

Инструкция по установке Secure-T
Awareness Platform.
Руководство администратора.

Оглавление

1. ОБЩЕЕ	3
2. ПОДГОТОВКА К РАБОТЕ	3
3. ПЕРВЫЙ ЗАПУСК.....	3
4. ДОСТУПНЫЕ РАЗДЕЛЫ.....	6
4.1. Управление.....	6
4.2. Сотрудники.....	8
4.3. Логи.....	8
4.4. Active Directory.....	9
4.5. Kerberos	9
4.6. Proxy	10
4.7. Настройки	10

1. ОБЩЕЕ

Платформа Secure-T EDU распространяется в виде образа виртуальной машины в формате ova/ovf. Вся инфраструктура платформы работает на Docker контейнерах, которые управляются с помощью утилиты dockercompose.

Система состоит из:

- Gunicorn - веб-сервер/бэкенд платформы nginx - балансировщик/сервер статики;
- PostgreSQL - база данных Redis - кэш и очереди;
- Postfix - почтовый сервер (Опционально);
- Minio - хранилище.

2. ПОДГОТОВКА К РАБОТЕ

Для интеграции с Active Directory необходимо заранее завести отдельного пользователя, через которого платформа будет синхронизировать сотрудников в платформе. Логин и пароль этого пользователя понадобятся вам при первом запуске и настройке системы.

Также для поддержки "сквозной авторизации" ваших сотрудников на платформе, понадобится файл аутентификации keytab.

Пример команды, выполнив которую на domain controller'e вашей Active Directory, можно сгенерировать keytab файл:

```
ktpass .exe `
/princ <уникальное_имя-сервиса> `
/mapuser <имя_пользователя_в-AD> `
/pass <пароль_пользователя_в-AD> `
/crypto ALL `
/ptype KRB5_NT_PRINCIPAL `
/mapop set `
/out c:\share\keytab
```

После того, как вы получите образ виртуальной машины, и перед первым ее запуском, проверьте следующий список:

- Добавлены DNS записи для виртуальной машины;
- В спам фильтрах ваших почтовых серверов внесены исключения для указанных нами заранее фишинговых доменов;
- Создан новый пользователь в AD с возможностью чтения данных других пользователей;

3. ПЕРВЫЙ ЗАПУСК

После запуска виртуальной машины перейдите на страницу первоначальной настройки. Страница доступна по адресу - <http://<домен-платформы>/admin>.

Шаг 1. Заполните все необходимые поля, чтобы начать работу.

Общее:

Название организации

Platform's domain name ⓘ

E-mail оператора ⓘ

Фильтрация сотрудников ⓘ

Тип фильтрации

Без фильтрации Whitelist Blacklist

Active Directory:

Domain Controller server uri: ⓘ

Bind DN: ⓘ

Password:

Search DN: ⓘ

User search filter string: ⓘ

Kerberos:

Realm: ⓘ

Realm KDC IP: ⓘ

Admin server IP: ⓘ

Service name: ⓘ

Keytab файл: ⓘ

Proxy:

HTTP proxy: ⓘ

HTTPS proxy: ⓘ

No proxy: ⓘ

Общее:

- *Название организации* - название вашей компании;
- *Platform's domain name* - домен платформы;
- *E-mail оператора* - e-mail будущего оператора платформы;
- *Фильтрация сотрудников* -

Active Directory:

- *Domain controller server uri* - uri для сервера, на котором находится контроллер домена ad (например, ldap://10.0.0.1);
- *Bind DN* - имя аккаунта в ad для платформы;
- *Password* - пароль от аккаунта;
- *Search DN* - DN для поиска сотрудников в AD;
- *User Search filter string* - параметр сотрудников в AD по которому сотрудники должны быть добавлены в платформу, например organization=<ваша-организация>

