Software Requirements Specification

27 Feb 2017

MALT: Malicious Login Tracker

Version 1.0

Intro & Overall Description Complete

Table of Contents

[1 Introduction 3](#_Toc475975157)

[1.1 Purpose 3](#_Toc475975158)

[1.2 Scope 3](#_Toc475975159)

[1.3 Glossary 3](#_Toc475975160)

[1.4 References 4](#_Toc475975161)

[1.5 Document Overview 4](#_Toc475975162)

[2 Overall Description 4](#_Toc475975163)

[2.1 System Environment 4](#_Toc475975164)

[2.2 Functional Requirements Overview 5](#_Toc475975165)

[2.3 Structural Models 5](#_Toc475975166)

[2.3.1 Analyst Use Cases 5](#_Toc475975167)

[2.3.2 Administrator Use Cases 9](#_Toc475975168)

[2.4 Object Diagrams 13](#_Toc475975169)

[2.4.1 Class Diagrams 13](#_Toc475975170)

[2.5 Dynamic Models 13](#_Toc475975171)

[2.5.1 Sequence Models 13](#_Toc475975172)

[2.5.2 Activity Models 13](#_Toc475975173)

[2.6 User Characteristics 13](#_Toc475975174)

[2.7 Nonfunctional Requirements Description 13](#_Toc475975175)

[3 Requirements Specification 13](#_Toc475975176)

[3.1 External Interface Requirements 13](#_Toc475975177)

[3.2 Detailed Functional Requirements 13](#_Toc475975178)

[3.3 Detailed Nonfunctional Requirements 14](#_Toc475975179)

**List of Figures**

Figure 1. System Environment 5

Figure 2. Use-Case Diagram. 6

# Introduction

## Purpose

This software requirements specification (SRS) will give a detailed description of the MALT network traffic analytics system. It is intended for both developers and stakeholders, and will serve as the definitive record of the purpose, features, behaviors, and interfaces of the software system. This document will provide an agreed-upon basis for the creation of the system between the client and developers. Changes to the proposed functionality of the system during development by either the client or the developers will result in update to this SRS.

## Scope

This software system, MALT, will be a network traffic analytics web app for UA Little Rock Information Security Services. MALT will alleviate the current manual data-processing workflow for visualization of suspicious login data. Access to our automated data storage, processing, and visualization tool will increase the efficiency of analytics tasks.

Specifically, our solution will extract information from human-readable email alerts, save the data in a database, process the data, and visualize appropriate metrics with an online dashboard. Our proposed system supersedes current commercial products as it integrates all the steps of the data analysis workflow, while avoiding the need to directly write code to gain understanding of the data. Upon software delivery, UA Little Rock Information Security Services will possess a scalable, automated analytics system, deployed to the school network, which can be easily modified by later developers.

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Stakeholder | Any person with an interest in the system who is not a developer. For example, a user, client, or administrator. |
| MALT | The proposed software system for analyzing UA Little Rock network traffic |
| Analyst | Person using MALT to investigate current or historical potentially malicious login attempts to the UA Little Rock network |
| Administrator | Person responsible for maintaining MALT and its data storage upon deployment of the web application. |
| Software Requirements Specification (SRS) | A document which describes the complete functionality of a proposed software system for both developers and stakeholders |

## References

1. None Currently

## Document Overview

This SRS has three main sections: Introduction, Overall Description, and Requirements Specification. The Overall Description section is intended to illustrate the functionality and potential uses of MALT. It provides the necessary context for understanding of the technical requirements in the third section, Requirements Specification. The Requirements Specification section describes MALT’s technical specifications fully. It is intended to assist developers in creation of the system.

