



CROCOTIME

Интеграция CrocoTime Server
с Microsoft Active Directory
(0.0.32)

Описание возможностей	3
1. Установка и настройка подключения к Active Directory	4
2. Настройка интеграции CrocoTime с Active Directory	6
2.1 Настройка соединения с Active Directory (обязательно)	6
2.2 Проверка соединения с Active Directory	7
2.3 Настройка синхронизации организационной структуры	8
2.4 Настройка задержки при синхронизации нового сотрудника	8
2.5 Настройка импорта отчетов	8
2.6 Настройка синхронизации статуса “включен\выключен” сотрудника	9
2.7 Настройка частоты синхронизации данных с Active Directory	10
2.8 Настройка импорта руководителя	10
2.9 Настройка объединения возникших дубликатов сотрудников в Crocotime	11
2.10 Разовый запрос на изменение часовых поясов в CrocoTime для сотрудников синхронизируемых с AD	12
2.11 Разовый запрос на включение сотрудников связанных с AD у которых в атрибуте присутствует допустимое одиночное, строковое значение	12
2.12 Разовый запрос на удаление руководителей у всех сотрудников	12
2.13 Разовый запрос на отключение сотрудников, не входящих в синхронизируемые объекты AD	13
3. Получение текущих настроек интеграции с AD	14
4. Частые вопросы	15

Описание возможностей

Актуальная интеграция CrocoTime Server с AD выполнена в виде отдельного приложения, которое выполняет функцию автоматического наполнения CrocoTime данными о сотрудниках.

Возможности интеграции:

- Автоматическое создание профилей сотрудников в Crocotime для каждой включенной уч. записи AD в указанных подразделениях (OU) или универсальных группах безопасности (Universal Security Group);
- Заполнение атрибутов "Фамилия" и "Имя" в профиле сотрудника в Crocotime на основании соответствующих атрибутов из AD. Отдельно можно настроить импорт отчества основываясь на атрибуте "DisplayName" (п.4);
- Заполнение атрибута "E-mail" в профиле сотрудника в Crocotime на основании соответствующего атрибута в AD;
- Заполнение атрибута "Должность" в профиле сотрудника в Crocotime из соответствующего атрибута (title) учетной записи в AD;
- Заполнение атрибута "Руководитель" в профиле сотрудника в Crocotime на основании соответствующего атрибута (manager) учетной записи сотрудника в AD (п. 7);
- Управление статусом "Включено/Отключено" профиля сотрудника в Crocotime на основании статуса соответствующей уч. записи AD (п. 5);
- Построение структуры групп сотрудников в CrocoTime на основе структуры подразделений (OU) в AD (п. 2).

Обратите внимание, что установка интеграции не является обязательным условием для работы аутентификации в веб-интерфейсе CrocoTime при помощи AD (SSO). Для того, чтобы пользователь мог войти в Crocotime используя аутентификацию через AD, должны быть выполнены следующие условия:

- На Crocotime Server в меню "Конфигурация" > "Авторизация" включено "Авторизация через AD";
- В профиле сотрудника во вкладке "Источники" есть запись, соответствующая доменной учетной записи сотрудника (Источник автоматически добавляется при установке агента на компьютер сотрудника или при интеграции CrocoTime с AD);
- CrocoTime Server должен быть установлен на компьютере входящим в домен (или доверенный домен) и служба сервера должна запускаться от имени System (настраивается по умолчанию при установке).

При этом настройка интеграции Crocotime с AD не является обязательным условием, но упрощает задачу заполнения нужных полей в профиле сотрудника.

1. Установка и настройка подключения к Active Directory

Шаг 1. Подготовка резервной копии Crocotime Server перед установкой интеграции

Этот шаг можно пропустить, если Вы только начинаете использовать CrocoTime и потеря данных, в случае непредвиденной ситуации, не критична.

- Перейдите в веб-интерфейс CrocoTime Server с правами администратора системы. Откройте "Конфигурация > Шифрование" и измените порт на котором работает CrocoTime Server на произвольный, отличный от рабочего. Это нужно, чтобы на время производимых операций агенты CrocoTime не могли передать данные на сервер и хранили их локально. Если понадобится выполнить откат системы на резервную копию, эти данные не будут потеряны т.к. временно хранились на агентах;
- Дождитесь, когда CrocoTime Server будет запущен на новом порту;
- Перейдите в оснастку "Службы" операционной системы (Win+R > введите services.msc > ОК);
- Остановите службу Crocotime Server;
- Перейдите в каталог "%ProgramData%\CrocoTime Server\DataBases";
- Создайте копию каталога "crocotime" в надежном месте, это каталог БД.

