ООО «ТИОНИКС»

Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС» (TIONIX VDI Security)

Версия 1.0

Руководство администратора

RU.НРФЛ.00003-01 95 01

Листов 23

2020

СОДЕРЖАНИЕ

АННОТАЦИЯ

Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС» (английское наименование: TIONIX VDI Security, сокращенное наименование: ПО «TIONIX VDI Security») представляет собой операционную систему (ОС), предназначенную для организации безопасного терминального доступа к рабочим столам клиентских операционных систем, поддерживающих протокол RDP, в т.ч. к рабочим столам виртуальных машин инфраструктуры центра обработки данных (ЦОД).

Документ содержит руководство по настройке и работе с ПО «TIONIX VDI Security». В руководстве приведены условия выполнения программы, состав дистрибутива и инструкции по установке.

Документ предназначен для администраторов ПО «TIONIX VDI Security».

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В документе использованы следующие термины:

Термин	Определение
Администратор системы	Лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
Идентификация	Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Контейнер (контур безопасности)	Изолированные друг от друга виртуальные среды ПО «TIONIX VDI Security», в каждой из которой могут независимо выполняться системные процессы и процессы пользователей ОС.
Контроль целостности	Контроль за сохранением неизменности информации в условиях случайного и (или) преднамеренного искажения (разрушения).
Пароль	Секретный набор символов, используемый субъектом доступа для аутентификации в системе.
Персональный идентификатор	Аппаратно-программное средство персонального использования (электронный ключ), предназначенное для идентификации и аутентификации пользователя.
Объект доступа	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
Учетная запись пользователя	Запись, содержащая информацию о пользователе системы, необходимую для его работы в системе, в том числе сведения, используемые для идентификации и аутентификации пользователя при его подключении (регистрации) к системе.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В документе использованы следующие сокращения:

Сокращение	**Определение**
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ЦОД	Центр обработки данных

1. Назначение программного обеспечения

ПО «TIONIX VDI Security» является операционной системой, реализующей технологию терминального доступа в рамках корпоративной глобальной или локальной вычислительной сети. Целью использования ПО «TIONIX VDI Security» является создание эффективной территориально распределенной безопасной инфраструктуры рабочих мест пользователей компании.

1.1. Описание возможностей

ПО «TIONIX VDI Security» может функционировать в одном из следующих режимах работы (ролей), выбор которого определяется при установке ПО на компьютер:

1. Роль «Сервер безопасности» (выполняется на сервере ЦОД).
2. Роль «Терминал» (выполняется на терминале пользователя).

ПО «TIONIX VDI Security» имеет следующие функциональные возможности:

- идентификация и аутентификация пользователей на терминале, а терминала в системе;
- разграничение доступа к ресурсам системы (файлам, каталогам, приложениям, устройствам и проч.);
- контроль целостности программного обеспечения;
- регистрация событий безопасности;
- возможность работы в нескольких изолированных друг от друга контурах;
- балансировка нагрузки.

1.1.1. Терминал пользователя

При установке ПО «TIONIX VDI Security» в роли «Терминал» на АРМ пользователя в функции ПО входит аутентификация пользователя на терминале, идентификация пользователя и оборудования в системе, проверка целостности загружаемой операционной системы. Также обеспечивается предоставление интерфейса пользователю для работы в различных контурах безопасности с удаленными рабочими столами по протоколу RDP.

1.1.2. Сервер безопасности

При установке ПО «TIONIX VDI Security» в роли «Сервер безопасности» на сервере ЦОД в функции ПО входит аутентификация и идентификация терминалов пользователей, хранение учетных записей пользователей, терминалов в единой базе; сбор и обработка журналов протоколирования событий, происходящих в системе; балансировка нагрузки в системе.

2. Условия применения

2.1. Сервер безопасности

ПО «TIONIX VDI Security» в роли «Сервер безопасности» может быть установлено на виртуальную или аппаратную платформу сервера безопасности, удовлетворяющую минимальным требованиям, указанным в таблице ниже (Таблица 1).

Таблица 1 – Системные требования для сервера безопасности

Параметр	**Значение**
Частота процессора, ГГц	от 2
ОЗУ, Гб	от 8
Жесткий диск, Гб	от 50
Порты для подключения	11391, 11381, 11361, 11371
Платформа	x64

2.2. Терминал

ПО «TIONIX VDI Security» в роли «Терминал» может использовать специализированные устройства, а также персональные компьютеры, отвечающие минимальным требованиям, указанным в таблице ниже (Таблица 2).

Таблица 2 – Системные требования для терминала

Параметр	**Значение**
Частота процессора, ГГц	от 1
ОЗУ, Гб	от 4
Платформа	x86, Baikal-T1

Рабочее место пользователя должно включать следующее оборудование:

- Системный блок (терминал).
- Устройства ввода/вывода (клавиатура, мышь).
- Монитор.

2.3. Состав дистрибутива

Дистрибутив ПО «TIONIX VDI Security» представляет собой файл **tionix2.2-13.10-amd64-14_04_14.iso**, который включает установочный образ операционной системы с компонентами ПО «TIONIX VDI Security», соответствующим различным ролям использования ПО:

- сервисы сервера безопасности;

- сервисы терминальной операционной системы;
- модуль системы разграничения доступа для сервера безопасности srp_shell и srp_auth;
- службы сервера безопасности audit, auth, lb и udd;
- установочный пакет провайдера аутентификации **CredentialProviderInstaller.exe**;
- установочный пакет модуля контроля целостности **hasher;**
- установочный пакет сервиса разграничения доступа **ServerApp.**

2.4. Установка дистрибутива

1. Установка ПО «TIONIX VDI Security» в роли «Сервер безопасности»:

