



 Email Protection

Руководство по быстрой настройке

Содержание

1. Предисловие	3
1.1. Введение	4
1.2. Для кого это руководство?	4
1.3. Иконки	4
2. Введение в Email Protection	5
2.1. Введение в Email Protection	6
3. Модель лицензирования	7
3.1. Модель лицензирования	8
4. Начальная настройка аккаунта Email Protection	10
4.1. Общие положения по настройке аккаунта Email Protection	11
4.2. Настройка фильтрации входящей почты в Email Protection	11
4.2.1. Настройка домена	12
4.2.2. Настройка почтовых ящиков	14
4.2.3. Настройка пользователя вручную	15
4.2.4. Импорт почтовых ящиков из списков	17
4.2.5. Автоматическая регистрация пользователей через SMTP	18
4.2.6. Автоматическая регистрация пользователей через LDAP (Active Directory)	19
4.2.7. Персонализация платформы	25
4.2.8. Настройка MX-записей Вашего DNS-сервера	26
4.2.9. Дополнительные настройки безопасности (файервол)	27
4.3. Настройка фильтрации исходящей почты в Email Protection	27
4.4. Настройка SPF-записей в Вашем DNS	28
5. Дополнительная и контактная информация	29

1. Предисловие

Введение

Для кого это руководство?

Иконки

1.1. Введение

Данное руководство содержит информацию для установки и настройки базовых аспектов продукта **Panda Email Protection**.

1.2. Для кого это руководство?

Технический персонал, ответственный за настройку сервиса корпоративной электронной почты:

- IT-Департамент в организации, которая хочет внедрить безопасный сервис электронной почты для пользователей сети.
- Провайдер управляемых услуг (MSP), который предлагает своим клиентам сервис безопасности электронной почты.

1.3. Иконки

В настоящем руководстве могут встречаться следующие иконки:



Дополнительная информация. Например, другой способ выполнения указанной задачи.



Предложения и рекомендации.



Важная информация по использованию определенной функции Panda Email Protection.

2. Введение в Email Protection

Ключевые функции

2.1. Введение в Email Protection

Panda Email Protection - это облачный сервис безопасности электронной почты. Облачные сервисы позволяют компаниям сфокусироваться на своем основном бизнесе, освободив себя от операционных расходов и решения управленческих задач, присущих традиционным решениям безопасности. **Email Protection** включает в себя многоуровневую систему, которая сочетает фильтры и механизмы защиты, использующих собственные технологии (Panda Email Protection PROACTIVE, доверительные списки...), а также стандартные технологии (репутация IP, Байесовские сети, белые и черные списки, серые списки, трафик-шейпинг и пр.) для обеспечения максимального уровня безопасности. Удаляя спам, вирусы и фишинг с помощью более десятка фильтров, решение не только снижает нагрузку на почтовый сервер, но также устраняет проблемы снижения производительности сотрудников, вынужденных тратить свое время на удаление спама.

Email Protection предоставляется с интуитивно понятным и простым в использовании интерфейсом, который позволяет администраторам быстро настроить защиту.

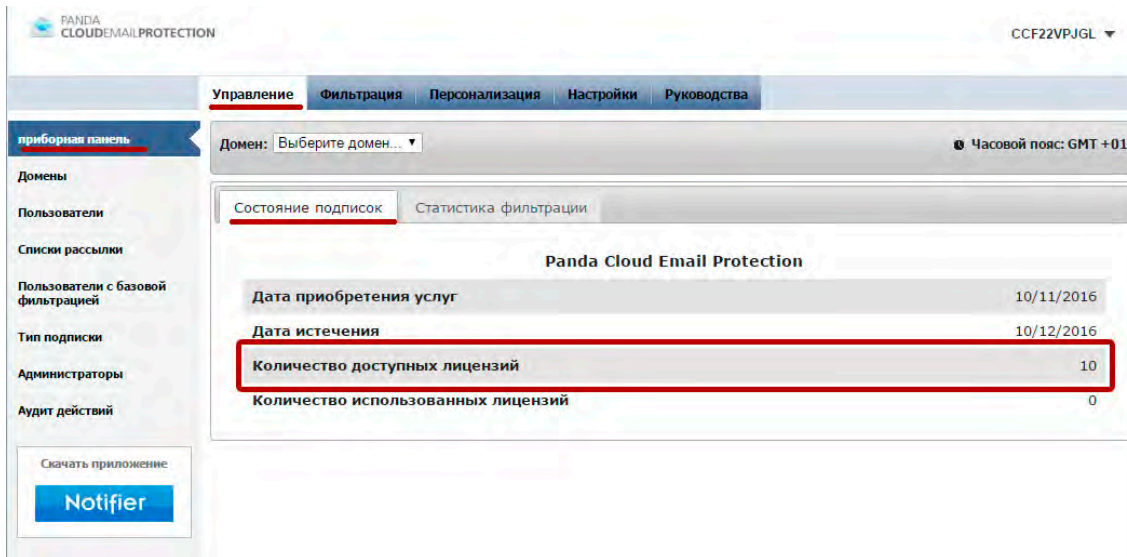
Некоторые ключевые функции, предоставляемые решением **Email Protection**:

- Централизованное конфигурирование
- Простое администрирование
- Многоуровневый антиспам
- Резервное копирование входящей почты
- Регистрация пользователей
 - Вручную
 - Импорт из списков
 - Интеграция с LDAP с определением алиаса
 - Интеграция с SMTP
- Делегирование администрирования по домену
- Логи электронной почты с возможностью открыть электронные письма, добавить отправителей и IP-адреса в белый или черный список, классифицировать письма как валидные или спам
- Доверительные списки по каждому пользователю
- Настраиваемые фильтры
- Уведомления о письмах, помещенных на карантин

3. Модель лицензирования

3.1. Модель лицензирования

Panda Email Protection предоставляется как сервис, а потому каждый почтовый ящик, защищенный решением, требует отдельной лицензии из пула лицензий, доступных для сервиса. Администратор может просмотреть количество доступных и используемых лицензий в **Управление -> Приборная панель -> Состояние подписок**.



Panda Cloud Email Protection	
Дата приобретения услуг	10/11/2016
Дата истечения	10/12/2016
Количество доступных лицензий	10
Количество использованных лицензий	0

Учтите следующие моменты при расчете общего количества лицензий, требуемых для Вашей организации:

Алиасы доменов

Если платформа защищает существующий домен (например, "pandatest.com") с пользователями, уже созданными в рамках данного домена, а у Вас имеется другой домен, который является алиасом существующего домена (например, "pandatest.es"), то алиас домена может быть настроен как первичный домен. Все пользователи, представленные в первичном домене, будут одновременно настроены на алиас домена. Эти пользователи не требуют дополнительных лицензий.

Алиасы почтовых адресов

Каждая лицензия позволяет защитить до 5 алиасов адреса электронной почты, связанных с основным почтовым ящиком, использующим одну лицензию.

Чтобы система могла распознавать алиасы почтового адреса в рамках единой лицензии, необходимо, чтобы эти алиасы были правильно настроены в системе. Алиасы почтовых адресов можно настроить вручную (смотрите главу 4.2.3) или используя автоматическую авторизацию через LDAP (смотрите главу 4.2.6), при условии, что опция **Включить обнаружение псевдонима** включена. Учтите, что обнаружение алиасов недоступно при использовании автоматической авторизации через SMTP. Таким образом, рекомендуется, чтобы Вы использовали интеграцию с LDAP в том случае, если в Вашей организации имеется большое количество алиасов почтовых адресов.