# Overall Description

## System Environment

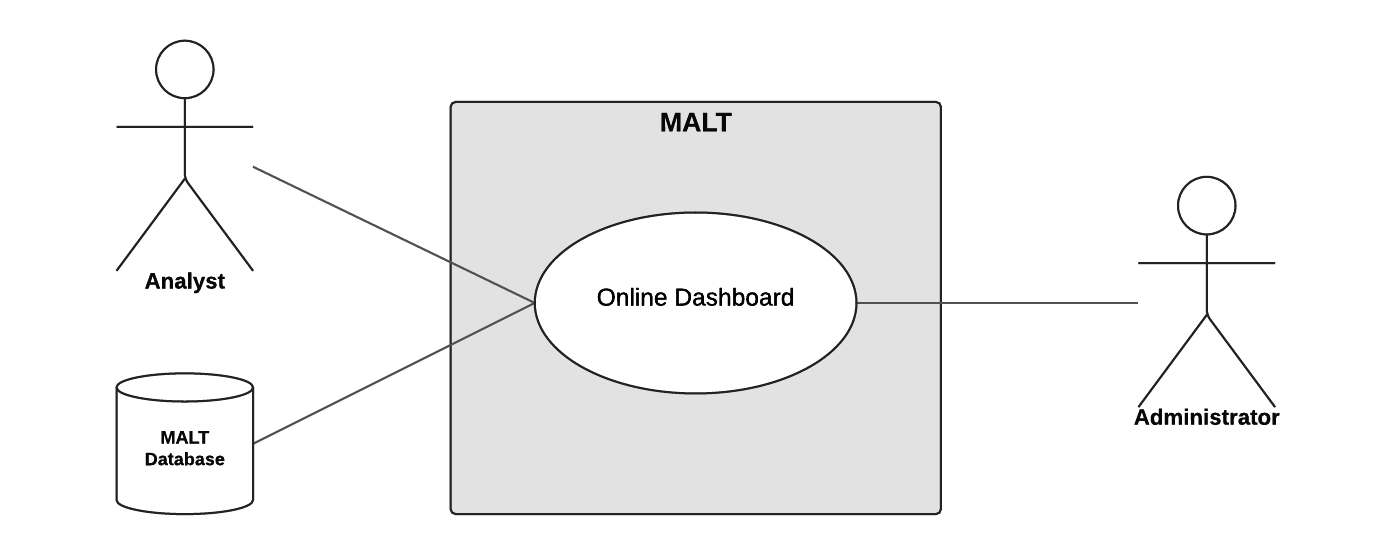


Figure 1. System Environment

The MALT system is hosted on a web server, and both analysts and the administrator access the system through the MALT web application over the Internet. The application database is stored locally on the web server hosting the MALT system.

## Functional Requirements Overview

This section describes the use cases for all users of the system. The Analyst is the most frequent user of the system, while the Administrator has maintenance responsibility.