- Примонтировать к машине образ **tionix2.2-13.10-amd64-14_04_14.iso**;
- Выполнить установку операционной системы из образа;
- Выполнить **sudo su** для получения прав администратора;
- Заменить файлы **audit**, **auth**, **lb** и **udd** в **/opt/tionix-dist/auth_co** в соответствующих директориях;
- Выполнить следующие команды:
- cd /opt/tionix-dist
- **install_simplified <ip>** (где <ip> - ip адрес машины)
- cp /opt/tionix-dist/srp_* /opt/tionix
- Заменить файлы srp_shell и srp_auth в /opt/tionix;
- Заменить файлы TermOS в /var/tionix/termos/default/;
- Установить пакеты из **/opt/tionix-dist/pckgs/** при помощи утилиты **dpkg**;
- Установить пакеты lsb-cprocsp-base, lsb-cprocsp-rdr, lsb-cprocsp-capilite, lsb-cprocsp-kc1 при помощи утилиты alien;
- Запустить как демон **/opt/tionix/srp_auth**;
- Выполнить export LD_LIBRARY_PATH=path:/home/tionix/hasher;
- Добавить в /etc/environment строку LD_LIBRARY_PATH=path:/home/tionix/hasher;
- Внести в **/home/tionix/hasher/list.txt** список файлов, подлежащих контролю целостности;
- Запустить /home/tionix/hasher/Integrity_Checker_Start.sh.

2. Установка ПО «TIONIX VDI Security» в роли «Терминал» описана в документе ««Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС». Руководство по установке firmware».

После установки рекомендуется изменить пароль администратора и отключить все неиспользуемые учетные записи пользователей.

3. Функциональные задачи администратора

В функции администратора входит:

- Осуществлять управление политиками безопасности в системе;
- Управлять учетными записями пользователей (добавление, блокирование);
- Устанавливать правила доступа к ресурсам системы (приложения, устройства, каталоги и т.п.) для пользователей;
- Проводить мониторинг событий безопасности;
- Настройка системы.

В разделе приводят инструкции по настройке системы. В тексте могут быть указаны инструкции по решению вопросов в случае возникновения сложностей или сбоев в работе системы.

4. Вход в систему

Настройка и управление системой осуществляется с помощью утилиты администрирования **Tionix Administration tool** непосредственно на сервере безопасности. В дальнейшем настройка системы может осуществляться с терминала пользователя.

4.1. Аутентификация на сервере безопасности

При запуске утилиты администрирования на сервере безопасности необходимо ввести учетные данные администратора (Рисунок 1). По умолчанию, имя пользователя и пароль имеют значение **admin/Ad-M!n.**

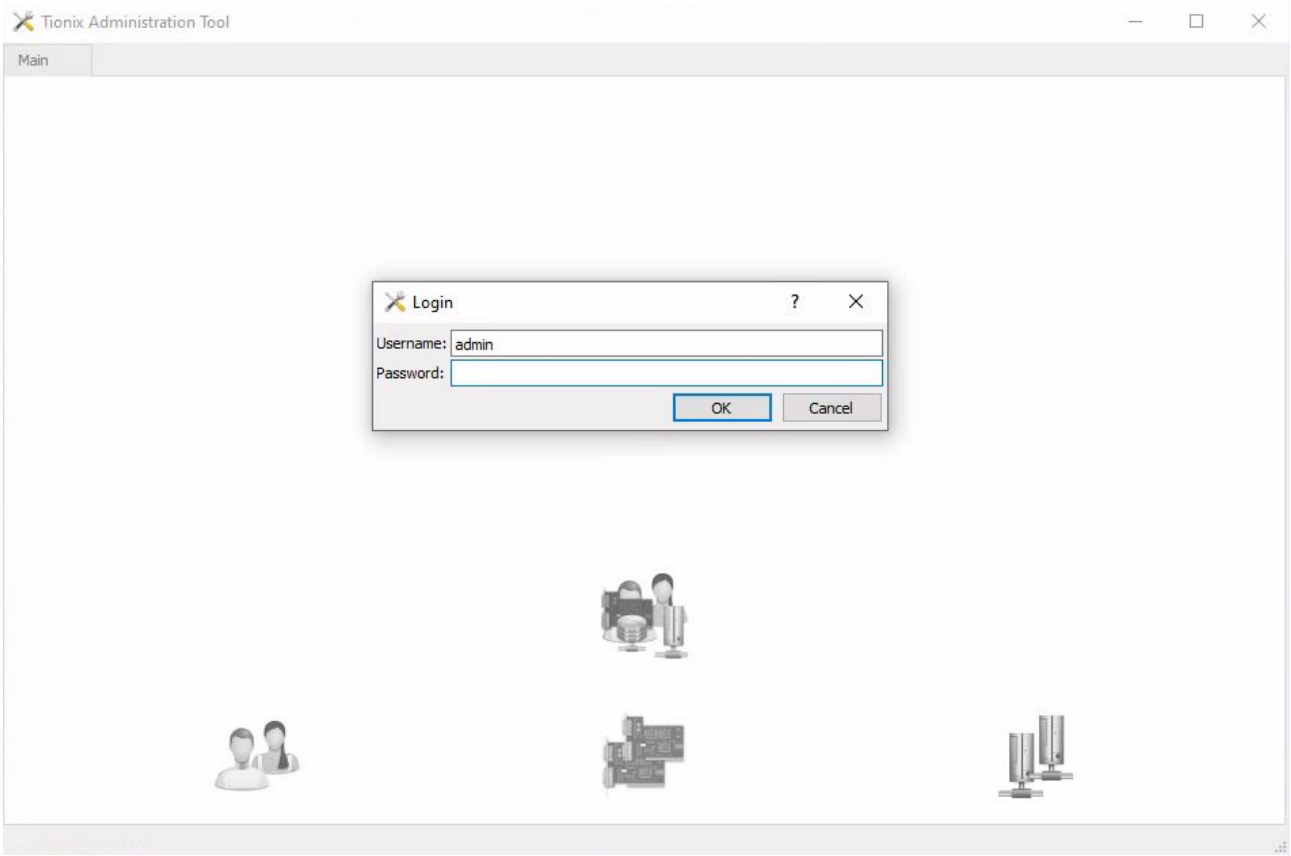

Рисунок 1. Окно ввода учетных данных при аутентификации на сервере безопасности

4.2. Аутентификация на терминале

Перед запуском утилиты администрирования на терминале необходимо начать сеанс работы, введя учетные данные администратора (Рисунок 2).

