pingdom to monitor application uptime.
Specific System Architecture Specifications Note:	**The minimum specifications for all system builds are for a system used by a maximum of ten users.**
General Software:	**MS .NET Framework 4.7** **IIS 7.5 Web Server & Application Server roles enabled** **SMTP Server for Notifications** **POP3 / IMAP Server for receiving notification replies**

1.2.1.3.2 Shared Architecture w ith IIS and SQA Running on the Same Server

Internet Information Service (IIS) and SQL Server configured to run on the same server. This architecture is not recommended for more than ten system users.

- Minimum Memory Requirement: 6GB RAM
- Windows Server 2008 R2 64bit
- Microsoft SQL Server 2008 R2 SP3 or 2012, Standard or Enterprise Editions
- 4 CPU Cores
- Minimum Hard Disk Space: 50GB Root Drive with 200GB drive/partition for Application Install. Recommended 100GB scratch space drive/partition for backups and update stores

1.2.1.3.3 Regular Rollout of Shared Cloud

System configuration using two separate servers, this is the recommended configuration for most installations.

Database Server Requirements:

- Minimum Memory Requirement: 16GB RAM
- Windows Server 2008 R2 64bit
- Microsoft SQL Server 2008 R2 SP3 or 2012, Standard or Enterprise Editions
- Recommended: 2.5 GHz Quad Core Processor, Minimum: 2 GHz Dual Core.
- 6 CPU Cores
- Minimum Hard Disk Space: 100GB for Application Database (In addition to 100 GB drive/ partition for SQL Server and TempDB, 50GB Root Drive and recommended 100GB scratch space drive/partition for backups and update stores)

Web Server:

- Minimum Memory Requirement: 4GB RAM
- Windows Server 2008 R2 64bit
- Microsoft SQL Server 2008 R2 SP2
- 4 CPU Cores
- Minimum Hard Disk Space: 50GB drive/partition for Application Install (in Addition to 50GB Root Drive with recommended 100GB scratch space drive/partition for backups and update stores)

1.2.1.3.4 Hybrid Cloud and Database Solution

System configuration using two separate servers, this is the recommended configuration for high traffic systems.

