Руководство администратора

Система управления безопасной разработкой

- О платформе 1
  - Краткий обзор системы управления безопасной разработкой 1
  - С чего начать 2
- Установка 2
  - Требования к оборудованию 2
  - Подготовка к установке 3
  - Установка системы управления безопасной разработкой 3
  - Обновление системы управления безопасной разработкой 4
  - Стандартные пароли 4
  - Настройки 5
- Интеграции 5
  - Jira интеграция 5
  - GitLab интеграция 6
    - Привязка существующего репозитория к репозиторию GitLab 7
- Загрузка результатов сканирований 7
- Администрирование 8
  - Загрузка файла лицензии 8
  - Добавление пользователей 9
    - Создание бот пользователя 9
    - Управление пользователями 11
    - Пользовательские роли 11
      - Репозиторий 11
      - Компоненты 12
      - Администрирование 13
  - Управление регистрацией пользователей 14
    - Регистрация пользователей 14
    - Подтверждение регистрации 14
  - Настройка LDAP 14
  - Настройка SMTP-уведомлений 16
  - Настройка SSL 17
  - Загрузка SSL-сертификатов в ASMP 17
  - Настройка HTTP/HTTPs 18
  - Настройка HTTP или TCP реверс-прокси с SSL-терминацией 18
    - Пример конфигурации nginx как HTTP реверс-прокси 19
  - Добавление корневых сертификатов 20
  - Конвертация CA-сертификата из .PFX 20
  - Настройка логотипа 21
  - Фоновые задачи 23
- Уведомления 24
  - Почтовые уведомления 24
  - Настройка SMTP уведомлений 24

О платформе

Краткий обзор системы управления безопасной разработкой

Система управления безопасной разработкой — это самостоятельная платформа, которая помогает максимально эффективно управлять уязвимостями и может быть интегрирована в ваш жизненный цикл разработки (SDLC).

Это универсальное решение агрегирует данные о безопасности из разных источников для работы с уязвимостями и ускоряет процесс тестирования безопасности, оптимизируя рабочий процесс SDLC.

Синяя команда (Blue Team) может легко работать с выявленными проблемами, создавать задачи в Jira и отслеживать прогресс в реальном времени, а разработчики могут исправлять ошибки и обеспечивать безопасность продуктов.

С чего начать

Добро пожаловать в Систему управления безопасной разработкой! Ознакомьтесь со следующими ссылками, чтобы начать свою работу:

1. Установка.
2. Загрузка результатов сканирований.
3. Интеграция с Jira.

Если вы не нашли ответы на свои вопросы, можете задать их сюда: support@hexway.ru.

Установка

Система управления безопасной разработкой поставляется в виде исполняемого веб-приложения в формате .RUN.

Подключение к веб-приложению осуществляется через любой современный браузер.

Требования к оборудованию

Ниже указаны системные требования:

Описание	Минимальные требования	Рекомендованные требования
RAM	4 GB	16 GB
CPU	2 ядра	4 ядра
Скорость диска	100 IOps	300 IOps
Место на диске	100 GB	300 GB

Подготовка к установке

Перед установкой подготовьте виртуальную машину или сервер с одной из поддерживаемых операционных систем:

- CentOS 8
- RHEL 8
- RedOS 7.3
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Astra Linux Орёл 1.7
- другие ОС, совместимые с указанными выше.

Некоторые дистрибутивы Linux в минимальной установке могут не включать следующие утилиты: `curl`, `find`, `groupadd`, `tar`, `gzip`, `useradd`, `xargs`. Однако эти утилиты используются в Платформе, и мы рекомендуем вам установить их.

Установите docker engine, включая docker compose plugin на машину.

> Примечание 1: `docker from snap` на данный момент **не поддерживается**.
>
> Примечание 2: docker-compose standalone поддерживается, но не рекомендуется.

Известные проблемы при использовании `docker` и `docker compose plugin` из репозиториев ОС, вместо docker.com:

- В репозиториях некоторых ОС есть только docker-compose 1.x который не поддерживается Платформой. Для установки `docker compose plugin` воспользуйтесь инструкцией со страницы Install the plugin manually, но обратите внимание, на пометки `for all users`. Если плагин будет установлен только текущего пользователя, даже если это будет `root`, запустить платформу корректно невозможно.

- В репозиториях некоторых ОС `docker` после установки не стартуется автоматически или не создаёт `socket`. В этих случаях его нужно запустить вручную.

Установка системы управления безопасной разработкой

1. После того как вы заполнили форму, вы получите электронное письмо со ссылкой на файл установки. Скачайте его на ваш сервер: `wget https://hexway.io/<link_path>/install_hw_vmp_en-US_<version>.run`

2. Чтобы начать установку, выполните команду: `bash ./install_hw_vmp_en-US_<version>.run`

3. После установки вы получите следующее сообщение: `hexway Vampy is ready to use. UI accessible on http://<ip-server> or https://<ip-server> Login as '<username>' password: '<password>'` > Примечание: при установке платформы без дополнительных параметров пароль пользователя root будет сгенерирован автоматически. >

4. Откройте Систему управления безопасной разработкой в браузере по адресу, указанному в сообщении: `http://<ip-server>/` или `http://<your-domain-name>/`. Логин по умолчанию для администратора: `root@ro.ot`.

