Консоль управления Aether

С чего начать

Panda Endpoint Protection

Panda Endpoint Protection Plus

Panda Adaptive Defense

Panda Adaptive Defense 360

Содержание

Список рисунков

Цель данного документа

Данный документ содержит описание процедуры быстрой установки корпоративного облачного решения безопасности Panda с веб-консолью централизованного управления Aether, а также основные шаги, которые Вам необходимо сделать для настройки и внедрения Panda в корпоративной сети.

Данный документ будет полезен при тестировании корпоративного решения Panda, а также при его первоначальном внедрении.

Информация, представленная в данном документе, справедлива для решений Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Adaptive Defense и Panda Adaptive Defense 360.

Предварительные действия

Прежде чем начать установку корпоративного решения Panda, убедитесь, что:

1. У Вас есть регистрационные данные для доступа к облачной консоли централизованного управления Aether корпоративного решения Panda.
2. Вы ознакомились с системными требованиями, а главное, - со списком **URL и портов для корректной работы продукта**:
    a. Windows: http://go.pandasecurity.com/endpoint-windows/requirements
    b. Mac OS: http://go.pandasecurity.com/endpoint-macos/requirements
    c. Linux: http://go.pandasecurity.com/endpoint-linux/requirements
    d. Android: http://go.pandasecurity.com/endpoint-android/requirements
    e. Требуемые URL и порты: https://www.pandasecurity.com/russia/support/card?id=700006
    f. Требования к кеш-компьютерам: https://www.pandasecurity.com/russia/support/card?id=700028
    g. Совместимые браузеры для доступа к консоли управления: https://www.pandasecurity.com/russia/support/card?id=700011
    h. Требования к прокси-компьютерам: https://www.pandasecurity.com/russia/support/card?id=700030
    i. Требования для опций обнаружения компьютеров и удаленной установки: https://www.pandasecurity.com/russia/support/card?id=700024

1. Подключение к консоли управления

Для того чтобы установить защиту корпоративного решения Panda, Вам необходимо войти в облачную консоль централизованного управления Aether.

1. **Если Вы – новый пользователь**: При регистрации лицензий корпоративного решения Panda на указанный Вами адрес электронной почты должно прийти **пригласительное письмо**, в котором имеется ссылка для активации корпоративного аккаунта Panda. Пройдите по ней, активируйте новый аккаунт, после чего сможете подключиться к облачной консоли Panda со своим логином (адрес электронной почты) и паролем.
2. **Если Вы – действующий пользователь:** Если лицензии были зарегистрированы на имеющийся у Вас корпоративный аккаунт Panda, то Вы можете использовать имеющиеся у Вас регистрационные данные для доступа к облачной консоли:
    a. Откройте страницу https://www.pandacloudsecurity.com
    b. Введите Ваши логин и пароль
    c. Нажмите кнопку **Войти**

2. Быстрая установка защиты на Ваш ПК

2.1. Установка защиты

Если Вы впервые заходите в консоль управления Panda и/или в рамках Вашего аккаунта Вы еще ни разу не устанавливали защиту, то Вы увидите начальную страницу с предложением добавить компьютеры. В рамках быстрой установки Вы сможете установить защиту на требуемые компьютеры с настройками по умолчанию. В любом случае позже Вы сможете изменить настройки компьютеров и безопасности по Вашему усмотрению.

Чтобы осуществить быструю установку на Ваш компьютер, нажмите кнопку **Добавить компьютеры**.

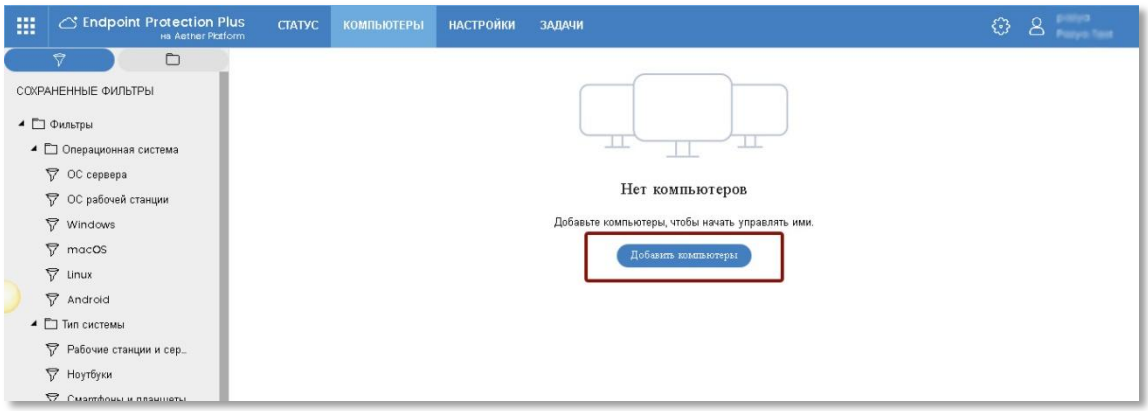


Рис. 1. Быстрая установка защиты

В результате этого откроется окно для выбора операционной системы компьютера, на который планируется установить защиту Panda.

Рис. 2. Выбор операционной системы компьютера

В рамках быстрой установки выберите операционную систему вашего компьютера (например, Windows), нажав на ее логотип. После этого откроется окно для выбора параметров установки.

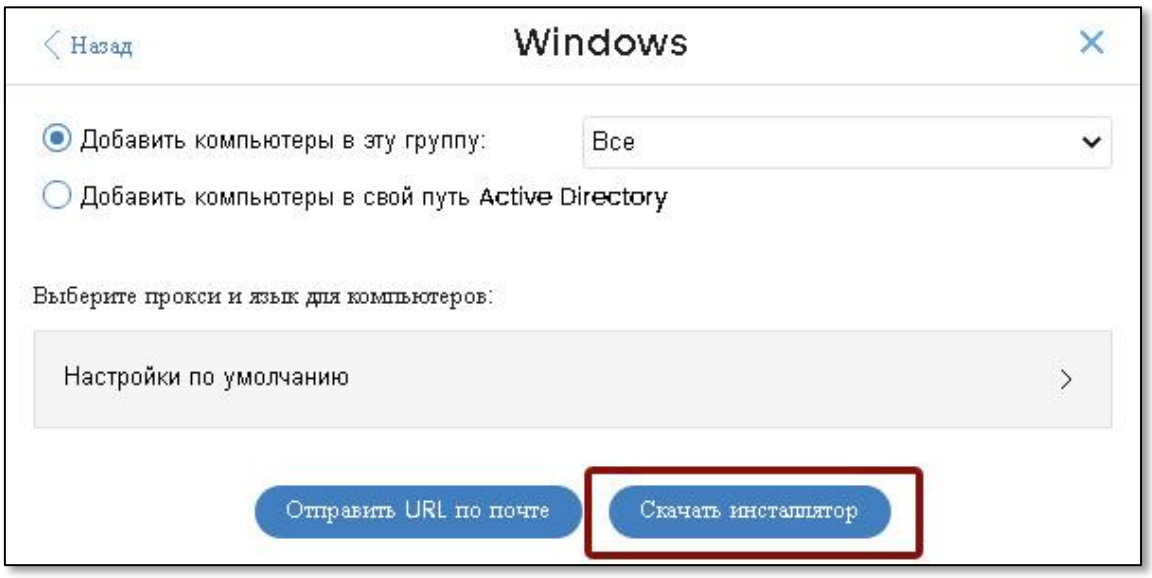


Рис. 3. Скачивание инсталлятора

В данном окне нажмите на кнопку **Скачать инсталлятор**. В результате этого на Ваш компьютер будет скачен файл **Panda Endpoint Agent.msi**. Далее выполните следующие действия:

1. Удалите Ваше текущее антивирусное решение и перезагрузите Ваш компьютер.
   Если Вы устанавливаете решение Panda Adaptive Defense, то удалять текущее корпоративное решение не требуется – просто пропустите этот шаг

2. Запустите **Panda Endpoint Agent.msi** для начала установки защита Panda.

3. Нажмите на кнопку **Next**, чтобы начать процесс установки, а после кнопку **Install**. На компьютер будет установлен локальный агент защиты *Panda Endpoint Agent*.

4. Нажмите на кнопку **Finish** для окончания работы мастера установки.

5. Дважды нажмите на иконку Panda, расположенную в системном трее на панели задач, чтобы увидеть индикатор установки *Panda Endpoint Protection*. Процесс установки может занять несколько минут.

   Также Вы можете увидеть индикатор установки в консоли. Подключитесь к консоли и выберите в главном меню **Компьютеры**.

В процессе установки Вас попросят перезагрузить компьютер для окончания установки. Пожалуйста, перезагрузите компьютер, когда это потребуется.

После выполнения вышеописанных шагов Ваш компьютер будет защищен с помощью корпоративного решения Panda.

2.2. Проверка корректности работы защиты

Чтобы проверить, что Ваша защита работает корректно, Вы можете выполнить следующее действие:

Откройте страницу http://www.eicar.org/download/eicar.com. В этом случае будет осуществлена попытка скачать файл, который каждое антивирусное решение распознает как Eicar-Test-File[1].

Поздравляем! Теперь Ваш компьютер корректно защищен с помощью корпоративного решения Panda.

Вы можете более корректно настроить Вашу защиту, выполнив основные шаги, которые представлены в следующей главе 2.

При установке защиты по умолчанию, вполне возможно, что защита будет установлена на английском языке. Вы всегда можете изменить настройки языка в консоли управления.

[1] Eicar-Test-File – это файл, разработанный European Institute for Computer Antivirus Research для тестирования отклика антивирусных программ. Для получения более подробной информации посетите: www.eicar.org.

3. Основные шаги по внедрению Panda в сети

Первая глава данного документа содержит информацию о быстрой установке корпоративной защиты Panda на Ваш компьютер в рамках настроек по умолчанию. В настоящей главе представлено несколько основных и очень простых шагов, выполнение которых позволит Вам более корректно внедрить и настроить защиту всех требуемых компьютеров и устройств с помощью корпоративного решения Panda.

Если Вам необходима справочная информация о работе продукта, доступ к руководству для администратора и т.д., просто нажмите на кнопку с шестеренкой в правом верхнем углу веб-консоли и в выпадающем меню выберите соответствующий пункт.

Если у Вас имеются вопросы или Вам необходима дополнительная помощь, пожалуйста, не стесняйтесь обращаться к своему поставщику или в офис компании Panda Security, все контактные данные которого представлены в конце документа.

3.1. Шаг 1: Настройка параметров

Консоль управления позволяет Вам настраивать параметры компьютеров, сети и безопасности. В результате формируются профили, которые впоследствии могут назначаться требуемым компьютерам. Настройку параметров можно осуществлять как до установки локальных агентов защиты, так и после.

Для настройки параметров перейдите в раздел **Настройки**.

3.1.1. Настройка безопасности рабочих станций и серверов

В разделе **Настройки** откройте подраздел **Безопасность** -> **Рабочие станции и серверы**. Здесь осуществляется настройка параметров безопасности для рабочих станций и серверов Windows, Linux и Mac.

По умолчанию имеется профиль *Настройки по умолчанию*, который невозможно изменить или удалить. Поэтому Вы можете создать собственный профиль, нажав на кнопку **Добавить**.

