# OpenTrust MFT

# Managed File Transfer

# Оглавление

1. Введение ... 3
2. OpenTrust MFT. Основные моменты. ... 4
3. Инновационная концепция, насыщенная функционалом ... 5
   3.1. Домены ... 5
   3.2. Категории пользователей ... 5
   3.3. Политики ... 6
   3.4. Контроль доступа ... 7
   3.5. «Проекты» ... 10
   3.6. Источники контактов ... 11
   3.7. Графические Темы ... 11
   3.8. Шаблоны уведомлений ... 11
4. Простота и интуитивность работы пользователя ... 14
   4.1. Оптимизация с использованием GWT™ ... 14
   4.2. Просмотр сообщений и Поиск ... 15
   4.3. История ... 15
   4.4. Детали сообщения ... 16
   4.5. Отправка файлов и документов ... 16
   4.6. Управление проектами ... 18
   4.7. Управление контактами ... 19
   4.8. Жетоны ... 19
   4.9. Параметры пользователей ... 21
5. Оптимизированная программная архитектура ... 22

# 1. Введение

**В прошлом**, обмен электронным конвентом между корпоративными сетями проходил посредством систем электронных сообщений (email/smtp) и традиционным путем через FTP.

**Сегодня**, задачи обмена документами, как с внутренними получателями, так и внешними, не могут быть решены традиционными средствами, так как:

- Системы электронных сообщений не предназначены для передачи файлов большого размера.
- Решения на базе FTP с одной стороны дольно трудозатратны и дороги для администрирования (когда рассматривается инфраструктура обслуживания большого количества пользователей), а с другой, сложны в использовании для конечного пользователя.
- Наконец, в большинстве случаев традиционные способы (электронная почта, FTP) не являются надежными с точки зрения безопасности, прозрачности контроля и соблюдения требуемого уровня конфиденциальности.

Однако, за счет того, что задача передачи документов большого размера является критической для продуктивностой работы и затрагивает аспекты соблюдение требований в области защиты информации в процессе обмена документами, сформировались определенные требования, предъявляемые к таким системам:

- Простота использования конечными пользователями, простота реализации и функционирования
- Минимальное влияние на рабочее место: обмен документами должен выполняться через привычный интернет-браузер или традиционное, ужу эксплуатируемое ПО
- Интерфейс дожжен соответствовать корпоративным стандартам
- Гибкость и возможность адаптации к требованиям организации (разделение пользователей, централизованное или делегируемое администрирование, детализированное управление правами и т.д.)
- Аутентификация постоянных пользователей и возможность организовать гостевой режим с минимальным привлечением администраторов
- Сквозная безопасность обмена, как на стадии передачи, так и хранения на протяжении всего времени эксплуатации
- Полная прозрачность активностей (пользователей и администраторов) и отслеживание статусов скачиваний переданных документов непосредственно из web-интерфейса
- Соответствие одной или нескольким политикам безопасности (правила аутентификации, парольная политика, фильтрация, разделение модулей администрирования и модуля конечного пользователя и т.д.)

**Завтра**, при практически полной «оцифровке» бизнес-процессов решение по защищенной передаче файлов должно обладать возможностью автоматизации этих задач за счет интеграция с бизнес-приложениями. Наряду с этим становится необходимым обеспечение невозможности отказа от авторства и подтверждения личности отправителя.

Начиная с 2003 мы работаем над разработкой системы защищенной передачи документов, и к сегодняшнему дню смогли реализовать наиболее полный набор инструментария в монолитном решении, обеспечивающем простоту эксплуатации и администрирования, высокий уровень безопасности предоставляемых сервисом и прозрачность активностей как конечных пользователей, так и администраторов, ответственных за настройки и сопровождение системы.

OpenTrust, как провайдер цифровых решений следующего поколения, обслуживает самые требовательные компании из Fortune 500, а так же государственные структуры многих стран (обеспечивающие национальную безопасность, объекты ядреной энергетики, авиакомпании и финансовый сектор), что накладывает вполне определенные требования к надежности и качество разрабатываемых решений

Основываясь на нашем опыте и понимании задач, в том числе и за счет положительной обратной связи от наших заказчиков, мы сформировали новую концепцию защищенной передачи документов и реализовали ее в решении нового поколения — OpenTrust MFT.

Решении может быть использовано в виде приобретаемых лицензий, с установкой внутри контура безопасности заказчик или на арендуемых мощностях стороннего ЦОД, или использоваться как сервис, предоставляемый сторонней компанией по принципу SaaS.

Если Вы желаете получить тестовый аккаунт и попробовать это простое и удобное решение прямо сейчас — отправьте запрос на info@powersecurity.ru

## 2. OpenTrust MFT. Основные моменты.

OpenTrust Managed File Transfer (MFT) — это решение нового поколения, предназначенное для защищенного и контролируемого обмена документами. Используя это решение, вы можете прозрачно контролировать активности пользователей и администраторов, делегировать административные полномочия и создавать различные политики безопасности в зависимости о категории групп пользователей.

Программное обеспечение устанавливается быстро и просто, а конфигурация выполняется с использованием полнофункционального web-интерфейса, который реализован в двух модулях: **MFT Admin** (модуль администрирования) и **MFT Zephyr** (пользовательский модуль).

**Для начального уровня** (маленький бизнес или даже фриланс) наиболее подходящий вариант — SaaS. Это позволяет использовать полнофункциональное решение, не задумываясь об администрировании и не решая задачи об обеспечении и затратах на аппаратное обеспечение.

**Малый и средний бизнес** (SMB-сектор) могут воспользоваться этим решением на базе одного сервера, выполнив быструю установку, используя «виртуальный аплаинс», или развернуть решение в виртуальной инфраструктуре.

**Большие предприятия** (корпоративный уровень) и территориально-распределенные организации могут использовать MFT в виде распределенной инсталляции или воспользоваться SaaS-предложением со специальными условиями.

# 3. Инновационная концепция, насыщенная функционалом

Перед детальным описанием проведем краткий экскурс, описав структуру и организацию электронного обмена документами.

## 3.1.Домены

Домены — центральная часть MFT. Они позволяют разделить инфраструктуру обмена на независимые контейнеры для:

- Моделирования организационных и административных отделов и подразделений организации
- Назначения правил (или политик) аутентификации, прав доступа, уведомлений и так далее в соответствии с доменов, к которому принадлежит пользователь
- Организовать администрирование и делегирование полномочий в соответствии с организационной структурой
- Кастомизировать интерфейс в рамках одной инсталляции для различных групп пользователей и подразделений (отделы, дочерние предприятия, партнеры и так далее)

Доменная концепция позволяет гибко моделировать среду обмена, делегировать административные полномочия и графически катомизировать интерфейс пользователя.

## 3.2.Категории пользователей

Существует две группы пользователей:

- **Зарегистрированные пользователи**, которые имеют постоянный или временный аккаунт в MFT и ассоциируются с определенной схемой аутентификации (AD/LDAP для внутренних пользователей, MFT-база для внешних пользователей)
- **Гости**, которые «приглашены» зарегистрированными пользователями скачать документы или, наоборот, загрузить их на сервер MFT. Такие пользователи не имеют своих аккаунтов и не обладают другими полномочиями. Гости получают электронное письмо со ссылкой, используя которую могу скачать «отправленные» для них файлы или выложить файлы для зарегистрированного пользователя (использовать «жетон»)

Зарегистрированные пользователи могут быть двух типов:

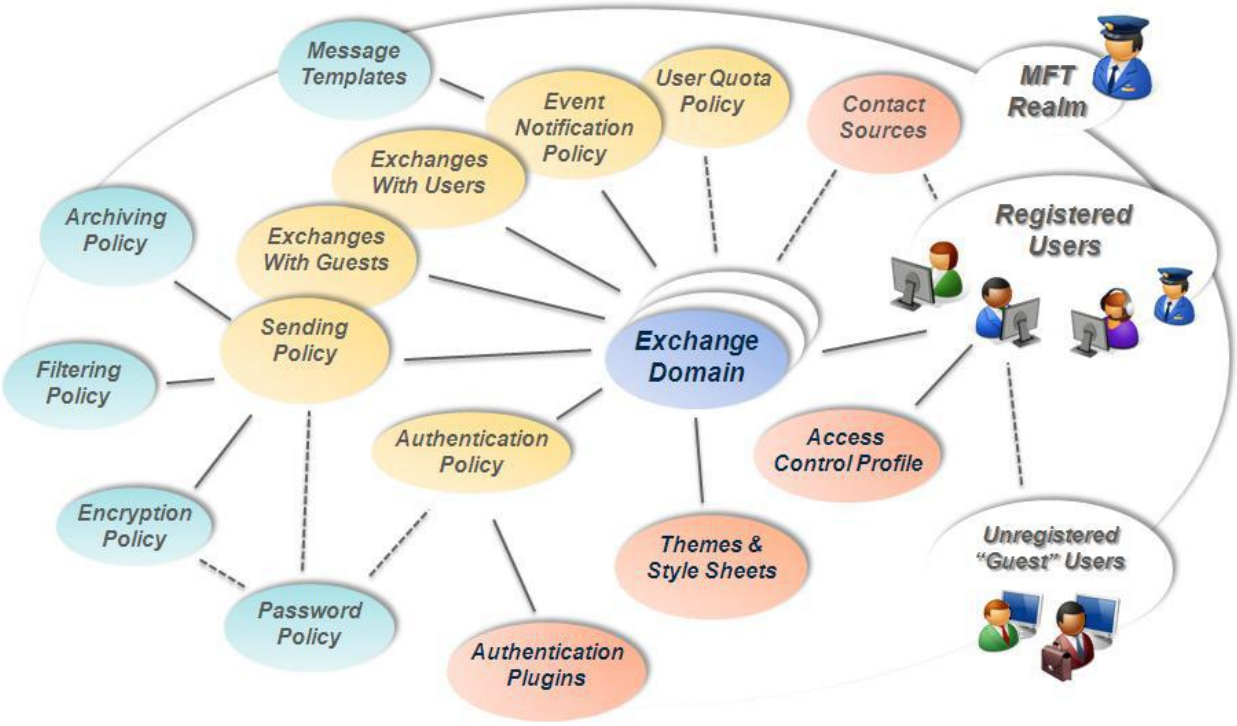
- **Внутренние пользовали**. «Взяты» из корпоративной службы каталогов, которые, как правило, работают внутри корпоративной сети.
- **Внешние пользователи**. Поставщики, партнеры, субподрядчики — в общем, все те, кому вы выходите дать доступ к MFT-функционалу, работаю, как правило, извне.