## Structural Models

### Use Case Diagram

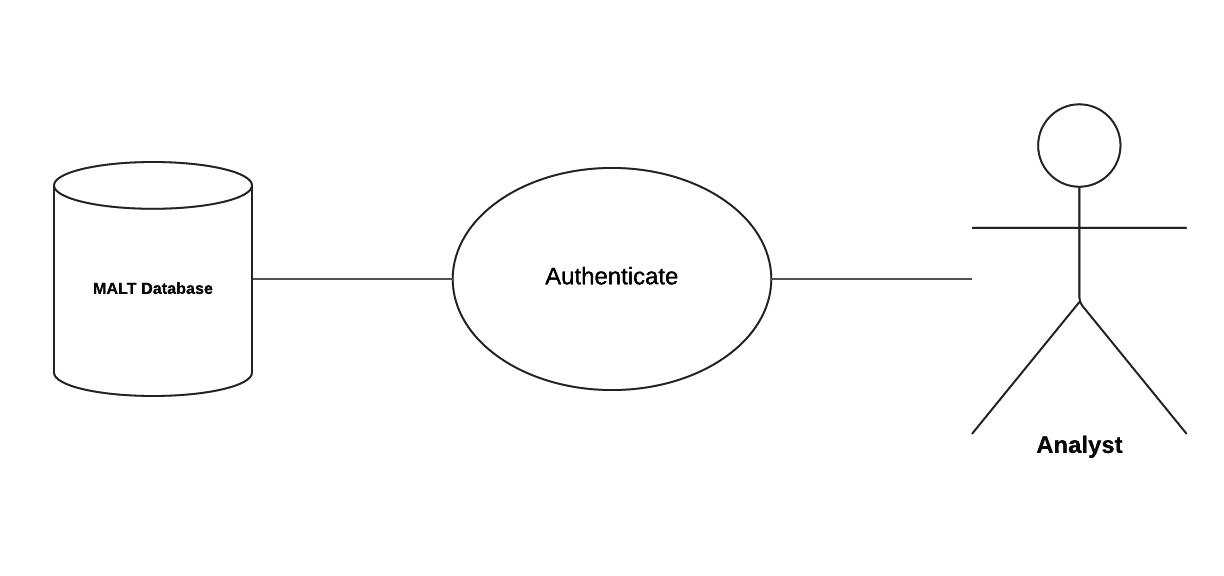
### 

Figure 2. Use-Case Diagram.

### Analyst Use Cases

#### Use Case: Authenticate

Diagram**:**



Brief Description:

Web server will require analyst-level username and password to access the dashboard

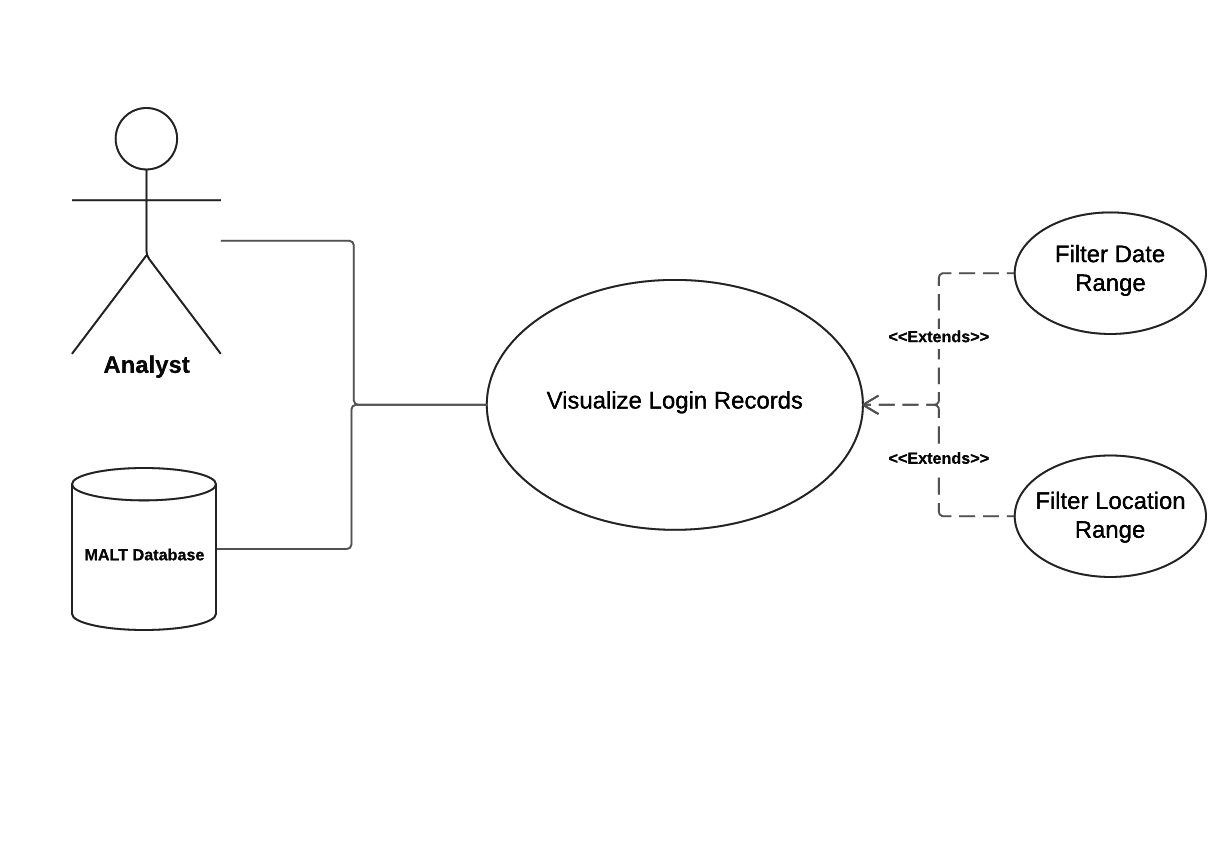
Initial Step-By-Step Description:

1. Analyst connects to the MALT online dashboard website
2. System prompts Analyst to enter appropriate username and password
3. Password validation will occur: at least 8 characters alphanumeric, including one uppercase letter.
4. If analyst-level username and password is supplied, the system will load the online dashboard with records from the database.
5. If an incorrect username/password combination is supplied, the system will prompt analyst for username and password again, up to 5 times.
6. If an incorrect username/password combination is entered 5 times, the System will block the account from which the attempts originated for 15 minutes.

Cross-Reference: xxxx

#### Use Case: Visualize Login Records

Diagram**:**



Brief Description:

Analyst will visualize the login records, which are loaded from the database. The analyst may optionally filter the records by a date range and/or by a location range.

Initial Step-By-Step Description:

Before this use case can be initiated, the analyst must be connected to the online dashboard site and authenticated.

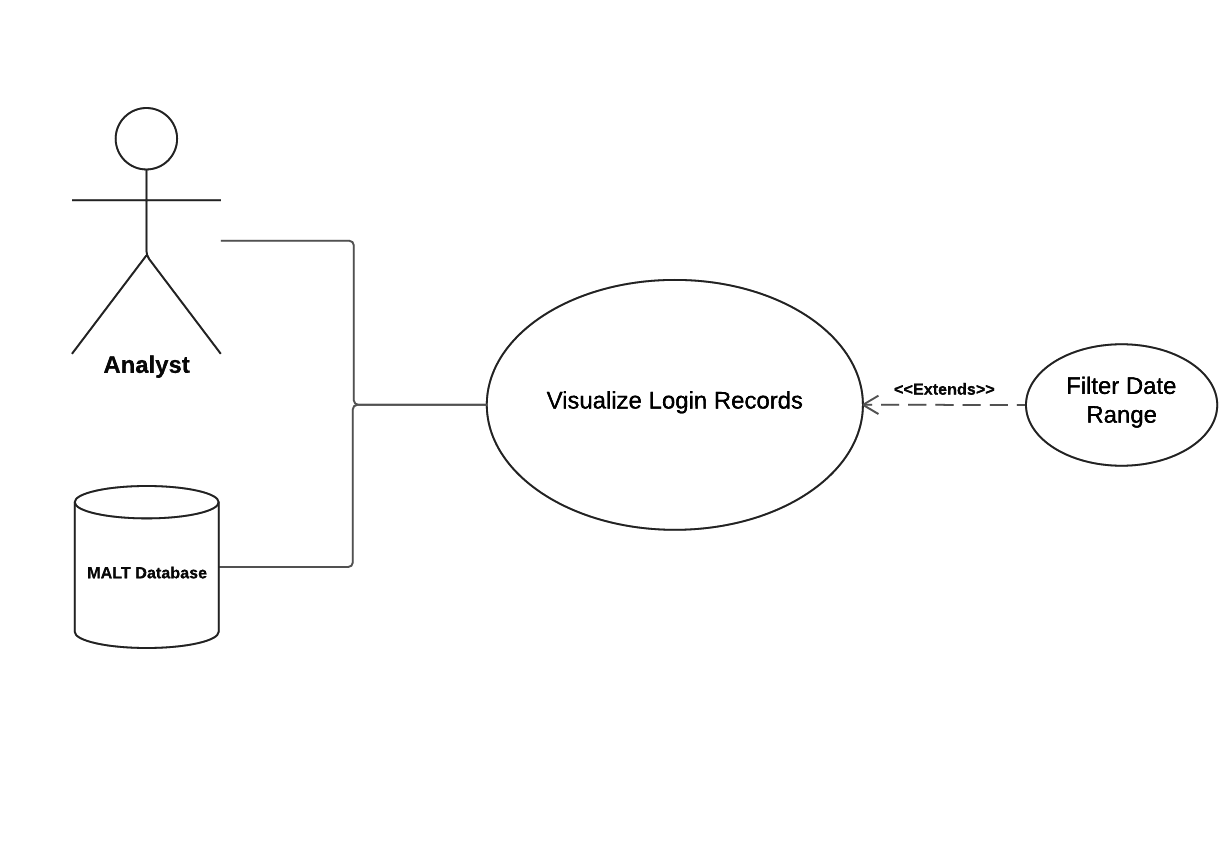
1. Online dashboard loads all records from the MALT database
2. Analyst views all metrics of the data