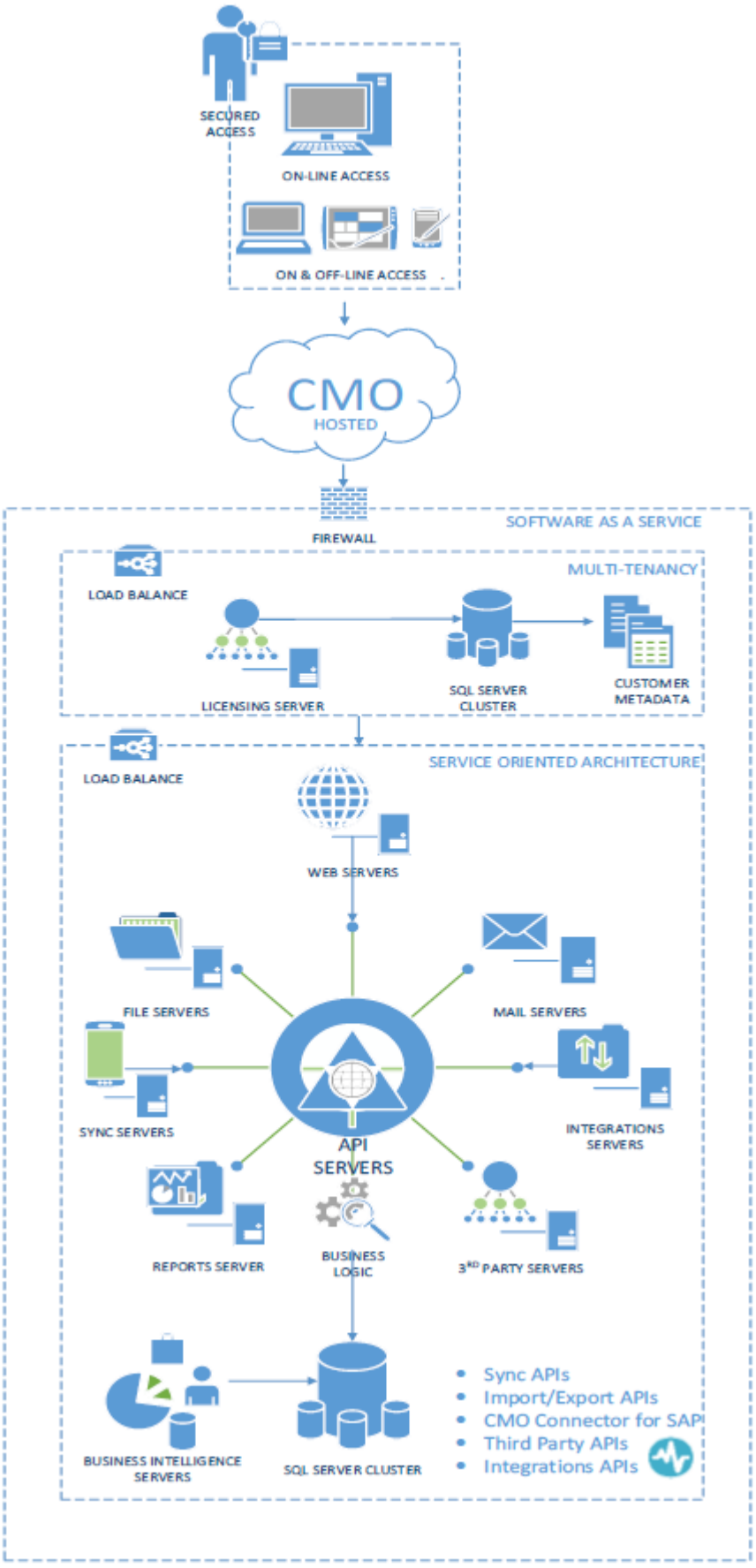
Database Server Requirements

- Minimum Memory Requirement: 20+GB RAM
- Windows Server 2008 R2 64bit
- Microsoft SQL Server 2008 R2 SP3 or 2012, Standard or Enterprise Editions
- 8 CPU Cores
- Minimum Hard Disk Space: 100GB for Application Database (In addition to 100 GB drive/ partition for SQL Server and TempDB, 50GB Root Drive and recommended 100GB scratch space drive/partition for backups and update stores). For high traffic environments we recommend storing both the database and TempDB on a SSD either in a SAN or using local storage SSDs. Alternatively using a SAN with a high iOPS.