Обновление системы управления безопасной разработкой

Для обновления платформы:

1. Скачайте файл на ваш сервер: `wget https://hexway.io/<link_path>/install_hw_vmp_en-US_<version>.run`
2. Запустите команду: `bash ./install_hw_vmp_en-US_<version>.run`

Во время обновления платформа сохранится в бэкап, после чего будут установлены последние обновления.

> Примечания:
>
> 1. Бэкап платформы сохранен здесь: `/opt/hw-vmp_backup`;
> 2. Система управления безопасной разработкой хранит три последних бэкапа.

Когда установка завершится, платформа запустится автоматически.

Стандартные пароли

Пароль по умолчанию для пользователя root генерируется автоматически во время установки и сохраняется в файле `/opt/hw-fh/config/local.ini`.

Вы можете проверить свой пароль по умолчанию после установки, используя команду:

```
grep v.root.password /opt/hw-vmp/config/local.ini
```

⚠ Пожалуйста, обратите внимание, что изменение `local.ini` не изменит пароль! Вы можете изменить пароль только через веб-интерфейс.

Настройки

Вы можете задать некоторые параметры перед установкой приложения.

Сначала давайте создадим директорию для файла конфигурации: `/opt/hw-vmp/config/` и сам файл `user.ini`.

Также в этой директории будет находиться файл со списком возможных параметров и их значений: `user-template.ini`.

⚠ Если вы хотите установить пользовательский пароль для root, вам нужно сделать это до установки! Просто добавьте в `user.ini` настройку `v.root.password = %ваш_пароль%`. В противном случае пароль для root будет сгенерирован автоматически. Вы можете проверить свой пароль по умолчанию после установки, используя команду:

```
grep v.root.password /opt/hw-vmp/config/local.ini
```

⚠ Обратите внимание, что изменение `local.ini` не изменит пароль! Вы можете изменить пароль только в веб-интерфейсе.

Интеграции

Система управления безопасной разработкой поддерживает интеграции с различными системами.

В этом разделе вы найдете информацию о том, как настроить интеграции.

Jira интеграция

В зависимости от вашего рабочего процесса, Система управления безопасной разработкой может быть интегрирован с внешними системами управления задачами с использованием REST API токенов и вебхуков.

Чтобы настроить интеграцию с **Jira**, выполните следующие шаги:

1. Войдите в платформу как администратор;
2. В левом меню выберите **Admin** > **Jira integrations**:
3. Нажмите на **+ Jira server** в центре страницы;
4. Заполните поля (все поля обязательны):
5. **Connect Name** - имя подключения,
6. **Web Url** - IP-адрес или имя хоста вашего сервера Jira.
7. Нажмите **Next**:

8. Платформа проверит соединение с сервером, и если все верно, в зависимости от настроек вашего сервера Jira, попросит заполнить поля:

9. подключение через вебхуки - укажите `Login`, `Password`

10. подключение через токены - укажите `Token` (см. статью Управление токенами API):

    > Примечание: вы можете использовать токен API для аутентификации скрипта или другого процесса с продуктом Atlassian Cloud. Токен можно сгенерировать из вашей учетной записи Atlassian, а затем скопировать и вставить в скрипт.

11. Нажмите **Next**;

12. В поле **Project** укажите ваш проект Jira;

13. В поле **Issue type** укажите тип задачи, которая будет создана для уязвимостей в вашем проекте Jira;

14. Опционально включите **Обратную синхронизацию** для назначения статусов задач Jira:

    > Примечание: вы можете назначить пользовательские статусы задач для задач Jira.

15. Нажмите **Next**;

16. В зависимости от настроек выбранного проекта Jira вам потребуется заполнить значения по умолчанию, с которыми задачи будут отправляться в Jira.

17. Нажмите **Save**.

Новое соединение Jira будет добавлено на страницу **Jira integrations**.

Нажмите **Copy webhook**, чтобы сохранить вебхук в буфер обмена. Используйте этот вебхук для подключения сервера Jira к платформе (см. статью Jira Webhooks), чтобы уметь синхронизировать статусы задач.

> Примечание: при настройке вебхука в Jira необходимо включить настройки статуса, если вы хотите отправлять/получать обновления статусов от Системы управления безопасной разработкой.

GitLab интеграция

Интеграция с GitLab значительно расширит функциональность Системы управления безопасной разработкой для анализа найденных дефектов. Это доступно для лицензии **Enterprise★**.

Для настройки GitLab вам нужно перейти в раздел Администратор → интеграция → GitLab.