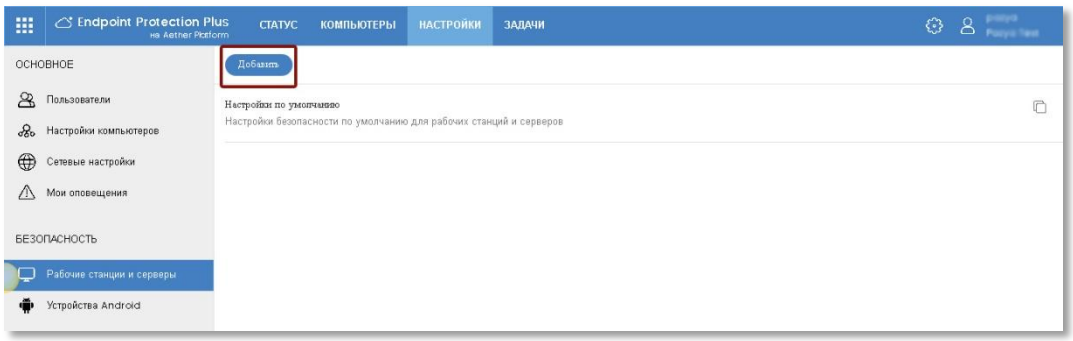


Рис. 4. Рабочие станции и серверы

На странице добавления профиля укажите его имя, краткое описание (необязательно) и нажмите кнопку **Сохранить**.

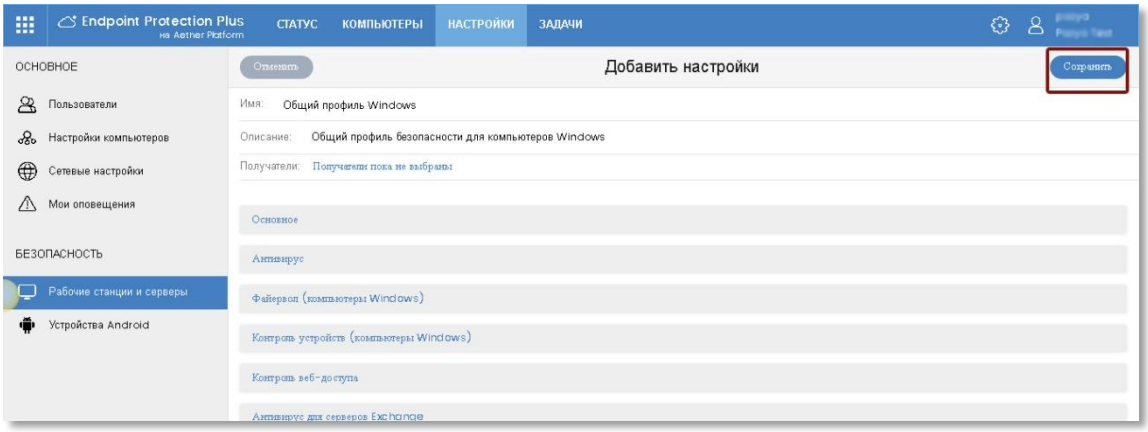


Рис. 5. Добавление профиля безопасности

После этого в сохраненном профиле Вы можете осуществить основные настройки параметров безопасности и все требуемые настройки различных модулей продукта.

*Если Вы собираетесь устанавливать Panda Adaptive Defense или Panda Adaptive Defense 360, то обратите внимание на настройку модуля Расширенная защита. Рекомендуется на первые несколько дней работы установить режим **Audit**, после чего можно будет перевести в режим **Hardening** или **Lock**. Подробнее смотрите в Руководстве пользователя.*

3.1.2. Настройка компьютеров

В разделе **Настройки** выберите подраздел **Настройки компьютеров**. Здесь осуществляется настройка основных параметров работы защиты на защищаемых устройствах. Здесь также есть профиль *Настройки по умолчанию*, но Вы можете создать собственные профили, нажав на кнопку **Добавить**.

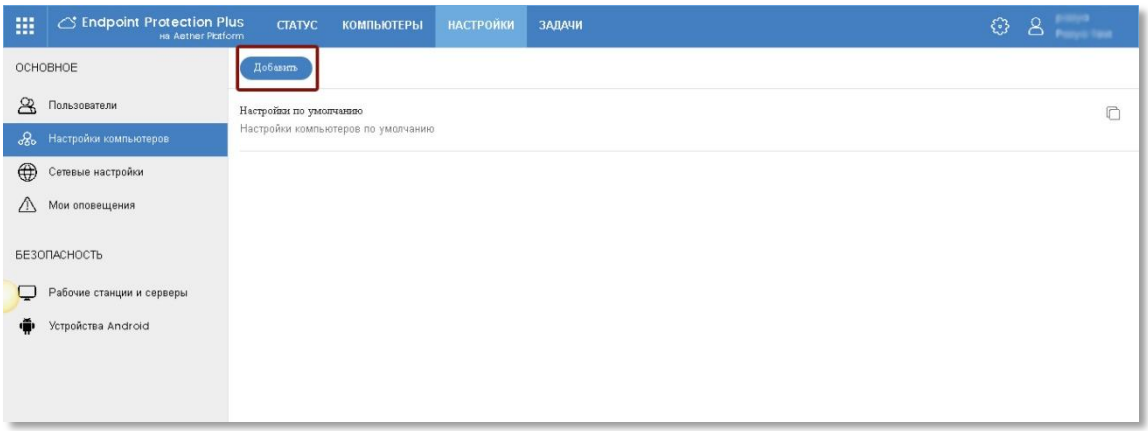


Рис. 6. Настройки компьютеров

В результате этого откроется страница с добавлением профиля настроек.

На странице добавления профиля укажите его имя, краткое описание (необязательно) и нажмите кнопку **Сохранить**.

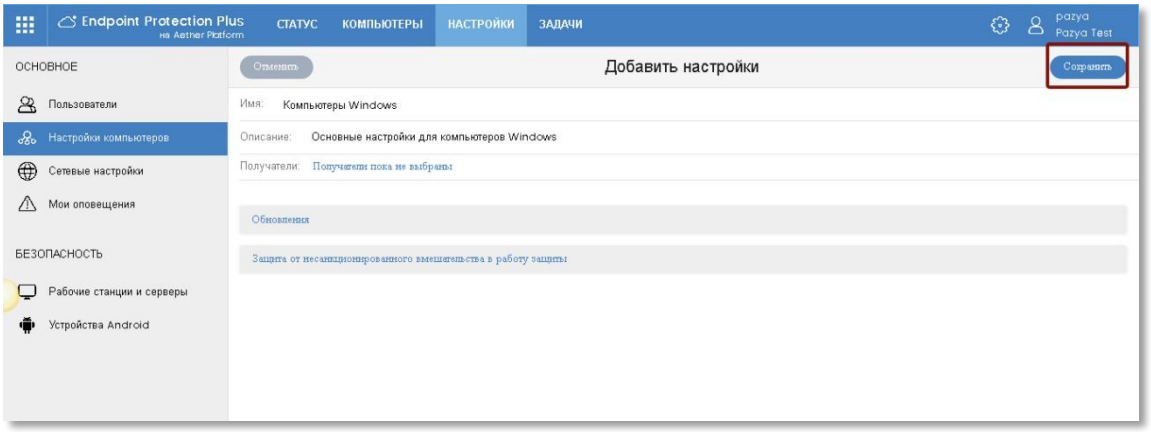


Рис. 7. Добавление профиля настроек компьютеров

Настройки представлены в двух секциях: **Обновления** и **Защита от несанкционированного вмешательства в работу защиты**. Укажите требуемые настройки.

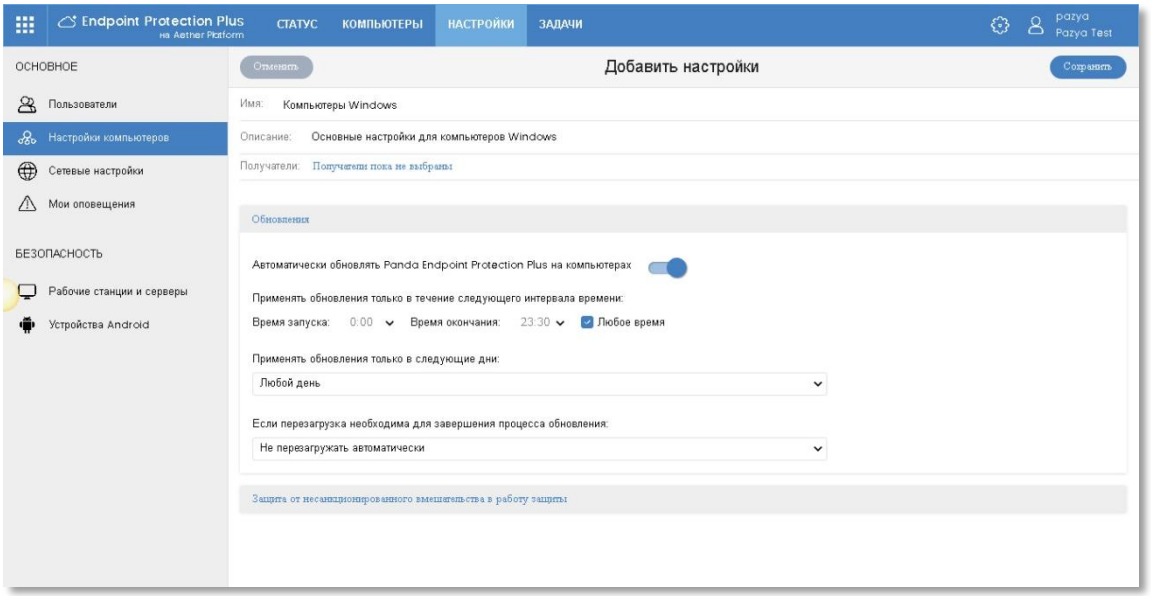


Рис. 8. Настройки обновления защиты компьютеров

В настройках обновлений Вы можете указать параметры обновления локальных агентов корпоративного решения Panda. Рекомендуемся включить автоматические обновления в любое время, но при необходимости Вы можете указать конкретный график обновлений (определенные дни и часы).

Кроме этого, укажите, следует ли автоматически перезагружать компьютеры для завершения процесса обновления (если требуется), и если требуется, то какие именно (только серверы, только рабочие станции или и то, и другое).

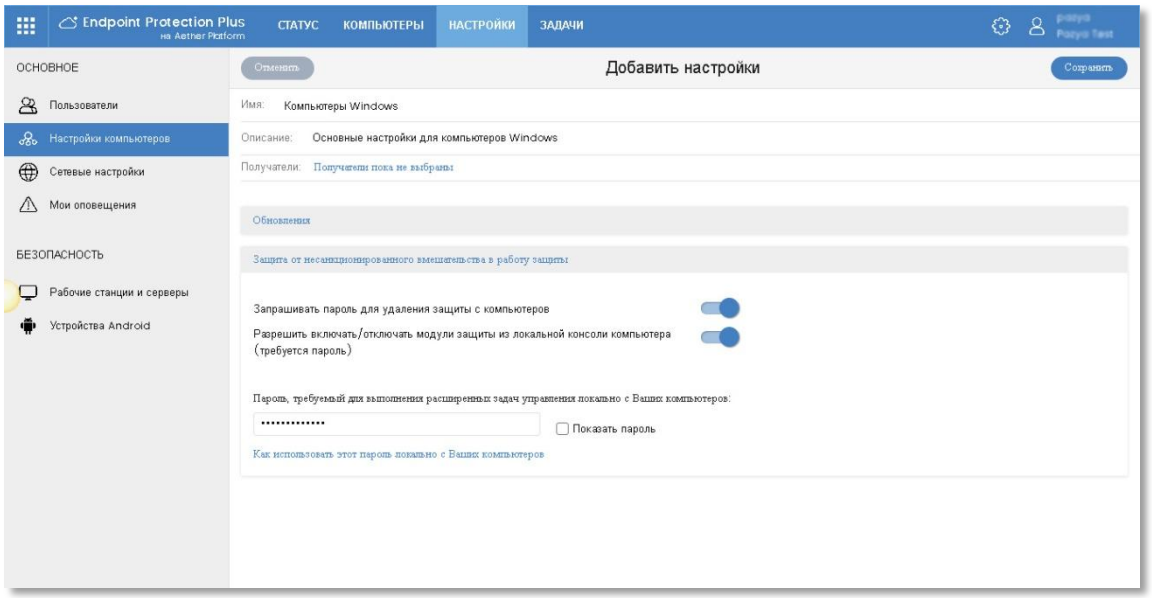


Рис. 9. Настройки защиты от несанкционированного вмешательства в работу защиты

В секции настроек защиты от несанкционированного вмешательства рекомендуется запрашивать пароль при удалении защиты с компьютеров, чтобы исключить случаи, когда сотрудники могут удалить локального агента.