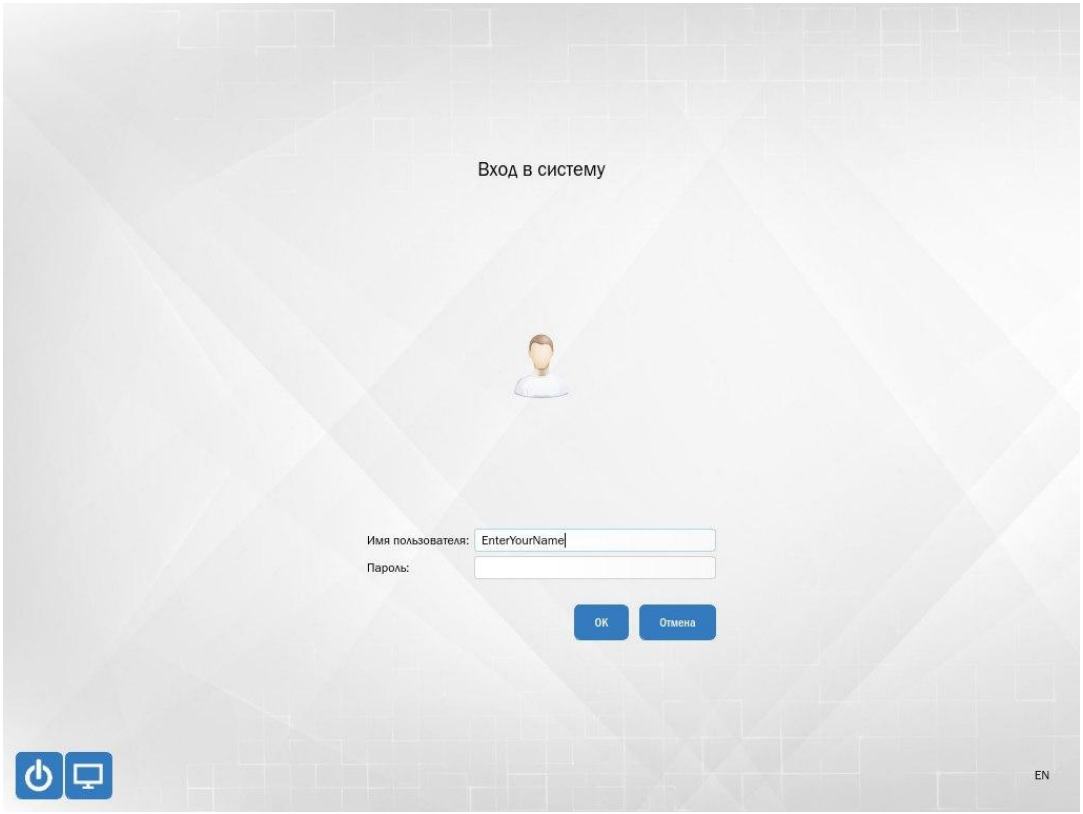

Рисунок 2. Окно ввода учетных данных при аутентификации на терминале пользователя

ВАЖНО

При первом входе в систему рекомендуется сменить пароль. Более подробно эта процедура рассмотрена в разделе 6.

ВАЖНО

При первом входе в систему через терминал в качестве рабочего стола пользователю назначается рабочий стол по умолчанию.

5. Управление политиками безопасности

Управление политиками безопасности осуществляется с помощью утилиты администрирования, вкладка **Main** (Рисунок 3).