## 3.3.Политики

Политика OpenTrust MFT — это объект, группирующий различные настройки. На базе политик реализуются различные правила (аутентификация, фильтрация и так далее) для пользователей в рамках одного домена.

Политики определяют следующие категории настроек:

- Правила аутентификации с использованием таких популярных технологий как: AD/LDAP-каталоги, SSO, X.509-сертификаты, внутренняя база, RADIUS и так далее)
- Парольная политика, используемая при аутентификации и защите передаваемых файлов
- Ограничения на популяцию (внутренние пользователи, внешние пользователи, гости)
- Правила, регламентирующие отправку файлов (фильтрация, максимальный размер, антивирусная проверка, шифрование и архивирование)
- Квотирование дискового пространства для различных групп пользователей
- Уведомления для различных случаев




Доменная структура MFT, управляемая политиками

Такая архитектура позволяет определить «поведения» системы в соответствии с корпоративными требованиями и адаптировать ее под существующие задачи. Вместе с этим становится возможным ответить на ряд вопросов, которые к этому моменты накопились в организации:

- Как мы аутентифицируем внутренних и внешних пользователей, давая внутренним полную свободу распространения контента (документов), в то же время предотвращая использование системы в личных целях внешними пользователями?
- Как мы используем аутентификацию на базе служб каталогов (или с использованием SSO) для внутренних пользователей без риска попасть под сетевую атаку, в то время как внешние пользователи должны пройти аутентификацию средствами самой системы?

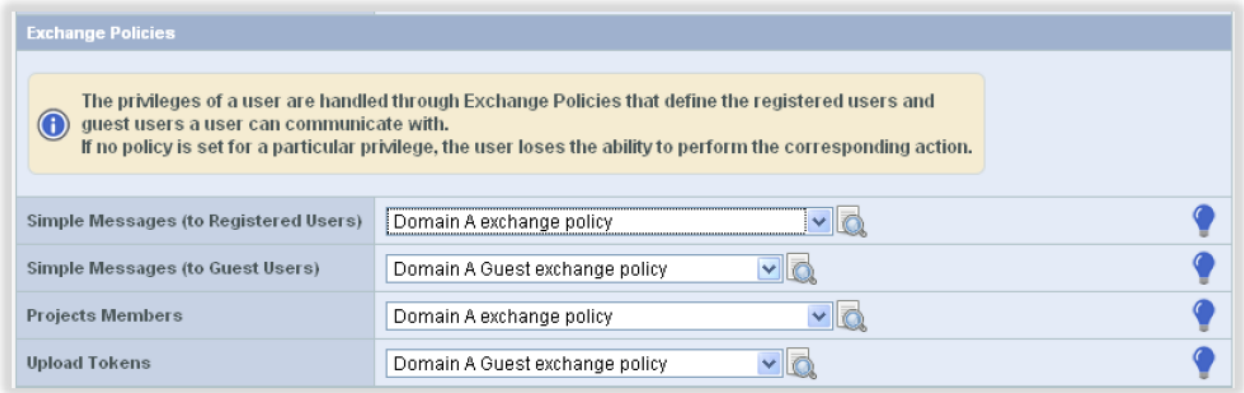
- Как быть уверенным, что внешние пользователи используют пароль, соответствующий нашим политикам?
- Как разрешить внешним пользователям обмениваться документами со всеми сотрудниками компании без предоставления им какого-либо доступа к корпоративным информационным ресурсам?
- Как организовать сквозное шифрование конфиденциальных документов (которых порядка 10%), не затрачивая ресурсы на шифрование остальных 90% передаваемых документов?

## 3.4.Контроль доступа

Контроль доступа определяет, что и как может и должен делать пользователь в контексте использования MFT при передаче и получении документов. Это включает в себя такие аспекты как:

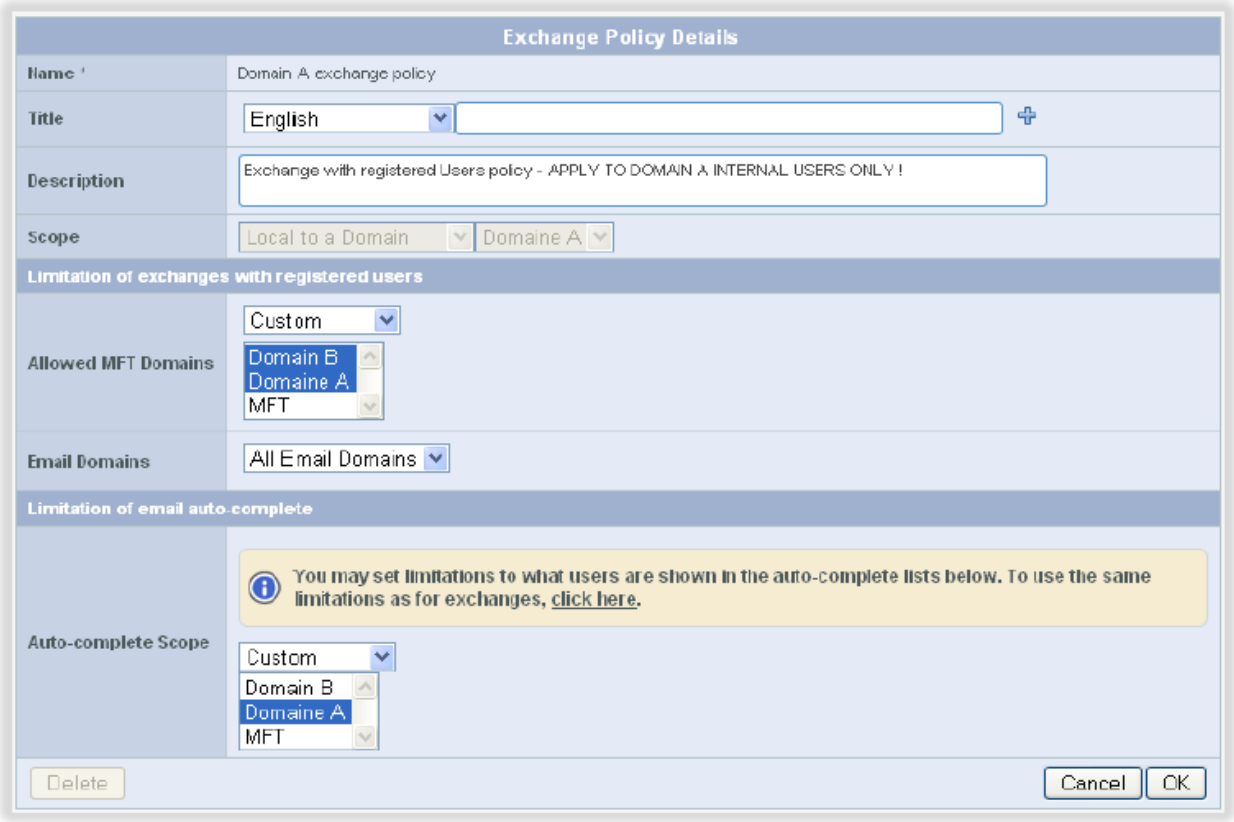
- Отправка документов зарегистрированным пользователям (разрешено, определяется политикой, запрещено)
- Отправка документов «гостевым» пользователям (разрешено, определяется политикой, запрещено)
- Создание/ удаление «проектов» определяется политикой (возможность добавлять членов различных доменов)
- Создание «жетонов» для загрузи документов «гостями» (разрешено, определяется политикой, запрещено)

Настройка этих полномочий выполняется через административный интерфейс редактированием параметров конкретного пользователя, что позволяет настраивать уникальные права доступа для каждого из них в отдельности.




MFT Admin —настройка полномочий пользователей через административный интерфейс

Пример ниже иллюстрирует прав доступа, в частности, для пользователей из домена А определяется разрешение на создание проектов, включать туда членов как домена А, так и домена В. Однако для отправки документов членам домена В необходимо указывать его адрес, так как функция автозаполнения адресов включена только для пользователей домена А.