Также на всякий случай можете разрешить управление модулями защиты из локальной консоли. Особых рисков тут нет, т.к. для этого все равно требуется знать специальный пароль (он настраивается тут же ниже), но в определенных случаях в целях администрирования или устранения неисправностей желательно, чтобы Вы имели возможность получить доступ к расширенным опциям в локальной консоли.

3.1.3. Сетевые настройки

В разделе **Настройки** выберите подраздел **Сетевые настройки**. Здесь осуществляется настройка основных сетевых параметров для работы защиты на защищаемых устройствах.

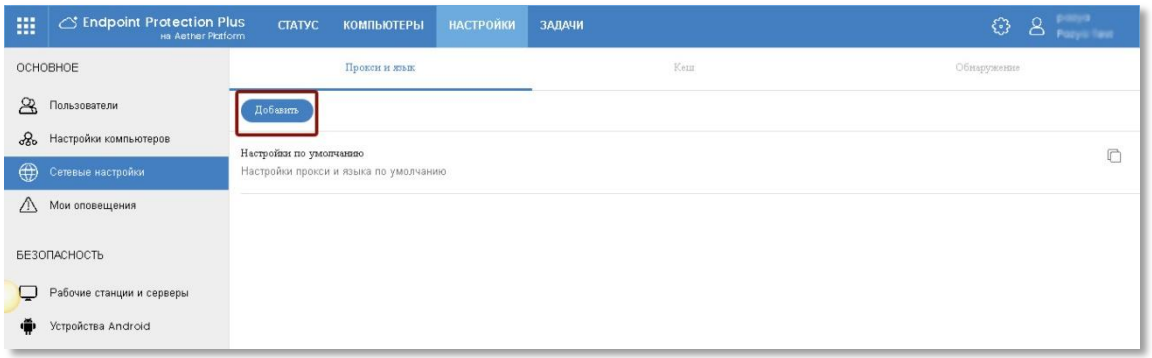


Рис. 10. Сетевые настройки

Данная страница имеет три закладки: **Прокси и язык**, **Кеш** и **Обнаружение**.

Прокси и язык

Самое главное – это проверить настройки в первой закладке, чтобы продукт в целом корректно функционировал. Здесь есть профиль *Настройки по умолчанию*, но рекомендуем создать собственные профили, т.к. в профиле по умолчанию, который нельзя изменить или удалить, в качестве языка защиты установлен английский язык, а также не сделаны настройки прокси (если это требуется).

Для добавления профиля нажмите кнопку **Добавить**. Укажите название профиля и его описание (если необходимо), а также установите требуемые опции в секциях **Язык** и **Прокси**.

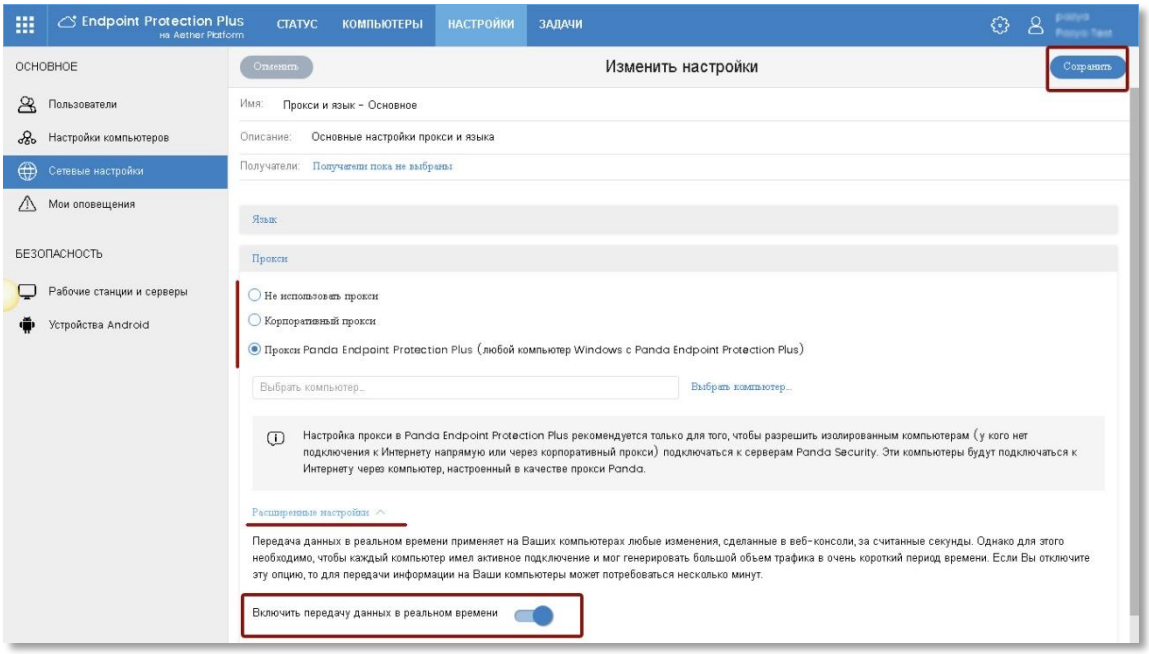


Рис. 11. Настройки языка и прокси

Что касается секции **Прокси**, то при необходимости Вы можете указать параметры корпоративного прокси или выбрать один из компьютеров, на которых установлен локальный агент Panda, который будет выполнять роль прокси Panda. Прокси Panda рекомендуется только для того, чтобы разрешить изолированным компьютерам (у кого нет подключения к Интернету напрямую или через корпоративный прокси) подключаться к серверам Panda Security. Эти компьютеры будут подключаться к Интернету через компьютер, настроенный в качестве прокси Panda.

Также рекомендуем по возможности в расширенных настройках включить опцию **Включить передачу данных в реальном времени**. По большому счету это не сильно увеличит трафик, однако выполнение удаленных задач и применение изменений настроек будет осуществляться в режиме реального времени.

Кеш

На закладке **Кеш** Вы можете настроить один или несколько компьютеров, которые будут работать в качестве кеша для хранения обновлений, инсталляторов и любых других пакетов, скаченных из Интернета. Таким образом, все обновления и скачивания будут передаваться внутри сети не с помощью пиринговых технологий с ближайших доступных обновленных компьютеров, а только с непосредственно настроенных кеш-компьютеров. Смотрите Руководство администратора.

Обнаружение

На этой закладке Вы можете настроить компьютеры, с которых будет осуществляться поиск неуправляемых / незащищенных компьютеров, на которые можно будет быстро установить защиту Panda.

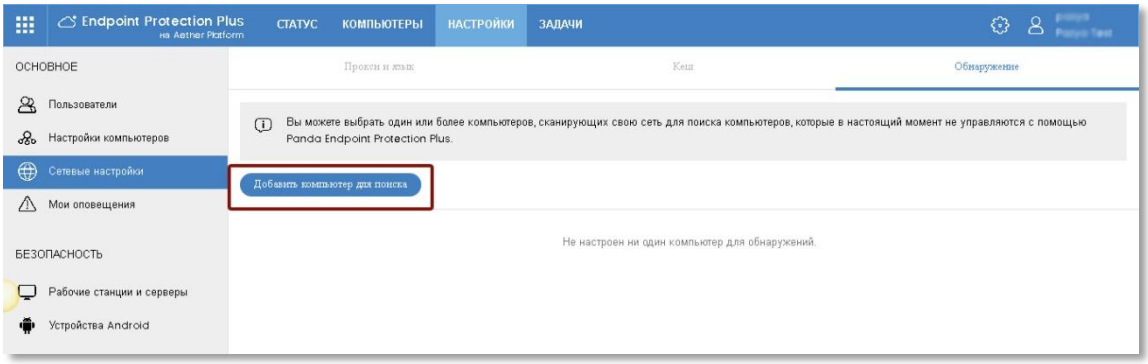


Рис. 12. Добавление компьютеров для поиска

Для добавления компьютера для поиска нажмите кнопку **Добавить**, после чего в списке компьютеров с установленной защитой Panda выберите компьютер, который будет использоваться для поиска других неуправляемых / незащищенных компьютеров. В том случае, если у Вас имеется несколько сетей / сегментов сетей, то для каждой из них рекомендуем указать отдельный компьютер.

После этого выбранный компьютер появится в списке. Чтобы осуществить автоматическую проверку прямо сейчас, нажмите у него ссылку *Проверить сейчас*. Нажмите у него ссылку *Настроить* для настройки работы функции обнаружения компьютеров.

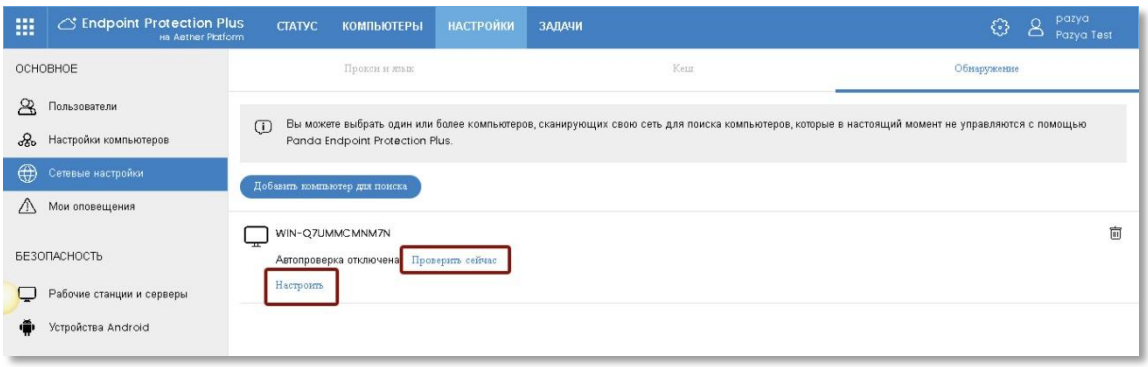


Рис. 13. Список компьютеров для поиска

На странице настроек укажите требуемые параметры опций обнаружения неуправляемых компьютеров. Для сохранения настроек нажмите кнопку **Сохранить**.