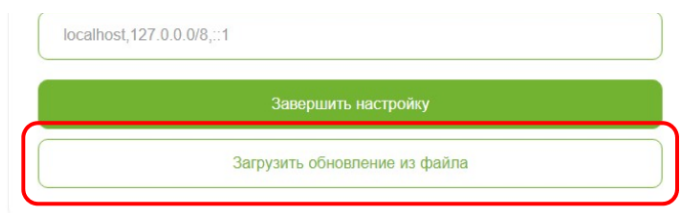
Kerberos:

- *Realm* - Realm в kerberos, в котором находится пользователь для платформы;
- *Realm KDC IP* - ip адрес сервера где находится key distribution center для kerberos'a. Чаще всего IP адреса для Realm KDC IP и Admin server IP совпадают с IP адрессом сервера, где находится контроллер домена ad.;
- *Admin server ip* - ip адрес сервера аутентификация для kerberos'a;
- *Service name* - имя, на которое был выписан keytab файл;
- Keytab файл - необходимо добавить ранее сгенерированный файл;

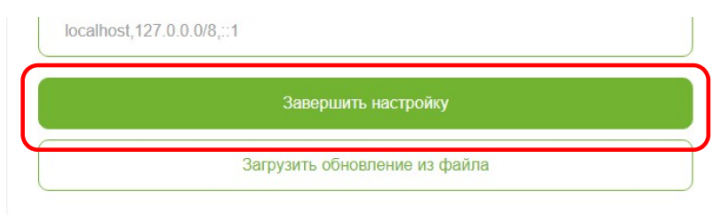
Proxy:

- *HTTP proxy* - "http://логин:пароль@ip_прокси:порт_прокси/" Адрес прокси для HTTP;
- *HTTPS proxy* - "http://логин:пароль@ip_прокси:порт_прокси/" Адрес прокси для HTTPS;
- *No proxy* - localhost,127.0.0.0/8,::1 Игнорируемые узлы

*Файл с обновлениями (zip. архив) для системы вы можете загрузить, нажав на кнопку “Загрузить обновление из файла” внизу страницы:



Шаг 2. Нажмите “Завершить настройку”.



4. ДОСТУПНЫЕ РАЗДЕЛЫ

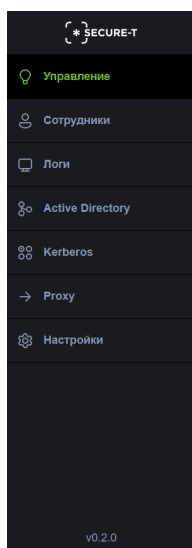
Для инициализации платформы по адресу <http://<доменплатформы>/admin>, необходимо ввести пароль, который будет предоставлен поддержкой Secure-T.

Авторизация

Пароль

Войти

4.1. Управление



Secure-T

Лицензия Использовано: 1/9714 Статус: ACTIVE Дата завершения: 26.11.2021 Загрузить новый файл лицензии скоро	Обновление Текущая версия: 1.0 Проверить наличие обновлений Загрузить обновление из файла
Active Directory Текущее количество сотрудников: 1 Последняя синхронизация: 05.02.2021 Синхронизировать сотрудников	Сервисы API: Работает База данных: Работает Веб-сервер: Работает Фишинг: Работает Перезапустить сервисы

На данной странице доступна следующая информация:

- **Лицензия:** количество подключенных пользователей и общее количество пользователей согласно приобретенной лицензии; статус лицензии, а также ее дата завершения. На данной странице вы можете загрузить новый файл лицензии для обновления.

Лицензия

Использовано: 1/9714
Статус: ACTIVE
Дата завершения: 26.11.2021

[Загрузить новый файл лицензии](#) скоро

- *Active Directory*: текущее количество сотрудников, подключенных к платформе, а также дата последней синхронизации. В данном пункте вы можете перезапустить сервисы, нажав на кнопку “Синхронизировать сотрудников”.