В окне настроек интеграции необходимо указать:

- Название интеграции
- URL сервера GitLab
- Токен доступа GitLab

Для интеграции с GitLab вам нужно сгенерировать **Access Token** на сервере GitLab. Это может быть токен для пользователя или группы репозиториев.

Документацию о том, как создать **Access Token**, можно найти в официальной документации GitLab.

При создании **Access Token** в поле Select scopes просто укажите значение **read_api**.

После ввода всех данных интеграция будет успешно создана.

Привязка существующего репозитория к репозиторию GitLab

Если у вас уже есть созданный репозиторий в Системе управления безопасной разработкой и вы хотите связать его с репозиторием в GitLab, это можно сделать несколькими способами:

1. В карточке репозитория

2. Через меню добавления репозитория

   После чего вам будет предложено «связать» репозитории.

Загрузка результатов сканирований

Вы можете загружать результаты сканирования с помощью API.

Чтобы загрузить данные на платформу:

- Создайте бота. Для корректной работы бота ему необходимо присвоить роль **Editor** или **Admin**. Запомните сгенерированный API токен.

- Выполните следующий запрос CURL:

  ```
  bash curl -X POST "$SEC_VV_URL/scan_uploads/" \ -H "accept: */*"
  \ -H "Content-Type: multipart/form-data" \ -H "Authentication:
  $SEC_VV_KEY" \ -F "repository=$VAMPY_REPO_SLUG" \ -F
  "repositoryBranch=$VAMPY_REPO_BRANCH" \ -F
  ```

```
"scannerResultFile=@$VV_REPORT_FILE_NAME" \ -F
"scannerType=$VV_SCAN_TYPE" #(1)!
```

Примечания:

- (1) Имя сканера. Поддерживаемые сканеры:
  - TRIVY_FS
  - RIVY_IMAGE
  - DEPENDENCY_CHECK
  - ESLINT
  - SEMGREP
  - GRYPE
  - TRUFFLEHOG

где

- **SEC_VV_UR** - путь к серверу Системы управления безопасной разработкой, напр. `http://vmp-demo.corp.hexway.io/api/`;
- **SEC_VV_KEY** - токен API для бота;
- **VAMPY_REPO_SLUG** - путь к проекту репозитория, для которого работает пайплайн. Эквивалентно `CI_PROJECT_PATH`;
- **VAMPY_REPO_BRANCH** - ветка, для которой работает пайплайн. Эквивалентно `CI_COMMIT_REF_NAME`;
- **VV_REPORT_FILE_NAME** - имя файла с результатами скана;
- **VV_SCAN_TYPE** - название сканера. Поддерживаемые сканеры можно посмотреть (на этой странице).

Администрирование

Загрузка файла лицензии

Когда вы скачиваете Систему управления безопасной разработкой, по умолчанию вы получаете версию Community. Это означает, что некоторые функции ограничены, пока вы не обновите свой Тарифный план.

> Примечание: только администратор платформы может загрузить или удалить лицензию.

Чтобы добавить лицензию на платформу:

1. Войдите в платформу как администратор;
2. В левом меню выберите **Admin** > **License**;
3. Нажмите **Upload license file** или перетащите файл лицензии в область с кнопкой.

После загрузки файла **License** на вкладке **License** появится информация о текущей лицензии и доступных опциях.

Когда лицензия истечет, платформа вернется к версии Community. В этом случае все существующие пользователи, проекты и настройки останутся, но вы не сможете добавить новые до тех пор, пока не обновите свой Тарифный план снова.

Добавление пользователей

Чтобы пригласить пользователей в ваши проекты, вы должны сначала добавить пользователей на Систему управления безопасной разработкой. Каждый может создать учетную запись на платформе. Однако все новые пользователи должны быть одобрены администраторами (см. раздел Управление регистрацией пользователей). Неодобренный пользователь не сможет работать в Системе управления безопасной разработкой.

> Примечание: только администраторы могут приглашать пользователей в Систему управления безопасной разработкой.

Чтобы добавить пользователей на платформу:

1. Войдите в платформу как администратор;
2. В левом меню выберите **Admin** > **Users**;
3. Нажмите **+ User** в верхнем левом углу страницы;

1. В окне **New user** заполните поля: `Имя`, `Фамилия`, `Логин`, `Email`, `Пароль` и `Подтверждение пароля`;

1. Назначьте роль пользователю: **Admin**, **Security Engineer**, **System Engineer**, **Editor** или **Readonly**. Ознакомьтесь с разрешениями ролей здесь.

2. Нажмите **Create**. Новый пользователь появится в списке **Manage users**.

   Примечания:

   - Пользователи LDAP автоматически появятся в списке пользователей после первого входа в платформу;
   - Когда LDAP включен, вы не сможете создавать новых локальных пользователей на платформе, однако вы можете добавлять ботов.

Создание бот пользователя

Пользователь-бот может быть использован для автоматизации работы на платформе. Например, для автоматизации поиска, просмотра сообщений, ответов на сообщения или для интеграции со сторонними приложениями.

