Содержание

Введение

Этот документ описывает, как установить и настроить Microsoft Azure AD и офис 365 для работы с Cisco Email Security Appliance (ESA).

Предварительные условия

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- AsyncOS для Безопасности электронной почты 9.9.5-039 (Белладжио), или более новый.

Этот документ также требует придерживающегося:

- Подписка учетной записи [офиса 365](#) (Удостоверьтесь, что ваша [подписка учетной записи офиса 365](#) включает доступ к электронной почте, такой как учетная запись Предприятия или Предприятия E5 E3.)
- Учетная запись [Microsoft Azure](#)
- И офис 365 и учетные записи Microsoft Azure AD связаны должным образом к активному *user@domain.com* адресу электронной почты, и вы в состоянии передать и получить электронные письма через тот домен и учетную запись.
- Доступ к Windows PowerShell, обычно администрируемому от Windows Server.
- Доменный активный Общий/Частный сертификат и секретный ключ, используемый для подписания сертификата или способности создать Общий/Частный сертификат и способность сохранить секретный ключ, использовали подписывать сертификат.

Настройте значения сертификата

Вход в систему к Windows и использование PowerShell завершают следующие команды, чтобы сопоставить и получить *$keyid*, *$base64Thumbprint* и *$base64Value*:

1. **$cer = ново-объектная система. Безопасность. Криптография. X509Certificates. X509Certificate2**

2. $cer. Импорт ('C:\path_to_cert\PEM_certificate.crt')
3. $bin = $cer. GetRawCertData ()
4. $base64Value = [Система. Преобразуйте]:: ToBase64String ($bin)
5. $bin = $cer. GetCertHash ()
6. $base64Thumbprint = [Система. Преобразуйте]:: ToBase64String ($bin)
7. $keyid = [Система. Гуид]:: NewGuid ().ToString ()
8. эха
9. эха
10. $keyid эха

В целях этого документа пример конфигурации будет основываться на "esatest.onmicrosoft.com". Команды, как выполнено через PowerShell должны быть подобны следующему примеру:

Сохраните выходные данные, которые вы получаете за *$keyid*, *$base64Thumbprint* и *$base64Value*, поскольку эти значения будут использоваться позже в *Создавании Явного* раздела этого документа. *$base64Thumbprint* будет использоваться во время конфигурации ESA.

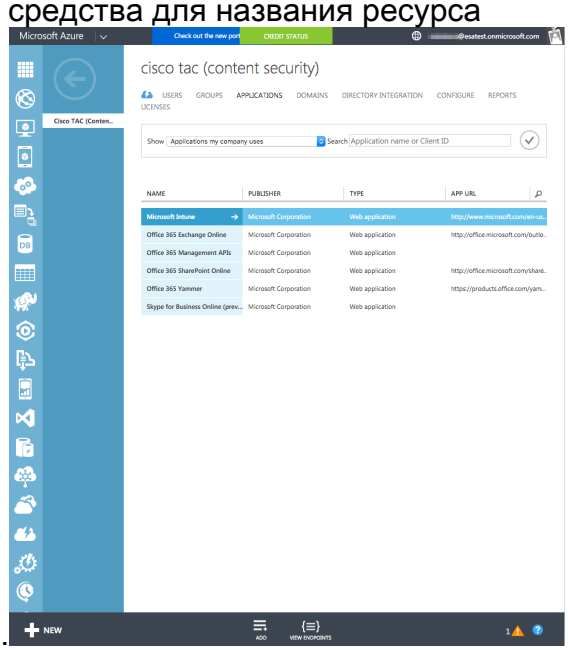
> **Примечание:** *$base64Value* требуется, чтобы быть отредактированным, чтобы быть отдельным каналом.

Сохраните Сертификат открытых ключей (.crt), и Секретный ключ использовал подписывать сертификат (.pem) локально. Секретный ключ будет необходим во время конфигурации ESA.