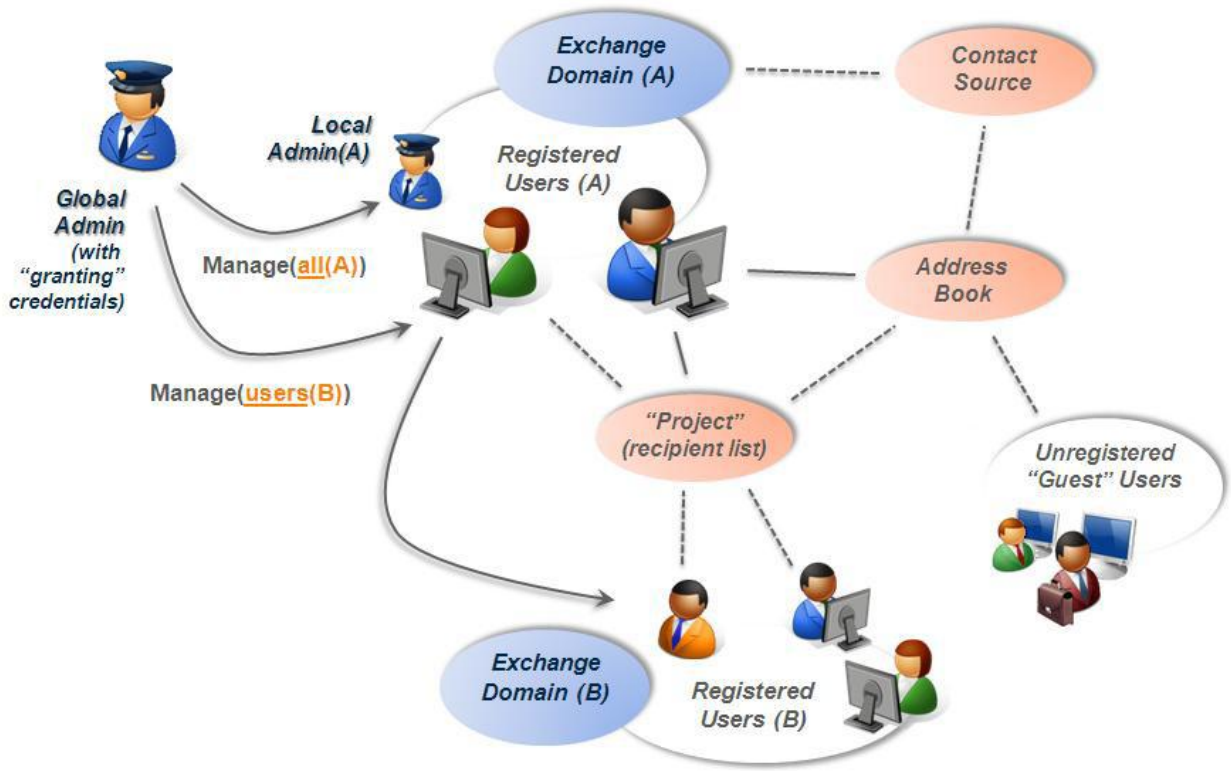



MFT Admin —редактирование доменных политик

**Управление администрированием и делегирование привилегий**

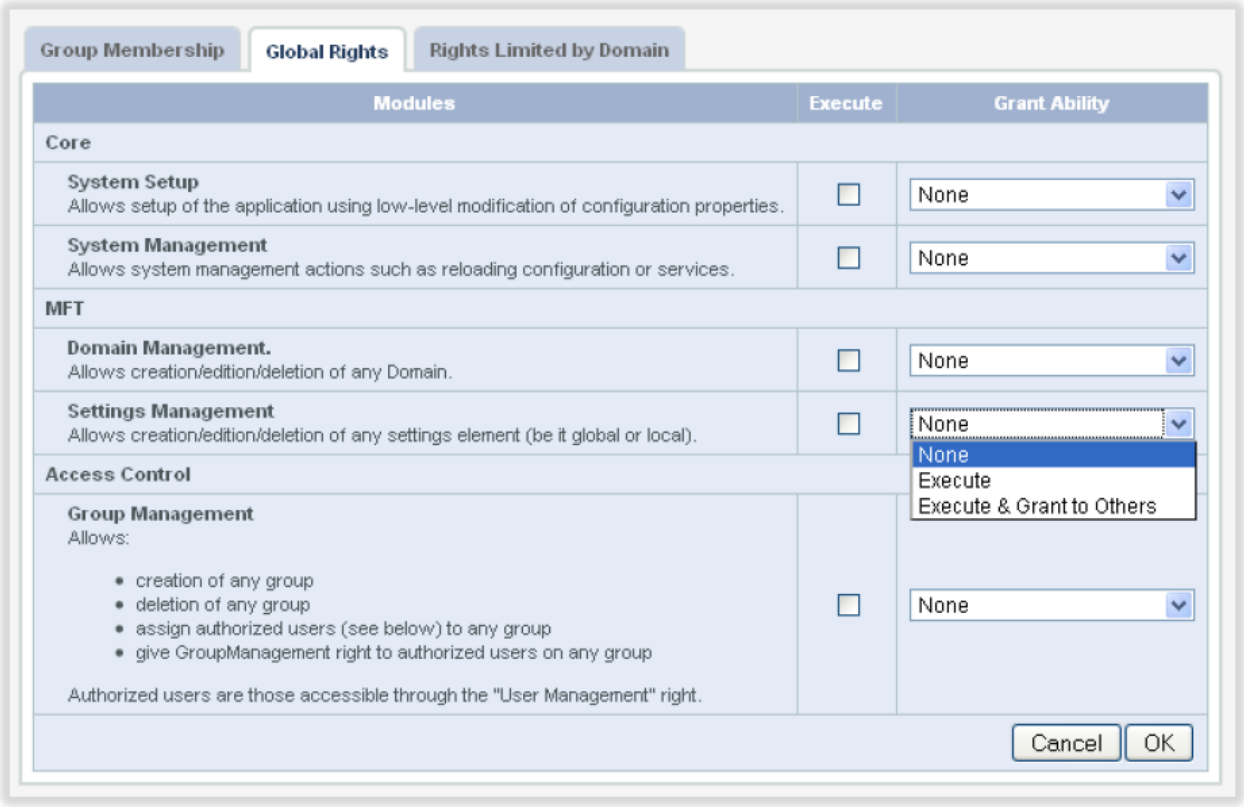
Права доступа определяются в разделе «Access Control» в административном интерфейсе. Для каждого администратора или группы администраторов можно определить разрешение на различные операции

- Глобальные права (применяемые глобально в рамках всей инсталляции MFT)
  - *Системные настройки*: низкоуровневый доступ к настройкам системы
  - *Управление системой*: перезагрузка конфигураций и сервисов
  - *Управление доменами:* создание/редактирование/удаление доменов
  - *Управление настройками:* создание/редактирование/удаление политик, как глобальных, так и локальных
- Локальные права (применяются индивидуально для каждого домена)
  - *Управление пользователями*
  - *Аудит активностей пользователей*
  - *Управление локальными настройками*
  - *Аудит лог-файлов*




Пример организации мультидоменной архитектуры с делегируемым администрированием

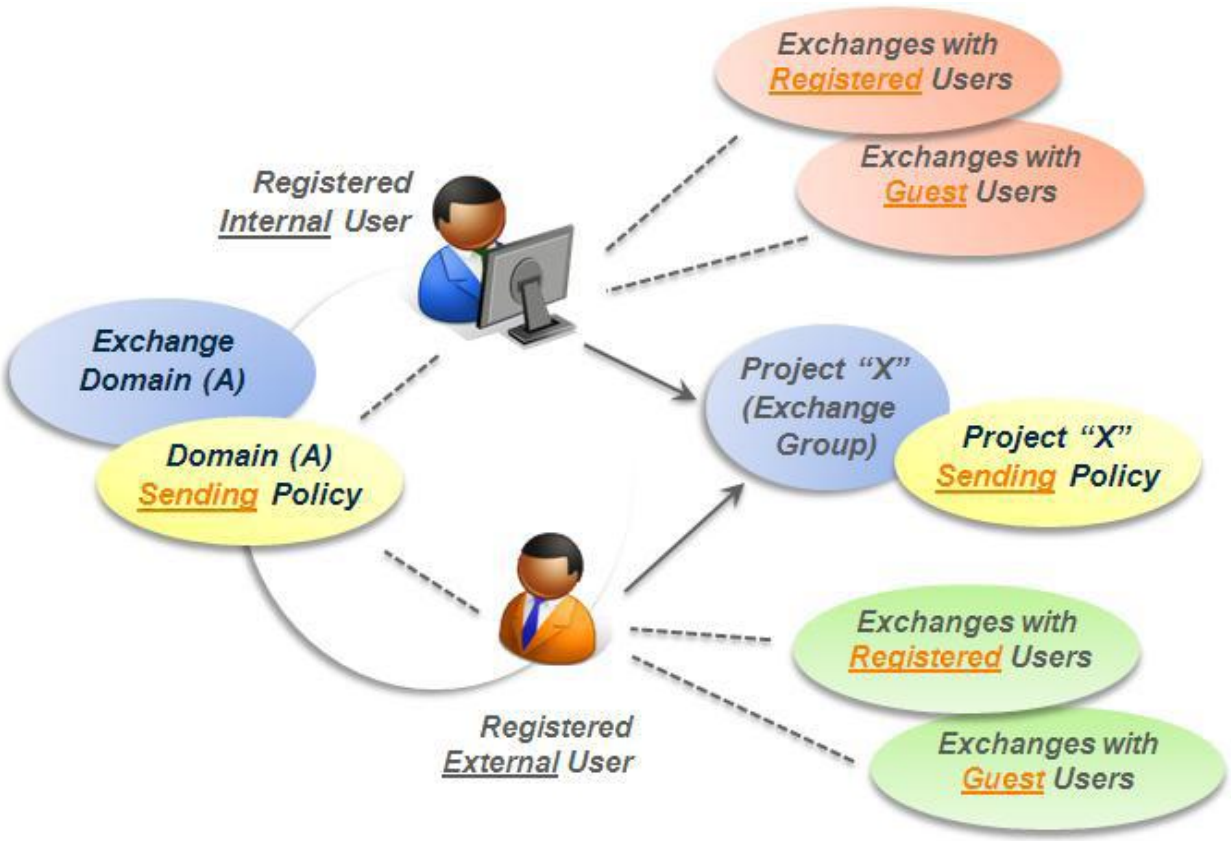
Кроме авторизации определенного администратора на выполнение определенных функций (Execute) ему может быт разрешено делегировать указанные полночи (Execute and Grand to others)



## 3.5.«Проекты»

В MFT могут создаваться группы зарегистрированных пользователей (как внутренних, так и внешних). Это позволяет упростить обмен документами среди участников такой группы, в терминологии MFT называемой «проектом».