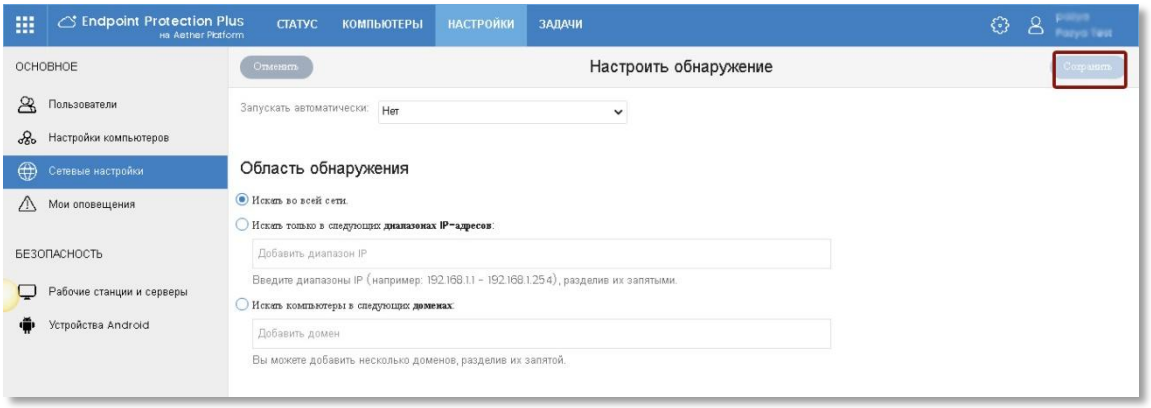


Рис. 14. Настройки компьютера для поиска

3.2. Шаг 2: Установка защиты

Решение Panda предлагает Вам несколько способов установки защиты. Но вне зависимости от выбранного способа в рамках процесса установки осуществляется скачивание и установка коммуникационного агента, который запускает процесс установки локальной защиты на требуемых устройствах.

Способы установки защиты Panda в Вашей сети:

1. **Инсталлятор**

   Позволяет скачать msi-файл, который Вы можете распространить на требуемых компьютерах как с использованием сторонних средств распространения ПО (SMS, Tivoli и т.д.), так и вручную. Подходит в тех случаях, если Вы используете в своей сети автоматизированные средства внедрения ПО.

2. **URL**

   Позволяет сгенерировать URL, при нажатии на которую запустится автоматический процесс установки. Данный URL можно отправлять по электронной почте. Этот способ более всего подходит для автоматизированной установки продукта на удаленные компьютеры, находящиеся за пределами локальной сети, к которым Вы не имеете административного доступа, а также если Вы не обладаете знаниями / возможностями использовать автоматизированные средства внедрения ПО или Ваша сеть достаточно небольшая.

3. **QR-код / Google Play (для Android)**

   Данный способ предназначен только для устройств с Android и позволяет передавать QR-код или ссылку для перехода в Google Play устройствам с Android

4. **Удаленное обнаружение компьютеров**

   Если у Вас настроены компьютеры для удаленного обнаружения неуправляемых компьютеров в сети, то Вы можете автоматически находить неуправляемые компьютеры, удаленно устанавливать на них защиту Panda, а потом привязывать эти компьютеры к требуемым группам и профилям.

Также имеется возможность автоматизированной установки с помощью интеграции с Active Directory. Смотрите Руководство администратора, а также нашу статью на Хабре.

Для добавления компьютеров перейдите в раздел **Компьютеры** и нажмите кнопку **Добавить компьютеры** и выберите соответствующий способ установки защиты.

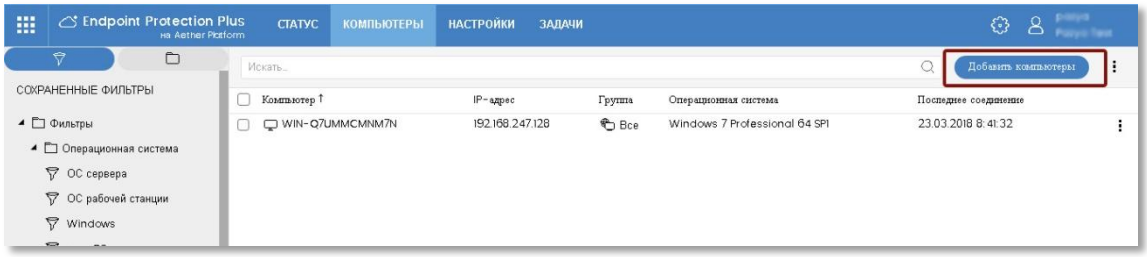


Рис. 15. Добавление компьютеров

3.2.1. Внедрение защиты с помощью удаленного обнаружения

В появившемся окне нажмите на ссылку *Обнаружение и удаленная установка.*

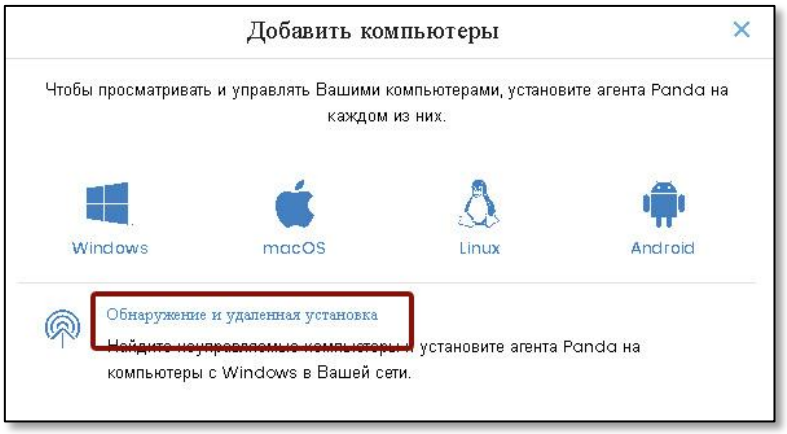


Рис. 16. Добавление компьютеров с помощью удаленного обнаружения

Затем укажите компьютер, который будет использоваться для поиска неуправляемых компьютеров. После выполнения поиска Вы сможете просмотреть обнаруженные неуправляемые компьютеры одним из способов:

- в разделе **Статус** в виджете *Статус защиты* появится предупреждение о найденных неуправляемых компьютерах
- в разделе **Статус** в контекстном меню *Мои списки* можно добавить быстрый переход для просмотра списка неуправляемых компьютеров

После этого в списке неуправляемых компьютеров Вы сможете удаленно запустить установку агента Panda, после чего эти компьютеры добавятся в раздел **Компьютеры**, где Вы сможете их привязать к требуемым группам и профилям. Подробнее смотрите в Руководстве администратора.

3.2.2. Внедрение защиты с помощью инсталлятора

В этом случае в окне добавления компьютеров (см. рис.16) выберите требуемую операционную систему (Windows, Linux, Mac), укажите соответствующую группу и профиль настройки и нажмите кнопку **Скачать инсталлятор**.

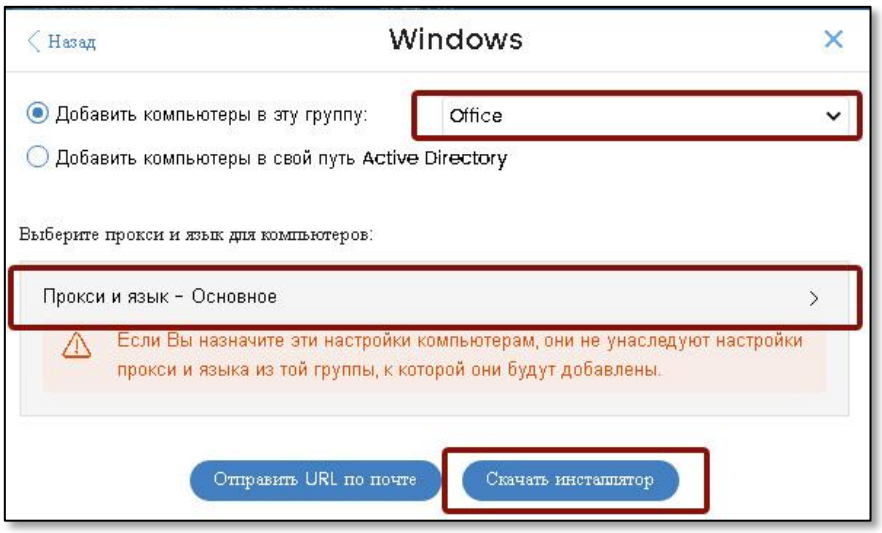


Рис. 17. Добавление компьютеров с помощью инсталлятора

В результате выполненных действий Вы скачаете на Ваш компьютер установочный файл в формате msi, который потом Вы сможете распространить с помощью автоматизированных средств внедрения ПО или запустить вручную. Имейте в виду, что все компьютеры, на которых будет запущен данный установщик, будут автоматически добавлены именно в ту группу компьютеров, которую Вы выбрали при его скачивании.

3.2.3. Внедрение защиты с помощью URL

Выполните аналогичные действия, как при установке с помощью инсталлятора (см. раздел 2.2.2), но в конце нажмите кнопку **Отправить URL по почте**. В

результате этого откроется окно Microsoft Outlook (или другого установленного и настроенного почтового агента) для отправки письма со ссылкой.

Кстати, данный способ может использоваться и для установки защиты на устройства Android.

В результате выполненных действий Вы сможете предоставить пользователям соответствующие ссылки для установки защиты на их компьютеры и устройства. Имейте в виду, что все компьютеры, на которых будет открыт данный URL, будут автоматически добавлены именно в ту группу компьютеров, которую Вы выбрали при его генерации. Обратите внимание, что в рамках данного способа процесс установки **зависит от конечного пользователя** (он должен нажать на URL, чтобы запустить автоматический процесс установки).

3.2.4. Внедрение защиты с помощью QR-кода или Google Play

В этом случае в окне добавления компьютеров (см. рис.16) выберите требуемую операционную систему (Android), укажите соответствующую группу, в которую хотите автоматически добавить данные устройства с Android.

Рис. 18. Добавление устройство Android с помощью QR-кода или Google Play

После этого Вы можете отсканировать QR-код или нажать на ссылку Google Play, если хотите установить защиту на текущее устройство с Android. QR-код Вы также можете отправить в качестве картинки требуемым пользователям любым доступным способом.

3.3. Шаг 3: Мониторинг защиты

Чтобы проверить корректность внедрения защиты Panda в Вашей сети, а также осуществлять мониторинг и контроль статуса защиты компьютеров и устройств и

выполнять требуемые задачи управления, контроля и защиты, Вам необходимо перейти в раздел **Компьютеры**.

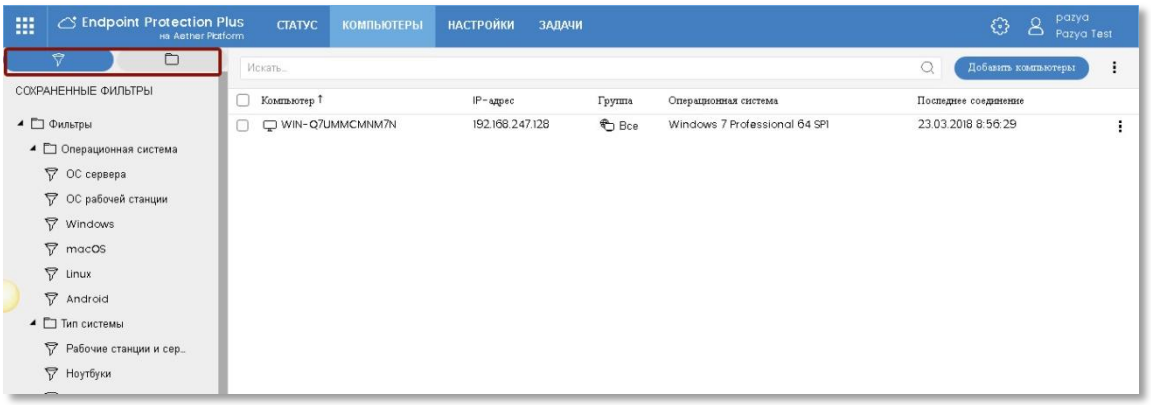


Рис. 19. Список компьютеров

В левой части экрана расположен блок выборки требуемых компьютеров либо по фильтрам, либо по организационному древу (группы и папки Active Directory). В центральной части расположена таблица со списком компьютеров.

В этом разделе Вы можете выбирать требуемые компьютеры, проверять их статус, удаленно выполнять различные задачи по отношению к требуемым компьютерам (группам компьютеров) и т.д. При нажатии на интересующий компьютер, можно перейти на страницу с подробной информацией о нем.