Шаг 2. Установка и настройка универсальной платформы Subsystems

- Включите службу CrocoTime Server;
- Установите интеграционную платформу с помощью файла setup-subsystems-x.x.x.exe;
- Авторизуйтесь в веб-интерфейсе Crocotime Server под администратором системы;
- Перейдите во вкладку "Конфигурация" > "Токены доступа". Введите в пустое поле произвольное имя для токена. Нажмите "Сохранить";
- Повторно зайдите в "Токены доступа" и скопируйте сформированный токен;
- Откройте файл "%Program Files%\Subsystems\config.json" с помощью блокнота запущенного от имени администратора;

В поле "url" укажите url-адрес Crocotime Server (если выполнялся первый шаг, помните, что порт приложения изменен);

- В поле "token" укажите сгенерированный токен доступа;
- Для безопасности в поле "host" можно указать значение "127.0.0.1", в этом случае веб-интерфейс настройки интеграции будет доступен только локально. "0.0.0.0" - означает, что доступ возможен с любого узла сети;
- После поля "port" укажите через запятую "web.path":"C:\\Program Files\\CrocoTime Server\\system\\modules\\web\\script";
- Сохраните файл.

Пример готового файла ниже.

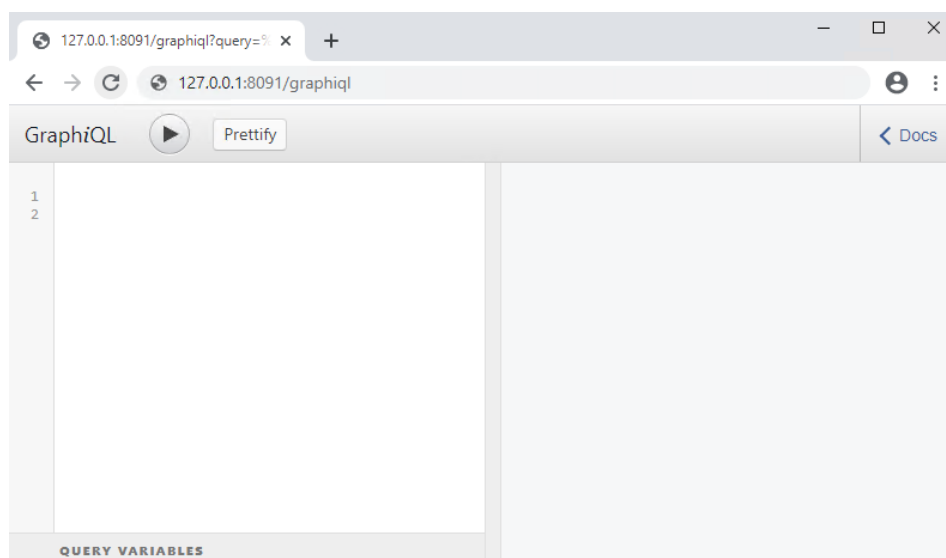
```
{
  "subsystems": {
    "com.infomaximum.subsystem.frontend":{
      "host":"127.0.0.1",
      "port":8091,
      "web.path":"C:\\Program Files\\CrocoTime Server\\system\\modules\\web\\script"
    },
    "com.infomaximum.crocotime":{
      "url":"http://127.0.0.1:8085",
      "token":"027952686c460dad145d9560d6e8e648d6988444164625712f28c19488c737d3"
    }
  }
}
```

Шаг 3. Установка модуля интеграции с Active Directory

- Скопируйте файл **"active-directory.jar"** в каталог **"%Program Files%\Subsystems\bin\jar\"**.

Шаг 4. Запуск службы и вход в интерфейс настройки

- Откройте оснастку "Службы" операционной системы. Запустите службу Subsystem Platform;
- В браузере откройте страницу **"http://<адрес Crocotime Server>:8091/"**. Введите логин и пароль администратора системы Crocotime;
- После успешного входа в Crocotime перейдите на страницу **"http://<адрес Crocotime Server>:8091/graphiql"**. Откроется интерфейс настройки интеграции.



Шаг 5. Настройка интеграции

- Далее необходимо выполнить настройку интеграции под Ваши задачи. Описание настроек приведено в следующем разделе документации;
- После успешной настройки, если выполнялась смена порта приложения в шаге 1, измените порт обратно на рабочий в настройках CrocoTime Server и в файле **"%Program Files%\Subsystems\config.json"**. Перезапустите службу Subsystem Platform.