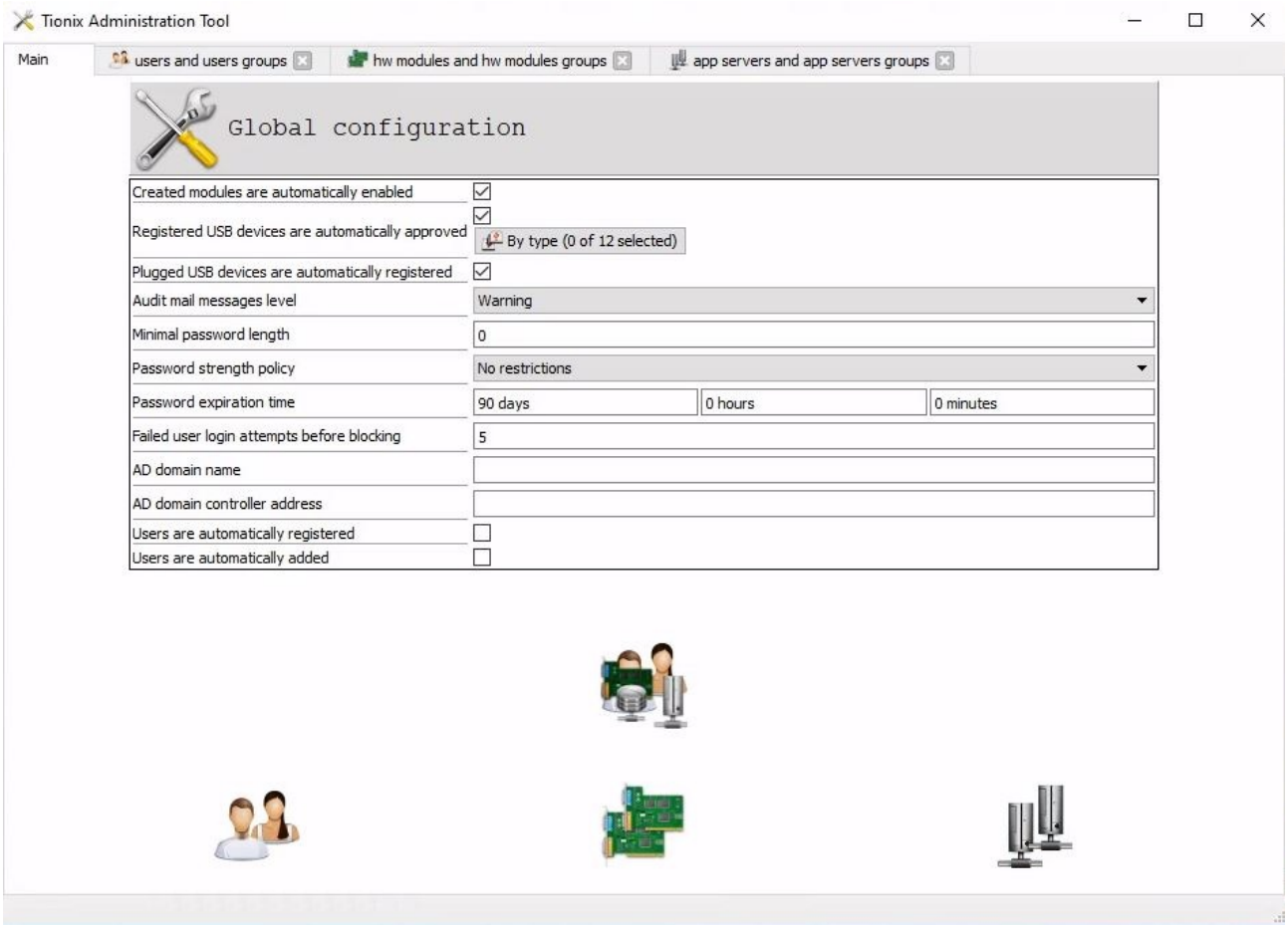

Рисунок 3. Утилита администрирования. Настройки политик безопасности

5.1. Политики для пароля доступа

Для всех пользователей устанавливаются единые политики сложности пароля доступа.

Регулируется длина пароля, задается минимальное количество символов **(Minimal password length)**.

Устанавливается период действия пароля **(Password expiration date)**.

Устанавливается политики стойкости пароля **(Password strength policy).**

Доступны следующие политики:

- Пароль должен содержать буквы и цифры **(letters and digits required)**. Требований к регистру не предъявляется;
- В пароле должны содержаться буквы (прописные и строчные) и цифры, **(letters of different case and digits required)**;

– В пароле должны содержаться буквы (прописные и строчные), цифры и специальные символы **(letters of different case, digits and special symbols required**).

5.2. Регистрация и подключение устройств

Система позволяет управлять политиками безопасности, устанавливая режим контроля подключенных устройств.

В случае если установлен флаг **Created modules are automatically enabled** - разрешение на автоматическую регистрацию модулей (устройств вычислительной техники, в том числе терминалов, серверов), то при подключении устройства к системе, его регистрация пройдет автоматически.

В случае если установлен флаг **Plugged USB devices are automatically registered** - разрешение на автоматическую регистрацию подключаемых к терминалу устройств**,** то при подключении устройства к терминалу, оно автоматически будет зарегистрировано.

В случае если установлен флаг **Registered USB devices are automatically approved** - разрешение на автоматическое подтверждение регистрации подключаемых устройств**,** то при регистрации устройства пользователем, оно будет автоматически одобрено администратором системы. Данная процедура проводится на стороне администратора системы.

Также можно выбрать определенный тип устройств, которые будут автоматически одобрены для использования в системе **(By type)** (Рисунок 3).

5.3. Сообщение о работе системы

Система позволяет установить уровень важности события, по которому будут сортироваться сообщения системы и направляться соответствующей группе пользователей **(log watchers);** параметр устанавливается в поле **(Audit mail messages level)**. Данное правило позволяет вовремя реагировать на нарушение режима безопасности, состояние системы, возможные сбои в работе и т.п. Уровни важности описаны в **разделе 8**.

5.4. Блокирование учетной записи пользователя

С целью предотвращения несанкционированного доступа и возможной атаке перебора пароля рекомендуется указать максимальное количество попыток для входа систему в случае набора неправильного пароля **(Failed user login attempts before blocking)**. После указанного значения данная учетная запись пользователя будет заблокирована.

5.5. Доступ к объектам

Доступ к объектам, таким как подключаемые устройства, приложения, осуществляется с помощью соответствующих инструментов утилиты администрирования. Процедуры описаны в разделе 7 настоящего руководства.

6. Управление учетными записями пользователей

6.1. Создание учетной записи пользователя

Чтобы создать новую учетную запись пользователя, необходимо:

1. Запустить утилиту администрирования **Tionix Administration tool** на сервере безопасности или терминале и перейти во вкладку **Users and users groups** (
2. Рисунок 4). Навести курсор на свободное поле окна со списком пользователей и нажать  ;
3. В появившемся меню выбрать **Create a new user** (создать нового пользователя) или **Create a new users group** (создать новую группу пользователей);
4. В новой строке списка задать имя учетной записи пользователя и нажать **Enter**;
5. Перейти форму данных и установить флаг **Is Active**;
6. Указать пароль доступа, нажав **Change password**;
7. Ввести данные пользователя. При необходимости добавить пользователя в группу. Вид формы ввода данных приведен на рисунке (
8. Рисунок 4). Описание полей формы приведено ниже;
9. Предоставить доступ к устройствам и приложениям для данного пользователя, добавив компоненты в поля и **User's_USB devices** и **User's applications**, соответственно.

Для удаления учетной записи, необходимо навести курсор на выбранного пользователя и нажать  .

6.2. Смена пароля доступа

Для смены пароля доступа необходимо в окне **Users and users groups** (Рисунок 4) утилиты администрирования **Tionix Administration tool,** выбрать учетную запись **admin**, нажать кнопку **Change password**, ввести новый пароль и его подтверждение.

В дальнейшем пароль доступа можно сменить либо с помощью утилиты администрирования, либо в панели управления терминальной операционной системы при работе с терминалом. Более подробно этот процесс описан в документе ««Программное обеспечение «Защита виртуальных рабочих столов ТИОНИКС». Руководство пользователя».