Cross-Reference: xxxx

#### Use Case: Filter Date Range

This use case extends the **Visualize Login Records** use case.

Diagram:



Brief Description:

Analyst filters data records by date. This use case can be combined with Filter Location Range Use Case.

Initial Step-By-Step Description:

Before this use case can be initiated, the Analyst has already entered the **Visualize Login Records** use case.

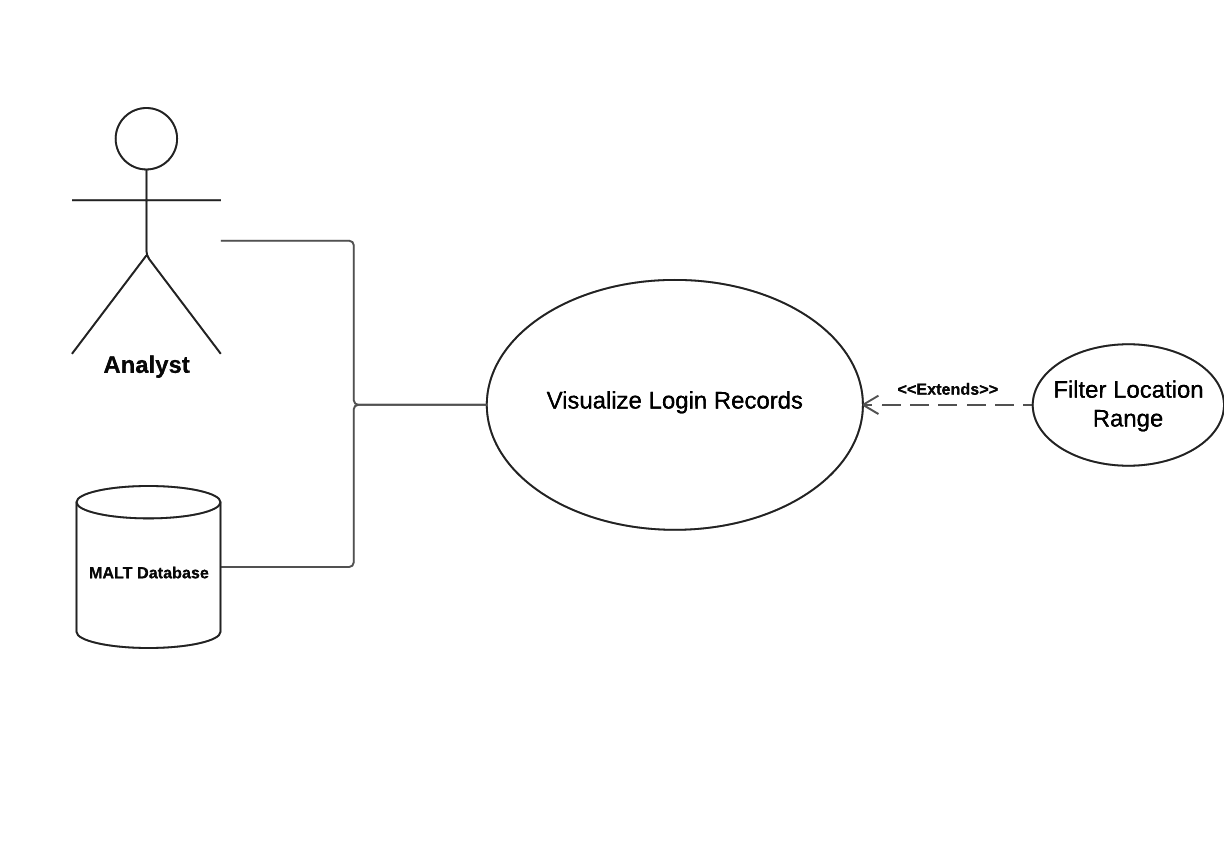
1. Analyst chooses a date range.
2. Dashboard removes data records not meeting the filter criteria.
3. Analyst views subset of data records