2. Настройка интеграции CrocoTime с Active Directory

Настройка интеграции происходит при помощи текстовых запросов определенного синтаксиса на странице "http://<адрес Crocotime Server>:8091/graphiql".

Для выполнения запроса используйте кнопку  в верхней области страницы

2.1 Настройка соединения с Active Directory (обязательно)

Для настройки соединения с Active Directory выполните следующий запрос:

```
mutation {
  app_config {
    active_directory {
      update_active_directory_config(
        domain_controller_host: "192.168.123.1",
        login: "username@some.domain",
        password: "Qwerty123"
        domain_paths: [
          "OU=Department1,DC=some,DC=domain",
          "OU=Department2,DC=some,DC=domain",
          "CN=Group1,OU=Department3,DC=some,DC=domain",
          "CN=Group2,OU=Department4,DC=some,DC=domain",
        ]
      ) {
        domain_controller_host
        login
        has_password
        domain_paths
      }
    }
  }
}
```

Где,

- *domain_controller_host* – адрес контроллера домена с которым будет происходить синхронизация;
- *domain_paths* – distinguished name подразделений (OU) или универсальных групп безопасности в Active Directory из которых необходимо синхронизировать сотрудников;

Дочерние объекты также будут синхронизироваться, поэтому не нужно указывать дочерние OU или группы, если в список уже добавлен родительский объект. Это может привести к некорректной работе интеграции.

- *login* – логин пользователя AD, который будет использоваться для соединения интеграции с доменом (Необходимы только права на чтение каталога. Достаточно “Обычного пользователя”);

- *password* – пароль пользователя AD.

После выполнения запроса, при следующей синхронизации с доменом (по умолчанию, раз в 15 минут), в CrocoTime Server в корень списка сотрудников будут добавлены все включенные сотрудники из указанных OU и групп AD. Те сотрудники, чьи профили уже появились в CrocoTime ранее при установке агента, будут обновлены.

Для того, чтобы ускорить вступление изменений в силу, можно выполнить перезапуск службы Subsystems Platform. Синхронизация с доменом начнется сразу после перезапуска.

Чтобы добавить новый OU или группу в конфигурацию, выполните запрос:

```
mutation{
  app_config{
    active_directory{
      update_domain_path(path: "OU=Department4,DC=some,DC=domain")
    }
  }
}
```

Для удаления одного объекта синхронизации:

```
mutation{
  app_config{
    active_directory{
      remove_domain_path(path: "OU=Department4,DC=some,DC=domain")
    }
  }
}
```

2.2 Проверка соединения с Active Directory

Для проверки того, что соединение с Active Directory настроено успешно выполните запрос:

```
query
{
  app_config {
    active_directory{
      is_connect
    }
  }
}
```

В случае положительного результата ответом будет - true. При невозможности соединиться - false.

2.3 Настройка синхронизации организационной структуры

Данная настройка позволит выстроить в CrocoTime структуру групп сотрудников по аналогии с структурой подразделений (OU) в AD.

Запрос для настройки:

```
mutation {  
  app_config {  
    active_directory {  
      update_sync_config(import_organization_structure: true) {  
        import_organization_structure  
      }  
    }  
  }  
}
```

2.4 Настройка задержки при синхронизации нового сотрудника

По умолчанию, интеграция не синхронизирует учетные записи AD, возраст которых меньше 1 суток. Для изменения данной задержки нужно выполнить следующий запрос с указанием нового значения времени в миллисекундах:

```
mutation {  
  app_config {  
    active_directory {  
      update_sync_config(delay_creation_employee: 86400000) {  
        delay_creation_employee  
      }  
    }  
  }  
}
```

2.5 Настройка импорта отчеств

По умолчанию интеграция синхронизирует только имя и фамилию сотрудника из соответствующих атрибутов AD. При включении данной опции при синхронизации будет производиться попытка извлечь имя и отчество сотрудника из AD-атрибута "Выводимое имя" (DisplayName). Полученное значение будет сохранено как имя сотрудника в CrocoTime. Запрос:

```
mutation {  
  app_config {  
    active_directory {  
      update_sync_config(import_patronymic: true) {  
        import_patronymic  
      }  
    }  
  }  
}
```

2.6 Настройка синхронизации статуса “включен\выключен” сотрудника

Интеграция может выставлять статус сотрудника “включен\выключен” в CrocoTime на основе состояния его учетной записи в AD (включена или отключена, блокировка не учитывается).