Также он используется для загрузки результатов сканирования.

Чтобы добавить пользователей-ботов на платформу:

1. Войдите в платформу в качестве администратора;
2. В левом меню выберите **Admin** > **Users**;

3. Нажмите **+ User** в верхнем левом углу страницы;
4. В окне **New user** нажмите **Create bot user**;

Укажите логин бота и назначьте ему роль: Admin, Editor or Readonly;

> Примечание: как только вы назначите роль пользователю-боту, вы не сможете изменить ее.

1. Нажмите **Create**. Новый пользователь-бот появится в списке **Manage users**;
2. Скопируйте токен пользователя-бота, чтобы подключить бота к вашему приложению;

Вы можете проверить соединение с пользователем-ботом с помощью команды ниже:

```
curl --silent 'http://vampy-hostname/api/projects/' \
  -H 'Authentication: <user_bot_token>'
```

Если всё настроено корректно, то ответ от сервера будет выглядеть так:

```
[
  {
    "completionDate": "2023-03-23",
    "connectionName": null,
    "created": "2023-03-23T08:47:14.358843Z",
    "description": "",
    "groupID": "4cd961ee-50ed-4d95-9340-4d1ace7038e9",
    "hawserID": null,
    "id": "ad09eb54-31f0-44d4-b991-6bbd83bbf0f7",
    "lastIncomingPong": null,
    "lastOutgoingPing": null,
    "name": "project_name",
    "owner": {
      "firstName": null,
      "id": "e2305102-84df-45b7-a779-f028b69229fc",
      "isAdmin": true,
      "lastName": null,
      "passwordChangeRequired": false,
      "userEmail": "root@ro.ot",
      "userLogin": "root@ro.ot"
    },
    "permission": null,
    "projectType": "",
    "scope": "",
    "startDate": "2023-03-23",
    "updated": "2023-03-23T08:47:14.358863Z"
  }
]
```

Управление пользователями

Чтобы отредактировать параметры пользователя, изменить роль пользователя или заблокировать пользователя, щелкните по имени пользователя в списке **Manage users**.

Для получения доступа к платформе все новые локальные пользователи должны быть одобрены администратором. Чтобы подтвердить или отклонить выбранных пользователей, измените их статус с **Pending** на **Accepted/Decline**.

> Примечание: пользователей с платформы удалить нельзя! Их можно только заблокировать.

Пользовательские роли

Репозиторий

Роли в репозитории:

- ✎ - Редактор
- ʘ - Только чтение
- ✖ - Нет доступа

Действие	**Admin ✖**	**Admin ʘ**	**Admin ✎**	**Security engineer ✖**	**Security engineer ʘ**	**Security engineer ✎**	**Sys eng**
Создание репозитория	✔	✔	✔	✔	✔	✔	
Импорт репозитория из VCS	✔	✔	✔	✔	✔	✔	
Привязать репозиторий из VCS	✔	✔	✔	✔	✔	✔	
Отвязать репозиторий из VCS	✔	✔	✔	✔	✔	✔	
Редактирование репозитория	✔	✔	✔	✔	✔	✔	
Загрузка результатов сканирования	✔	✔	✔	✔	✔	✔	
Создание issue вручную	✔	✔	✔	✔	✔	✔	
Удаление issue из репозитория	✔	✔	✔	✔	✔	✔	
Отправка issue из репозитория в таск-трекер	✔	✔	✔	✔	✔	✔	
	✔	✔	✔	✔	✔	✔	

Действие	**Admin ✖**	**Admin ʘ**	**Admin ✎**	**Security engineer ✖**	**Security engineer ʘ**	**Security engineer ✎**	**Sys eng**
Редактирование статуса и критичности issue							
Просмотр уровня критичности	✔	✔	✔	✔	✔	✔	
Просмотр приоритета репозитория	✔	✔	✔	✔	✔	✔	
Просмотр информации о репозитории(название, описание, url, slug, дата создания)	✔	✔	✔	✔	✔	✔	
Просмотр дашборда репозитория	✔	✔	✔	✔	✔	✔	
Просмотр списка репозиториев	✔	✔	✔	✔	✔	✔	
Просмотр компонент репозитория	✔	✔	✔	✔	✔	✔	
Просмотр статистики issue в репозитории	✔	✔	✔	✔	✔	✔	
Просмотр списка пользователей репозитория	✔	✔	✔	✔	✔	✔	
Добавление или удаление участника репозитория	✔	✔	✔	✔	✔	✔	
Изменение роли участника репозитория	✔	✔	✔	✔	✔	✔	

Компоненты

Действие	**Admin**	**Security engineer**	**System engineer**	**Editor ✖**	**Editor ʘ**	**Editor ✎**	**Read-only ✖**	**Read-only ʘ**
Создание компонента	✔	✔	✔	✔	✔	✔	✔	✔
Редактирование компонента	✔	✔	✘	✘	✘	✘	✘	✘
	✔	✔	✔	✘	✔	✔	✘	✔