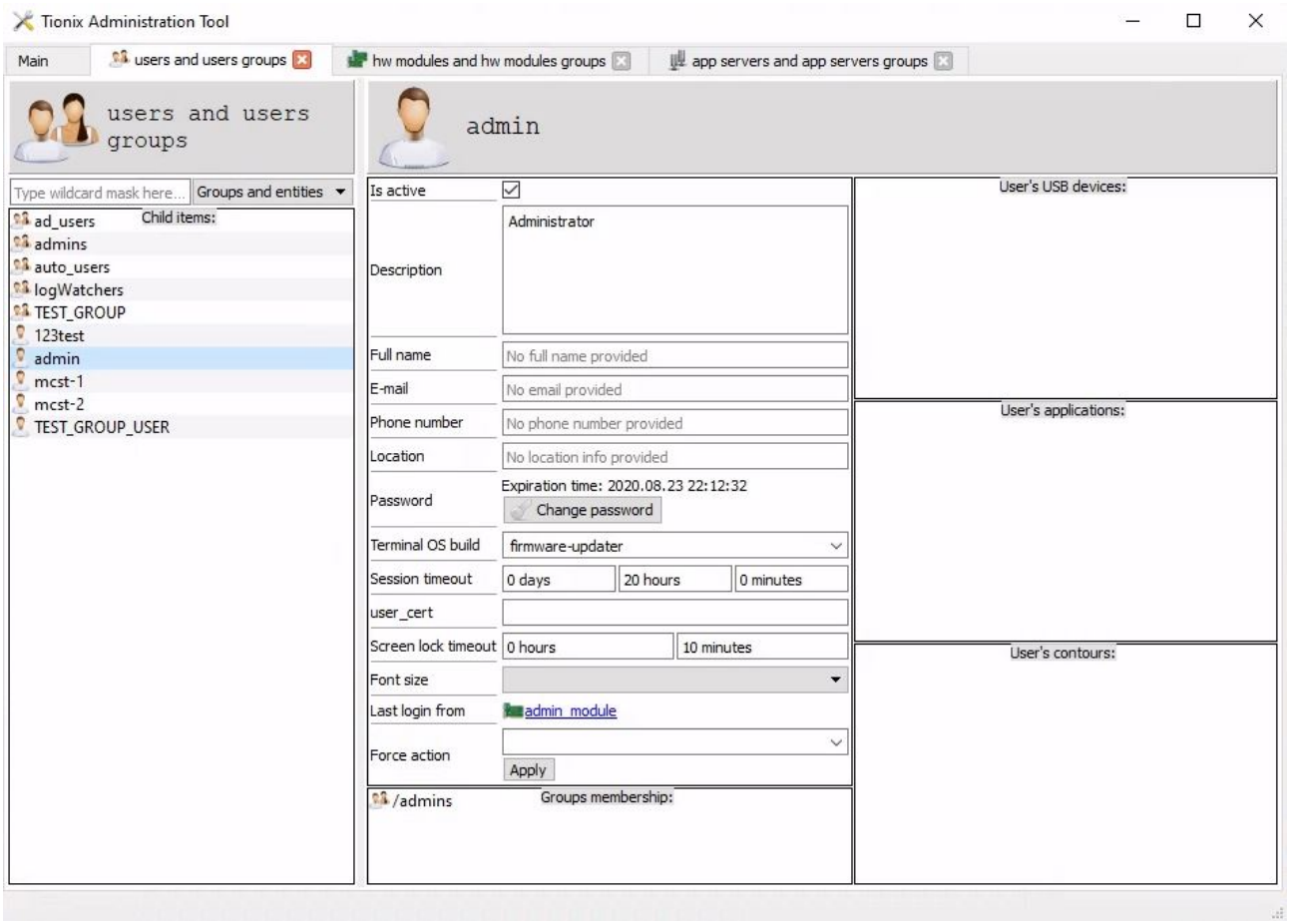

Рисунок 4. Утилита администрирования. Управление данными учетной записи пользователя

Is active – флаг активации объекта доступа;

Description – краткое описание для пользователя;

Full Name – полное имя пользователя;

E-mail – электронный адрес пользователя;

Phone number – номер телефона пользователя;

Location – место расположения рабочего места пользователя;

Password – пароль для учетной записи пользователя. Также указывается дата окончания действия пароля;

Terminal OS build – назначается тип сборки операционной системы;

Session timeout – время до блокировки сессии пользователя при отсутствии действий;

Screen lock timeout – время до отключения экрана в случае неактивности пользователя;

Font Size – размер шрифта, на рабочем столе пользователя;

Last login from – указывается идентификационный номер устройства, с которого пользователь заходил в систему в прошлый раз.

6.3. Группы пользователей

Во время установки системы автоматически создается две группы пользователей:

- **Группа администраторов системы (Admin).** В данную группу включаются администраторы системы, администраторы безопасности;
- **Группа наблюдателей (log watchers).** В данную группу могут быть включены любые пользователи, включая системных администраторов и администраторов безопасности, а также лица, в должностные обязанности которых входит контроль соблюдения установленных политик информационной безопасности на предприятии. Сообщения о работе системы будут направляться им на указанный в профиле пользователя адрес электронной почты.

6.3.1. Создание групп пользователей

Чтобы создать новую группу пользователей необходимо:

1. Запустить утилиту администрирования **Tionix Administration tool** на сервере безопасности или терминале и перейти во вкладку **Users and user groups** (Рисунок 4)**.** Навести курсор на свободное поле окна со списком пользователей и нажать на кнопку  ;
2. Навести курсор на свободное поле окна со списком пользователей и нажать  ;
3. В появившемся меню выбрать **Create a new users group** (создать новую группу пользователей);
4. В новой строке списка задать имя группы и нажать **Enter**;
5. Перейти в форму и установить флаг **Is Active**;
6. Ввести данные группы;
7. Предоставить доступ к устройствам и приложениям для данного пользователя, добавив компоненты в поля и **User's_USB devices** и **User's applications**, соответственно**.**

Чтобы удалить запись, необходимо навести курсор на выбранную группу и нажать  .

6.3.2. Добавление пользователя в группу

Чтобы добавить пользователя в группу, необходимо навести курсор на поле **Groups membership**, во вкладке **Users and user groups** форме пользователя нажать  и выбрать группу из списка. Установить флаг **Is Active** и заполнить форму.

6.3.3. Блокировка пользователя или группы пользователей

Для блокировки необходимо во вкладке **Users and users group** (Рисунок 4) выбрать необходимую запись и в открывшемся окне убрать флаг **Is Active**. После того как пользователь будет заблокирован, доступ к системе будет запрещен.