Есть несколько режимов синхронизации состояния:

- 1) SIMPLEX (установлен по умолчанию) - для синхронизации только отключения учетной записи Active Directory. Запрос:

```
mutation{
  app_config{
    active_directory{
      update_sync_config(sync_enable_status_account: SIMPLEX) {
        sync_enable_status_account
      }
    }
  }
}
```

- 2) DUPLEX - для полной синхронизации состояния учетной записи в соответствии с Active Directory. Данный режим корректно только, если количество доступных лицензий CrocoTime не меньше числа синхронизируемых сотрудников в AD. Запрос:

```
mutation{
  app_config{
    active_directory{
      update_sync_config(sync_enable_status_account: DUPLEX) {
        sync_enable_status_account
      }
    }
  }
}
```

- 3) DISABLE - статус сотрудников не синхронизируется с AD. Запрос:

```
mutation{
  app_config{
    active_directory{
      update_sync_config(sync_enable_status_account: DISABLE) {
        sync_enable_status_account
      }
    }
  }
}
```

2.7 Настройка частоты синхронизации данных с Active Directory

Данный параметр задает период синхронизации учетных записей Active Directory с Crototime. Значение периода синхронизации по-умолчанию установлено в 900000 миллисекунд, что равно 15 минутам. Для изменения периода синхронизации нужно выполнить следующий запрос с указанием нового значения в миллисекундах:

```
mutation{
  app_config{
    active_directory{
      update_sync_config(period_sync:60000) {
        period_sync
      }
    }
  }
}
```

Значение данного параметра должно быть больше либо равно 60000 миллисекунд, что соответствует 1 минуте (`period_sync >= 60000`).

2.8 Настройка импорта руководителя

По умолчанию руководитель сотрудника синхронизируется согласно значению AD-атрибута (`manager`). При желании эту функцию необходимо отключить запросом:

```
mutation{
  app_config{
    active_directory{
      update_sync_config(import_manager: false) {
        import_manager
      }
    }
  }
}
```

Аналогично используя `true` можно включить обратно.

2.9 Настройка объединения возникших дубликатов сотрудников в Crocotime

Из-за особенностей работы Crocotime Agent и Crocotime Server в некоторых ситуациях, когда происходит переименование существующего сотрудника в AD (например, при смене фамилии), в Crocotime Server может появиться дубликат данного сотрудника.

Интеграция может объединить возникающие дубликаты сотрудников, для этого необходимо выполнить следующий настройки.

1) Указать учетную запись сотрудника в Crocotime от имени которой в системе будет происходить слияние сотрудников. Данная учетная запись должна обладать правами полного доступа.

```
mutation {  
  app_config {  
    active_directory {  
      update_crocotime_web_api_config(login:"my@mail.test", password:"") {  
        login  
        has_password  
      }  
    }  
  }  
}
```

2) Включить функционал объединения дубликатов сотрудников.

```
mutation {  
  app_config {  
    active_directory {  
      update_sync_config(merge_employees:true) {  
        merge_employees  
      }  
    }  
  }  
}
```

2.10 Разовый запрос на изменение часовых поясов в CrocoTime для сотрудников синхронизируемых с AD

Интеграция изменить часовой пояс для всех профилей сотрудников в CrocoTime, которые синхронизируются с AD, следующим запросом:

```
mutation {  
  app_config {  
    active_directory {  
      auto_time_zone_for_employees(isAutoTimeZone: true)  
    }  
  }  
}
```

2.11 Разовый запрос на включение сотрудников связанных с AD у которых в атрибуте присутствует допустимое одиночное, строковое значение

Интеграция позволяет массово оставить включенными в CrocoTime только профили с определенными атрибутами. Запрос:

```
mutation {  
  app_config {  
    active_directory {  
      active_employees_with_attribute_values(attribute:"comment", values:["ОЦО",  
"НИЦ"])  
    }  
  }  
}
```

Поле attribute: название атрибута.

Поле values: допустимые значения атрибута.

При выполнении запроса, если у сотрудника в атрибуте будет присутствовать одно из указанных значений, то он будет включен, а остальные отключены.