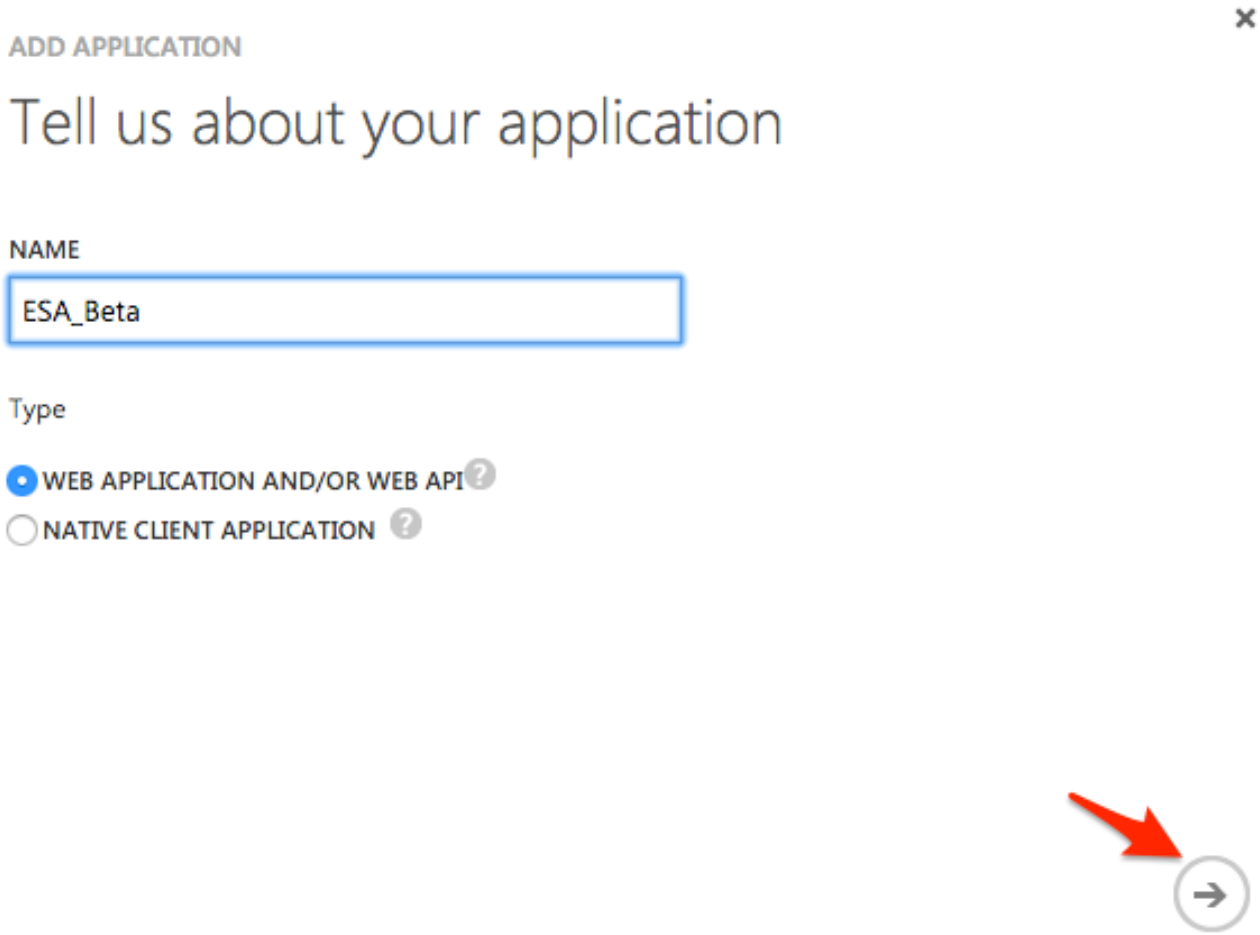
Настройте Microsoft Azure AD

Создайте пользовательский Web - приложение

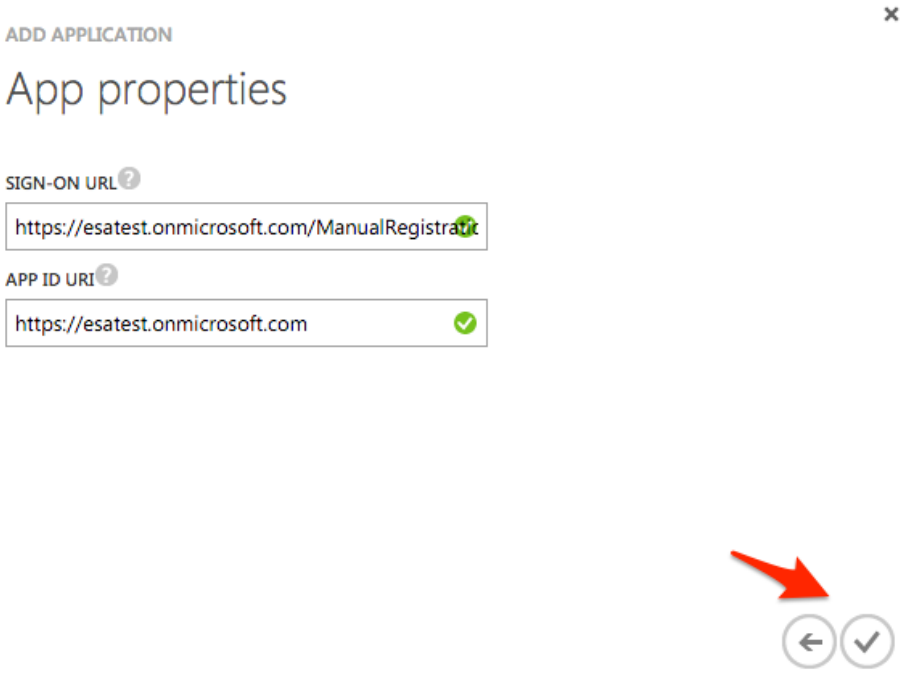
1. Вход в систему к Microsoft Azure.
2. Перейдите к **ЭЛЕМЕНТАМ ALL**.
3. Щелкните по названию ресурса для своего домена.
4. От вкладок программного средства для названия ресурса выберите **APPLICATIONS**.



5. От нижней панели инструментов выберите **ADD**:
6. Когда представлено, *"Что вы хотите сделать?"*, выберите**, добавляют приложение, которое разрабатывает моя организация**.
7. Создайте с соответствующим названием, и оставьте *Тип* как **Web - приложение и/или веб-API**, и нажмите стрелку для продолжения:



8. Чтобы закончить добавлять пользовательский Web - приложение, введите следующие значения для своего домена и нажмите проверку для завершения: ВОЙДИТЕ В СИСТЕМУ URL: **https://*<your.domain.com>*/*ManualRegistration***URI ИДЕНТИФИКАТОРА ПРИЛОЖЕНИЯ:



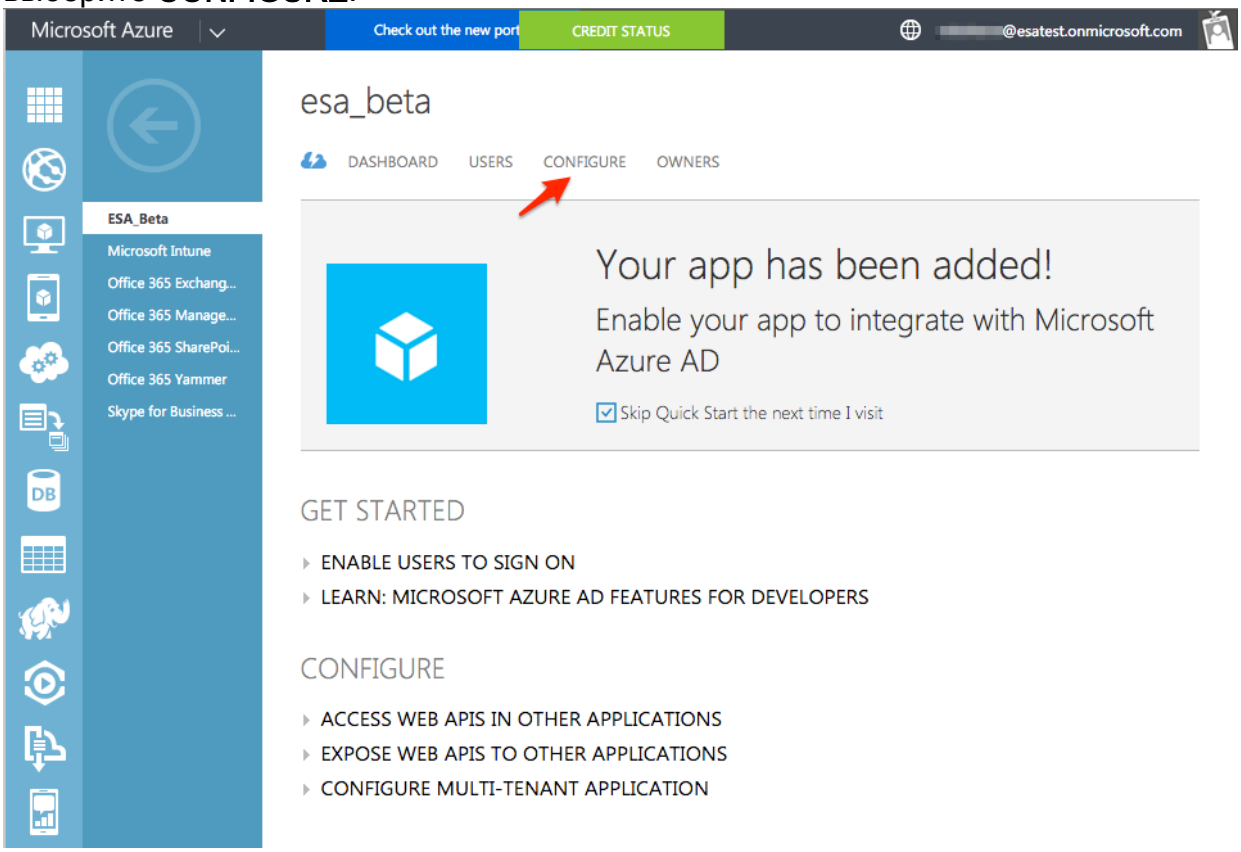
https://*<your.domain.com>*

9. От Microsoft, относительно URI Идентификатора приложения: "Поскольку URI Идентификатора приложения является логическим идентификатором, он не должен решать к интернет-адресу. Это представлено вашим приложением при отправлении запроса единой точки входа к AD Azure. AD Azure определяет ваше приложение и передает ответ входа в систему (маркер SAML) к URL Ответа, который был предоставлен во время регистрации приложений. Используйте значение URI Идентификатора приложения для установки wtrealm свойства (для Федерации WS) или свойства Issuer (для SAML-P) при выполнении запроса входа в систему. **URI Идентификатора приложения** должен быть уникальным значением в AD Azure вашей организации".