Cross-Reference: xxxx

#### Use Case: Filter Location Range

This use case extends the **Visualize Login Records** use case.

Diagram:



Brief Description:

Analyst can filter data records by geographical location. This use case can be combined with Filter Date Range use case.

Initial Step-By-Step Description:

Before this use case can be initiated, the Analyst has already entered the **Visualize Login Records** use case.

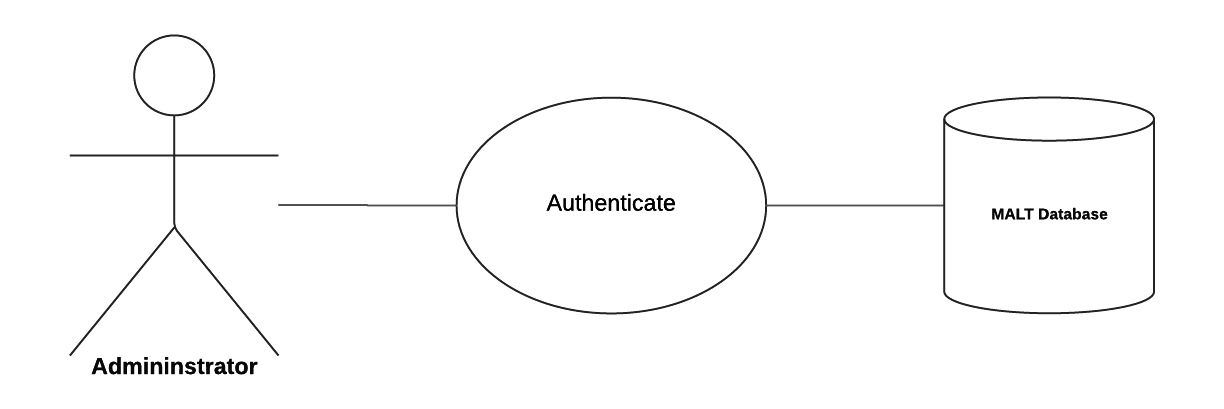
1. Analyst chooses a range for geographical location.
2. Dashboard removes data records not meeting the filter criteria.
3. Analyst views subset of data records

Cross-Reference: xxxx

### Administrator Use Cases

#### Use Case: Authenticate

Diagram:



Brief Description:

Web application will require administrator-level credentials (username and password) to have access to the MALT Database.