Web Server

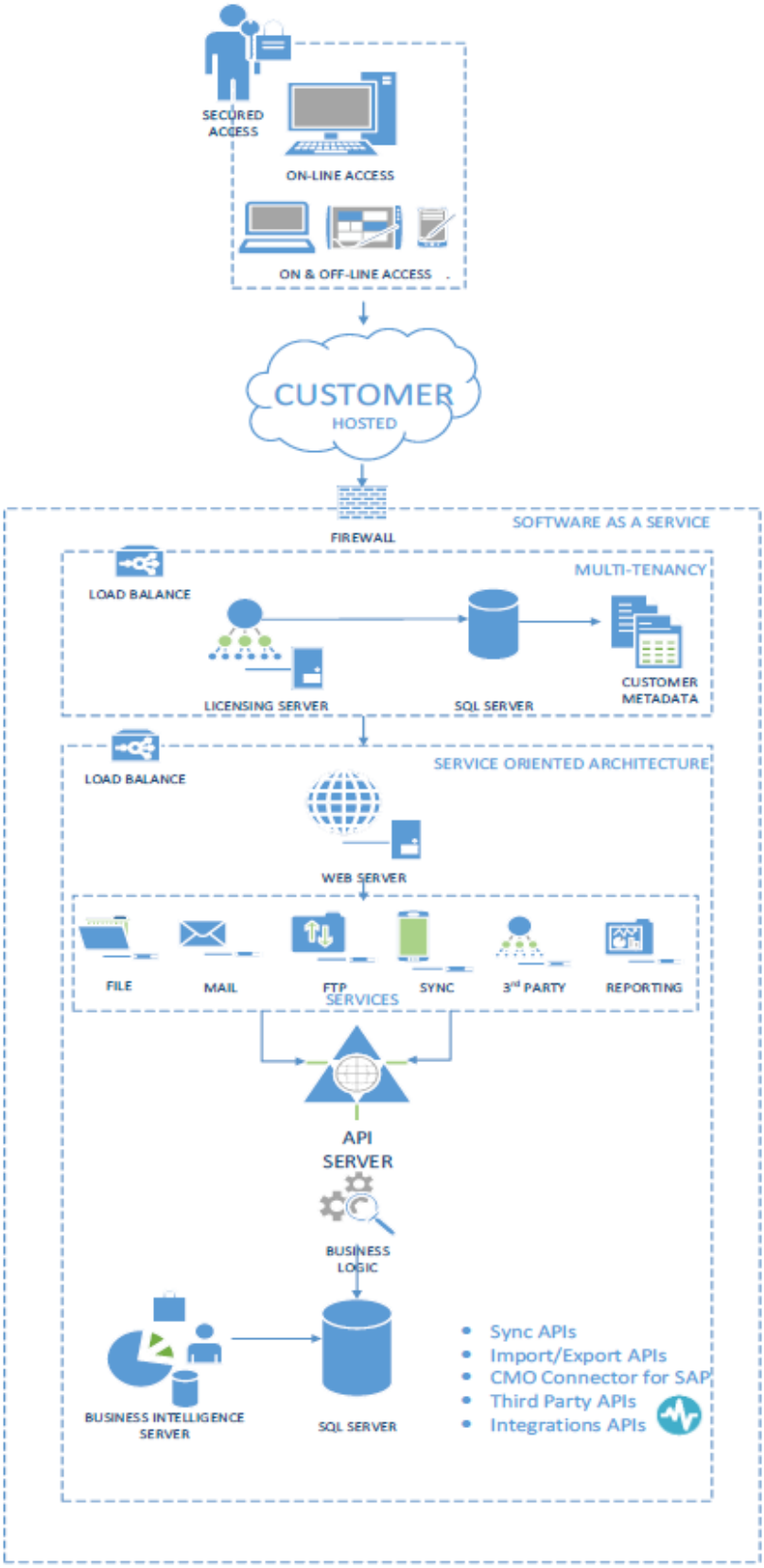
- Minimum Memory Requirement: 6GB RAM
- Windows Server 2008 R2 64bit
- 4 CPU Cores
- Minimum Hard Disk Space: 50GB drive/partition for Application Install (in Addition to 50GB Root Drive with recommended 100GB scratch space drive/partition for backups and update stores)

Technical Architecture: Typical Public Cloud Deployment Architecture Diagram to handle multiple tenants:


SECURED ACCESS
ON-LINE ACCESS
ON & OFF-LINE ACCESS
CMO
HOSTED
FIREWALL
SOFTWARE AS A SERVICE
MULTI-TENANCY
LOAD BALANCE
LICENSING SERVER
SQL SERVER CLUSTER
CUSTOMER METADATA
LOAD BALANCE
SERVICE ORIENTED ARCHITECTURE
WEB SERVERS
FILE SERVERS
MAIL SERVERS
SYNC SERVERS
INTEGRATIONS SERVERS
API SERVERS
REPORTS SERVER
BUSINESS LOGIC
3RD PARTY SERVERS
BUSINESS INTELLIGENCE SERVERS
SQL SERVER CLUSTER
Sync APIs
Import/Export APIs
CMO Connector for SAP
Third Party APIs
Integrations APIs

1.2.1.4 Technical Architecture: Typical Private Cloud Deployment

Below is the Technical Architecture Diagram for a Typical Private Cloud Deployment, where distributed servers become services within the hosting server to handle a single tenant and reduce complexity.


SECURED ACCESS
ON-LINE ACCESS
ON & OFF-LINE ACCESS
CUSTOMER
HOSTED
FIREWALL
SOFTWARE AS A SERVICE
LOAD BALANCE
MULTI-TENANCY
LICENSING SERVER
SQL SERVER
CUSTOMER METADATA
LOAD BALANCE
SERVICE ORIENTED ARCHITECTURE
WEB SERVER
FILE
MAIL
FTP
SYNC
3rd PARTY
REPORTING
SERVICES
API SERVER
BUSINESS LOGIC
BUSINESS INTELLIGENCE SERVER
SQL SERVER
Sync APIs
Import/Export APIs
CMO Connector for SAP
Third Party APIs
Integrations APIs

1.2.1.5 Data Transfer

If you use a handheld device, when the handheld device is synchronised with the CMO web server, the data is transferred as a dataset in XML format. This data transfer is encrypted over HTTPS to ensure security of data.