7. Разграничение доступа к ресурсам системы

Система позволяет управлять доступом к различным объектам системы: приложениям и устройствам. Доступ к объектам системы может быть установлен как для отдельных пользователей, так и для групп пользователей. Управление осуществляется с помощью утилиты администрирования.

7.1. Файлы и каталоги

Настройка разграничения доступа к файлам и каталогам осуществляется администратором, согласно правилам доступа, установленным на предприятии.

7.2. Приложения

Список всех приложений, доступных для данного пользователя (Рисунок 4) представлен в окне **User's Applications** .

Чтобы предоставить пользователю доступ к приложению, необходимо:

- Перейти во вкладку **User and User's group** утилиты администрирования. Навести курсор на поле **User's applications** и нажать  .
- Выбрать из появившегося списка нужные приложения, и нажать **Ок**. После этого на рабочем столе пользователя появятся иконки опубликованных приложений.
- Если иконки отсутствуют, необходимо проверить доступно ли данное приложение для использования в системе. Для этого нужно перейти во вкладку **App servers and app servers groups** (Рисунок 6.), выбрать сервер, на котором установлены выбранные приложения.
- Далее перейти в свойства объекта и проверить установлен ли флаг **Is Active.** Для этого необходимо выделить строку с нужным объектом и нажать среднюю кнопку мыши.

Чтобы заблокировать доступ к приложению для пользователя необходимо выделить его в окне **User's applications** и нажать  .

Чтобы удалить приложения из списка доступных на данном сервере, необходимо в свойствах объекта убрать флаг **Is Active**.

7.3. Управление внешними устройствами

7.3.1. Устройства

Чтобы предоставить доступ к подключенному устройству в системе необходимо зарегистрировать устройство в определенном контуре.

ВАЖНО

Перед тем как пользователь сможет зарегистрировать устройство в контуре, необходимо установить драйверы для него.

После подключения устройства к терминалу, его наименование появится в списке подключенных устройств в панели управления терминальной операционной системы (Рисунок 5)**.**

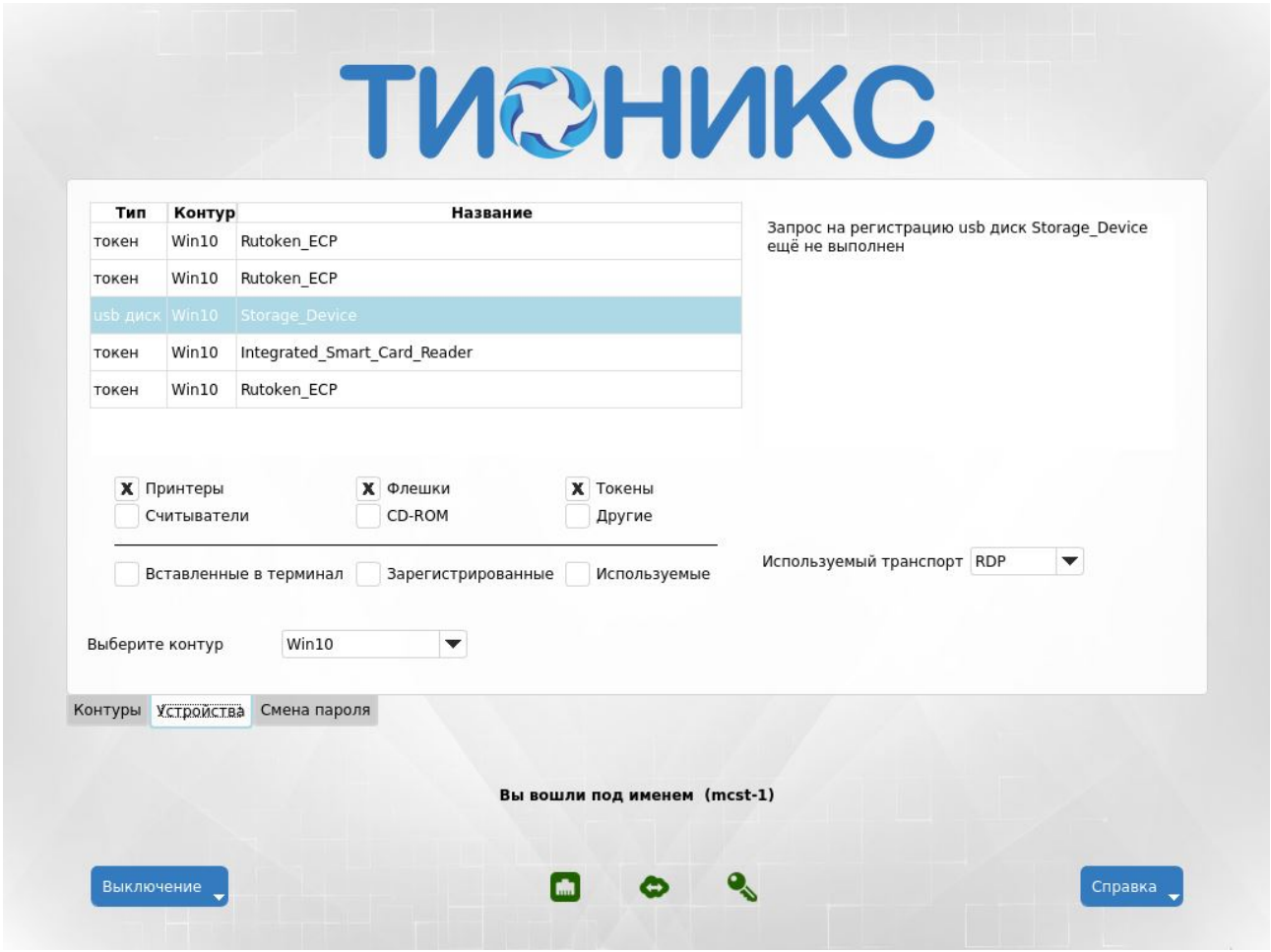

Рисунок 5. Панель управления терминальной операционной системы. Устройства

Далее необходимо проверить контур, в котором будет зарегистрировано устройство (устройство регистрируется в том контуре, в котором находится в данный момент пользователь). Выделить строку с устройством и нажать **Подключить.**

Для подтверждения регистрации USB устройства, необходимо запустить утилиту администрирования и перейти во вкладку **App servers and app servers groups**. В поле **Child items** выбрать подключенное пользователем и зарегистрированное в контуре устройство, отметить установить флаг **Is Active**. После этого устройство становится доступным для пользователя.