Active Directory

Текущее количество сотрудников: **1**
Последняя синхронизация: **05.02.2021**

Синхронизировать сотрудников

- *Обновление*: текущая версия платформы. Вы можете проверить наличие обновлений, нажав на кнопку “Проверить наличие обновлений”, либо же загрузить их через файл.

Обновление

Текущая версия: **1.0**

Проверить наличие обновлений

Загрузить обновление из файла

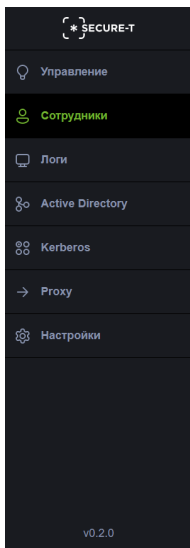
- *Сервисы*: в случае необходимости вы можете перезапустить сервисы в данном разделе.

Сервисы

API:	Работает
База данных:	Работает
Веб-сервер:	Работает
Фишинг:	Работает

Перезапустить сервисы

4.2. Сотрудники



Сотрудники

Поиск по сотрудникам

ФИО	Отдел	Должность	Роль
Иванов Ярослав	Отдел Финансов	Начальник	Оператор

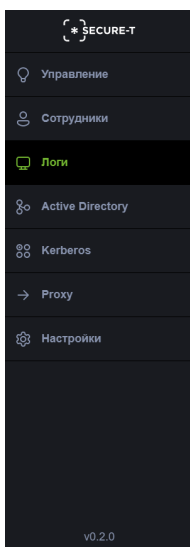
На данной странице доступна информация о всех подключенных к платформе сотрудников: ФИО, отдел, должность и роль, которая присваивается пользователю (оператор, контент-менеджер, сотрудник). При необходимости вы можете найти сотрудника через ввод информации о нем в поле сверху.

Сотрудники

Поиск по сотрудникам

ФИО	Отдел	Должность	Роль
Иванов Ярослав	Отдел Финансов	Начальник	Оператор

4.3. Логи



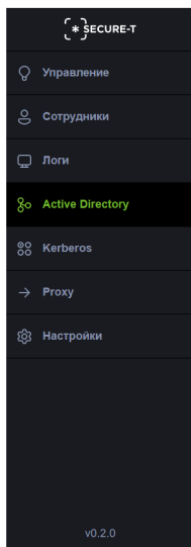
Логи

Выгрузить логи

```
1 [nginx] - /docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configuration
2 [nginx] - /docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
3 [nginx] - /docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
4 [nginx] - 10-listen-on-ipv6-by-default.sh: error: /etc/nginx/conf.d/default.conf is not a file or does not exist
5 [nginx] - /docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
6 [nginx] - /docker-entrypoint.sh: Configuration complete; ready for start up
7 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:29 +0000] GET / HTTP/1.0 200 7445 "-" Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.97 Safari/537.36
8 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:29 +0000] GET /edu-front/static/css/4.76b4f99f.chunk.css HTTP/1.0 200
9 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/css/main.3d6d5522.chunk.css HTTP/1.0 200
10 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/main.726c3556.chunk.js HTTP/1.0 200
11 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/4.f45793a2.chunk.js.map HTTP/1.0 200
12 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/main.726c3556.chunk.js.map HTTP/1.0 200
13 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/css/8.76ba3a09.chunk.css HTTP/1.0 200
14 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/0.0a0979f8.chunk.js HTTP/1.0 200
15 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/0.0a0979f8.chunk.js.map HTTP/1.0 200
16 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/css/8.18814f48.chunk.css HTTP/1.0 200
17 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/js/8.df02c50d.chunk.js HTTP/1.0 200
18 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:30 +0000] GET /edu-front/static/media/Montserrat-Regular.364c3ba6.woff2 HTTP/1.0 200
19 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/css/11.5115553f.chunk.css HTTP/1.0 200
20 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/js/11.45508462.chunk.js HTTP/1.0 200
21 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
22 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
23 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
24 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
25 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
26 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/js/0.8a079f98.chunk.js.map HTTP/1.0 200
27 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
28 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/media/Montserrat-Bold.d19169a.woff2 HTTP/1.0 200
29 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/media/GothamPro.3c44b37.woff HTTP/1.0 200
30 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/js/11.45508462.chunk.js.map HTTP/1.0 200
31 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/favicon.ico HTTP/1.0 200 15886 "http://web-secure-t.offline/"
32 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
33 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /api/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
34 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
35 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
36 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 401 581 "http://web-secure-t.offline/"
37 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 200 912 "http://web-secure-t.offline/"
38 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 200 240 "http://web-secure-t.offline/"
39 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 200 431 "http://web-secure-t.offline/"
40 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET / HTTP/1.0 200 74 "http://web-secure-t.offline/"
41 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /media/upload/avatars/avatar.svg HTTP/1.0 200 848 "http://web-secure-t.offline/"
42 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 200 722 "http://web-secure-t.offline/"
43 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /api/organizations/1/employees/5/ HTTP/1.0 200 785 "http://web-secure-t.offline/"
44 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /api/organizations/1/ HTTP/1.0 200 150 "http://web-secure-t.offline/"
45 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/css/14.06388ff1.chunk.css HTTP/1.0 200
46 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] GET /edu-front/static/js/14.0629f50.chunk.js HTTP/1.0 200
47 [nginx] - 172.22.0.1 - [28/Jun/2021:14:31:31 +0000] POST /api/graphql/ HTTP/1.0 200 2338 "http://web-secure-t.offline/"
```