Если Ваша организация имеет алиасы почтовых адресов, защищенные данным решением, но при этом они не настроены корректно как алиасы в **Email Protection**, то платформа будет тратить по одной лицензии на каждый такой алиас. В этом случае необходимо будет проверить конфигурацию почтовых ящиков в **Email Protection**.

4. Начальная настройка аккаунта Email Protection

Настройка фильтрации входящей почты
Настройка фильтрации исходящей почты
Настройка SPF в DNS

4.1. Общие положения по настройке аккаунта Email Protection

Данное руководство по быстрой настройке объясняет первоначальные шаги, которые необходимо предпринять для защиты доменов и пользователей корпоративной электронной почты. Все шаги по настройке выполняются из консоли управления. Доступ к консоли управления предоставляется администратору вместе с этим руководством по быстрой настройке. Консоль управления доступна по ссылке <https://mep.pandasecurity.com/admin/>. Для авторизации используйте Ваши уникальные регистрационные данные.



Адрес страницы для доступа к консоли управления может отличаться от указанного в настоящем документе. Пожалуйста, проверьте приглашительное письмо, которое было отправлено на адрес электронной почты, указанный для регистрации сервиса.

Пожалуйста, учтите, что в целом начальная настройка, описанная в данной главе 4, обязательна. Если шаги, описанные в этом руководстве, не будут полностью выполнены до изменения MX-записей в Вашем DNS на наше решение безопасности, то входящие и исходящие письма будут возвращаться назад с постоянным кодом ошибки. В этом случае письма никогда не дойдут до адресата.

Шаги по настройке, описанные при настройке фильтрации исходящей почты (глава 4.3), необходимо выполнять только в том случае, если Вы хотите, чтобы **Email Protection** фильтровал исходящие письма. Процедура настройки, описанная в разделе "Дополнительные настройки безопасности" (глава 4.2.9), также может быть не обязательна.

4.2. Настройка фильтрации входящей почты в Email Protection

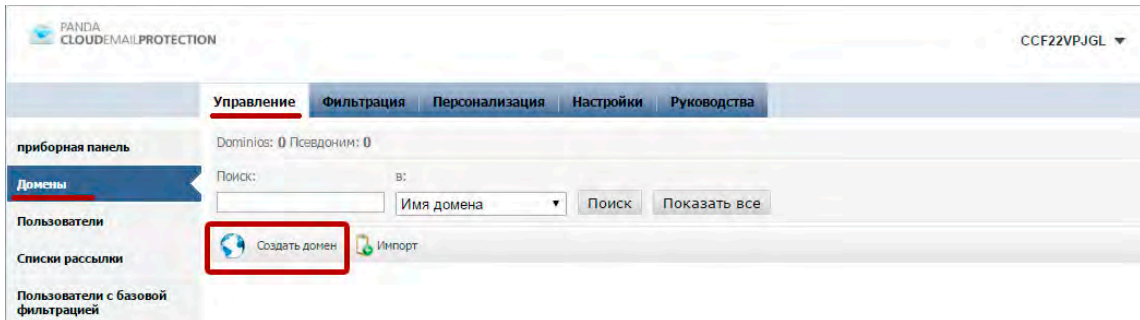
Следуйте нижеприведенным шагам, чтобы выполнить начальную настройку решения **Panda Email Protection**.

1. Настройте домен (-ы), которые должны быть защищены платформой.
2. Настройте почтовые адреса, которые должны быть защищены платформой.
3. Настройте платформу, если Вы хотите изменить дизайн пользовательского интерфейса и коммуникации, отправляемые на почтовые адреса, защищаемые решением.
4. Измените Ваши MX-записи для перенаправления Вашей почты на платформу **Panda**.

Далее мы подробно опишем каждый из этих шагов.

4.2.1. Настройка домена

Первый шаг - это настройка домена или доменов, которые должны быть защищены решением **Email Protection**. Для этого перейдите в **Управление -> Домены**. Для каждого защищаемого почтового домена настройте новый домен, нажав на **Создать домен**.

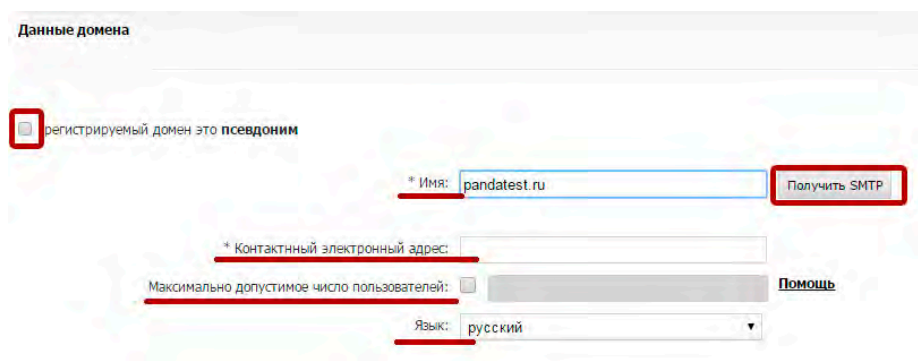


Для каждого нового домена требуется следующая информация:

Поставьте галочку у опции **Регистрируемый домен это псевдоним**, если настраиваемый домен является алиасом существующего домена, который уже настроен в платформе. В поле **Имя** укажите название защищаемого домена (например, "pandatest.ru"). Укажите контактный адрес почты для получения уведомлений об этом домене (например, уведомлений о процессе синхронизации пользователей или достижении доменом максимально доступного числа лицензий).

Вы можете ограничить максимальное количество лицензий, которое может быть использовано пользователями данного домена.

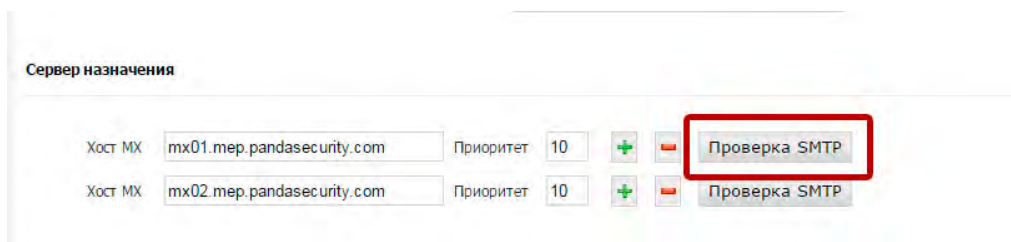
Кроме того, Вы можете выбрать язык по умолчанию, который будет использоваться для домена. Все уведомления для конечных пользователей, а также консоли управления для пользователей этого домена будут доступны на указанном языке.



Затем Вам необходимо настроить имя хоста или IP-адрес, куда **Panda Email Protection** будет доставлять входящие письма после их фильтрации. Это должен быть текущий адрес, на котором расположен Ваш сервер электронной почты. Если Вы все еще не перенаправили Ваши MX-записи в DNS на Email Protection, используйте кнопку **Получить SMTP** для автоматического заполнения полей **MX Host**. Проверьте, что это поле указывает на текущее местоположение почтового сервера, где находятся почтовые ящики, которые необходимо защитить.

Платформа позволяет Вам настроить несколько серверов, на которые будут доставляться отфильтрованные сообщения. Каждый из них может быть настроен с различным приоритетом. Проверьте, что поле **Приоритет** содержит ненулевое значение, а также утите, что MX-хост с самым высоким приоритетом должен минимальное значение.

После того как все необходимые MX-хосты настроены корректно, нажмите на **Проверка SMTP** для проверки того, что платформа может связаться с указанными MX-хостами.