Чтобы отключить USB устройство, необходимо в меню управления USB устройствами выделить строку с нужным устройством и нажать **Отключить.**

Работа с подключенными устройствами ведется так же, как если бы они были подключены к локальному компьютеру пользователя.

Чтобы заблокировать доступ к USB устройству необходимо перейти во вкладку **App servers and app servers groups** (Рисунок 6) и выбрать терминал, в котором зарегистрировано устройство. Далее необходимо выбрать устройство в поле **Child items** и в открывшемся окне убрать флаг **Is Active**.

7.3.2. Внешние устройства, подключаемые к серверу или терминалу

При подключении новых устройств к терминалу пользователя их идентификаторы (номер, присвоенный в процессе идентификации) автоматически заносятся в группу

auto_registered утилиты администрирования. Информацию об этом можно просмотреть во вкладке **Hw modules and hw modules groups утилиты** администрирования (Рисунок 6). Описание полей формы приведено ниже.

Чтобы просмотреть включенные в группу устройства, необходимо выделить ее название и в правой колонке отобразится весь перечень оборудования.

Чтобы заблокировать устройство, необходимо выбрать нужную запись и в открывшемся окне убрать флаг **Is Active**.

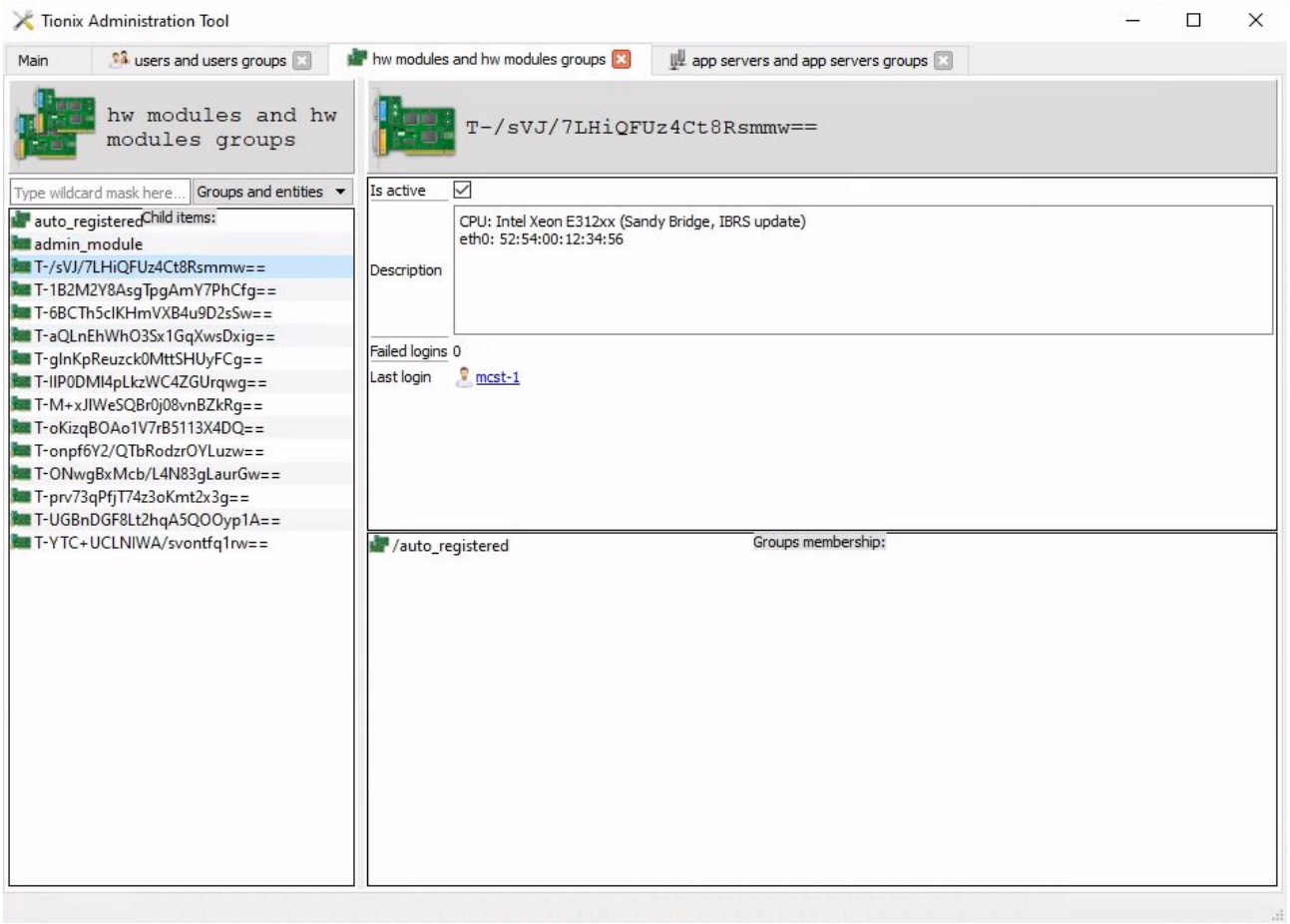

Рисунок 6. Утилита администрирования. Настройка параметров подключенных устройств

Is Active – флаг активации объекта доступа;

Description – краткое описание объекта доступа;

Last Login – учетная запись пользователя, который проходил процедуру авторизации на этом оборудовании или идентификатор оборудования;

Failed Login – количество неудачных попыток авторизации с текущего устройства.

ПРИМЕЧАНИЕ

В системе регистрируются только те устройства, которые подключены к терминалу пользователя.

7.3.3. Управление ресурсами системы

Для удобства работы в системе предусмотрена возможность просмотра всех имеющихся объектов доступа и настройки их параметров с помощью вкладки **Everything** (Рисунок 7).