На данной странице вы можете посмотреть и выгрузить логи. Для загрузки нажмите на кнопку в верхнем углу.

4.4. Active Directory



Настройка Active Directory

Domain Controller server url:

Bind DN:

Password:

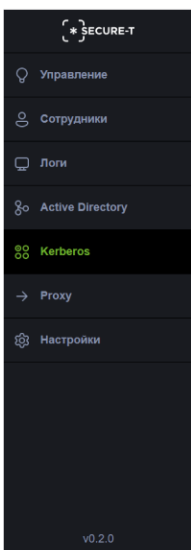
Search DN:

User search filter string:

Найдено пользователей с данным фильтром: 8714

В данном разделе вы можете посмотреть и изменить текущие настройки для синхронизации с AD. После внесенных изменений необходимо их сохранить.

4.5. Kerberos



Настройка Kerberos

Realm:

Realm KDC IP:

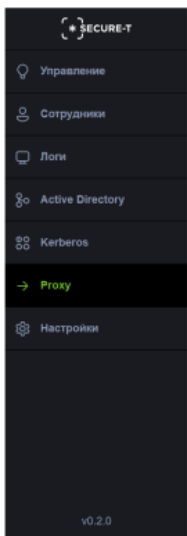
Admin server ip:

Service name:

Keytab файл:

В данном разделе вы можете посмотреть и изменить настройки Kerberos. После внесенных изменений необходимо их сохранить.

4.6. Proxy



Настройка Proxy

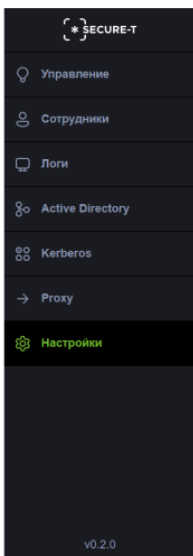
HTTP proxy:

HTTPS proxy:

No proxy:

В данном разделе вы можете посмотреть и изменить настройки Proxy. После внесенных изменений необходимо их сохранить.

4.7. Настройки



Базовые настройки

Название организации:

Platform's domain name:

Фильтрация сотрудников

Тип фильтрации:

E-майлы сотрудников которые смогут попасть на платформу:

В данном разделе вы можете изменить системные настройки:

- Название организации;
- Домен платформы;
- Фильтрация для отправки системных писем.

После внесенных изменений необходимо их сохранить.