Сервер назначения				
Хост MX	<input type="text" value="mx01.mep.pandasecurity.com"/>	Приоритет	<input type="text" value="10"/>	<input type="button" value="Проверка SMTP"/>
Хост MX	<input type="text" value="mx02.mep.pandasecurity.com"/>	Приоритет	<input type="text" value="10"/>	<input type="button" value="Проверка SMTP"/>

Если имеются проблемы с соединением, проверьте, что дата-центры **Panda Email Protection** могут установить SMTP-соединение с Вашими почтовыми серверами. Ниже представлены диапазоны IP-адресов наших дата-центров:

92.54.39.0/24 188.94.13.128/25

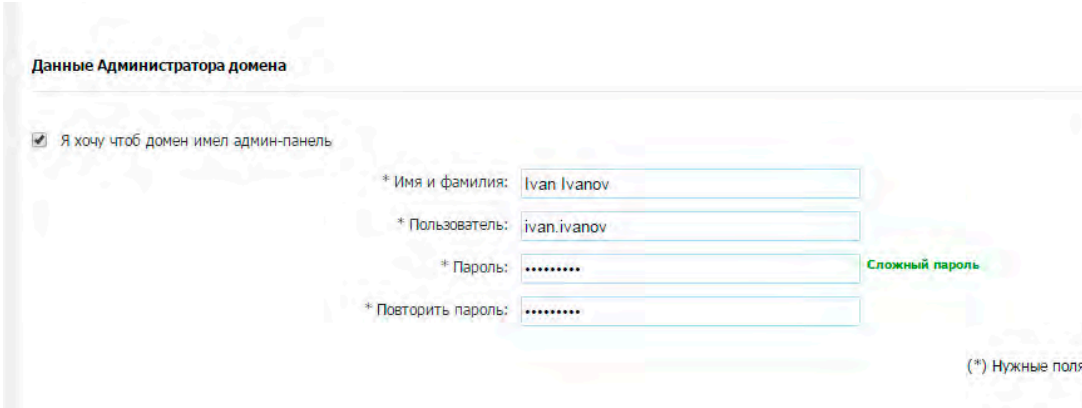
92.54.22.0/24 80.67.107.0/24

92.54.27.0/24 80.67.109.0/24



Диапазоны IP-адресов могут отличаться от указанных в данном документе. Для их проверки, пожалуйста, перейдите в раздел "Руководства" -> "Информация о настройках" в консоли управления.

Здесь Вы можете либо завершить настройку защищаемого домена, либо определить **Администратора домена**. С помощью предоставленных регистрационных данных администратор домена сможет войти в консоль управления (<https://mep.pandasecurity.com/admin/>), чтобы изменить параметры конфигурации домена, настроенные в данной главе:



После того как все поля будут настроены, сохраните параметры домена и перейдите на следующий шаг: настройка почтовых адресов.

4.2.2. Настройка почтовых ящиков

Panda Email Protection требует, чтобы Вы настроили каждый почтовый ящик, который должен защищаться платформой. Если Вы не настроите почтовые ящики, защищаемые решением (вручную или в режиме автоматической авторизации), **Panda Email Protection будет отклонять все входящие и исходящие письма, если решение обрабатывает входящую/исходящую почту Вашей организации.**

Существует два способа настройки защищаемых почтовых ящиков:

Вручную: Администратор вручную регистрирует каждый почтовый ящик (или алиасы почтовых адресов) по отдельности. Администратор также может импортировать список пользователей (в формате .TXT или .CSV).

Автоматически: Администратор должен настроить защищаемые домены, используя одну из доступных процедур автоматической регистрации: SMTP или LDAP.

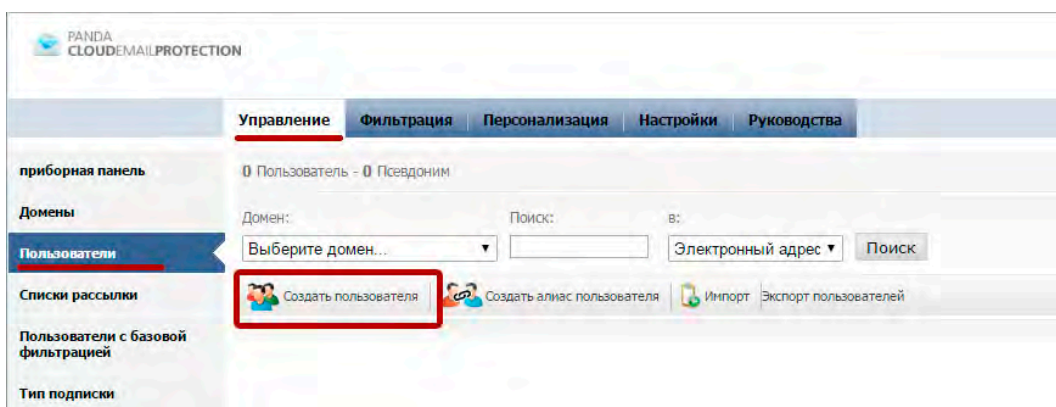


Эти методы не являются взаимоисключающими: администратор может настроить часть ящиков вручную, а остальные - автоматически. Обе процедуры можно использовать параллельно.

4.2.3. Настройка пользователя вручную

Почтовые адреса, которые должны быть защищены решением, могут быть добавлены вручную через консоль управления. Перейдите в **Управление -> Пользователи**. Этот экран позволяет администратору создавать пользователей с первичным адресом почты или алиасом почтового адреса, связанного с первичным почтовым ящиком, уже существующим в системе.

Чтобы создать пользователя с первичным адресом почты, нажмите **Создать пользователя**:



Для создания нового пользователя в системе необходима следующая минимальная информация:

Домен: Выберите домен, который будет содержать первичный почтовый ящик защищаемого пользователя.

Язык: Язык по умолчанию. Он будет использоваться для консоли управления и уведомлений для пользователя. По умолчанию система будет выбирать тот язык, что был выбран при создании защищаемого домена.

Имя, Фамилия: Данная информация используется для административных целей при составлении списка пользователей с их именами и фамилиями.

Логин пользователя: Адрес электронной почты, связанный с пользователем в защищаемом домене. Вам необходимо только ввести имя почтового ящика без домена, к которому он принадлежит.

Пароль: Система требует, чтобы каждый пользователь имел пароль для доступа к пользовательской консоли управления.

Данные

Домен: Выберите домен...

Язык: русский

(*) Имя, Фамилия: Sergey Kovalev [Помощь](#)

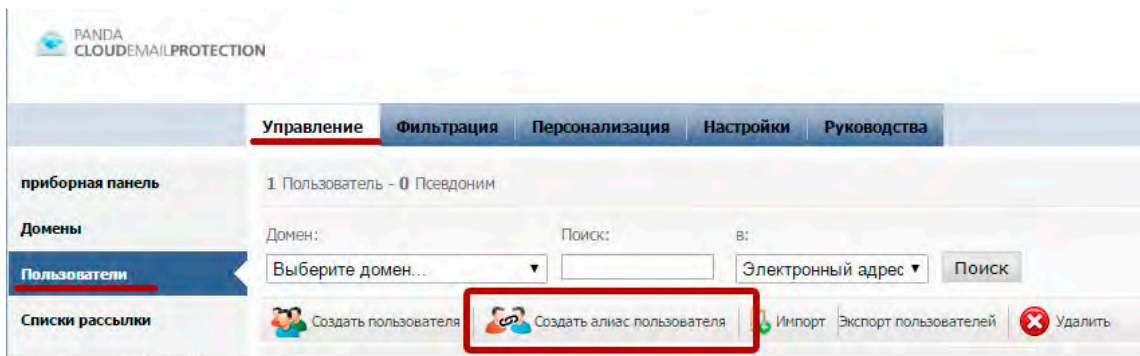
(*) Логин пользователя: sergey.kovalev
Введите имя, которое будет использоваться для почты без домена.