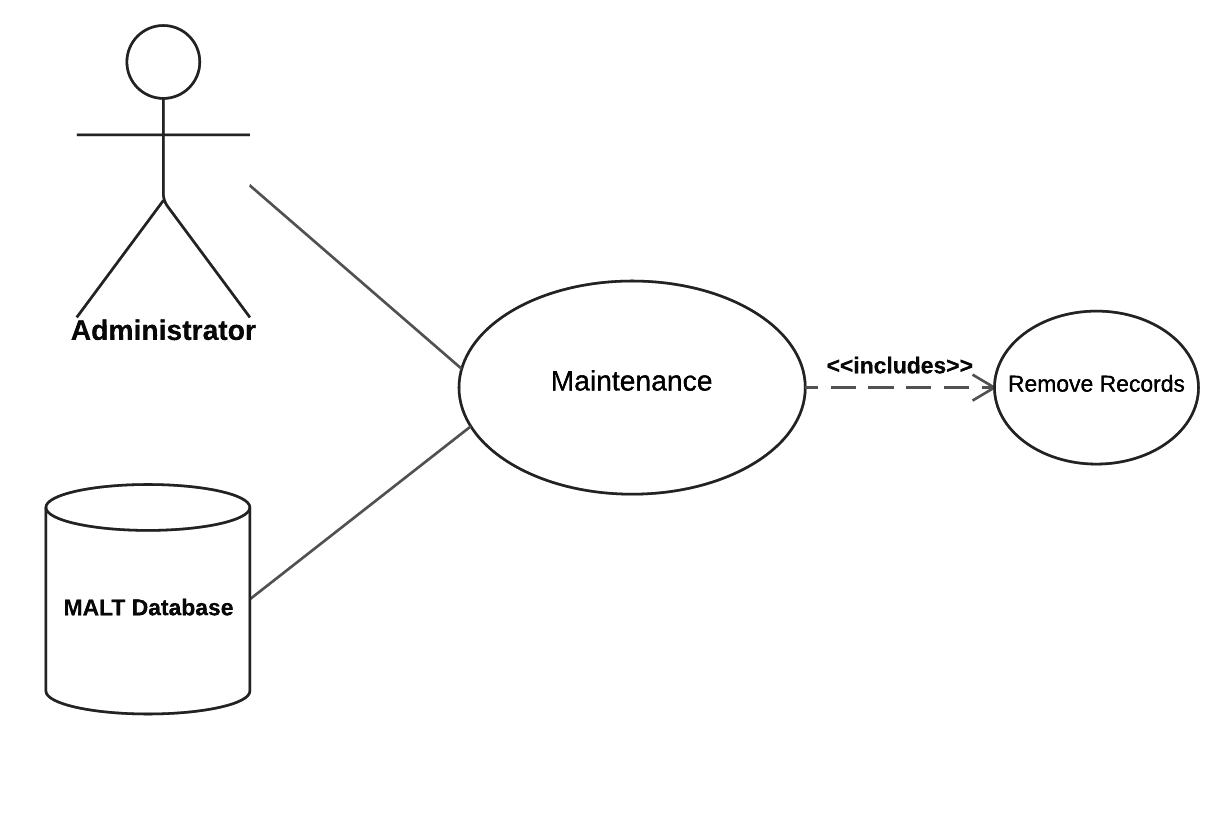
Initial Step-By-Step Description:

1. Administrator will connect to the web application site.
2. If administrator-level username and password matches the record, the system will direct the administrator to the web application site.
3. Password validation will occur: at least 8 characters alphanumeric, including one uppercase letter.
4. If an incorrect username/password combination is supplied, the system will prompt user for username and password again, up to 5 times.
5. If an incorrect username/password combination is entered 5 times, the System will block the account from which the attempts originated for 15 minutes.

Cross-Reference: xxxx

#### Use Case: Maintenance

Diagram:



Brief Description:

Administrator will maintain the login records in the system. The records will be deleted from the database as specified by the administrator.

Initial Step-By-Step Description:

Before this case can be initiated, the administrator must be connected to the system database and authenticated.

1. Administrator access all the records in the MALT database.
2. Administrator will view data on the dashboard and plan necessary record maintenance.

Cross-Reference: xxxx

#### Use Case: Remove Records

This use case is included in the **Maintenance** use case.