Какие действия и как можно сделать по отношению к компьютерам, смотрите в Руководстве администратора.

4. Управление патчами

Если у Вас зарегистрированы лицензии на модуль **Panda Patch Management**, то Ваше корпоративное решение Panda позволяет Вам централизованно управлять обновлениями, патчами и уязвимостями. При этом не требуется никакая дополнительная установка на конечные устройства, т.к. вся работа модуля осуществляется через стандартный локальный агент Panda.

Данный модуль позволяет управлять всеми обновлениями, патчами и уязвимостями для операционной системы Windows и сотен других приложений под него. Список таких приложений:

https://www.pandasecurity.com/business/PatchManagementApp

Прежде чем использовать данный модуль, проверьте его системные требования:

- требования к Windows:
  https://www.pandasecurity.com/russia/support/card?id=700047
- требуемые URL и порты:
  https://www.pandasecurity.com/russia/support/card?id=700044

4.1. Настройка политик управления патчами

Для настройки политик перейдите в раздел **Настройки**, в котором выберите подраздел **Безопасность** -> **Patch Management**. В данном разделе Вам будет доступна политика по умолчанию, которую нельзя изменять или удалять. При необходимости Вы можете добавить свои собственные политики, нажав на кнопку **Добавить**.

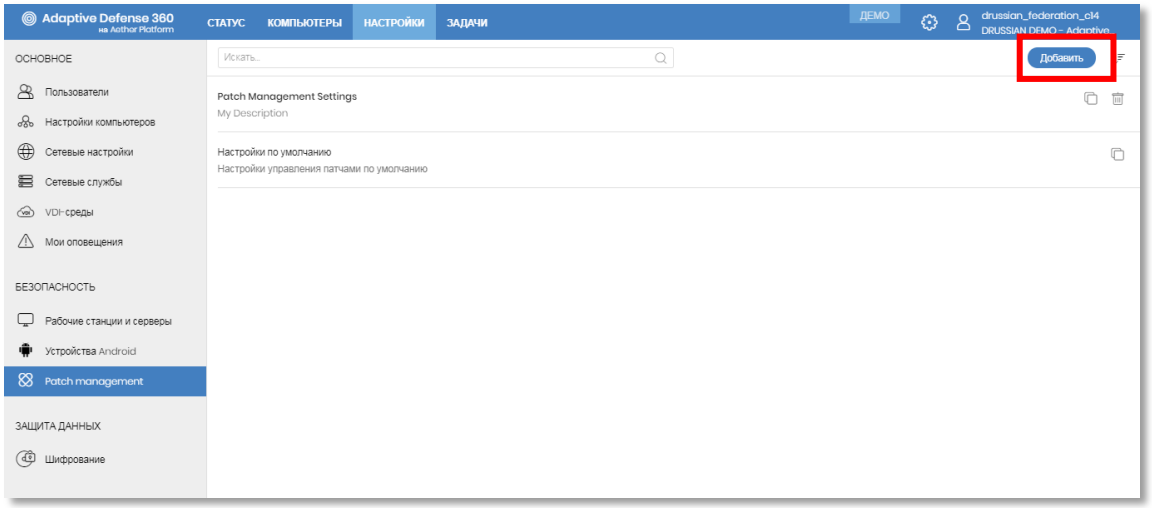


Рис. 20. Добавление политики управления патчами

При добавлении политики Вам необходимо указать название, описание и настроить соответствующие опции. Рекомендуем Вам включить опцию *Отключить обновление Windows на компьютерах*, чтобы централизованно управлять всеми обновлениями через Ваше решение Panda.

Для работы модуля должна быть включена опция *Автоматический поиск патчей*.

Также при добавлении политики Вы можете указать те компьютеры, на которых будет применена данная политика.

После настройки политики нажмите кнопку **Сохранить**.

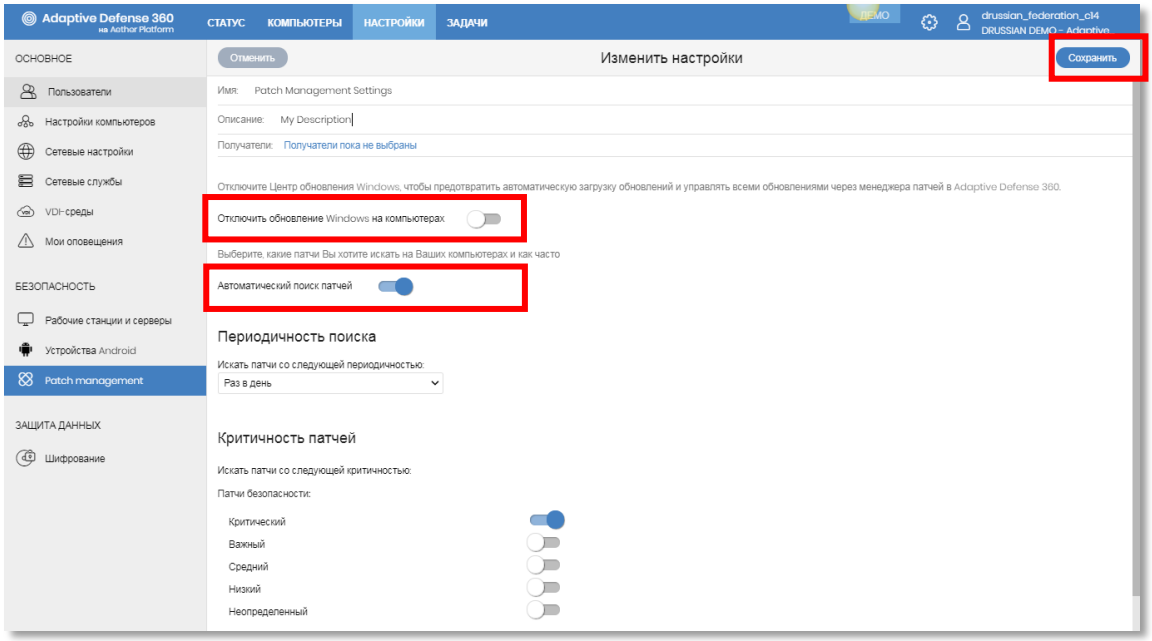


Рис. 21. Настройка политики управления патчами

4.2. Мониторинг патчей, обновлений и уязвимостей

Мониторинг за работой модуля Patch Management осуществляется в разделе **Статус** -> **Patch Management**.

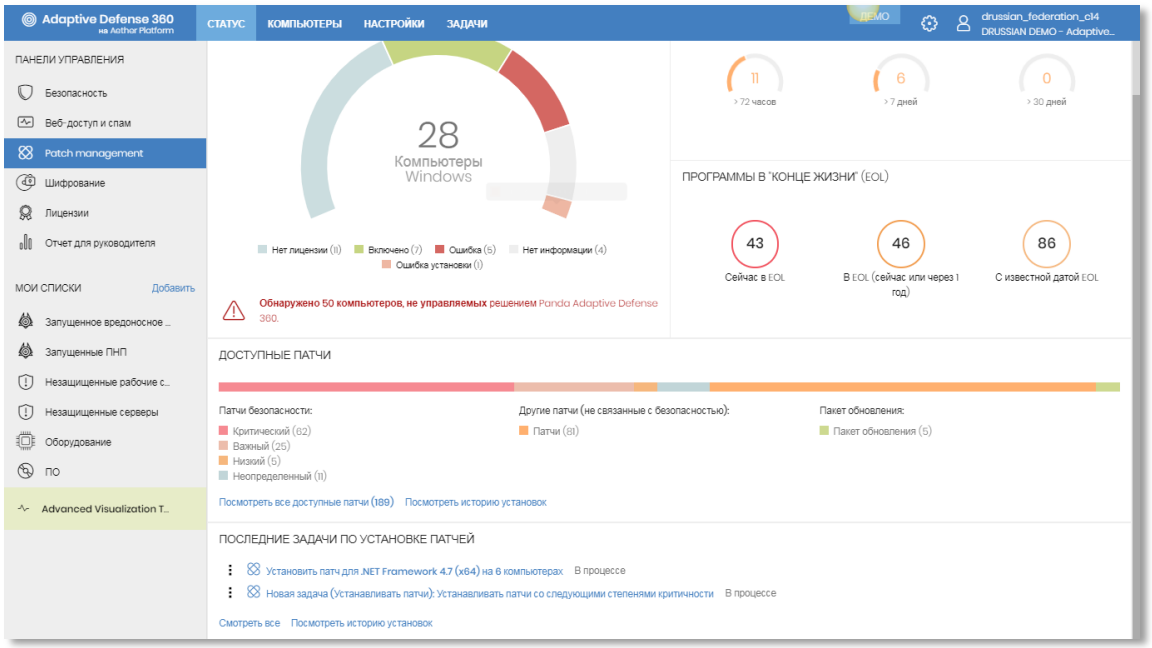


Рис. 22. Настройка политики управления патчами

Здесь Вы можете использовать доступные виджеты для получения всей необходимой информации о статусе работы модуля, прошедшего времени с последней проверки, наличии в Вашей сети программ с EoL (дата окончания жизненного цикла), доступности новых патчей, а также наличие задач по установке патчей.

4.3. Установка патчей

Установка патчей осуществляется с помощью соответствующих задач, которые можно создать различными способами.

4.3.1. Установка через список доступных патчей

Создать задачу для массовой установки патчей можно через список **Доступные патчи**. Открыть этот список можно различными способами:

- В разделе **Статус** –> **Patch Management** нажмите на ссылку *Посмотреть все доступные патчи* в виджете **Доступные патчи**.
- Там же в разделе **Статус** в левом меню **Мои списки** можно добавить список Доступные патчи, нажав на ссылку Добавить и выбрав данный список

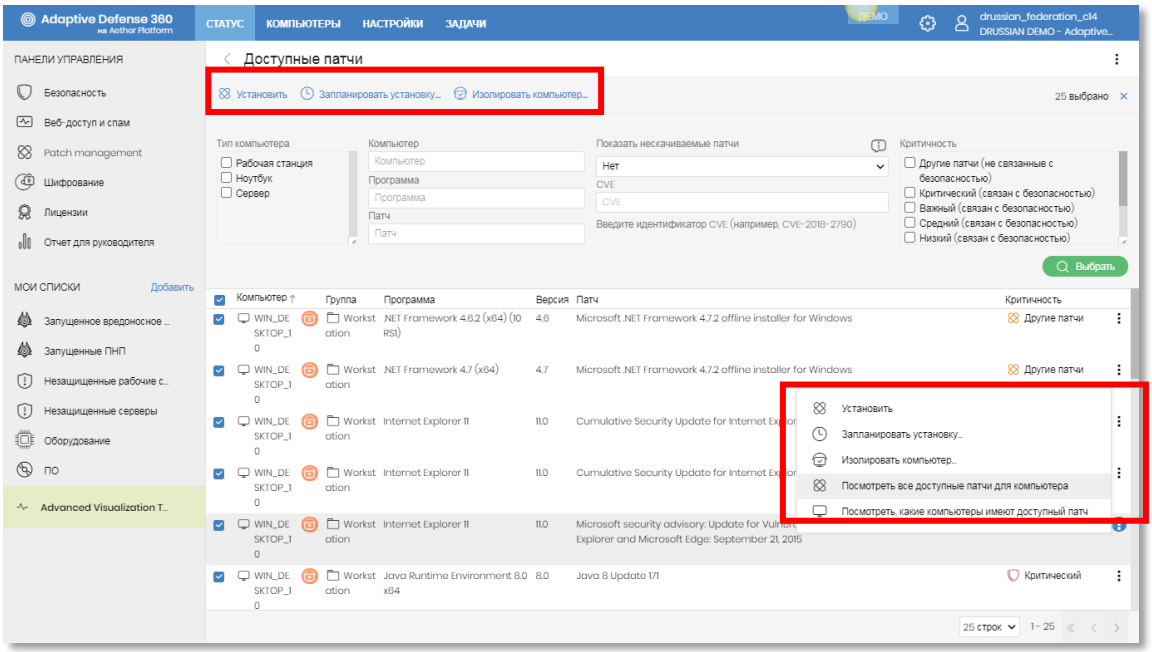


Рис. 23. Список доступных патчей

В списке доступных патчей Вы можете:

- Массово устанавливать все доступные патчи, один или несколько, выбирая их с помощью опций фильтров с возможностью мгновенной установки или запланированной по расписанию
- Просматривать все доступные патчи для конкретного компьютера
- Просматривать компьютеры, имеющие данный доступный патч

- Изолировать компьютеры с определенными доступными патчами (в случае, если Вы используете Panda Adaptive Defense или Panda Adaptive Defense 360)

При выборе пунктов меню *Установить* или *Запланировать установку* будет создана соответствующая задача на установку патчей. Донастройте ее опции и нажмите кнопку **Сохранить**.