(*) Пароль: [Сложный пароль](#) [Помощь](#)

(*) Подтверждение пароля:

В примере выше мы зарегистрировали следующий почтовый ящик, который должен быть защищен платформой: "sergey.kovalev@pandatest.ru". После того как Вы указали все данные защищаемого пользователя, сохраните настройки.

Чтобы настроить алиас почтового адреса, связанного с первичным почтовым ящиком, перейдите в **Управление -> Пользователи** и нажмите **Создать алиас пользователя**.



Для создания алиаса пользователя необходима следующая информация:

Домен, в котором будет создан псевдоним: Домен, на котором размещен алиас почтового адреса. Он не должен совпадать с доменом, на котором размещен первичный адрес электронной почты.

Основной домен: Домен, содержащий первичный адрес электронной почты, с которым Вы хотите связать создаваемый алиас почтового адреса.

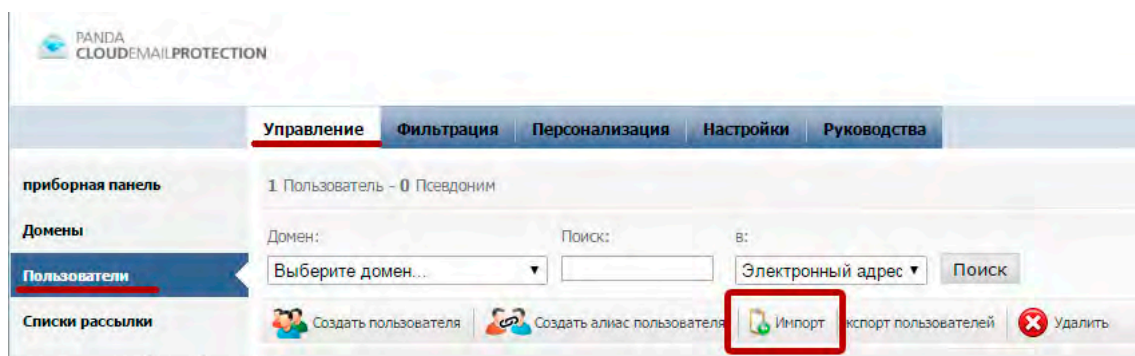
Псевдоним: Название алиаса почтового адреса, который должен быть защищен решением, без "@" и домена.

Основной аккаунт: Выберите название существующего первичного почтового аккаунта.

После того как введены все данные по алиасу, **сохраните** настройки.

4.2.4. Импорт почтовых ящиков из списка

Email Protection позволяет администратору вручную импортировать список пользователей из файла. Для этого перейдите к **Управление -> Пользователи -> Импорт**.



Прежде чем импортировать список, подготовьте файл, содержащий названия почтовых ящиков (и алиасы), которые должны быть защищены Email Protection. Импортируемый файл должен быть в виде файла .CSV или .TXT в следующем формате:

- ФИО, адрес электронной почты, пароль.
- ФИО, адрес электронной почты.
- ФИО, адрес электронной почты, пароль, список разделенных запятыми алиасов почтовых адресов.

Пароль и список разделенных запятыми алиасов не обязательны. Если пароля нет, то Email Protection сгенерирует случайный пароль во время импорта пользователей. Пожалуйста, обратите внимание на следующие советы при создании сложных паролей для пользователей:

Используйте прописные и заглавные буквы от "а" до "z". Используйте цифры от 0 до 9.

Допустимые символы: _ . -

Длина: От 8 до 64 символов.

Адрес электронной почты, включенный в импортируемый файл, должен быть указан в любом из следующих двух форматов:

- включая домен, к которому принадлежит почтовый ящик:

Michael Perk, mperk@example.com, aras249gt

Anthony Perkins, aperkins@example.com, 32kios5d

Anthony Perkins, aperkins@example.com, aperkins.alias1@example.com,
aperkins.alias2@example.com

- не включая домена, к которому принадлежит почтовый ящик:

Michael Perk, mperk, aras249gt

Anthony Perkins, aperkins, 32kios5d

Anthony Perkins, aperkins, aperkins.alias1, aperkins.alias2



Очень важно корректно импортировать файл в зависимости от того, содержит ли импортируемый список почтовых ящиков домен или нет. Если домен присутствует в файле, то Вы должны оставить поле "Домен:" пустым в меню импорта. Иначе импорт не удастся.

Учитывая предыдущие пункты, выберите импортируемый файл и нажмите **Импорт**.

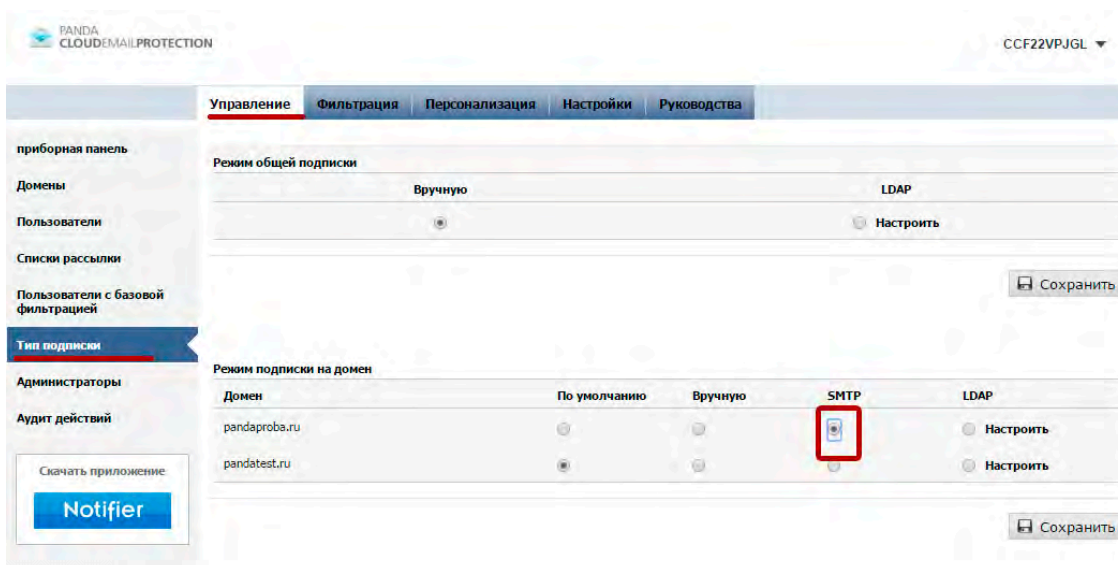
Процесс импорта происходит не сразу. Он может занять несколько минут в зависимости от количества импортируемых пользователей. **Email Protection** сообщит администратору аккаунта о результатах процесса импорта по электронной почте.

4.2.5. Автоматическая регистрация пользователей через SMTP

Email Protection может быть настроен на автоматическую регистрацию пользователей с использованием SMTP-протокола. Этот автоматический механизм позволяет автоматически инициализировать пользователей, которые еще не представлены в системе, в момент обработки первого сообщения, адресованного на защищаемый почтовый ящик.