Для каждого проекта могут быть сформированные собственные политики, что позволит учесть существующую специфику данной рабочей группы.




Пример на картинке выше иллюстрирует концепцию доменов, политик и групп в процессе обмена документами

- Политики отправки для домена А определят шифрование как опцию, в то время как политика проекта Х делает шифрование обязательным.
- Политика отправки позволяет внутренним зарегистрированным пользователям отправлять сообщения всем пользователям любых доменов и Гостям, а так же возможность создавать проекты.

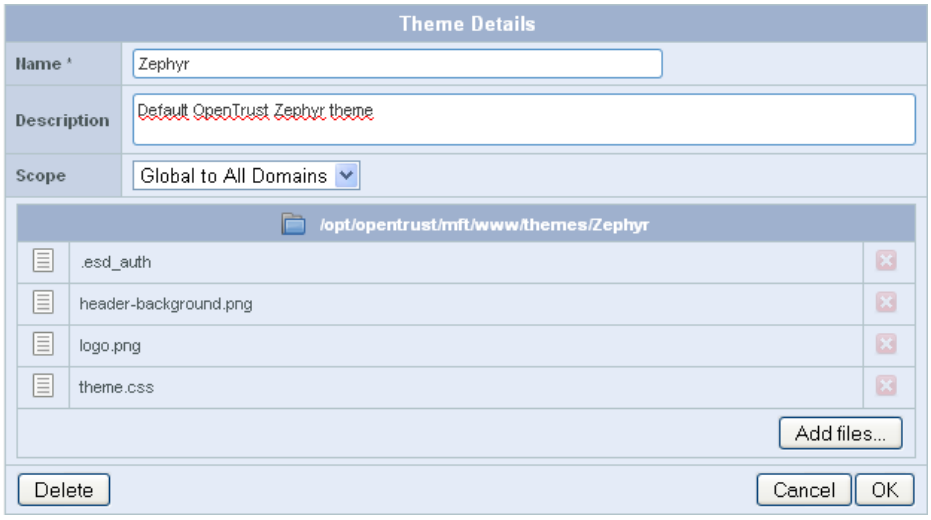
Сценарии, описанные здесь, и многие другие могут быть настроены администратором за пару кликов.

## 3.6.Источники контактов

Источники контактов это некоторая внешняя база, которая может использоваться для функции автозаполнения в процессе подготовки файлов к отправке. Обычно это используется для совместного использования зарегистрированными пользователями электронных адресов.

## 3.7.Графические Темы

Для сохранения стилистического соответствия корпоративным стандартам в MFT возможно использовать собственные «скины» с кастомизацией цветовой гаммы, шрифтов, логотипов и так далее.

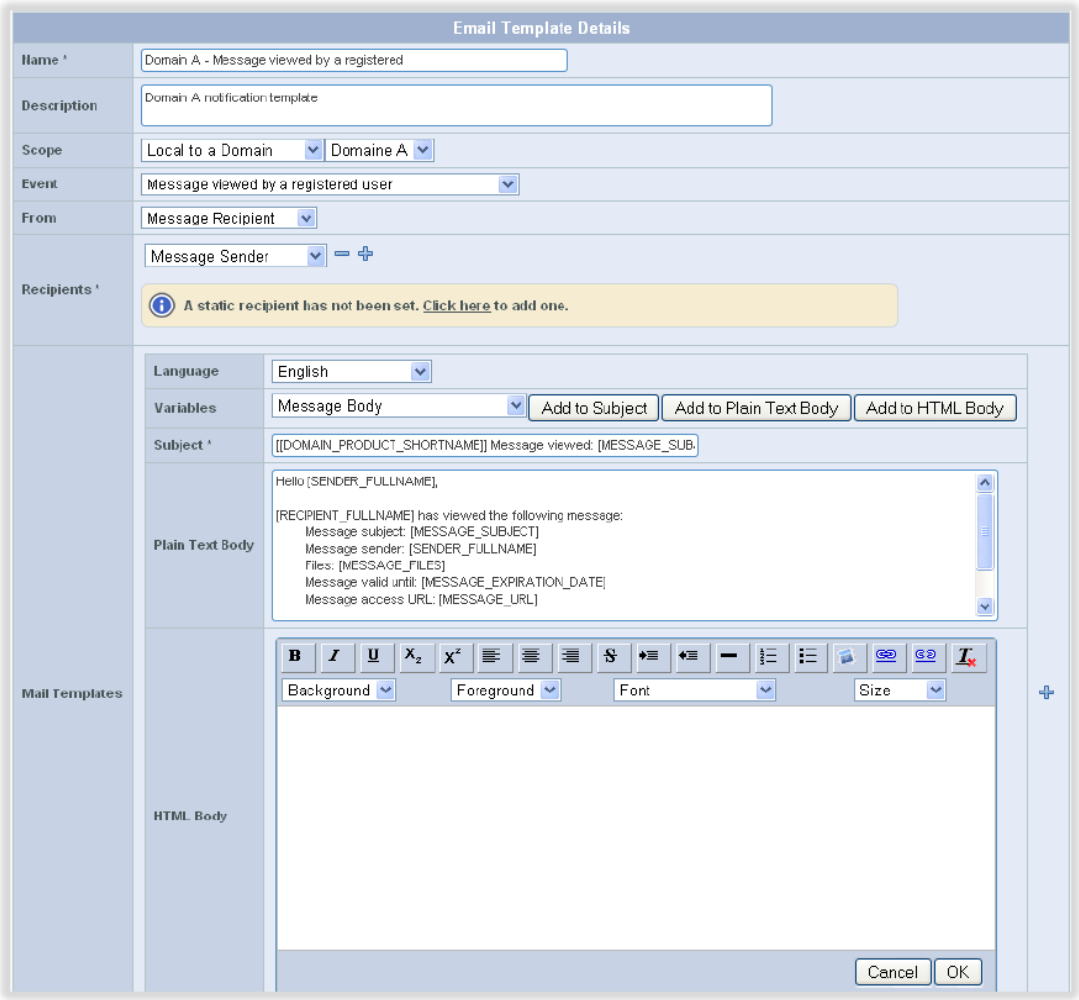



MFT Admin — редактирование графической темы

Редактирование параметров визуального отображения выполняется через административный интерфейс и может применяться для различных доменов.

## 3.8.Шаблоны уведомлений

MFT позволяет автоматически отправлять уведомления при возникновении какого-либо события. Например, если отправленный документ скачен получателем, то отправитель получит уведомление. Гибкая система шаблонов электронных писем позволяет настроить уведомления на разные события для различных групп пользователей.

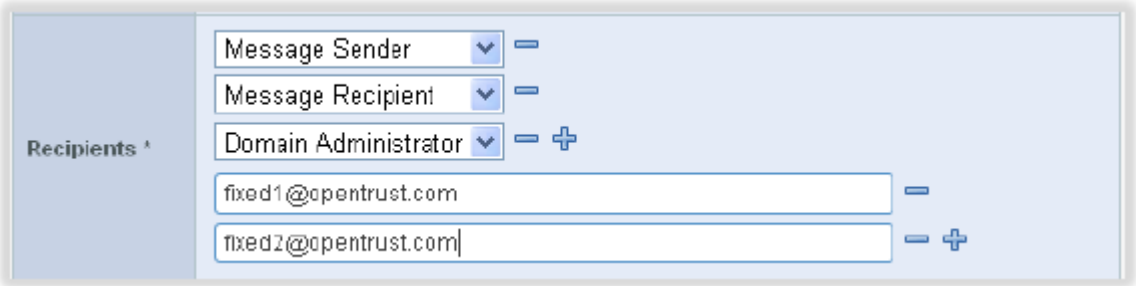



MFT Admin — редактирование дефолтных уведомлений

В дополнение к изменению текста в теле и теме письма можно использовать **динамический контент (переменные, связанные с определенными событиями)**.

В примере показано изменение таких аспектов как:

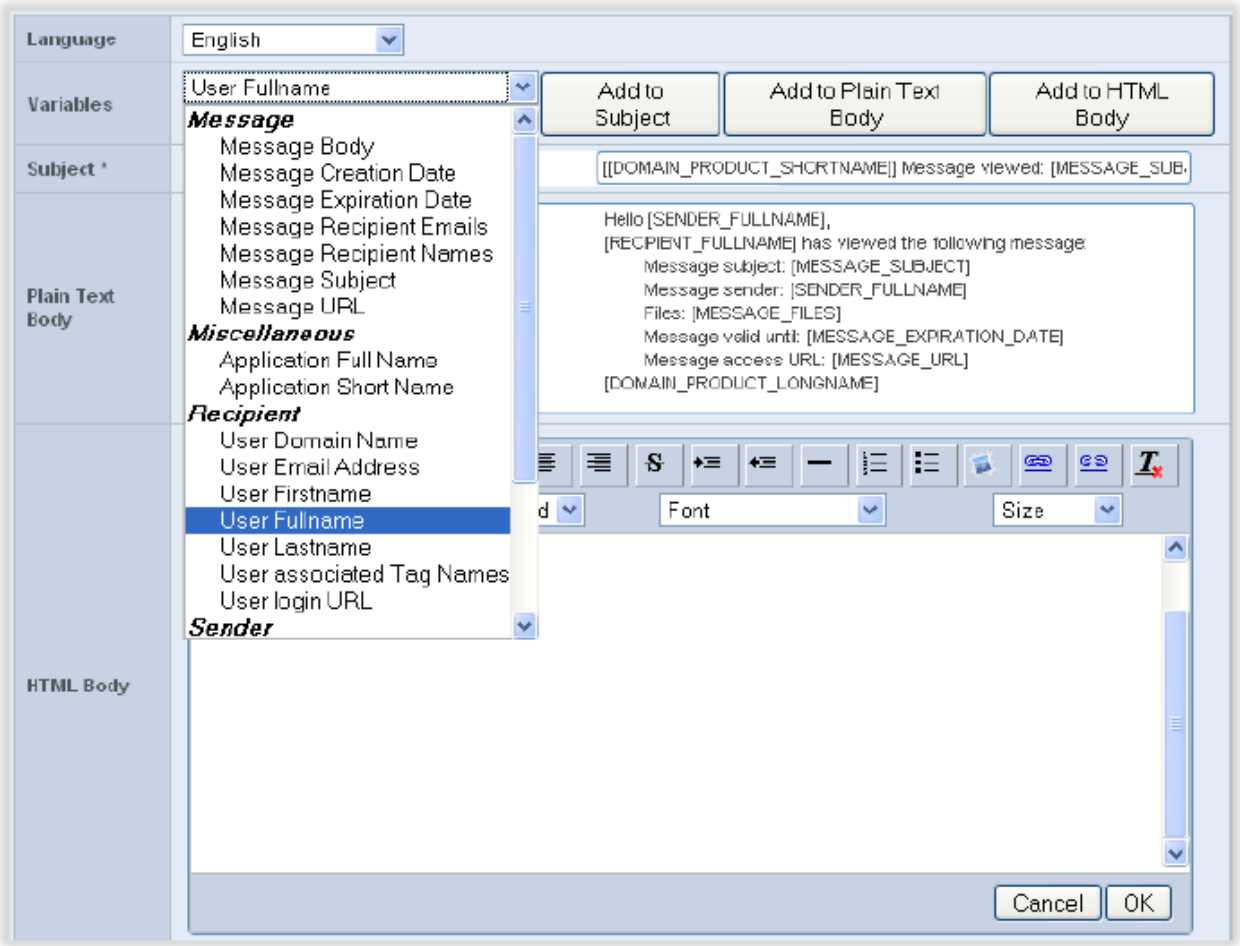
- Границы применения: глобальное или для определенного домена.
- Тип события, для которого выполняется это уведомление.
- Отправитель сообщения.
- Получатель уведомления. Кнопки +/- позволяют динамически (в зависимости от контекста) и статически (не зависит от контекста) добавлять адреса получателей, как показано на иллюстрации ниже.




MFT Admin — шаблон сообщения с тремя динамическими и двумя статическим получателями

- Контетн сообщения  может быть представлен на нескольких языках (кнопки +/- позволяют добавлять языковые версии). Каждый языковой вариант обладает следующими характеристиками:
  - *Язык: позволяет определить, на каком языке отправить уведомление пользователю в зависимости от его зарегистрированного языка*
  - *Тема: определят содержание поля «тема»*
  - *Тело: определяет содержания тела письма*

В процессе подготовки или редактирования шаблона довольно просто использовать данные о событии, например: дату скачивания, названия файлов, получатель и так далее — соответствующие  переменные можно просто вставлять из выпадающего списка в нужные вам места шаблона сообщения.



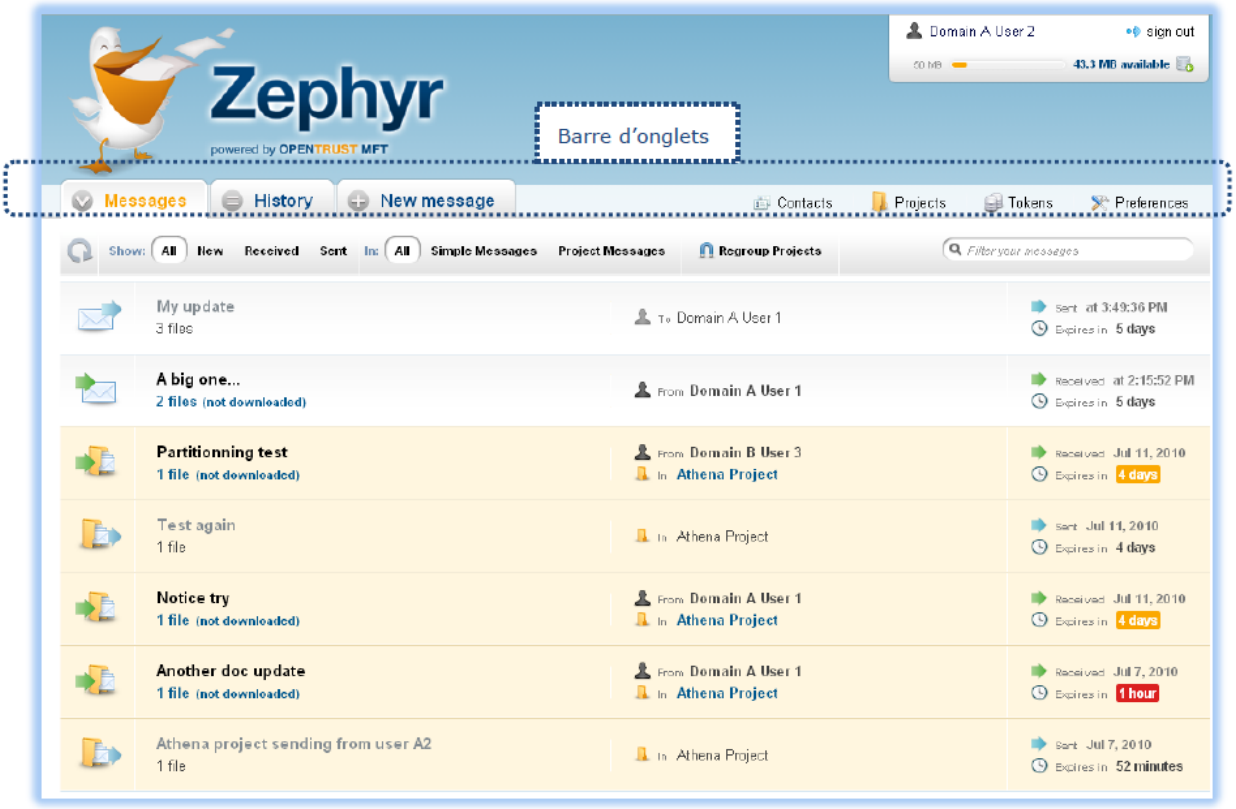

MFT Admin — использование переменных при подготовке шаблона сообщения

# 4. Простота и интуитивность работы пользователя

Понятно, что простота ввода в эксплуатацию — важный аспект применимости выбираемого решения, но внедрение — однократный процесс, в то же время простота администрирования позволят снизить нагрузку на администраторов системы, но и это не столь принципиально, так как администрированием может заниматься пусть и высококлассный специалист, но один. Самое главное в решениях такого рода — это понятность пользовательского интерфейса и простота выполняемых конечным пользователем действий. Именно их — конечных пользователей, подавляющее большинство и именно на них ориентирована система, поэтому при разработке MFT уделялось большое внимание максимальной простоте и очевидности действий, которые необходимо выполнить пользователю в процессе отправки или получения документов.

## 4.1.Оптимизация с использованием GWT™

Для упрощения пользовательского интерфейса используется технология Google Web Toolkit™ (GWT). Закладки, кнопки и графические компоненты позволяют выполнить требуемую операцию в один клик и не требуют специальной подготовки пользователя. Основной принцип: одна функция — одна закладка, доступная все время через соответствующую панель.




MFT Zephyr — закладка сообщения

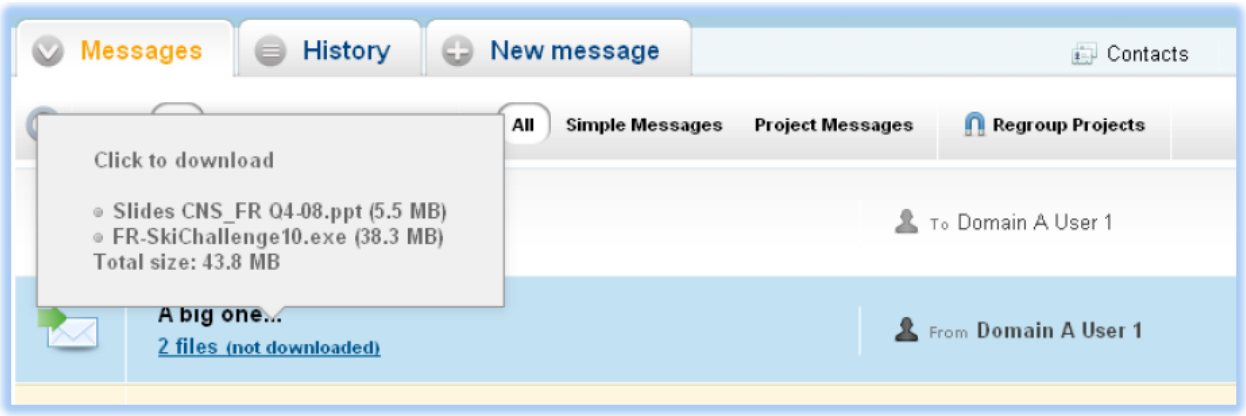
Интерфейс MFT Zephyr так же используют технологии динамических представлений GWT (подсказки и советы, возникающие при наведении мыши на кнопки, поля ввода и прочие активные элементы). Интерфейс может быть представлен на нужном языке в формате UTF-8. OpenTrust MFT уже содержит локализации на такие языки как: русский, французский, английский,

немецкий т п.д. Между прочим, язык интерфейса определяется автоматически по настройкам браузера пользователя, а при необходимости может быть изменен на требуемый.