2.12 Разовый запрос на удаление руководителей у всех сотрудников

Интеграция позволяет очистить атрибут “Руководитель” во всех профилях CrocoTime, которые синхронизируются с AD. Запрос:

```
mutation {  
  app_config {  
    active_directory {  
      delete_all_chief  
    }  
  }  
}
```

2.13 Разовый запрос на отключение сотрудников, не входящих в синхронизируемые объекты AD

Для отключения в Crocodile Server всех сотрудников, кроме тех, что находятся в синхронизируемых группах или подразделениях AD выполните следующий запрос.

```
mutation {  
  app_config {  
    active_directory {  
      disable_not_existing_employees  
    }  
  }  
}
```

После его выполнения запустится процесс отключения сотрудников. Это может занять длительное время. По успешному завершению в правой части интерфейса GraphQL появится следующий ответ.

```
{  
  "data": {  
    "app_config": {  
      "active_directory": {  
        "disable_not_existing_employees": true  
      }  
    }  
  }  
}
```

3. Получение текущих настроек интеграции с AD

Узнать текущие настройки соединения с доменом Active Directory можно при помощи запроса:

```
{
  app_config {
    active_directory {
      active_directory_config
    }
  }
}
```

Узнать текущие дополнительные настройки интеграции можно запросом:

```
{
  app_config {
    active_directory {
      sync_config
    }
  }
}
```

4. Частые вопросы

При выполнении запроса выходит ошибка “access denied”

Данная ошибка чаще всего сигнализирует, что сессия для работы с веб-страницей истекла. Выполните повторный вход в CrocoTime по адресу “<адрес CrocoTime>:8091/”, после этого вернитесь на страницу “<адрес CrocoTime>:8091/graphiql” и выполните запрос.

Как настроить интеграцию на работу с несколькими доменами

Если речь идет о разных доменах в рамках одного леса AD, можно настроить интеграцию на соединение с глобальным каталогом (GC). Для этого нужно при настройке соединения с доменом в поле “domain_controller_host” указать адрес контроллера домена с портом глобального каталога 3268, например,

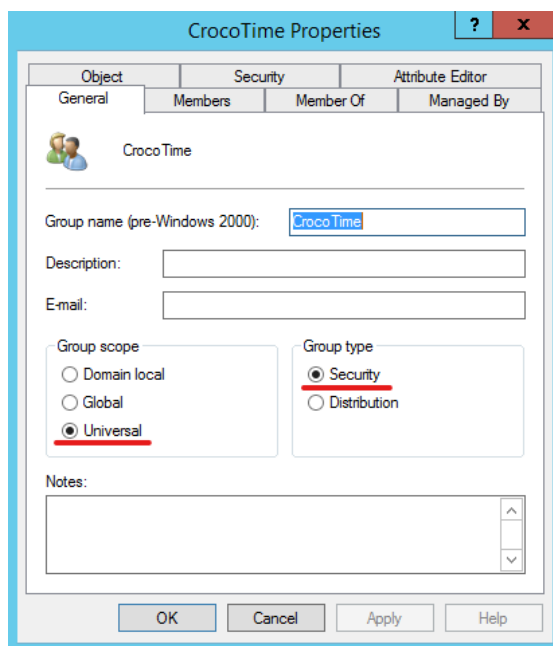
domain_controller_host: “dc1.somedomain.com:3268”

Обратите внимание, что по умолчанию атрибут “Должность” (title) не реплицируется в глобальный каталог, поэтому поле “Должность” в профиле сотрудника в CrocoTime не сможет быть заполнено при такой настройке.

Описание того, как добавить атрибут в схему глобального каталога - <https://msdn.microsoft.com/ru-ru/windows/desktop/cc737521>

Не синхронизируются сотрудники из указанной группы в AD

Убедитесь, что данная группа является универсальной группой безопасности. С иными группами интеграция не работает.



Логи работы интеграции

Работа интеграции логируется в файл “C:\Program Files\Subsystems\logs\main.log”.

Если у Вас возникли проблемы при синхронизации сотрудника выполните поиск по его логину (UserPrincipalName) по данному файлу для поиска возможных ошибок.

Уникальность e-mail в CrocoTime

В CrocoTime e-mail является уникальным значением для профилей сотрудников. Если в AD некоторые сотрудники имеют одинаковы e-mail, интеграция добавит в CrocoTime данные только одного сотрудника, а остальных проигнорирует.

Что будет с сотрудником в CrocoTime, если в AD переместить его учетную запись в подразделение (OU) или удалить из группы безопасности, которые настроена на синхронизацию

В такой ситуации, интеграция перестанет обновлять данные из AD по этому сотруднику. Профиль не будет удален или отключен.