Автоматическая регистрация пользователей через SMTP настраивается по домену.

Перейдите в **Управление** -> **Тип подписки** и выберите SMTP, как показано на картинке:



The screenshot shows the 'Управление' (Management) section of the Panda CloudEmail Protection interface. The 'Тип подписки' (Subscription Type) tab is active. Under 'Режим общей подписки' (General Subscription Mode), 'Вручную' (Manual) is selected. Under 'Режим подписки на домен' (Domain Subscription Mode), a table shows configurations for two domains: pandaproba.ru and pandatest.ru. For both, the 'SMTP' option is selected and highlighted with a red box. The 'Сохранить' (Save) button is visible at the bottom right.

Домен	По умолчанию	Вручную	SMTP	LDAP
pandaproba.ru	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/> Настроить
pandatest.ru	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/> Настроить

Затем сохраните настройки. После сохранения настроек система попросит администратора указать адрес почты существующего пользователя в домене, которого необходимо защитить.

Это нужно для проверки того, действителен ли сервер электронной почты для автоматической регистрации пользователей через SMTP. Если проверка не пройдет, то Ваш почтовый сервер не пригоден для автоматической регистрации пользователей.

Как правило, это связано с тем, что почтовый сервер не способен отклонять адреса почты у несуществующих пользователей в организации. В Microsoft Exchange эта функция известна как "Recipient Validation" и она должна быть включена для работы автоматической регистрации.



Если эта проверка не пройдет, Email Protection не позволит Вам настроить автоматическую регистрацию пользователей через SMTP.

После настройки автоматической регистрации через SMTP, система будет автоматически инициализировать нового пользователя в момент, когда для него в **Email Protection** будет получено первое сообщение .

Один важный момент, который необходимо учитывать при включении автоматической регистрации через SMTP: **все почтовые адреса в Вашей организации (неважно, это основные почтовые ящики или алиасы почтовых адресов) будут добавлены в Email Protection в виде основного почтового ящика**. Это важный аспект при подсчете требуемого количества лицензий для организации. Если Ваша организация активно использует алиасы почтовых ящиков, то мы советуем Вам включить автоматическую регистрацию через LDAP, а также обнаружение алиасов.

4.2.6. Автоматическая регистрация пользователей через LDAP (Active Directory)

Другой механизм автоматической регистрации, предоставляемый платформой, - это использование запросов LDAP к службе каталогов в Вашей организации. Это рекомендуемый механизм регистрации для средних и крупных организаций.

Главное отличие между автоматической регистрацией через SMTP и LDAP заключается в том, что инициализация LDAP позволяет обнаруживать алиасы почтовых ящиков и автоматически связывать их с основными почтовыми ящиками.

Автоматическая регистрация через LDAP может быть включена глобально или для каждого домена. Мы рекомендуем Вам настроить ее глобально, если все защищаемые решением домены регулируются одним и тем же контроллером доменов или службой каталогов LDAP. Настройте автоматическую регистрацию через LDAP для каждого домена, если Ваша организация имеет независимый сервер директорий на каждый домен.

Минимальные требования для настройки автоматической регистрации через LDAP:

Облачные серверы **Panda Security** должны быть способны подключиться к Вашей службе каталогов (Active Directory/Lotus/LDAP) по публичному IP-адресу или используя полностью указанное имя домена, доступное в Интернете.

Облачные серверы Panda Security будут запрашивать Вашу службу каталогов, используя протоколы LDAP или LDAPS.

Облачные серверы Panda Security могут делать анонимные запросы, хотя мы советуем создать выделенного пользователя для выполнения LDAP-запросов.

Диапазоны IP-адресов, с которых мы будем отправлять запросы в Вашу службу каталогов:

188.94.13.128/25

92.54.22.0/24

92.54.27.0/24



Диапазоны IP-адресов могут отличаться от указанных в данном документе. Для их проверки, пожалуйста, перейдите в раздел "Руководства" -> "Информация о настройках" в консоли управления.

При интеграции автоматической регистрации через LDAP с Active Directory, Вам необходимо создать пользователя, который принадлежит группе "Domain Users", со своими регистрационными данными. Выполните следующие действия в контроллере основного домена Вашей организации для создания этого пользователя:

1. Создайте пользователя, принадлежащего группе "Domain Users".
2. Пароль, назначенный пользователю, может содержать только буквы, цифры и символы "_" и "-". Пожалуйста, не используйте другие символы.
3. Укажите, что пароль не может быть изменен пользователем и срок его действия никогда не заканчивается.

После того, как Вы создали пользователя, Вы должны получить путь к уникальному имени (Distinguished Name) пользователя. Для этого откройте окно с командной строкой в Вашем контроллере домена и выполните следующую команду:

```
dsquery.exe user -name [USER]
```

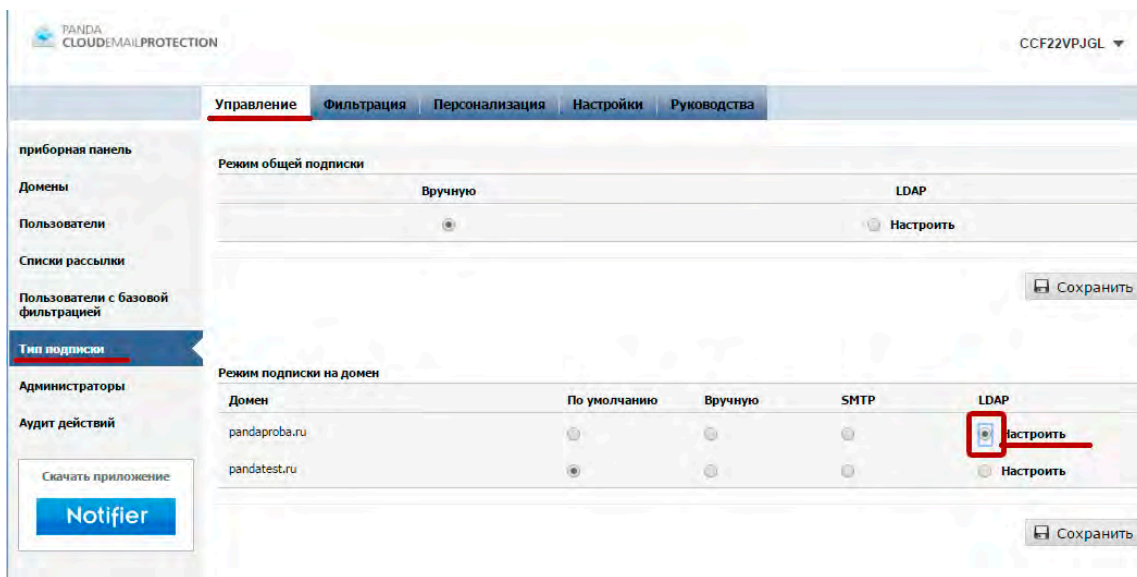
Пример: Если пользователь, которого Вы создали для LDAP-запросов, был назван "panda", то запускаемая команда и ее вывод будет следующим:

```
dsquery.exe user -name pandaCN=panda,CN=Computers,DC=dctest,DC=local
```

Пользователь для запросов, который должен быть настроен в консоли управления, будет таким же, как возвращается предыдущей командой:

```
'CN=panda,CN=Computers,DC=dctest,DC=local'
```

После того как Вы получили уникальное имя (Distinguished Name) пользователя, настройте автоматическую регистрацию через LDAP в разделе **Управление -> Тип подписки -> LDAP [Настроить]**.