Пример использования русского вариант интерфейса

## 4.2.Просмотр сообщений и Поиск

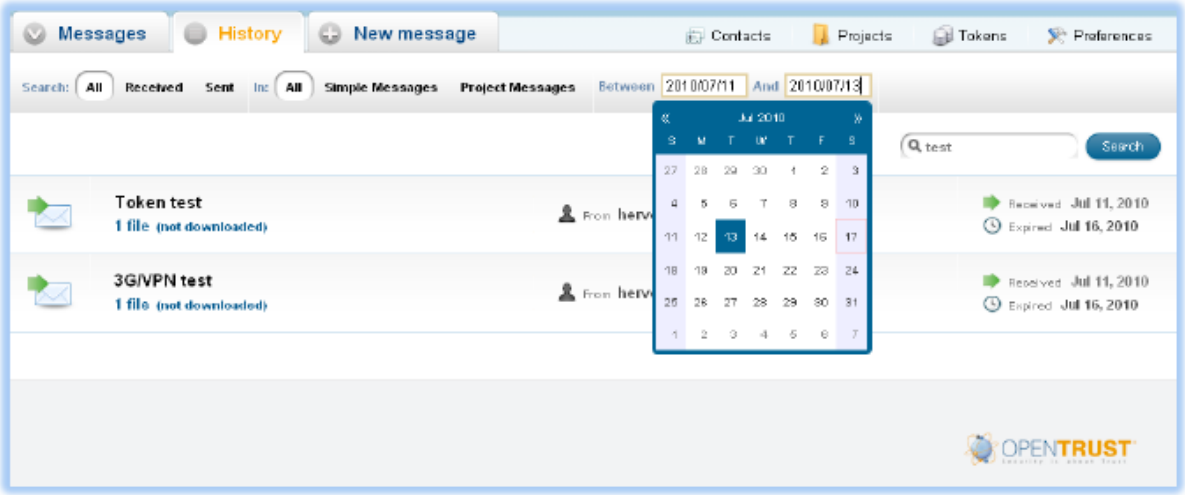
Закладка «Сообщения» отображает все, что связано с обменом документами. Фильтр позволяет отображать сообщения, отсортированные по определенному статусу (все, новые, отправленные, полученные и т.д.) и/или типу сообщения (простые сообщения или «проектные»). Так же доступен поиск по названию или части названия.




Пример подсказки, отображающий параметры документа

## 4.3.История

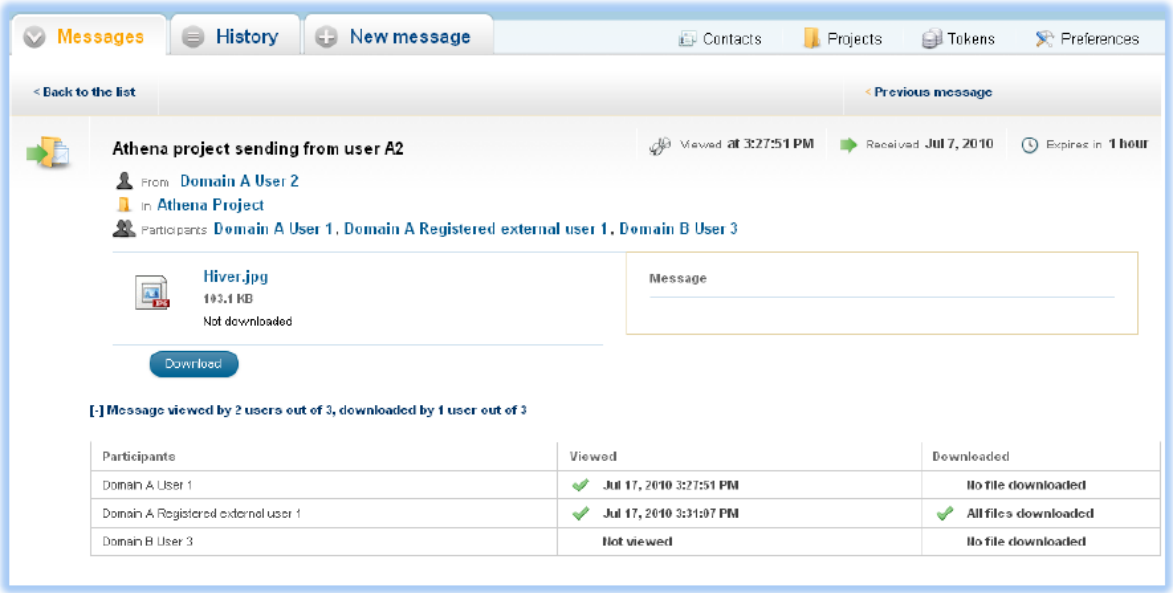
Закладка «История» отображает все текущие и «просроченные» документы. Отображение похоже на закладку «Сообщения» и позволяет выполнять фильтрацию по различным параметрам.




Закладка «История»: отображение результатов поиска по ключевому слову «test» при условии, что истечения срока будет в указанных границах

## 4.4.Свойства сообщений

Щелчком мыши по сообщению в закладках «Сообщения» или «История» открывается выбранное сообщение, с детализацией всех параметров и историй скачивания.



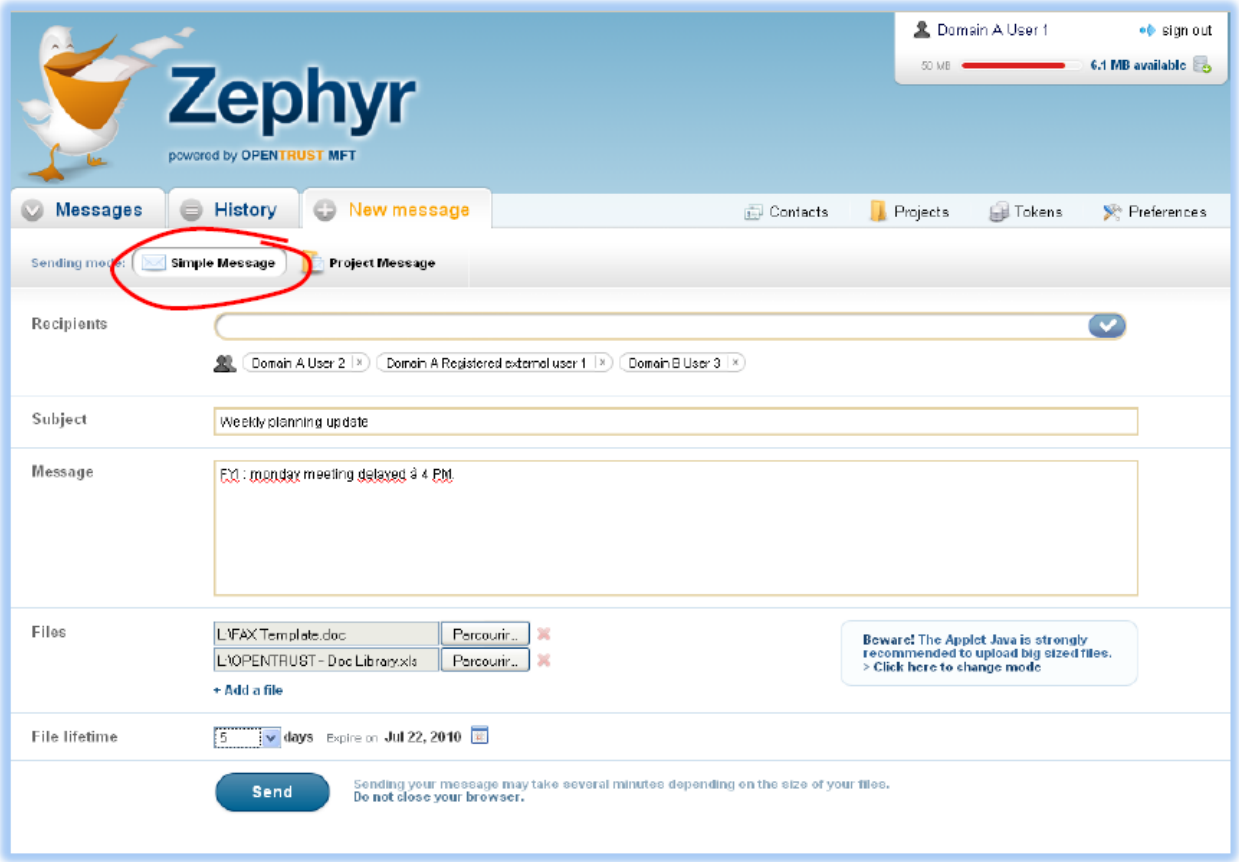

## 4.5.Отправка файлов и документов

Существует два варианта отправки документов:

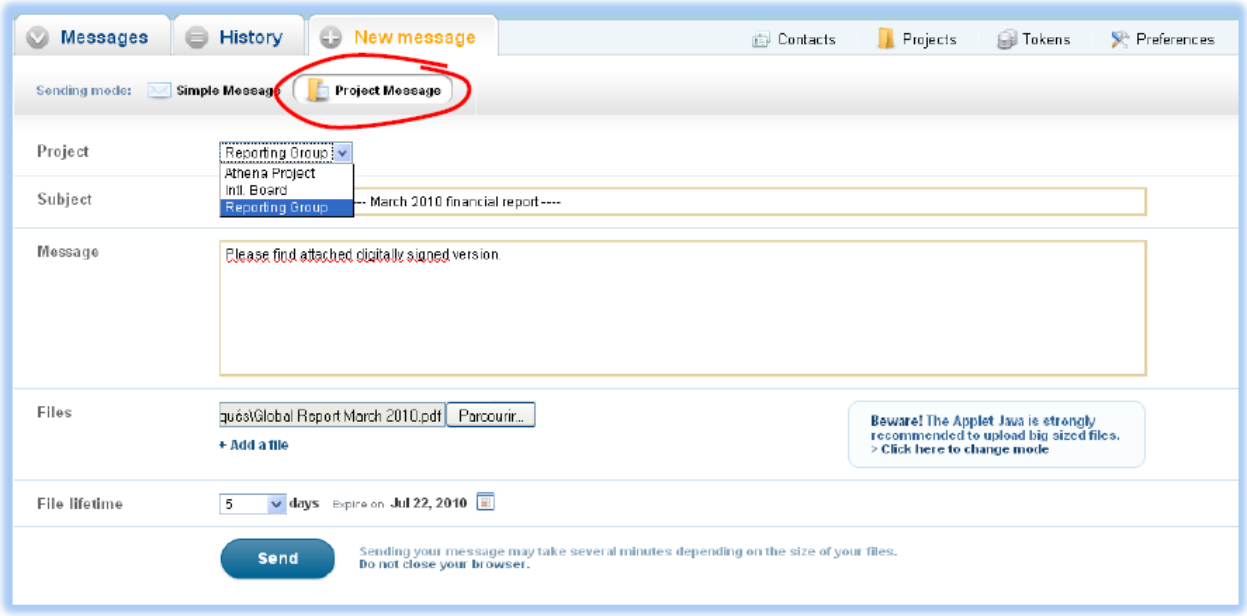
- Простая отправка, при которой список получателей формируется отправителем, при этом понятно, возможно использовать функцию автозаполнения и пользоваться адресной книгой.
- Групповая отправка (или отправка членам проекта), при которой список получателей формируется автоматически из членов выбранного проекта.