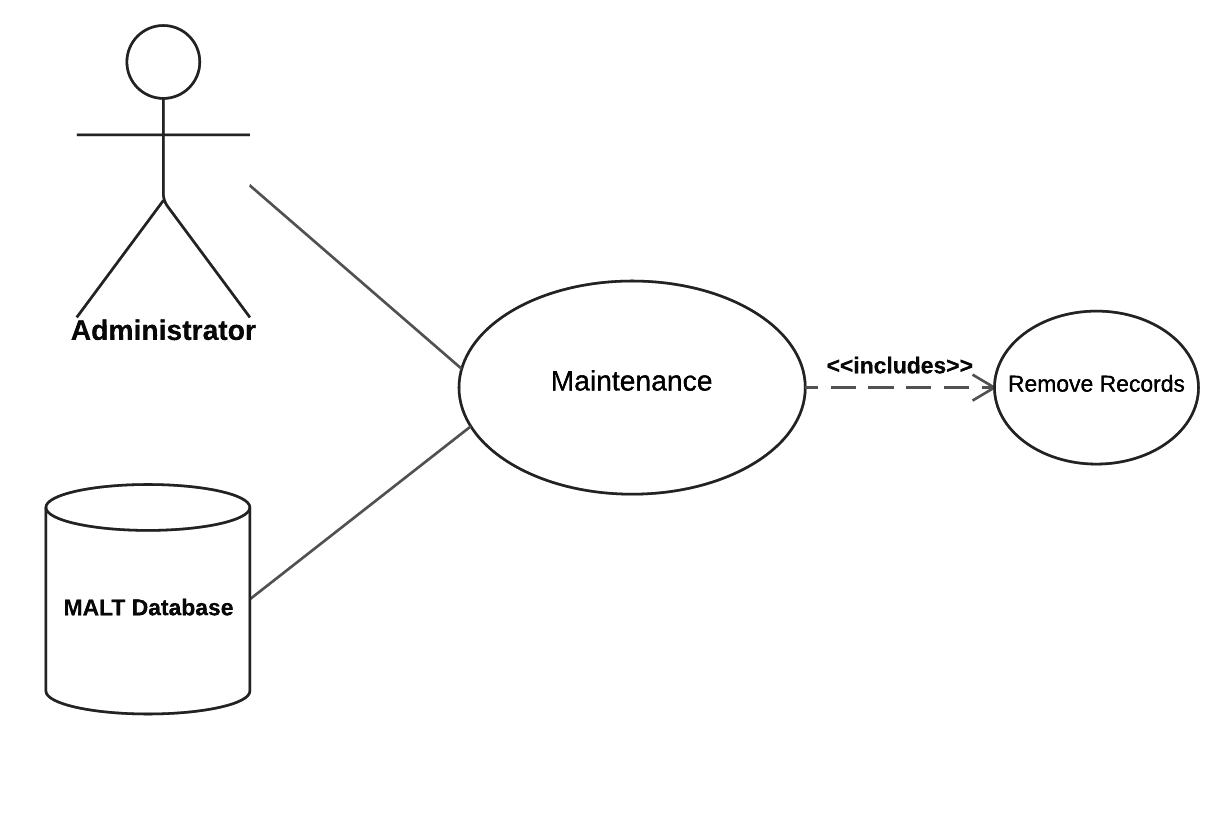


Diagram:

Brief Description:

Administrator can archive any data record deemed irrelevant for analysis

Initial Step-By-Step Description:

Before this case can be initiated, the administrator must be connected to the system database and authenticated.

1. The administrator selects data for archival.
2. The administrator archives the data specified on the step above using the dashboard interface.

Cross-Reference:

## Object Diagrams

### Class Diagrams

## Dynamic Models

### Sequence Models

### Activity Models

## User Characteristics

There are two target users of the MALT system: analyst and administrator.

**Analyst**

The analyst is expected to be able to navigate a web application, and have an understanding of UA Little Rock’s Information Security Services context, in which MALT operates. They will understand UA Little Rock’s expected network traffic and be able to identify malicious or other noteworthy login patterns.

**Administrator**

The administrator will be familiar with the system’s design, implementation, and interfaces. She will handle exceptions, either notifying the development team or solving them autonomously through her solution-domain knowledge.

## Nonfunctional Requirements Description

MALT will be hosted on a UA Little Rock private server with high-speed Internet capability. A Linux system running a production http server will be used for hosting all portions of the system, including web application and database. The web application interface will be used for all interaction with MALT.

# Requirements Specification

## External Interface Requirements

## Detailed Functional Requirements

1. <Use Case Table>
2. <Use Case Table>
3. <Use Case Table>

## Detailed Nonfunctional Requirements