В следующем разделе описываются наиболее распространенные параметры, используемые при настройке автоматической регистрации через LDAP с помощью Microsoft Active Directory:

LDAP сервер

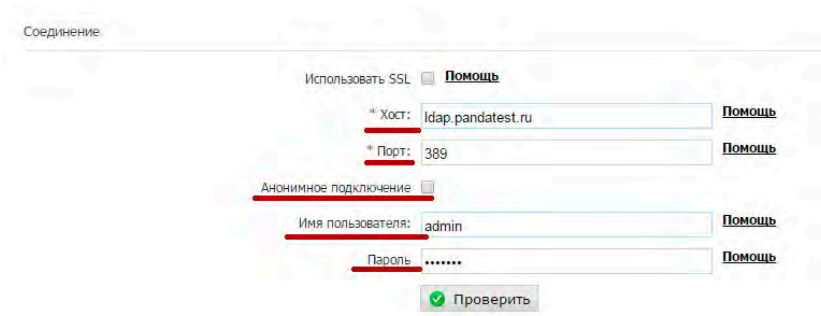
- Active Directory. Если у Вас другая служба каталогов, введите ее здесь.

LDAP сервер

Сервер: [Помощь](#)

Соединение

- **Хост:** IP-адрес службы или FQDN, чтобы иметь возможность подключиться к Вашему контроллеру домена. Пожалуйста, учтите, что этот IP/FQDN должен быть доступен с облачных серверов Panda.
- **Порт:** 389 (по умолчанию).
- **Анонимное подключение :** [Не отмечено] Microsoft Active Directory не допускает анонимные соединения. Эта опция должна остаться не отмеченной.
- **Имя пользователя:** Здесь должен быть введен валидный CN-путь. Введите CN-путь, возвращаемой командой "dsquery.exe", запущенной на контроллере домена:
CN=panda,CN=Computers,DC=dctest,DC=local
- **Пароль:** Укажите пароль, назначенный пользователю, который был создан для LDAP-запросов.



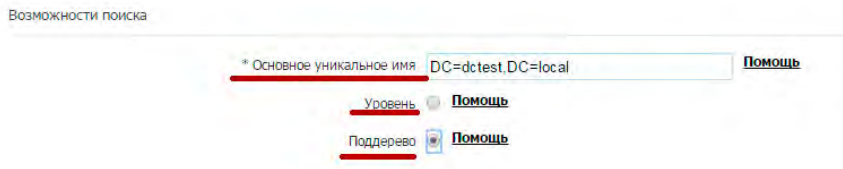
После того как все данные были правильно введены, нажмите кнопку **Проверить**. Система проверит, могут ли облачные серверы Panda Security подключиться к указанным хосту и порту, а также корректны ли указанные регистрационные данные. Если возникает ошибка, пожалуйста, еще раз проверьте, разрешено ли соединение от облачных серверов Panda Security к Вашей инфраструктуре, и корректны ли регистрационные данные пользователя.

Возможности поиска

- **Основное уникальное имя:** Стартовая точка в дереве LDAP, из которой Email Protection будет "смотреть" на пользователей в Вашей организации.

Рекомендуется настроить стартовую точку как можно ближе к корню дерева организации, чтобы решение смогло найти всех пользователей вне зависимости от подразделения организации, в котором они настроены. Основное уникальное имя может быть получено из CN пользователя, созданного для LDAP-запросов. При настройке Active Directory, как правило, оно совпадает с той частью CN пользователя, что начинается с DC. В нашем примере это будет: *DC=dctest,DC=local*

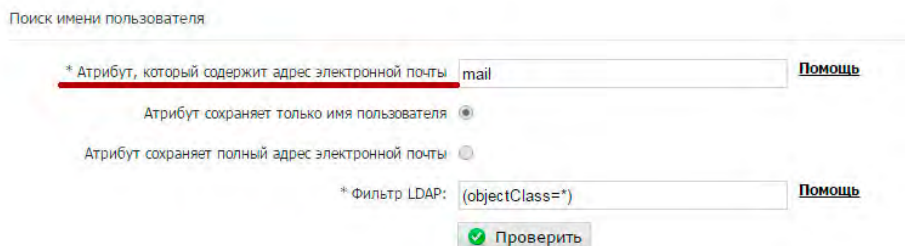
- **Уровень:** Выберите эту опцию, если все пользователи в Вашей организации размещены в той точке, где осуществляется поиск.
- **Поддерево:** Выберите эту опцию, чтобы искать пользователей на данном уровне и всех других уровнях, указанных выше в структуре LDAP. Рекомендуется выбрать данную опцию в том случае, когда Основное уникальное имя было настроено близко к корню дерева.



В нашем примере необходимо использовать опцию Поддерево, чтобы была возможность искать пользователей на уровнях, расположенных выше выбранного пути.

Поиск имени пользователя

Эти значения будут заполняться автоматически при выборе типа службы каталогов, используемой в Вашей организации (Active Directory/Open LDAP/Lotus Domino). Если Вы настроили службу Active Directory, то обычно необходимо выбрать опцию **Атрибут, который содержит адрес электронной почты**.



Затем нажмите кнопку **Проверить**, чтобы проверить корректность настройки для службы каталогов. Администратора попросят ввести действующий основной адрес электронной почты Вашей организации (не алиас электронного адреса!), а система проверит, может ли она найти его по запросу, чтобы проверить текущие настройки.

Если указанный адрес электронной почты не найден во время проверки, пожалуйста, проверьте еще раз конфигурацию, указанную в этом разделе, с администратором Вашего домена. Схема, используемая в Вашей организации, может отличаться от используемых здесь примеров.

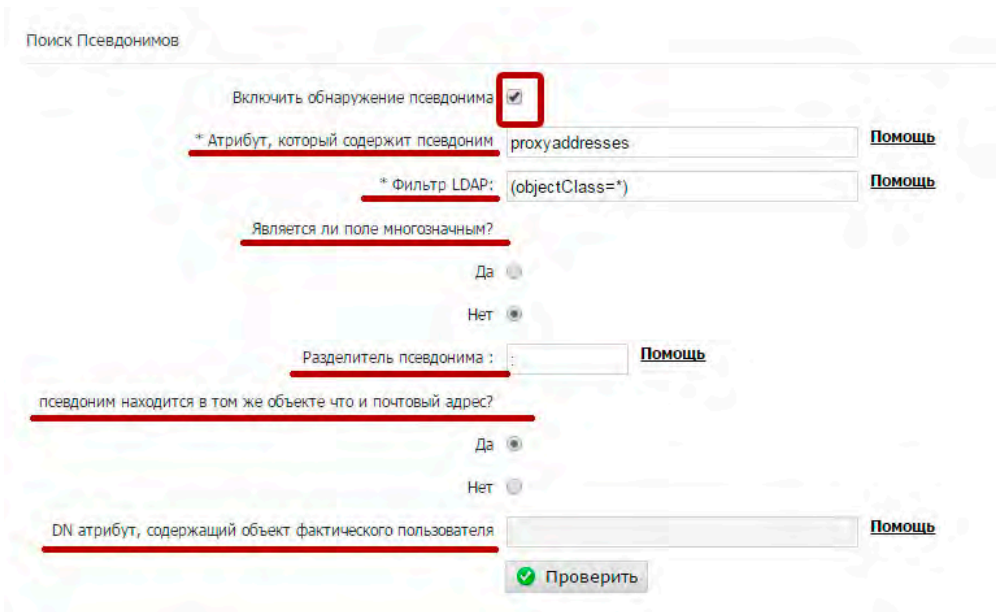
Поиск псевдонимов

Данная функция делает автоматическую регистрацию пользователей через LDAP намного более привлекательной, чем при использовании SMTP. Мы настоятельно рекомендуем Вам включить данную опцию, если Вы настроили регистрацию через LDAP.