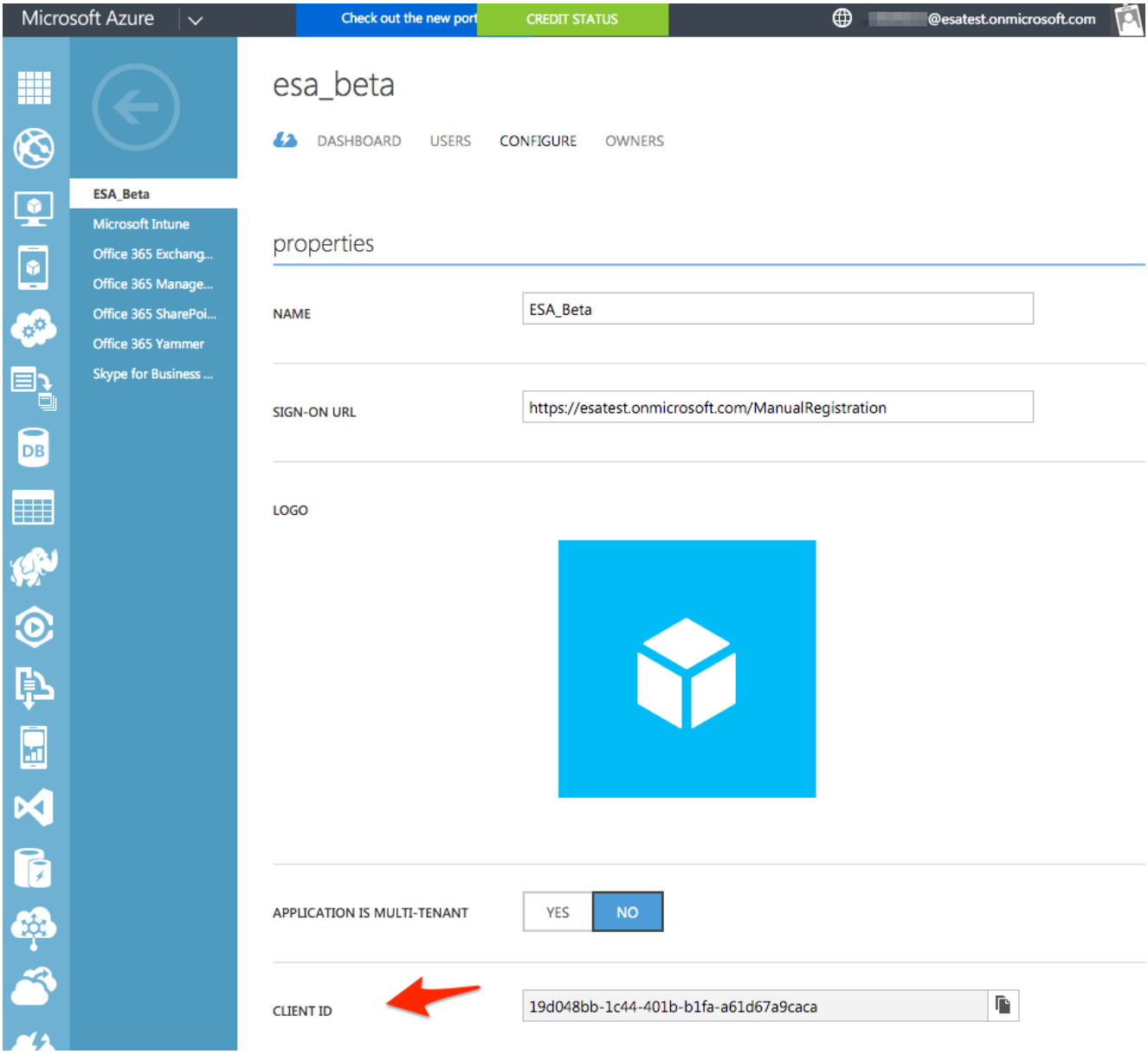
   Примечание: "При включении приложения для внешних пользователей значение URI Идентификатора приложения приложения должно быть адресом в одном из проверенных доменов каталога. В результате это не может быть URN. Эта гарантия препятствует тому, чтобы другие организации задали (и взяли) уникальное свойство, которое принадлежит вашей организации. Во время разработки можно изменить URI Идентификатора приложения на местоположение в исходном домене организации (если вы не проверили пользовательское доменное / доменное тщеславие), и обновите свое приложение для использования этого нового значения. Исходный домен является доменом с 3 уровнями, во время которого вы создаете, регистрируются в системе, такие как contoso.onmicrosoft.com".