1.2.1.6 Network Settings

Whether running a CMO Compliance solution on a Public or Private Cloud, your System Administrator should ensure that CMO is added as a Trusted Site, as well as added to your Intranet Zone. This is essential if Active Directory Authentication is being used.

1.2.1.7 Corporate Firewalls

Corporate firewalls do not create an issue when using CMO Compliance. If you use tablet or handheld devices, there is a component built into CMO on the handheld device to ensure even the most secure firewalls can be navigated, to ensure that data can be transferred successfully to either our server if you have licensed the public cloud edition of CMO, or to your servers if you have purchased a dedicated installation of CMO.

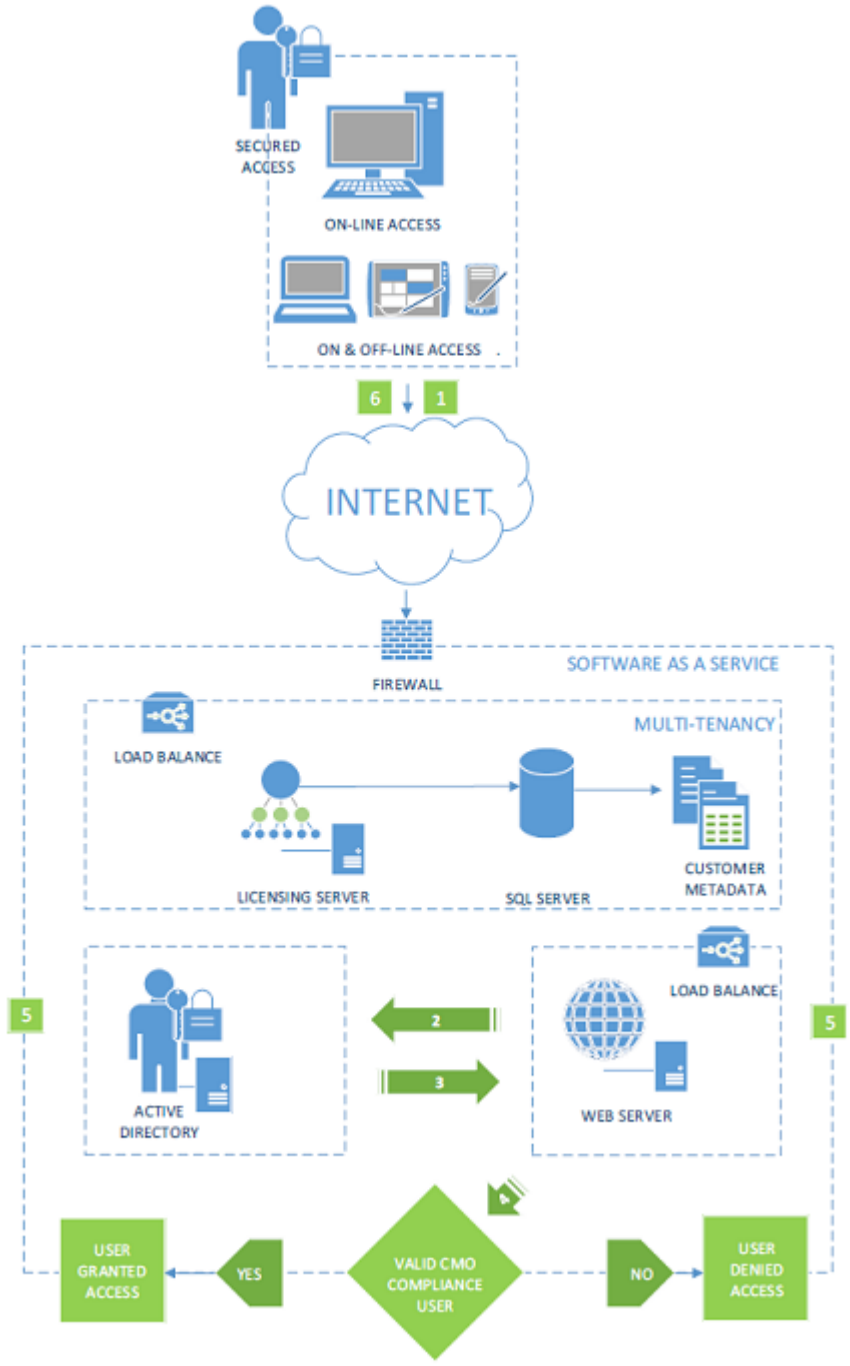
1.2.2 Authentication

A wide variety of security access options are available to clients, using a combination of CMO-specific configurations and external software options, such as IIS.

1.2.2.1 IIS Authentication

IIS provides seamless integration with Active Directory including Active Directory Federation Services (ADFS) which enables users to collaborate across organizational boundaries and easily access applications on public or private clouds whilst maintaining application security, as well as providing options like SSL and integration with third party authentication mechanisms. Integrated Authentication is the typical method, but basic authentication allows for a wider range of choices.

The CMO Compliance software provides two simple options to complement this: controlling how users can log on and log off, and using concepts such as the Default (generic) User. During the deployment phase, we will work with the client to identify the most appropriate configuration. This is depicted in the diagram below:



1.2.2.2 Automatic Logon (Single Sign On)

IIS Integrated Authentication

CMO Compliance allows for Integrated Auto logon, also commonly known as Single Sign On (SSO).

The steps for this process are:

1. The user accesses the web page being serviced by IIS.

2. IIS collects the user details and passes them to the Active Directory for authentication.
3. If the user is a valid Active Directory user, Active Directory returns a positive result and goes to step 4. If no user exists, access is denied.
4. IIS redirects traffic to the application.
5. Depending on whether the user exists in CMO, they will either be granted access as a defined user, or granted access as a default or generic user.
6. CMO Compliance passes the traffic back to IIS.
7. IIS returns the traffic to the browser.

For SSO to function correctly: All users must be internal (LAN based users). Power Users are defined in the system, but other users are logged on as such, with a limited set of rights (for example, the ability to complete actions).