4.3.2. Установка через древо компьютеров

В разделе **Компьютеры** в левом меню выберите закладку *Моя организация*, после чего выберите группы компьютеров, на которых требуется установить доступные патчи, а затем – галочками отметьте конкретные компьютеры (или все). После этого в верхнем контекстном меню выберите пункт *Запланировать установку патчей…*

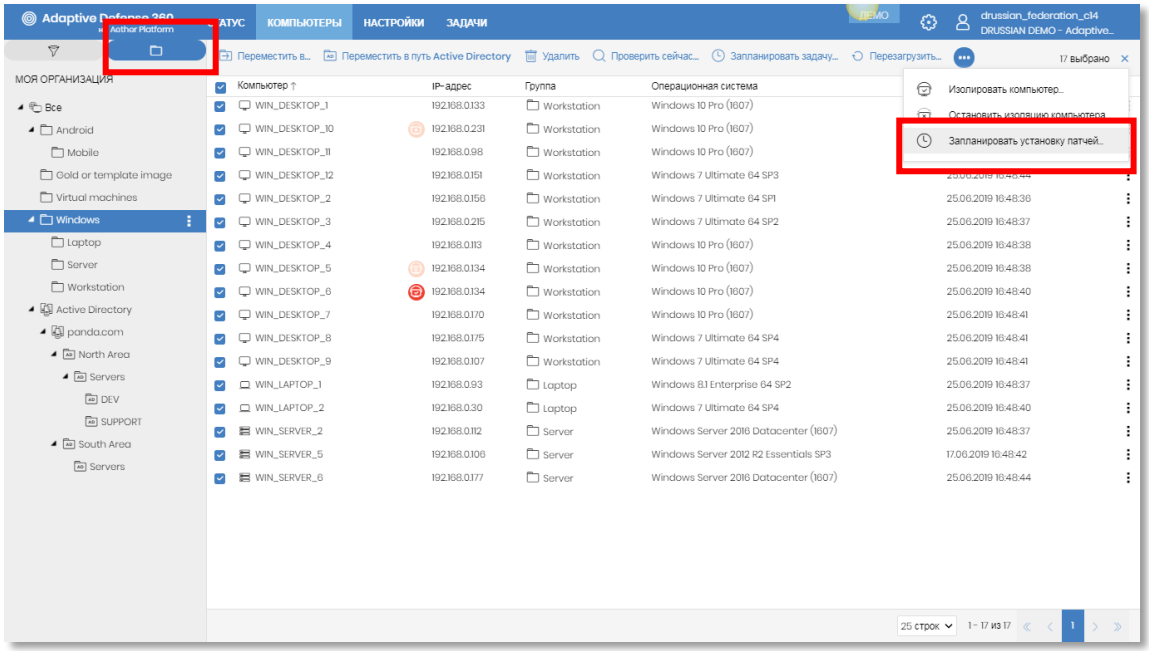


Рис. 24. Установка патчей через древо компьютеров

Для установки доступных патчей на все компьютеры конкретной группы Вы также можете в левом меню нажать на кнопку контекстного меню требуемой группы и в выпадающем меню выбрать пункт *Запланировать установку патчей…*

4.3.3. Установка через раздел Задачи

Также установку патчей можно настроить непосредственно в разделе **Задачи**. Для этого нажмите кнопку **Добавить задачу** и в выпадающем меню выберите пункт *Устанавливать патчи…*

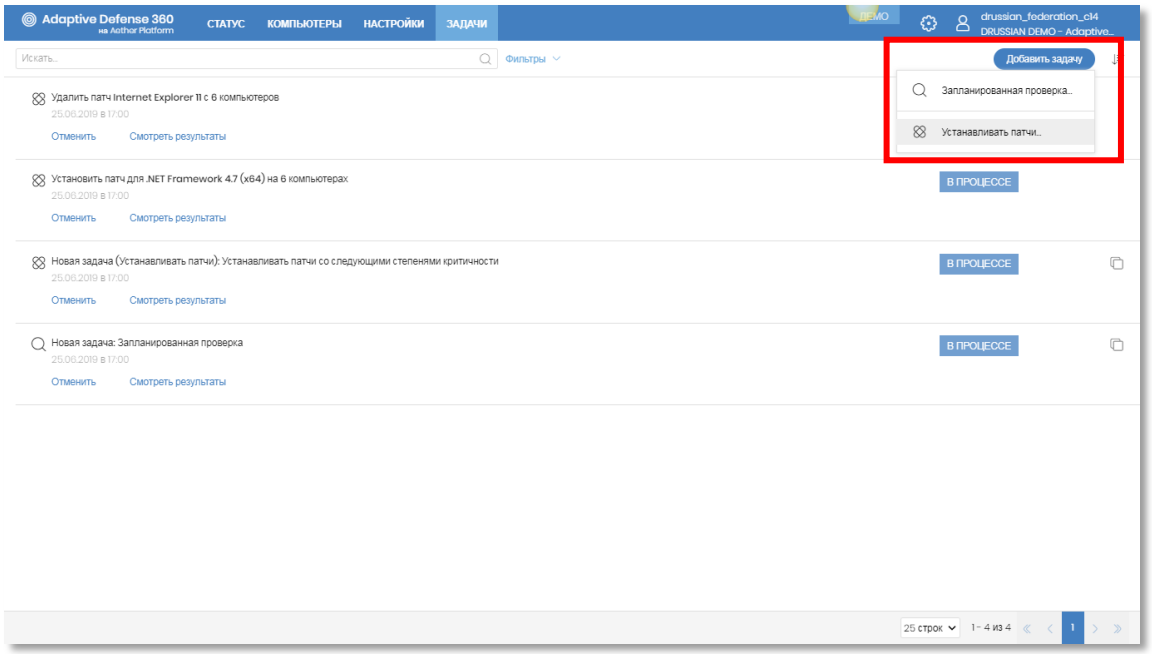


Рис. 25. Добавление задачи на установку патчей

На открывшейся странице настройте опции задачи по установке патчей и нажмите кнопку **Сохранить**.

4.4. Другие возможности управления патчами

Помимо вышеперечисленных функций Вы также можете просматривать историю установок патчей, осуществлять отмену установки патчей (если это допустимо производителем патча) и выполнять другие действия. Для получения более подробной информации смотрите Руководство пользователя.

5. Управление шифрованием дисков

Если у Вас зарегистрированы лицензии на модуль **Panda Full Encryption**, то Ваше корпоративное решение Panda позволяет Вам централизованно управлять шифрованием жестких дисков на рабочих станциях, ноутбуках и серверах с Windows. Все управление осуществляется в облачной консоли через стандартный локальный агент Panda.

Для шифрования жестких дисков на компьютерах с операционной системой Windows используется встроенная технология **BitLocker**. Данная технология поддерживается не на всех версиях Windows. Алгоритм шифрования – **AES-256**. Поддерживаются следующие типы аутентификации: TPM, TPM+PIN, USB-ключ, пароль.

Подробнее системные требования смотрите здесь:

http://go.pandasecurity.com/full-encryption/requirements

Внимание! Не забудьте до окончания срока действия лицензий корпоративного решения Panda расшифровать все жесткие диски, которые были зашифрованы с помощью модуля Panda Full Encryption, иначе Вы не сможете получить к ним доступ.

5.1. Настройка политик шифрования

Для настройки политик шифрования перейдите в раздел **Настройки** -> **Шифрование**. Вам будет доступна политика шифрования по умолчанию, которую нельзя изменить или удалить. Если же Вам требуется добавить новую политику, нажмите кнопку **Добавить**.

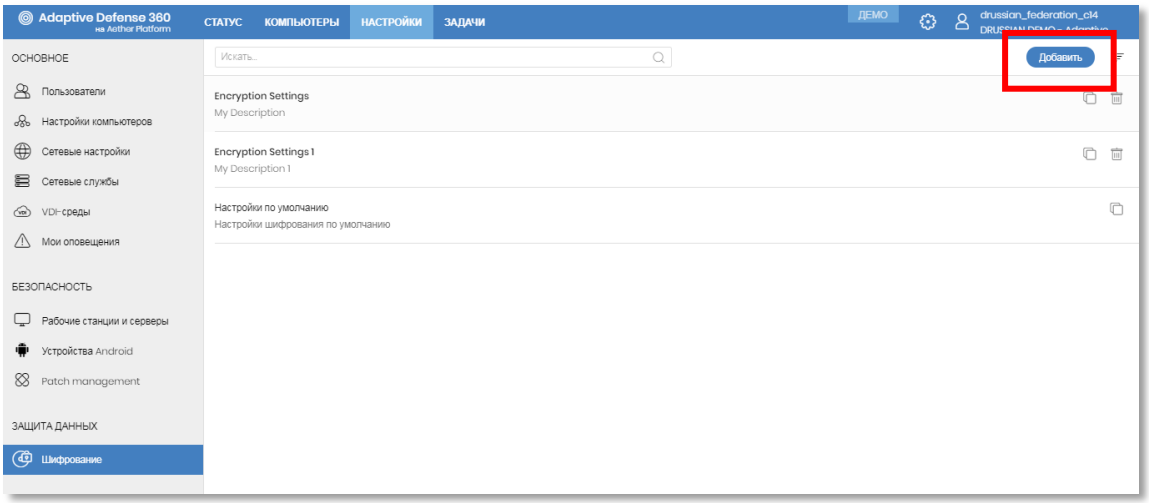


Рис. 26. Добавление политики шифрования

На открывшейся странице Вам необходимо указать название политики, ее краткое описание, выбрать компьютеры, к которой будет применяться данная политика, а также настроить все требуемые опции.

Для включения модуля шифрования должна быть включена опция *Шифровать все жесткие диски на компьютерах*.

Рекомендуем Вам включить опцию *Запрашивать пароль для доступа к компьютеру*, т.к. она позволит повысить уровень защиты доступа к компьютеру. Кроме того, она является необходимой для тех устройств, которые не поддерживают TPM.

Рекомендуем Вам отключить опцию *Шифровать только используемое дисковое пространство*, чтобы шифровался весь диск целиком, включая и логически (но не физически) удаленные данные.