Кнопка «Новое сообщение» открывает окно, в котором выполняется настройка параметров отправления, среди которых:

- Тип отправки: простой или групповой (проектный)
- Тема отправки
- Тело сообщения, где можно написать различные комментарии (фактически электронное письмо)
- Перечень отправляемых документов
- Срок жизни файлов (длительность в днях или указание даты, до который документы будут храниться на сервере и могут быть скачены получателями)
- Пароль шифрования
- Архивирование файлов при истечении срока их жизни



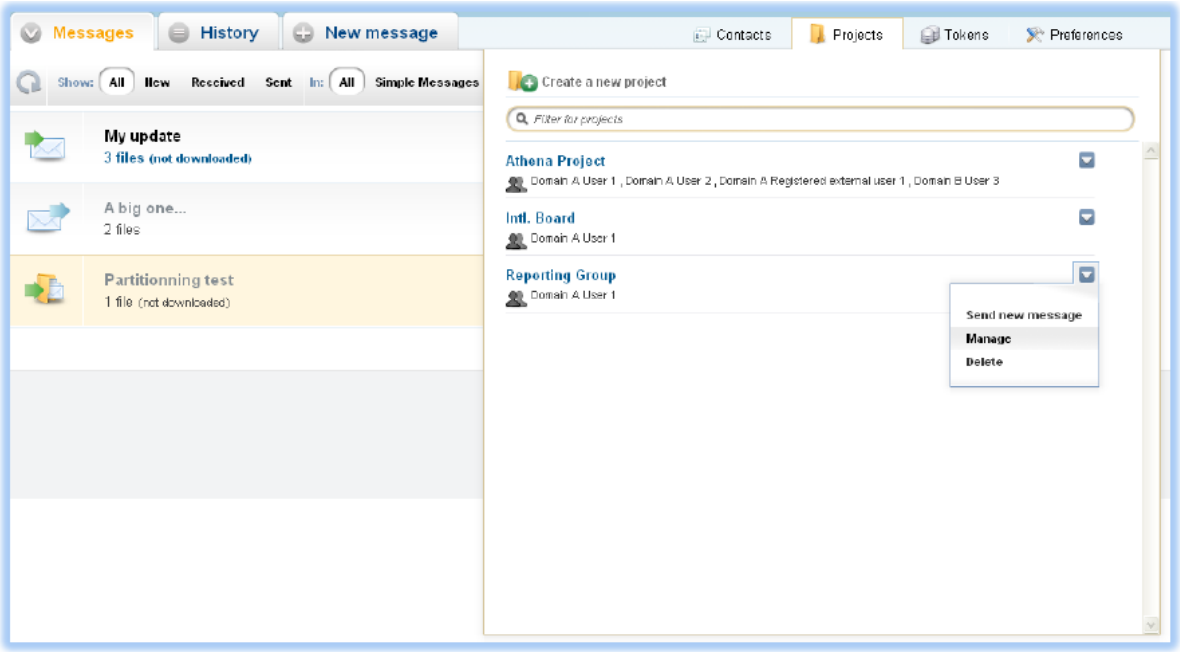

Простая отправка




Групповая (проектная) отправка

## 4.6.Управление проектами

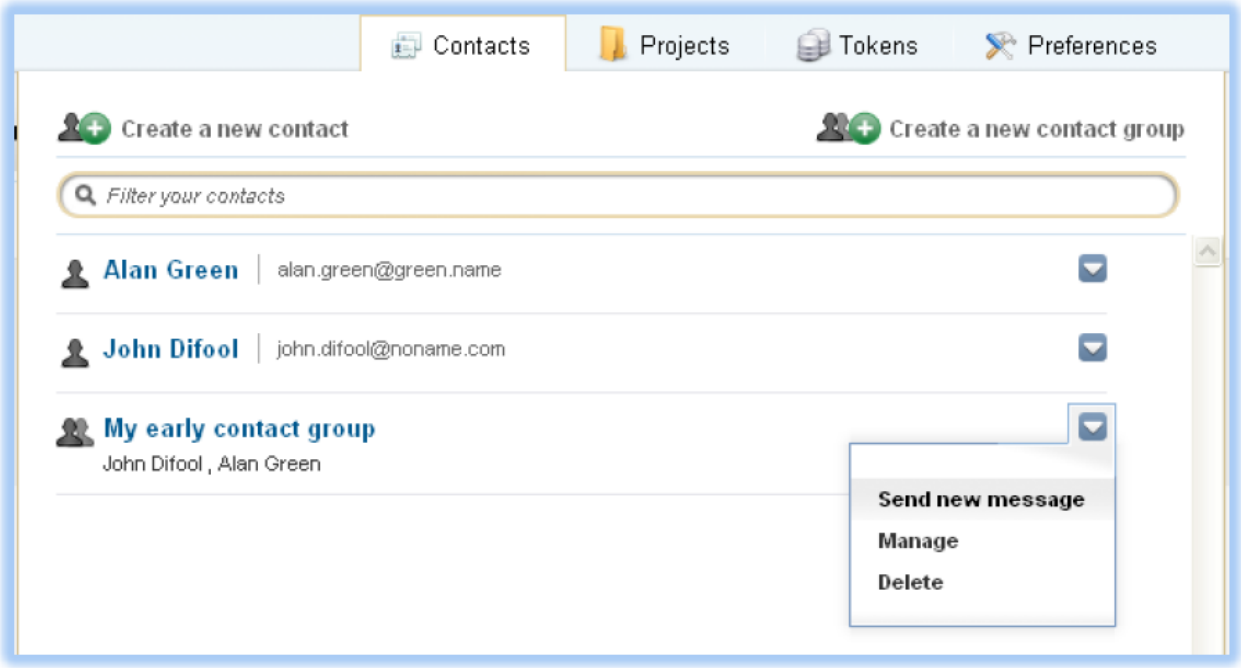
Если пользователю разрешено создавать проекты, в его кабинете будет доступна соответствующая закладка «Проекты», где пользователь может создавать проекты и группировать тем самым получателей, используя как встроенную адресную книгу, так и добавляя новых получателей вручную.




Создав один раз проект, пользователь может быстро и просто отправить нужные документы всем его участникам, исключив составление перечня получателей каждый раз. Такой подход очень удобен в том случае, когда пользователь оправляется постоянной группе пользователей документы на регулярной основе. При необходимости для каждого проекта можно указать специфическую политику отправки, учитывая таким образов специфику каждой группы.

## 4.7.Управление контактами

Данные о гостевых пользователях могут храниться в локальной адресной книге. При первой отправке документов гостевым пользователям (не зарегистрированным в MFT) их адреса автоматически сохраняются в локальной адресной книге и могут в дальнейшем использоваться при автозаполнении (при необходимости этот функционал можно выключить в разделе «Настройки»)



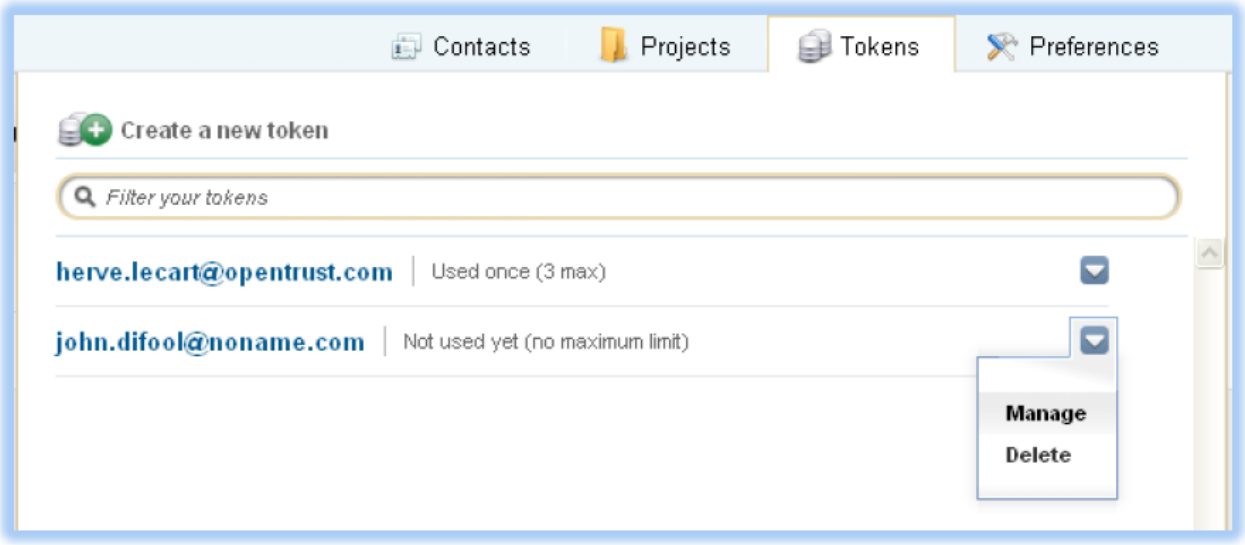

Управление Контактами

В дополнение к этому пользователь может вручную формировать собственную адресную книгу, добавляю новых получателей к тем, которые были импортированы из корпоративной службы каталогов или автоматически сохранены в процессе  отправки документов.