Действие	Admin	Security engineer	System engineer	Editor ✖	Editor ⊙	Editor ✎	Read-only ✖	Read-only ⊙
Просмотр списка компонент								
Просмотр issues у компонента	✔	✔	✔	✘	✔	✔	✘	✔
Импорт SBOM	✔	✔	✘	✘	✘	✘	✘	✘
Экспорт SBOM	✔	✔	✔	✔	✔	✔	✔	✔
Просмотр версий компонента	✔	✔	✔	✘	✔	✔	✘	✔
Просмотр имени репозитория в панели информации компонента	✔	✔	✔	✔	✔	✔	✔	✔
Переход к репозиторию через ссылку в панели информации компонента	✔	✔	✔	✔	✔	✔	✘	✔

Администрирование

Действие	Admin	Security engineer	System engineer	Editor	Read-only
Создание пользователя/бота	✔	✘	✔	✘	✘
Управление пользователями	✔	✘	✔	✘	✘
Изменение роли пользователя/бота	✔	✘	✔	✘	✘
Управление лицензиями	✔	✘	✔	✘	✘
Управление SLA	✔	✘	✔	✘	✘
Управление интеграцией с Jira	✔	✘	✔	✘	✘
Управление LDAP	✔	✘	✔	✘	✘

Действие	Admin	Security engineer	System engineer	Editor	Read-only
Управление SMTP	✔	✘	✔	✘	✘
Просмотр статусов фоновых задач	✔	✘	✔	✘	✘

Управление регистрацией пользователей

Регистрация пользователей

1. Отредактируйте файл `/opt/hw-vmp/config/user.ini` (требуются права root). Свойству `v.users.registration` укажите значение `off`. Возможные значения:

    - `on` для включения регистрации;
    - `off` для выключения регистрации.

2. Чтобы применить изменения, выполните команду (требуются права root):

    ```
    /opt/hw-vmp/bin/reconfig
    ```

Подтверждение регистрации

Используйте эту опцию только в том случае, если регистрация пользователей включена (`v.users.registration = on`).

1. Откройте для редактирования файл `/opt/hw-vmp/config/user.ini` (требуются права root). Свойству `v.users.confirmation` укажите значение `manual`. Возможные значения:

    - `auto` - автоматическое подтверждение зарегистрированного пользователя;
    - `manual` - ручное подтверждение зарегистрированного пользователя (администратором).

2. Чтобы применить изменения, выполните следующую команду (требуются права root):

    ```
    /opt/hw-vmp/bin/reconfig
    ```

Настройка LDAP

Вы можете добавлять пользователей с использованием аутентификации LDAP.

> Примечание: пользователи могут принадлежать как корневому домену, так и поддоменам. Если вам необходимо добавить

пользователей из поддоменов, используйте Глобальный каталог.

Чтобы подключиться к серверу LDAP:

1. Войдите в платформу как администратор.
2. В левом меню выберите **Admin > LDAP**:
3. Включите **LDAP connection**.
4. Заполните все обязательные поля:
   - **LDAP Protocol** – метод подключения к серверу LDAP (обычный `ldap` или защищенный `ldaps`).
   - **LDAP Port** – номер порта сервера LDAP (обычное значение для этого поля - 389). **Примечание**: когда вы добавляете пользователей из поддоменов, используйте порты Глобального каталога – 3268 или 3269.
     - **Host** – IP-адрес или имя хоста сервера LDAP;
     - **Base DN** – каталог, в котором выполняется поиск пользователей. Вы должны заполнить это поле одним или несколькими атрибутами в синтаксисе LDAP, например, `DC=host,DC=test,DC=domain`;
     - **Blocked Group DN** – определяет значения атрибутов объектов, которые будут идентифицированы как блокированные группы пользователей. Значения атрибутов должны быть введены в соответствии с синтаксисом LDAP, например:

     ```
     CN=U.VampyBlocked,CN=Users,DC=dc,DC=corp,DC=hexway,DC=com
     ```
   - **Service Login** – пользователь LDAP, имеющий право просматривать содержимое ветви Base DN. Рекомендуется использовать формат `userPrincipalName` (например, `t.adm@test.domain`), но вы также можете использовать полное имя;
   - **Service Password** – пароль пользователя LDAP;
   - **User filter** – определяет значения атрибутов объектов, которые будут идентифицированы как пользователи. Значения атрибутов должны быть добавлены в соответствии с синтаксисом LDAP. **Примечание**: в большинстве случаев правильное значение фильтра пользователей - `user`, но если ваш сервер LDAP нестандартный, попробуйте другие варианты. Примеры:
     - `(objectClass=*)` – поиск будет выполнен среди всех доступных записей;
     - `(&(objectClass=user)(loginAttr=login))` – поиск будет выполнен по объектам с соответствующими значениями атрибутов;