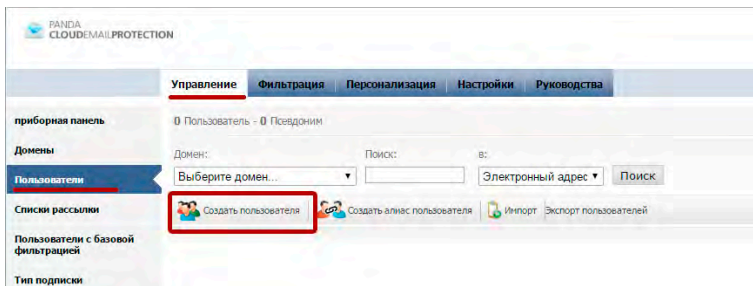
- **Атрибут, который содержит псевдоним:** proxyAddresses. Большинство инсталляций Active Directory + Exchange будут использовать этот атрибут (proxyAddresses) для указания алиаса электронного адреса данного пользователя.
- **Фильтр LDAP:** (objectclass=*). Вы можете указать здесь различные опции фильтра, чтобы получать только требуемую информацию.
- **Является ли поле многозначным?** Нет
- **Разделитель псевдонима:** Введите ':'
- **Псевдоним находится в том же объекте, что и почтовый адрес?** Да

Эти значения являются обычными для стандартной схемы Active directory. После того как Вы настроили данный раздел, Вы должны проверить настройки, используя кнопку "Проверить". Введите действующий алиас электронной почты в Вашей организации. Система должна вернуть соответствующий основной адрес электронной почты для алиаса. На следующем

рисунке показан способ настройки данного раздела, а также результат проверки:



Если проверка не вернула основной адрес электронной почты, связанный с указанным алиасом почтового адреса, пожалуйста, еще раз проверьте значения, указанные в этом разделе, вместе с администратором Вашего домена, т.к. Ваша корпоративная схема может отличаться от стандартной схемы, поставляемой с продуктами Microsoft.



Восстановление данных пользователя

В данном разделе можно указать, какие атрибуты внутри Вашей схемы каталогов содержат полные имена пользователей для того, чтобы было проще его определять при автоматической регистрации в системе. Типичная конфигурация для Microsoft Active Directory выглядит следующим образом:

- **Атрибут, который содержит фамилию пользователя:** displayName
- **Хранит имя и фамилию вместе:** Выбрано.

Восстановление данных пользователя

Атрибут, который содержит фамилию пользователя: [Помощь](#)

Хранит имя и фамилию вместе

Хранит имя и фамилию раздельно

Атрибут, который содержит имя пользователя:

(*) Обязательные поля

После указания всей необходимой информации, сохраните настройки.

Обратите внимание на следующие моменты при указании необходимой информации для настройки режима регистрации через LDAP.

Вы должны проверить следующие настройки:

- Проверьте, что соединение с Вашим контроллером домена корректное.
- Проверьте, что Email Protection способен находить пользователей на Вашем сервере каталогов (раздел **Поиск имени пользователя**).
- Если опция **Включить обнаружение псевдонима** включена, проверьте, что Email Protection способен возвращать основной адрес электронной почты по алиасу электронного адреса.



Если во время любой из предыдущих проверок возникает ошибка, то сохраните конфигурацию и вернитесь позже к соответствующему разделу, чтобы перенастроить опции после проверки значений вместе с Вашим Администратором домена.

Пример, приведенный в настоящем разделе, соответствует службе каталогов Active Directory. Конкретная конфигурация может сильно отличаться в зависимости от схемы, используемой в Вашей организации, или если схема Microsoft Active Directory по умолчанию была изменена.

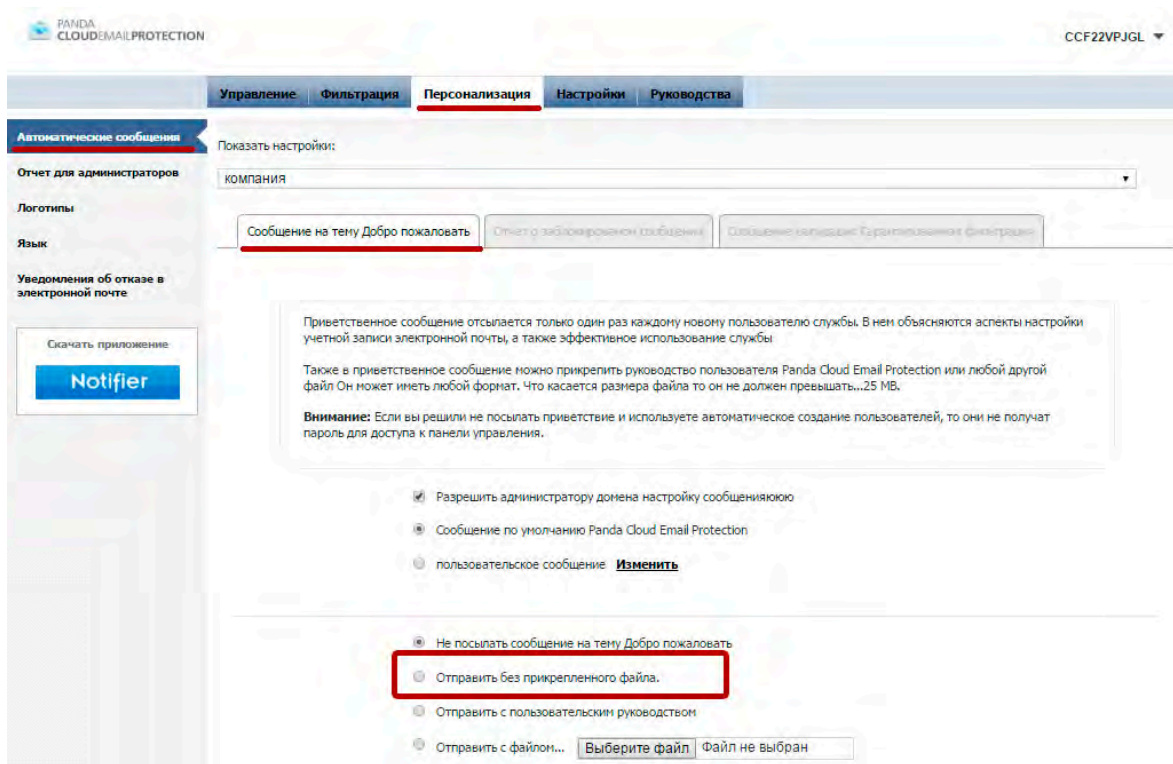
4.2.7. Персонализация платформы

После выполнения настройки домена и пользователей, платформа готова защищать пользователей, принадлежащих к настроенным доменам. Следующий шаг связан с персонализацией самой платформы с помощью меню **Персонализация**.

Рекомендуется настроить следующие основные параметры:

Сообщение на тему Добро пожаловать

Если был выбран любой из доступных режимов автоматической регистрации (SMTP или LDAP), можно настроить платформу таким образом, чтобы она отправляла приглашительные письма автоматически зарегистрированным пользователям. Данное сообщение будет содержать регистрационные данные, которые позволят пользователю получить доступ к своей пользовательской консоли. Если Вы хотите, чтобы Ваши пользователи знали, что существует панель управления, где они могут управлять своими опциями фильтрации электронной почты и получать доступ к спамовым сообщениям, хранящимся в карантине системы, то включите соответствующую опцию (**по умолчанию она отключена**).