1.2.2.3 IIS Basic Authentication

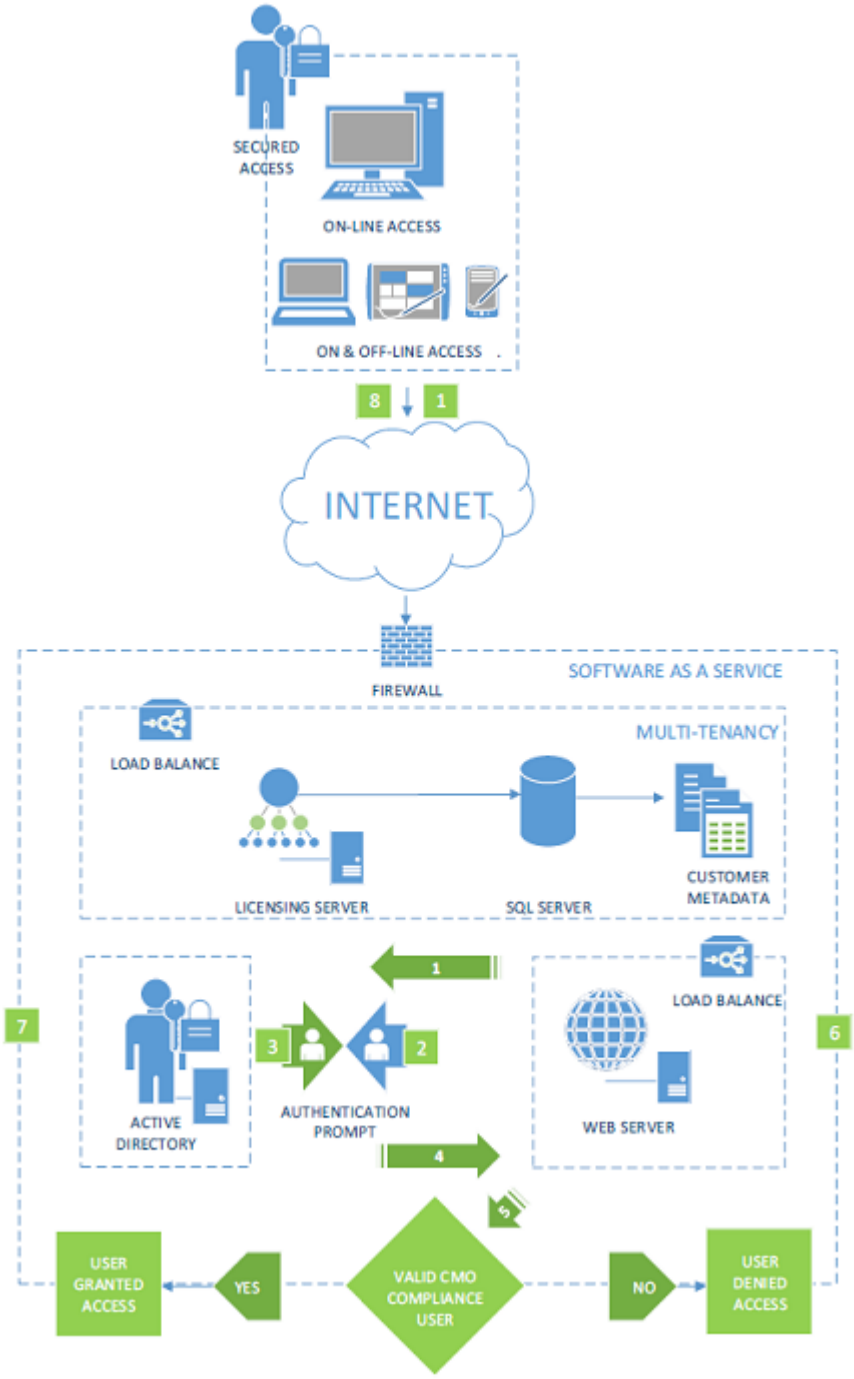
CMO Compliance supports Single Sign On (SSO) via ADFS and SAML 2.0. This may be the preferred option if users:

- Are accessing an externally facing web site
- Are sharing a PC but need to maintain separate access to the CMO application
- Log-on to another type of authentication system, so do not have a valid Active Directory token, but accounts are replicated in Active Directory.

It is similar to the previous integrated model, except that:

1. The user accesses the web page being serviced by IIS.
2. The user is prompted for credentials.
3. IIS collects the user details and passes them to the Active Directory for authentication. SSL is used to maintain security.
4. If the user is a valid Active Directory user, Active Directory returns a positive result and goes to step 4. If no user exists, access is denied.
5. IIS redirects traffic to the CMO COMPLIANCE.
6. Depending on whether the user exists in CMO COMPLIANCE, they will either be granted access as a defined user, or granted access as a default or generic user.
7. CMO COMPLIANCE passes the traffic back to IIS.
8. IIS returns the traffic to the browser.

This is depicted in the diagram: **IIS Basic Authentication**



1.2.2.4 IIS or Integrated/BASIC Authentication Model - Options

Options within the CMO Compliance application can be used to provide a greater level of security if desired are:

Disable Default User: This would mean that ONLY defined users in CMO, who also have an Active Directory account, would be able to gain access to the system.

1.2.2.5 User Profiles

Users are stored in the database. When a user uses the system and opens a session, profile values are also cached.

When a user (authenticated or unauthenticated) logs onto CMO, the system retrieves the profile values and caches it for the session. The cache is maintained for that session until the user logs out and closes the browser.

When a user accesses List Views, or uses forms that make use of user profile defaults, the values are retrieved from the cache.

When a user accesses the **My Profile** form, the system retrieves the values from the database. If the user makes a change to the profile values and saves, then the cache is updated. Note that if the user saves the My Profile form without making any changes, then the cache is not updated, as the record is not updated.

1.3 Support and Resources

Contact Support

For any questions, contact CMO Support via the Online Support Portal or by calling one of the phone numbers listed below:

United States: +1 678-388-9439

Australia: +61 (0)3 9251 7077

UK: +44 (0)207 078 7414

Online Documentation

Users can access the Client Success Center for online Help articles. Visit www.success.mitratech.com/CMO for more details.