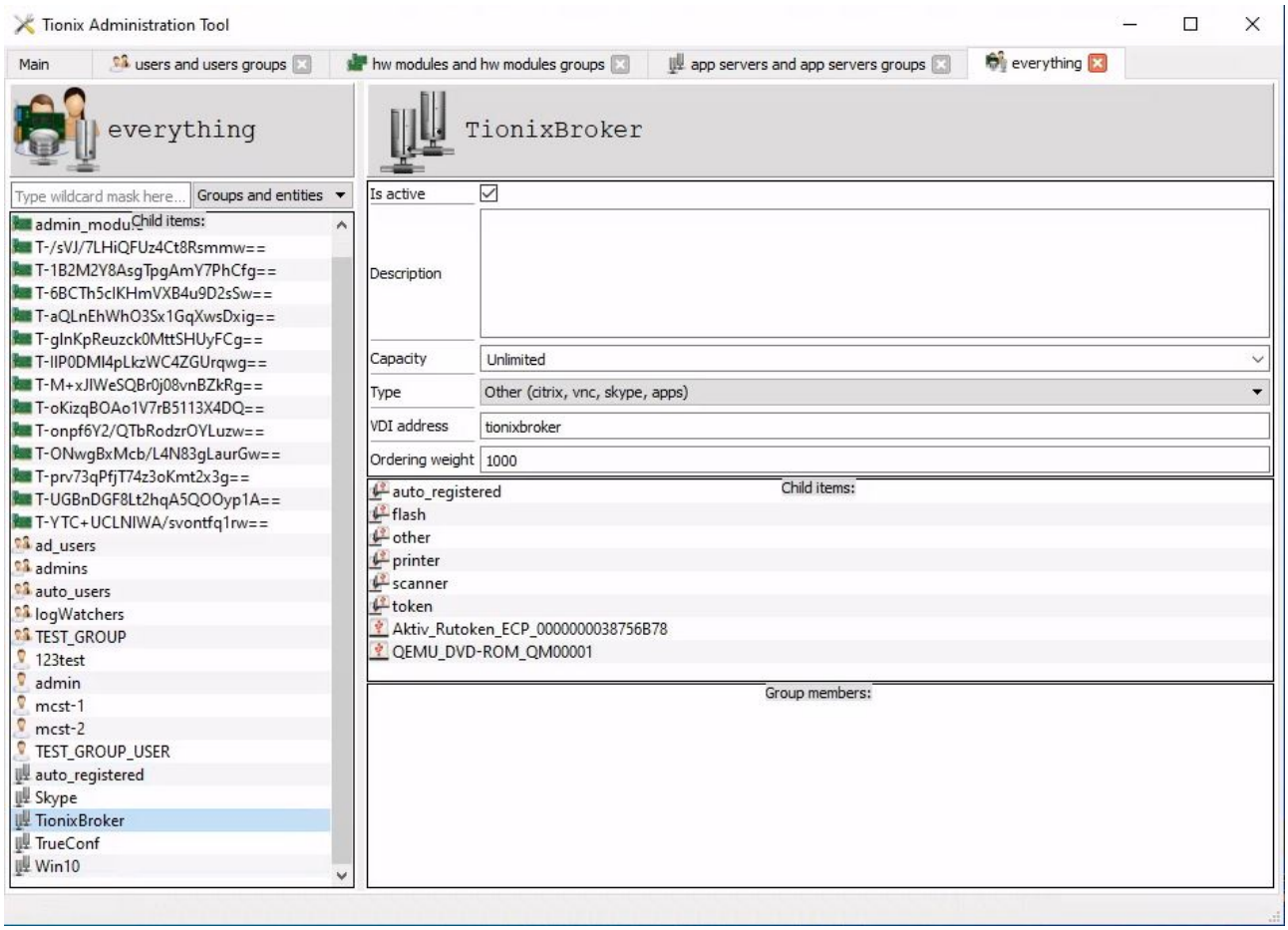

Рисунок 7. Утилита администрирования. Настройка параметров

8. Просмотр журнала событий

Просмотр журналов регистрации событий осуществляется при помощи утилиты **Tionix audit tool**.

Установка утилиты производится при инсталляции ПО «TIONIX VDI Security» в роли «Сервер безопасности». Для запуска и работы программы дополнительных настроек не требуется.

Запуск утилиты возможен как локально на сервере безопасности, так и через терминал. Для возможности запуска через терминал.

Производится регистрация следующих событий:

- Попытки входа/выхода субъектов доступа в систему/из системы. Должна осуществляться регистрация введения новых пользователей системы и изменения их полномочий;
- Изменение статуса объектов доступа с регистрацией внесенных изменений, времени и даты внесения изменений, а так же кем внесены изменения;
- Попытки несанкционированного доступа субъектов к именованным объектам;
- Создание/модификация/удаление пользователей, модулей, группы пользователей, групп модулей, групп серверов (контуров), приложений, USB-устройств администратором;
- Все неудачные попытки обращения к сервисам (например, попытка модификации контура пользователем без администраторских прав);
- Загрузка пользователем терминальной операционной системы;
- Запуск и корректная остановка приложений пользователем;
- Подключение/отключение USB-устройств пользователем;
- Выключение терминала пользователем;
- Очистка журнала.

Для каждого события обязательно сохраняются следующие поля:

- **time_recv** – время получения;
- **level** – уровень важности;
- **sender** – отправитель;
- **message** –текст сообщения.

Чтобы установить количество записей, отображаемых на экранной странице, необходимо в поле **Items per page** выбрать нужное значение.

Чтобы отсортировать события по важности, необходимо выставить значение в поле **Level:**

Warning – Сообщения, предупреждающие о подключении устройств к терминалам пользователей, ошибках в авторизации пользователей;

Notice – Сообщения о попытке подключения зарегистрированных устройств, смене пароля и т.п.;

Info – Информация о работе системы;

Debug – Информация о работе системы, включая служебную информацию.

Чтобы очистить журнал, необходимо нажать кнопку **Clear**.

Чтобы обновить журнал, необходимо нажать кнопку **Refresh**.