- **Admin Group DN** – определяет значения атрибутов объектов, которые будут идентифицированы как группы пользователей. Значения атрибутов должны быть введены в соответствии с синтаксисом LDAP. **Примечание**: в большинстве случаев правильное значение фильтра групп - `(objectClass=group)`, но если ваш сервер LDAP нестандартный, попробуйте другие варианты. Пример:

  `CN=U.VampyAdmins,CN=Users,DC=dc,DC=corp,DC=hexway,DC=com`

- **Login attribute** – атрибут, который будет использоваться для аутентификации пользователей, например, `sAMAccountName` – соответствует формату логина, такому как `t.adm`;

- **E-mail attribute** – название атрибута, содержащего электронные адреса пользователей, например, `userPrincipalName` – соответствует формату логина, такому как `t.adm@test.domain`. **Примечание**: если вы хотите подключиться только к поддомену, используйте логин в формате `userPrincipalName` (например, `t.adm@test.domain`);

- **First Name attribute** – название атрибута, содержащего имя пользователя (например, `givenName`);

- **Last Name attribute** – название атрибута, содержащего фамилию пользователя (например, `sn`).

5. Нажмите **Test connection**, чтобы проверить соединение с сервером LDAP. Если настройки верны, вы увидите * Connection established*:

6. Нажмите `i`, чтобы увидеть всех доступных пользователей:

7. Нажмите **Save**. Пользователь появится на вкладке [Users tab](#) после первого входа в платформу.

   Примечание: после сохранения настроек LDAP вы не сможете добавлять локальных пользователей на платформу.

Настройка SMTP-уведомлений

Чтобы настроить SMTP:

1. Войдите в Систему управления безопасной разработкой как администратор;
2. В левом меню выберите **Admin > SMTP**;
3. Включите SMTP;
4. Заполните следующие поля:
5. `Host` - IP-адрес или имя хоста SMTP-сервера;
6. `Port` - номер порта SMTP-сервера;
7. `Username` - логин отправителя;
8. `Password` - пароль отправителя;

9. `Connection security` - использование протокола безопасности (NONE, STARTTLS, SSL/TLS);

10. `From` - адрес электронной почты, с которого вы будете получать уведомления.

11. Нажмите **Save**, чтобы применить настройки.

12. Чтобы проверить, что все настройки SMTP верны, нажмите `+ Test e-mail configuration`. С помощью этой опции вы можете отправить тестовое электронное письмо на свой почтовый ящик:
13. `To` - адрес электронной почты, на который будет отправлено тестовое письмо;
14. `Subject` - заголовок электронного письма;

15. `Message` - текст письма.

16. Нажмите **Send test e-mail**.

Настройка SSL

Важно!

Сразу после установки Системы управления безопасной разработкой WebUI доступен только через HTTP.

Вы можете настроить SSL одним из следующих методов:

1. Загрузить свой SSL сертификат на платформу и настроить HTTP/HTTPs;
2. Настроить HTTP или TCP реверс-прокси с SSL-терминацией.

Загрузка SSL-сертификатов в ASMP

Загрузите SSL-сертификаты в формате PEM в каталог `/opt/hw-vmp/vssl`. Обратите внимание, что загруженные файлы не будут перезаписаны при обновлении до следующей версии, поэтому можете смело хранить их в этом каталоге.

Вы можете изменить каталог по умолчанию, если он вам не подходит:

1. Откройте файл `/opt/hw-vmp/config/user.ini` (требуются права root);
2. Добавьте опцию `v.ssl.dir` в раздел `[main]` и укажите новый путь:

```
[main]
v.ssl.dir = /opt/hw-vmp/vssl
```

Чтобы применить изменения, выполните команду:

```
/opt/hw-vmp/bin/reconfig
```

Настройка HTTP/HTTPs

Чтобы настроить перенаправление с HTTP на HTTPs, добавьте следующие параметры в раздел `[main]` файла `/opt/hw-vmp/config/user.ini` (требуются права root):

```
[main]
v.ssl.enabled = ssl_redirect
v.deck.ip.expose = 0.0.0.0
v.deck.port.expose = 80
v.deck.https.ip.expose = 0.0.0.0
v.deck.https.port.expose = 443
```

где:

- `v.ssl.enabled` - опция, которая включает SSL. Возможные значения:
  - `no_ssl` - используется только незащищенное HTTP-соединение (значение по умолчанию);
  - `ssl_both` - используются как незащищенное HTTP-соединение, так и защищенное HTTPs-соединение;
  - `ssl_redirect` - перенаправление с незащищенного HTTP-соединения на защищенное HTTPs-соединение;
  - `ssl_only` - используется только защищенное HTTPs-соединение.
- `v.deck.ip.expose` - IP-адрес для незащищенного HTTP-соединения (`0.0.0.0` - публичный IP-адрес, `127.0.0.1` - локальный IP-адрес). Обязательно для `no_ssl`, `ssl_both` и `ssl_redirect`.
- `v.deck.port.expose` - номер порта для незащищенного HTTP-соединения (значение по умолчанию - 80). Обязательно для `no_ssl`, `ssl_both` и `ssl_redirect`.
- `v.deck.https.ip.expose` - IP-адрес для защищенного HTTPs-соединения (`0.0.0.0` - публичный IP-адрес, `127.0.0.1` - локальный IP-адрес). Обязательно для `ssl_only`, `ssl_both` и `ssl_redirect`.
- `v.deck.https.port.expose` - номер порта для защищенного HTTPs-соединения. Обязательно для `ssl_only`, `ssl_both` и `ssl_redirect`.