## 4.8.Жетоны

Каждый пользователь MFT может отправлять документы другим пользователя и любым другим коллегам, контрагентам и так далее — всем тем, кто не имеет учетной записи в MFT. Если же возникает обратная задача: пользователь MFT должен получить документы от внесшего незарегистрированного пользователя, который не имеет учетной записи в системе? Для решения этой задачи можно создать так называемый Жетон.

Жетон — это фактически приглашение, которое  отсылается  на указанный адрес. Получая такое приглашение  внешний отправитель просто переходит по уникальной ссылке и используя интерфейс MFT, ограниченный по функционалу, загружает требуемые документы. После этого пользователь, создавший Жетон получит уведомление по электронной почте и том, что для него выполнена загрузка документов.

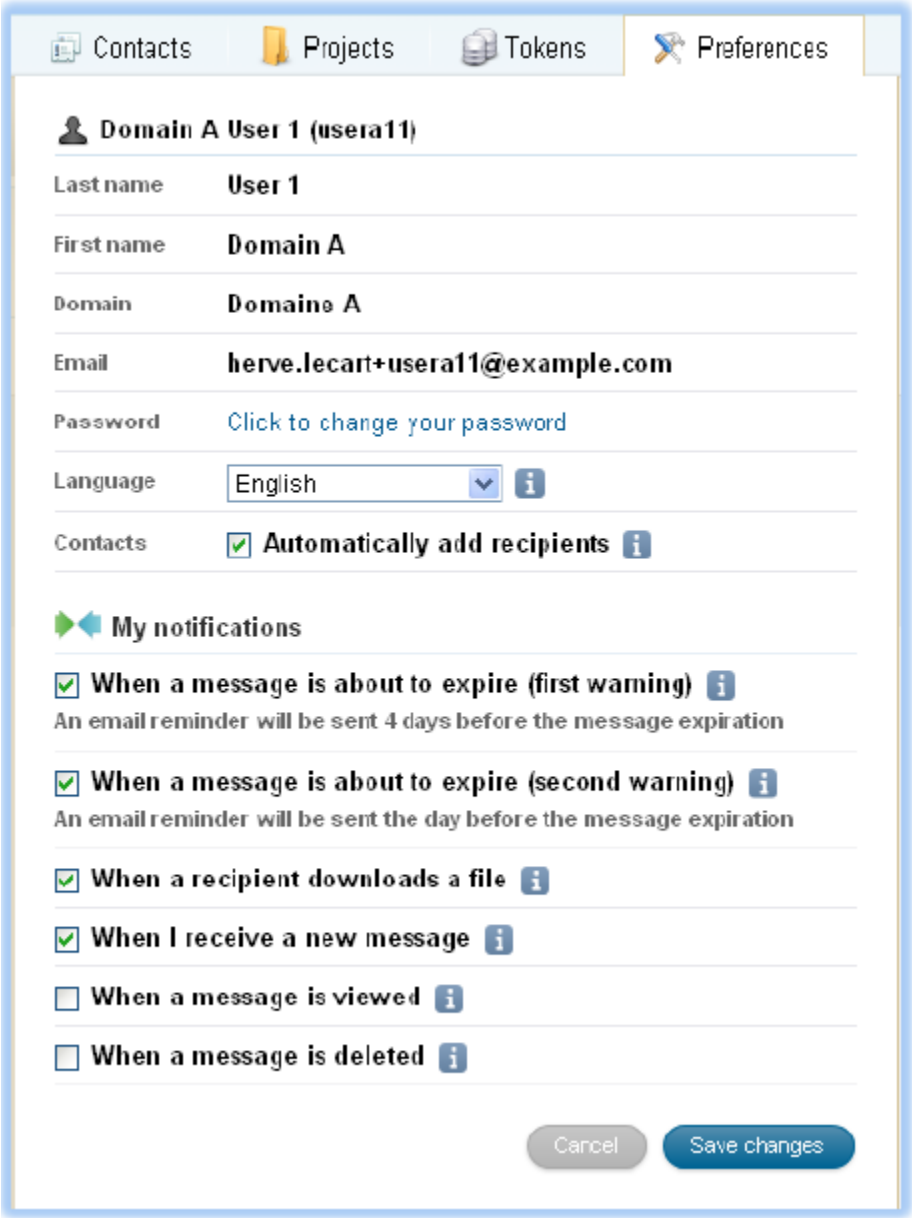



В процессе создания Жетона пользователь может указать следующие параметры:

- Время жизни Жетона
- Количество сообщений (загрузок) которое можно выполнить, используя этот Жетон
- Общая квота на дисковое пространство

## 4.9.Параметры пользователей

Пользователям доступно редактирования параметров, для настраивания, например, параметров уведомлений, предпочтительный язык и прочее



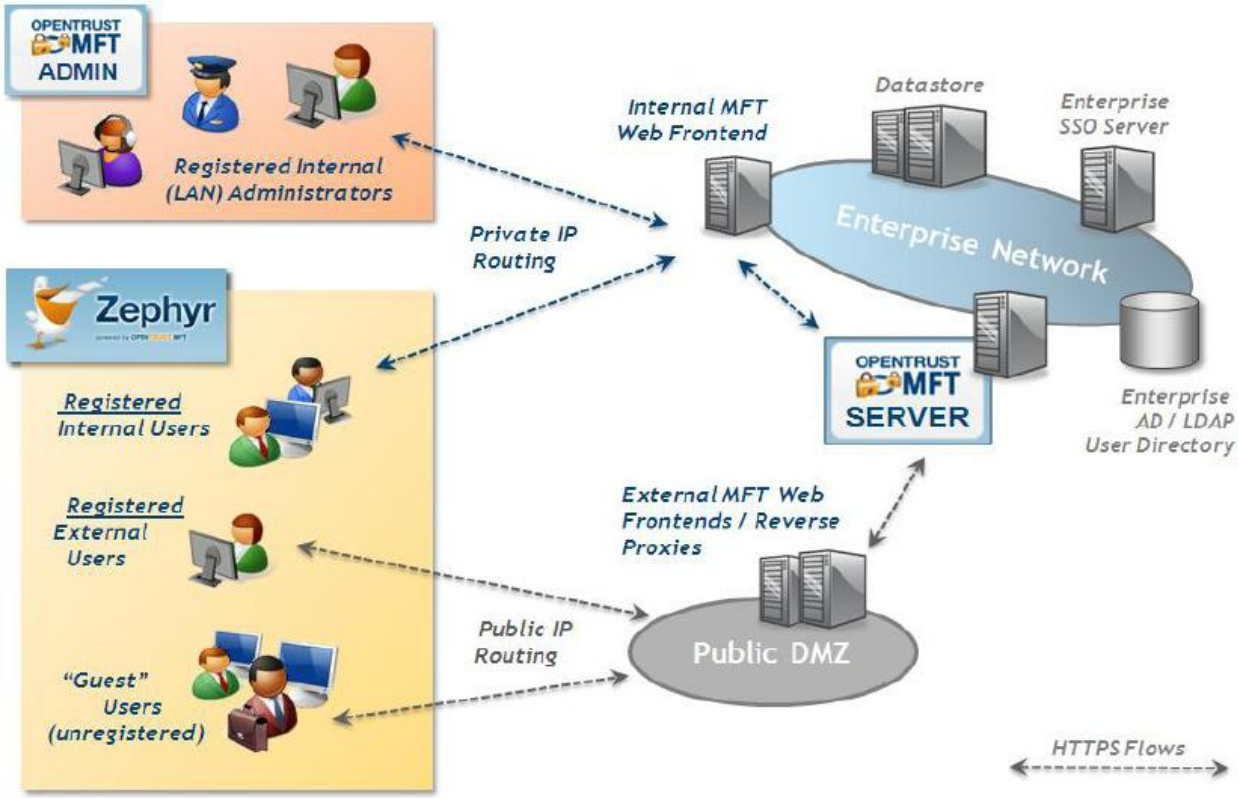

Закладка «Параметры»

# 5. Оптимизированная программная архитектура

OpenTrust MFT спроектировано в модульной архитектуре, что позволяет адаптироваться к требованиях заказчика и учитывать различные аспекты (качество обслуживания и отказоустойчивость, архитектура, сетевая организация и т.д.).

OpenTrust MFT реализует два независимых web-приложения:

- **MFT Admin**: административный интерфейс (управление пользователями и правами доступа, настройка системы)
- **MFT Zephyr**: пользовательский интерфейс




Пример архитектуры

На примере, показанном выше, модуль администрирования MFT Admin доступен только изнутри сети компании, доступ извне (из публичных сетей) запрещен. При этом доступ к пользовательскому интерфейсу MFT Zephyr разрешен как изнутри так и снаружи. В зависимости от требований к QoS/доступности сервиса, модули MFT могут работать параллельно на нескольких серверах (физических или виртуальных) в режиме актив-актив, в том числе для балансировки нагрузки.