Логотипы

Администратор компании может загрузить ее логотип, который будет включен во все системные уведомления для пользователей, которые защищены данным решением, а также в пользовательской консоли управления. Для этого перейдите в раздел **Персонализация** ->

Логотипы.



Учтите, что все действия по персонализации могут быть выполнены глобально или для каждого домена в отдельности. Уровень, на котором будут применены опции кастомизации, может быть выбран с помощью опции "Показать настройки" наверху страницы.

4.2.8. Настройка MX-записей Вашего DNS-сервера

После того как все предыдущие шаги были завершены, платформа будет готова защищать входящие письма, предназначенные для Вашей организации. Чтобы интегрировать **Email Protection** в систему доставки электронной почты в Вашу организацию, измените MX-записи защищаемых доменов, чтобы они указывали на следующие хосты сервиса:

mx01.mep.pandasecurity.com

mx02.mep.pandasecurity.com

mx03.mep.pandasecurity.com (ipv6 для входящего почтового трафика)

smtp.mep.pandasecurity.com



Указанные здесь MX-записи могут отличаться в зависимости от Вашей конфигурации. Проверьте Ваши текущие MX-записи сервиса, для чего перейдите в "Руководства" -> "Информация о настройках". Проверьте этот раздел до того, как сделаете какие-либо изменения в DNS.



Мы советуем Вам указать одинаковый приоритет (например, "10") у обеих MX-записях для достижения балансировки нагрузки внутри платформы Email Protection.



Учтите, что Panda Security не имеет доступа к Вашим MX-записям. Эта задача должна быть выполнена Вами, т.к. DNS-записи доступны только Вам. Пожалуйста, уточните этот момент с Вашим провайдером DNS-сервиса или сетевым администратором для получения дополнительной информации о том, как изменить Ваши настройки DNS.

После внесения соответствующих изменений, **Email Protection** начнет обрабатывать входящие письма, предназначенные для Вашей организации, блокируя спамовые сообщения и доставляя на Ваши почтовые серверы только "чистые" электронные письма.

4.2.9. Дополнительные настройки безопасности (файервол)

Как только MX-записи доменов, защищаемых данным решением, были изменены, можно ограничить доставку входящих писем на почтовые серверы, защищенные Email Protection, разрешив доставку входящих писем только с определенного диапазона IP-адресов, принадлежащих облачным серверам Panda Security. Ниже приведены диапазоны IP-адресов, с которых осуществляется доставка входящей почты в Вашу организацию:

188.94.13.128/25

92.54.22.0/24

92.54.27.0/24

При этом для этих IP-адресов должны быть открыты следующие порты:

SMTP: 25

LDAP: 389

LDAP через SSL: 636



Диапазоны IP-адресов могут отличаться от указанных в данном документе. Для их проверки, пожалуйста, перейдите в раздел "Руководства" -> "Информация о настройках" в консоли управления. Ограничить можно как на уровне файервола на периметре сети, так и на уровне почтового сервера.

4.3. Настройка фильтрации исходящей почты в Email Protection

После завершения настройки фильтрации входящей почты, **Email Protection** может быть настроен для фильтрации исходящей почты, отправляемой из Вашей организации в Интернет. Этот шаг не обязателен. Фильтрация исходящей почты не зависит от фильтрации входящей почты. Впрочем, чтобы фильтрация исходящей почты работала корректно, необходимо правильно настроить фильтрацию входящей почты (домены и пользователи должны быть правильно настроены в Email Protection).

Чтобы настроить фильтрацию исходящей почты через **Email Protection**, Вам необходимо определить "Smart Host" на почтовом сервере Вашей компании, чтобы все исходящие сообщения доставлялись в облако **Panda Security**. Email Protection будет фильтровать Ваши исходящие сообщения, отправляя на почтовый сервер получателя только "чистую" почту. Пожалуйста, проверьте документацию на Ваш почтовый сервер для получения подробной информации о том, как настроить "Smart Host".

При настройке "Smart Host" используйте следующий hostname сервиса:

smtp.mep.pandasecurity.com



Шаги по настройке хоста сервиса, используемого для отправки исходящей почты, могут отличаться в зависимости от Вашей конфигурации. Используемый Smart Host указан в консоли управления ("Руководства" -> "Информация о настройках"). Пожалуйста, проверьте этот раздел до внесения каких-либо изменений в Вашем почтовом сервисе.

SMTP-сессия с Вашим Smart Host должна быть настроена как Authenticated SMTP session. Используйте те же самые регистрационные данные (пользователь и пароль), которые были предоставлены Вам для доступа к консоли управления:

<https://mep.pandasecurity.com/admin/>.

4.4. Настройка SPF-записей в Вашем DNS

Вне зависимости от того, настроили ли Вы фильтрацию исходящей почты или настроили только фильтрацию входящей почты в **Email Protection, Panda Security** рекомендует Вам изменить SPF-записи Ваших доменов, чтобы включить диапазоны IP-адресов наших дата-центров. Сделайте это, если Ваш исходящий трафик фильтруется через решение **Panda Email Protection**. Таким образом, Вы сможете предотвратить ситуации, когда почтовые серверы получателей будут отказывать в доставке писем, приходящих с облачных серверов Panda Security. Для этого добавьте в Ваши SPF-записи следующие диапазоны IP-адресов:

ip4:92.54.39.0/24 ip4:188.94.13.128/25
ip4:92.54.22.0/24 ip4:80.67.107.0/24
ip4:92.54.27.0/24 ip4:80.67.109.0/24



Диапазоны IP-адресов могут отличаться от указанных в данном документе. Для их проверки, пожалуйста, перейдите в раздел "Руководства" -> "Информация о настройках" в консоли управления.

Пример SPF-записи, связанной с доменом: "v=spf1 ip4:188.94.13.128/25 ip4:92.54.22.0/24 ip4:92.54.27.0/24 ip4:92.54.39.0/24 ip4:80.67.107.0/24 ip4:80.67.109.0/24 ip4: [OTHER CUSTOMER IP ADDRESSES] ~all"

Мы рекомендуем, чтобы Вы добавили IP-адреса облачных серверов Panda Security к Вашим текущим SPF-записям в Вашем DNS.

5. ДОПОЛНИТЕЛЬНАЯ И КОНТАКТНАЯ ИНФОРМАЦИЯ

Для получения более подробной информации о настройке и опциях фильтрации, предоставляемых нашим продуктом, смотрите следующую документацию:

- Руководство администратора по Email Protection
<https://mep.pandasecurity.com/download/manual/en/corp.pdf>
- Руководство пользователя по Email Protection
<https://mep.pandasecurity.com/download/manual/en/user.pdf>

Если Вам необходима техническая поддержка, пожалуйста, свяжитесь с нашими специалистами по адресу: support@rus.pandasecurity.com

Email Protection

Ni los documentos ni los programas a los que usted pueda acceder pueden ser copiados, reproducidos, traducidos o transferidos por cualquier medio electrónico o legible sin el permiso previo y por escrito de Panda Security, C/ Gran Vía Don Diego López de Haro 4, 48001 Bilbao (Bizkaia), ESPAÑA.

Marcas registradas. Windows Vista y el logotipo de Windows son marcas o marcas registradas de Microsoft Corporation en los Estados Unidos y otros países. Todos los demás nombres de productos pueden ser marcas registradas de sus respectivas compañías.

© Panda Security 2015. Todos los derechos reservados.