Чтобы применить изменения, выполните команду:

```
/opt/hw-vmp/bin/reconfig
```

Настройка HTTP или TCP реверс-прокси с SSL-терминацией

При необходимости вы можете запустить ASMP за вашим собственным реверс-прокси. Например, настройте `nginx`, который будет проксировать все запросы к ASMP.

Чтобы использовать свой прокси-сервер на той же машине, измените следующие параметры в `/opt/hw-bw/config/user.ini` (требуются права root):

```
[main]
v.ssl.enabled = no_ssl
v.deck.ip.expose = 127.0.0.0
v.deck.port.expose = 10001
```

Чтобы применить изменения, выполните команду:

```
/opt/hw-vmp/bin/reconfig
```

Пример конфигурации nginx как HTTP реверс-прокси

1. Пример конфигурации `nginx`:

   ``` server { server_name yourasmp.example.com; access_log /var/log/nginx/yourasmp.example.com-access.log full_log; error_log /var/log/nginx/yourasmp.example.com-error.log;

   ```
   client_max_body_size 0;

   location / {
       proxy_pass http://localhost:10001;
       proxy_set_header Host $host;
       proxy_set_header X-Forwarded-For
   $proxy_add_x_forwarded_for;
       proxy_set_header X-Real-IP $remote_addr;
   }

   listen 443 ssl;
   ssl_certificate /path/to-your/certs/fullchain.pem;
   ssl_certificate_key /path/to-your/certs/privkey.pem;
   }

   server {
       if ($host = yourasmp.example.com) {
           return 301 https://$host$request_uri;
   }

   listen 80;
       server_name yourasmp.example.com;
       return 404;
   }
   ```

   ```

   где:

   - `10001` - номер порта, который вы установили для `v.deck.port.expose` в файле `user.ini`;
   - `yourasmp.example.com` - имя хоста или IP-адрес вашей виртуальной машины.

2. Пример конфигурации `Let's Encrypt` с `certbot`. Вы должны установить эту конфигурацию перед тем, как выдавать сертификаты с помощью `certbot`.

``` server { listen 80; server_name yourasmp.example.com; access_log /var/log/nginx/yourasmp.example.com-access.log full_log; error_log /var/log/nginx/yourasmp.example.com-error.log;

```
   client_max_body_size 0;

   location / {
     proxy_pass http://localhost:10001;
     proxy_set_header Host $host;
     proxy_set_header X-Forwarded-For
```

$proxy_add_x_forwarded_for; proxy_set_header X-Real-IP $remote_addr; } }
```

где:

- `10001` - номер порта, который вы установили для `v.deck.port.expose` в файле `user.ini`;
- `yourasmp.example.com` - имя хоста или IP-адрес вашей виртуальной машины.

Добавление корневых сертификатов

Сначала вам нужно создать каталог `/opt/certs` и скопировать корневой сертификат на платформу:

```
cp ca.pem /opt/certs
```

После этого необходимо указать путь к каталогу с корневыми сертификатами в файле `/opt/hw-vmp/config/user.ini`, добавив там опцию:

```
custom.root.certs.path = /opt/certs
```

Перезапустите платформу (`systemctl restart hw-vmp`) или выполните `/opt/hw-vmp/bin/reconfig`, если вы изменили файл `/opt/hw-vmp/config/user.ini`.

Конвертация CA-сертификата из .PFX

Вам может понадобиться конвертировать CA из .pfx.

1. Создайте SSL-ключ: `openssl pkcs12 -in your_file.pfx -nocerts -nodes -out key.pem`

2. Создайте SSL-сертификат: `openssl pkcs12 -in your_file.pfx -clcerts -nokeys -out domain.pem`

Примечание: если удалить флаг `-out`, то ключ со всей информацией будет выведен на экран. Скопируйте всё, начиная со строки `BEGIN PRIVATE KEY` / `BEGIN CERTIFICATE` и до `END PRIVATE KEY` / `END CERTIFICATE`, и сохраните в файл.

3. Создайте корневой сертификат: `openssl pkcs12 -in your_file.pfx -cacerts -nokeys -chain -out ca.pem`

   Примечание: вы получите цепочку корневых сертификатов. Вам понадобится только последний сертификат в этой цепочке. Например, вы можете открыть файл для редактирования и удалить все, кроме последнего.