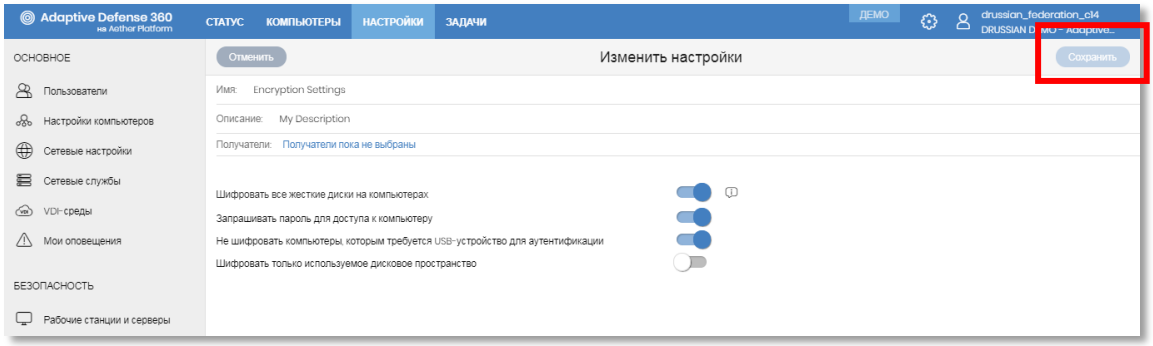


Рис. 27. Настройка политики шифрования

После настройки политики нажмите кнопку **Сохранить**. В результате этого на выбранных компьютерах сразу же запустится задача на шифрование всех жестких дисков. Если в настройках политики была включена опция запроса пароля для доступа к компьютеру, то пользователю данного устройства будет предложено настроить данный пароль. Данный пароль доступа будет запрашиваться у пользователя перед каждой загрузкой компьютера – он не загружает в память компьютера ключ шифрования, а потому система защищена от атак непосредственно на память.

5.2. Мониторинг статуса шифрования

Для централизованного мониторинга статуса шифрования жестких дисков на компьютерах предприятия в разделе **Статус** -> **Шифрование** доступны соответствующие виджеты, которые показывают сведения о компьютерах, поддерживающих шифрование, статусе шифрования компьютеров и примененном методе аутентификации.

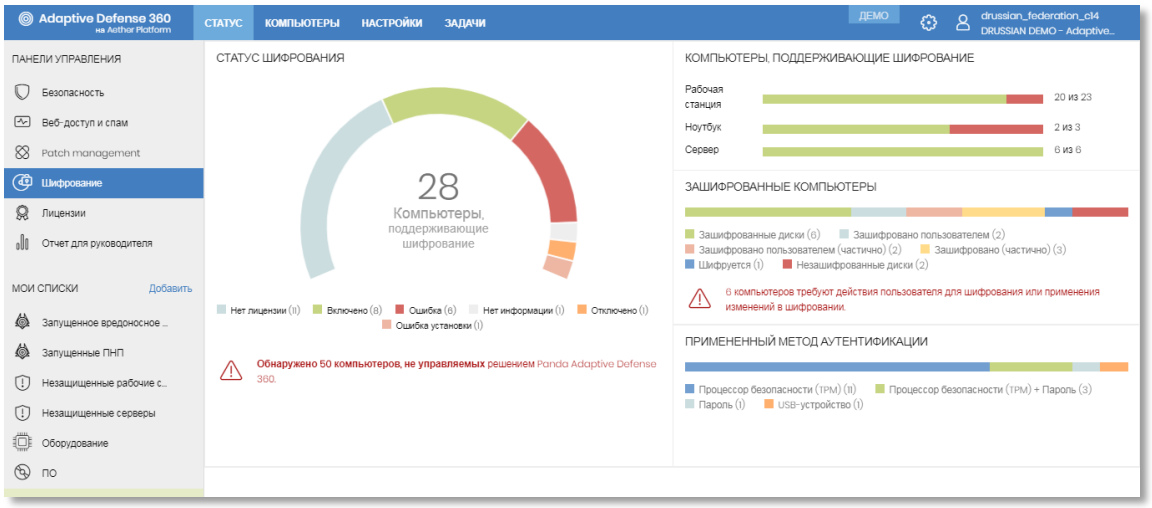


Рис. 28. Мониторинг статуса шифрования

Кроме того, из виджетов можно переходить на соответствующие списки компьютеров с предустановленными фильтрами по многочисленным критериям шифрования.

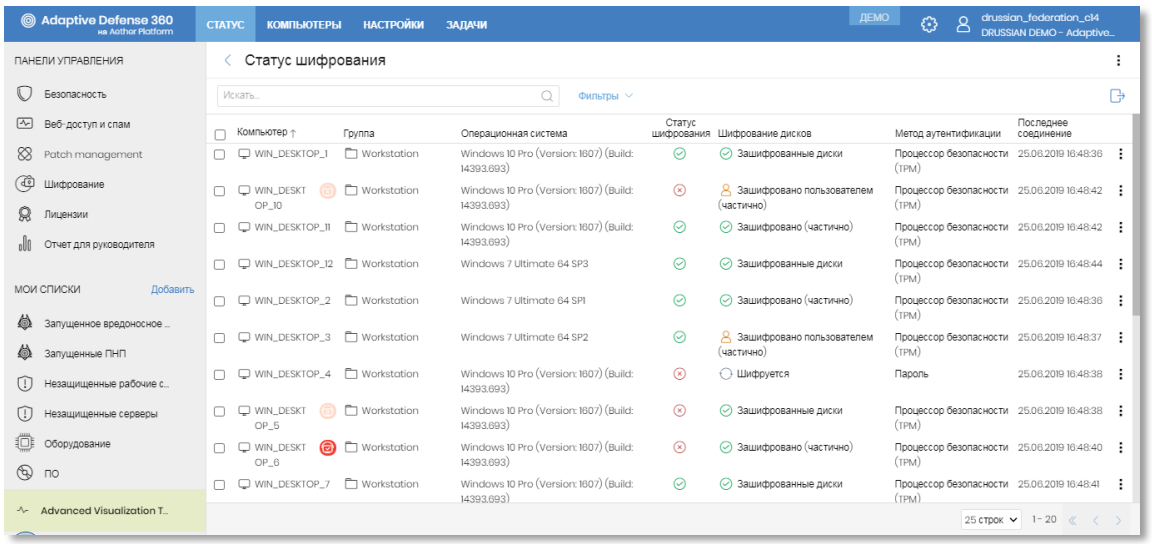


Рис. 29. Список компьютеров с требуемым статусом шифрования

При переходе на страницу с подробными сведениями о зашифрованном компьютере можно просмотреть более детальную информацию.

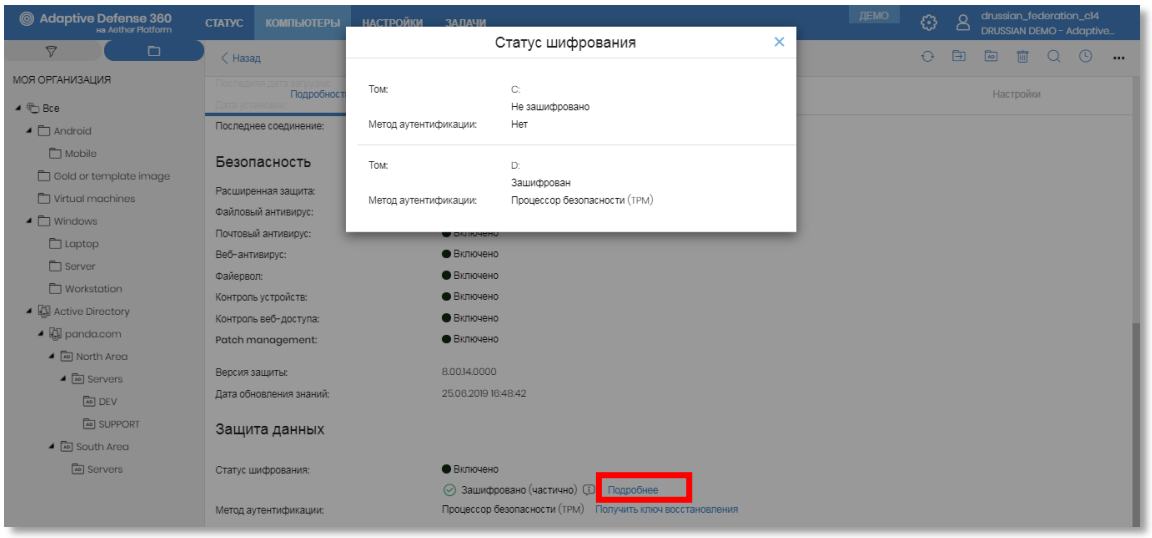


Рис. 30. Просмотр сведений о статусе шифрования компьютера

5.3. Ключи восстановления

Ключ восстановления – это 48-разрядный ключ, который может потребоваться при восстановлении доступа к зашифрованному компьютеру в следующих случаях:

- когда пользователь забыл свой pin-код или пароль для загрузки компьютера
- когда компьютер, защищенный с помощью TPM, обнаруживает изменение в последовательности загрузки (жесткий диск, защищенный с помощью TPM, подключается к другому компьютеру)
- когда изменили материнскую плату и, соответственно, TPM
- при отключении или удалении содержимого TPM
- при изменении настроек загрузки компьютера или когда изменен процесс загрузки (обновлен BIOS, прошивка материнской платы, видеокарты, контроллера дисков, UEFI, изменены сектор загрузки, главная загрузочная запись, диспетчер загрузки и другие компоненты, влияющие на загрузку компьютера)

Ключ восстановления для требуемого компьютера можно получить в облачной консоли управления Panda на странице с подробными сведениями о данном устройстве.

В облачной консоли хранятся только ключи восстановления для тех компьютеров, на которых управляется шифрование жесткими дисками, в консоли не показываются пароли для компьютеров, зашифрованными пользователями, и для тех устройств, шифрование на которых не управляется через модуль Panda Full Encryption.

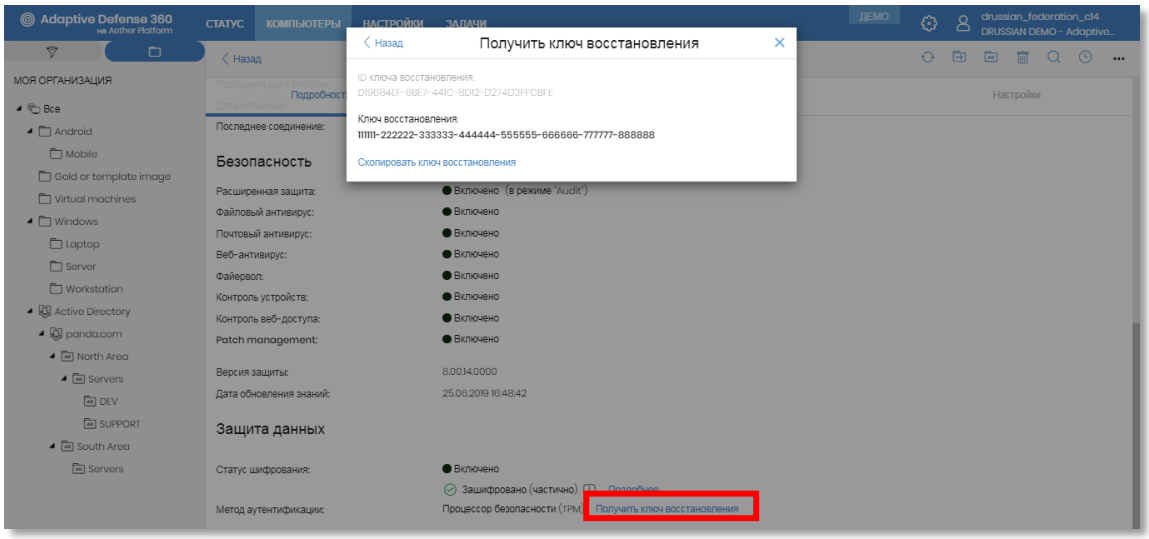


Рис. 31. Получение ключей восстановления

6. Advanced Reporting Tool

Модуль **Advanced Reporting Tool** является упрощенной SIEM-системой, которая позволяет глубоко анализировать все ИТ-процессы, происходящие в Вашей сети для анализа ситуации, выявления нежелательных приложений, несанкционированного доступа к данным и пр.