4. Объедините файлы в один сертификат: `cat domain.pem ca.pem > cert.pem`

5. Скопируйте SSL-сертификаты на виртуальную машину с установленной платформой в каталог с SSL-сертификатами: `cp cert.pem /opt/hw-vmp/vssl/ cp key.pem /opt/hw-vmp/vssl/`

Настройка логотипа

Вы можете кастомизировать платформу, добавив в неё свои лого и фавикон на окне входа в платформу, в левую панель навигации и верхний левый угол главной страницы.

Чтобы это сделать, выполните следующие шаги:

To do it, perform the following steps:

1. Откройте консоль виртуальной машины;

2. Создайте новую директорию, например: `mkdir /opt/my-logo`

3. Загрузите лого и фавикон в новую директорию. В большинстве случаев вам понадобятся только 3 файла: :

   - favicon.ico - иконка во вкладке браузера, закладках и адресной строке;
   - logo-mini.svg - лого в левой панели навигации (размер лого должен быть 200 x 55 px);
   - logo.svg - лого в верхней панели навигации и странице логина (размер лого должен быть 200 x 55 px).

4. Откройте файл `/opt/hw-fh/config/user.ini` (требуются права root);

5. Добавьте строку `v.deck.logotypes.dir` в раздел `[main]` и укажите путь к лого: `v.deck.logotypes.dir = /opt/my-logo`

6. Чтобы применить изменения, выполните команду: `/opt/hw-vmp/bin/reconfig`

7. Помимо этого, вы можете использовать любой генератор иконок для создания собственного набора фавиконок в разных форматах для разных браузеров (например, Chrome, Safari, и т.п.) и платформ (например, iOS, Android, и т.д.), после чего также добавить в вашу директорию. Пример:

    - apple-touch-icon.png
    - favicon-32x32.png
    - favicon-194x194.png
    - android-chrome-192x192.png
    - favicon-16x16.png
    - safari-pinned-tab.svg

Если вы хотите использовать фавиконы разных размеров, добавьте файл `site.webmanifest` в вашу директорию с логотипом и пропишите необходимые настройки. Пример:

```
{
  icons: [
   {
     src: './android-chrome-36x36.png',
     sizes: '36x36',
     type: 'image/png',
   },
   {
     src: './android-chrome-48x48.png',
     sizes: '48x48',
     type: 'image/png',
   },
   {
     src: './android-chrome-72x72.png',
     sizes: '72x72',
     type: 'image/png',
   },
   {
     src: './android-chrome-96x96.png',
     sizes: '96x96',
     type: 'image/png',
   },
   {
     src: './android-chrome-144x144.png',
     sizes: '144x144',
     type: 'image/png',
   },
   {
     src: './android-chrome-192x192.png',
     sizes: '192x192',
     type: 'image/png',
   },
   {
     src: './android-chrome-256x256.png',
     sizes: '256x256',
```

```
      type: 'image/png',
    },
    {
      src: './android-chrome-384x384.png',
      sizes: '384x384',
      type: 'image/png',
    },
    {
      src: './android-chrome-512x512.png',
      sizes: '512x512',
      type: 'image/png',
    },
  ],
}
```

Фоновые задачи

Иногда при импорте данных могут возникнуть ошибки.

Чтобы выяснить, в чем произошла ошибка, есть раздел в **Administration** под названием **Background tasks**.

На главной странице этого раздела вы можете увидеть список всех процессов, которые выполняются каждый раз, когда вы импортируете результаты сканирования.

Если у вас уже есть UUID ошибки, используйте Ctrl+F или ⌘+F и введите UUID в поле поиска.
Если вы получили ошибку при загрузке скана самостоятельно, вы увидите сообщение в верхней части страницы со ссылкой на неудачную задачу.

Например, на этом скриншоте мы видим, что последний результат сканирования не был загружен.

Давайте нажмем на него, чтобы увидеть, что произошло.

Мы видим, что процесс завершился неудачей на первом этапе - процессе парсинга. Поэтому другие этапы были пропущены.

Также есть значок ошибки. Он кликабельный, и он покажет вам детали ошибки.

Вы можете скопировать результат, нажав кнопку **Copy**.

Если у вас есть какие-либо проблемы с парсерами, вы можете отправить нам сообщение с ошибкой на support@hexway.ru.

Уведомления

Почтовые уведомления

Уведомления отправляются по электронной почте, когда issue со значением severity Critical получает статус **New** или **Reopened**. Каждый член команды репозитория/продукта, к которому относится issue, получает уведомление. Вы можете узнать больше о ролях для репозиториев здесь и для продуктов здесь.

По умолчанию администраторы платформы не получают уведомления об изменениях в репозитории, если они не назначены в репозиторий.

Это может быть изменено в `/opt/hw-vmp/config/user.ini` с помощью добавления строки:

```
v.background.notification.assigned.only = False
```

Настройка SMTP уведомлений

О настройке SMTP уведомлений можно прочитать здесь.