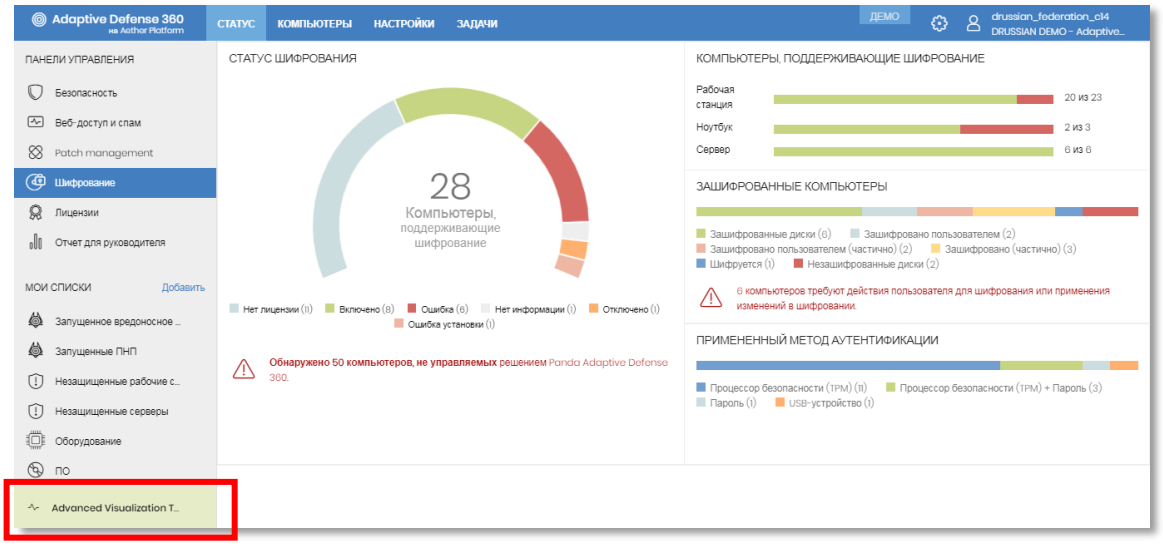
Данный модуль автоматически собирает огромный объем информации с локальных агентов Panda и предоставляет их пользователям в виде графического интерфейса.

Модуль начинает работать автоматически с момента его подключения.

Данный модуль доступен только для пользователей Panda Adaptive Defense и Panda Adaptive Defense 360.

Вы можете посмотреть нашу [статью на Хабре] о данном модуле, а также Руководство пользователя.

Чтобы открыть модуль Advanced Reporting Tool, в разделе **Статус** в левом меню нажмите на **Advanced Vizualization Tool**.



7. Локальный агент

В результате внедрения решения на защищаемых устройствах будет установлен локальный агент, а в системном трее будет показываться иконка продукта.

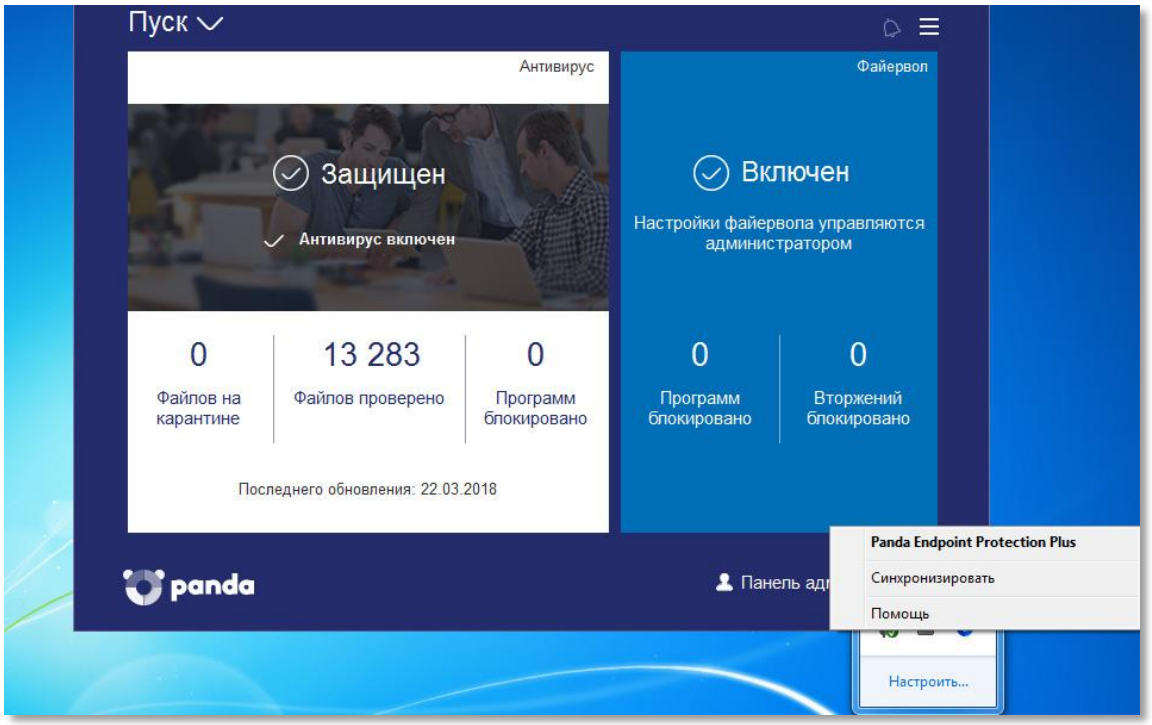


Рис. 32. Локальная консоль

В локальном агенте пользователь может проверить информацию по последним обнаружениям, запустить антивирусную проверку по требованию, синхронизировать локального агента с облаком и обратиться к онлайн-справке.

В том случае, если профиль безопасности подразумевает возможность локального управления файерволом, то в локальной консоли пользователь также сможет управлять им.

Кроме того, локальная консоль имеет ссылку для доступа к панели администратора, доступ к которой ограничен паролем администратора (см. раздел 2.1.2.). В этом случае администратор может перейти к этой панели, чтобы внести изменения в работу модулей.

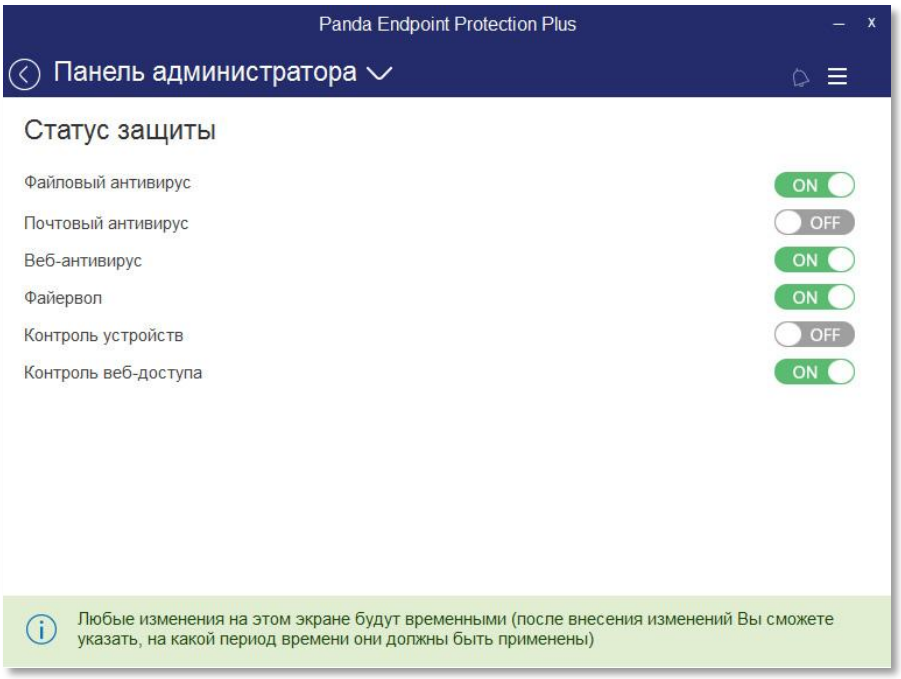


Рис. 33. Панель администратора в локальной консоли

В том случае, если внесены какие-то изменения в работу модулей, то они по умолчанию будут активны в течение 6 часов, хотя Вы можете установить другой период их активности.

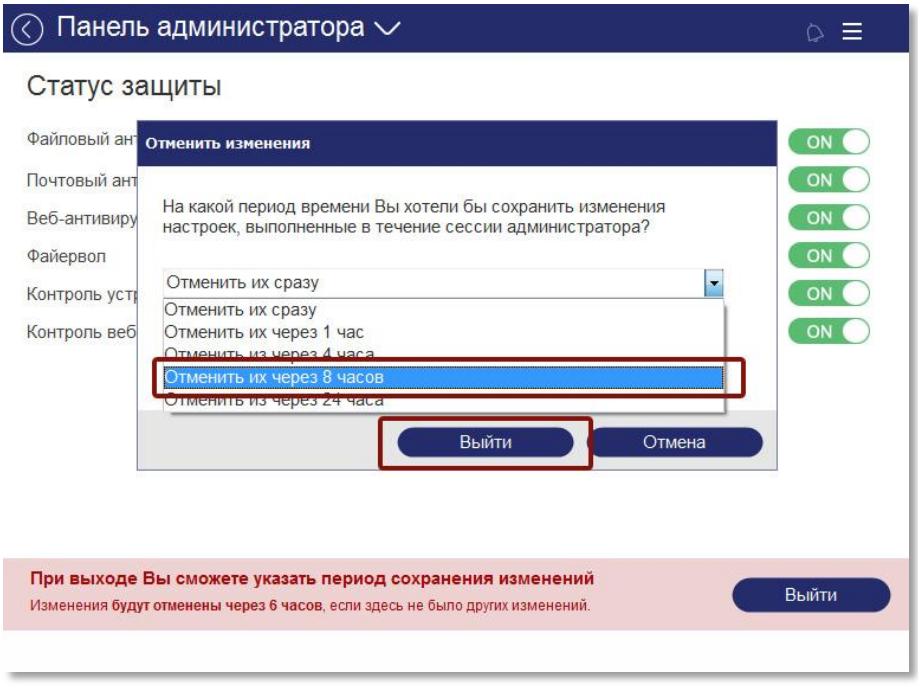


Рис. 34. Выбор срока отмены изменений в панели администратора локальной консоли

Заключение

В результате выполнения представленных выше шагов Вы сможете централизованно и удаленно внедрить корпоративную защиту Panda на требуемых компьютерах и устройствах.

Предлагаем Вам ознакомиться с Руководством администратора, чтобы узнать о том, как настроить параметры работы продукта, централизованные обновления, автоматическую генерацию и отправку отчетов, удаленно подключаться к требуемым компьютерам с помощью интегрированных утилит удаленного доступа и многое другое.

В этом случае Вы сможете максимально использовать все возможности корпоративного решения Panda для обеспечения эффективной и надежной защиты с низкой полной стоимостью владения.

Благодарим Вас за интерес к решениям Panda!

APPENDIX A. Контакты Panda Security в России

A.1. Контакты Службы продаж

Почта: sales@rus.pandasecurity.com

Телефон: +7 495 105 94 51

A.2. Контакты Службы технической поддержки

Почта: support@rus.pandasecurity.com

Телефон: +7 495 105 94 51

A.3. Адрес сайта

Русская версия: www.cloudav.ru

Глобальный сайт (англ.): www.pandasecurity.com