Настройте пользовательский Web - приложение

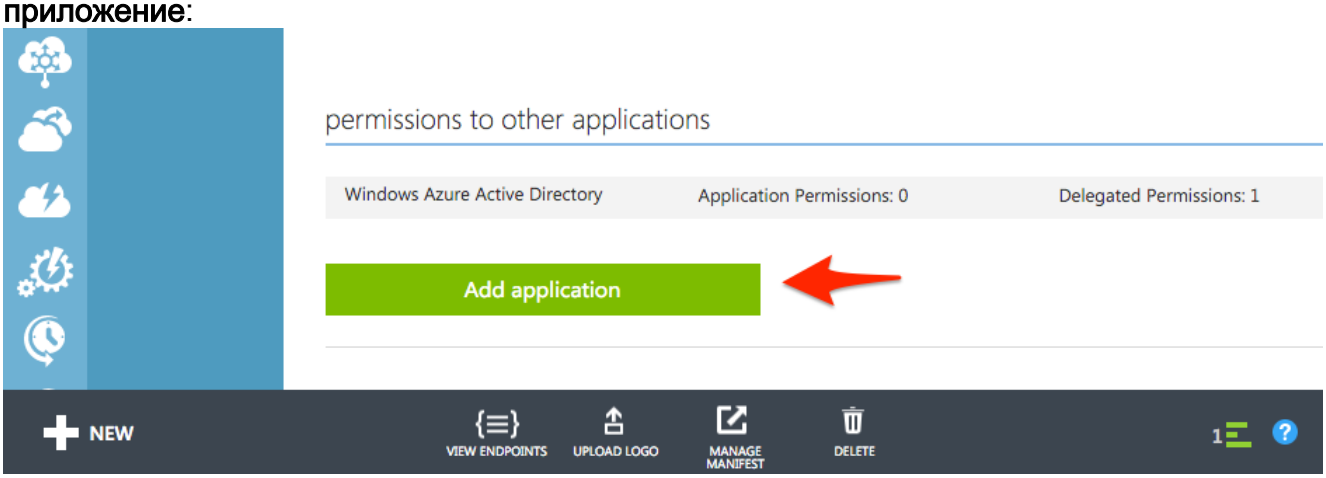
1. Как только пользовательский Web - приложение был создан, по вам автоматически проводят в сам пользовательский Web - приложение. Отсюда, во вкладках программного средства,
   выберите **CONFIGURE**:



2. С этого экрана можно просмотреть URL Входа в систему и другие элементы конфигурации, как создано. **Примечание:** ***Идентификатор клиента*** перечислен на этом экране. Это
значение

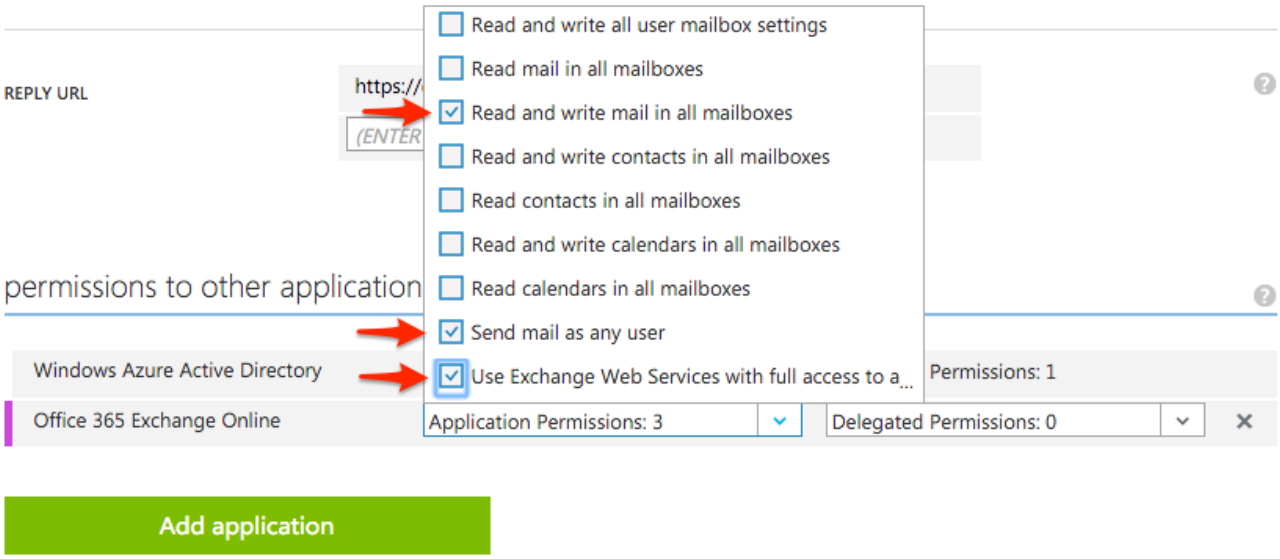


3. С этого того же экрана для пользовательской конфигурации Web - приложения перейдите к нижней части и **нажмите Add приложение**:

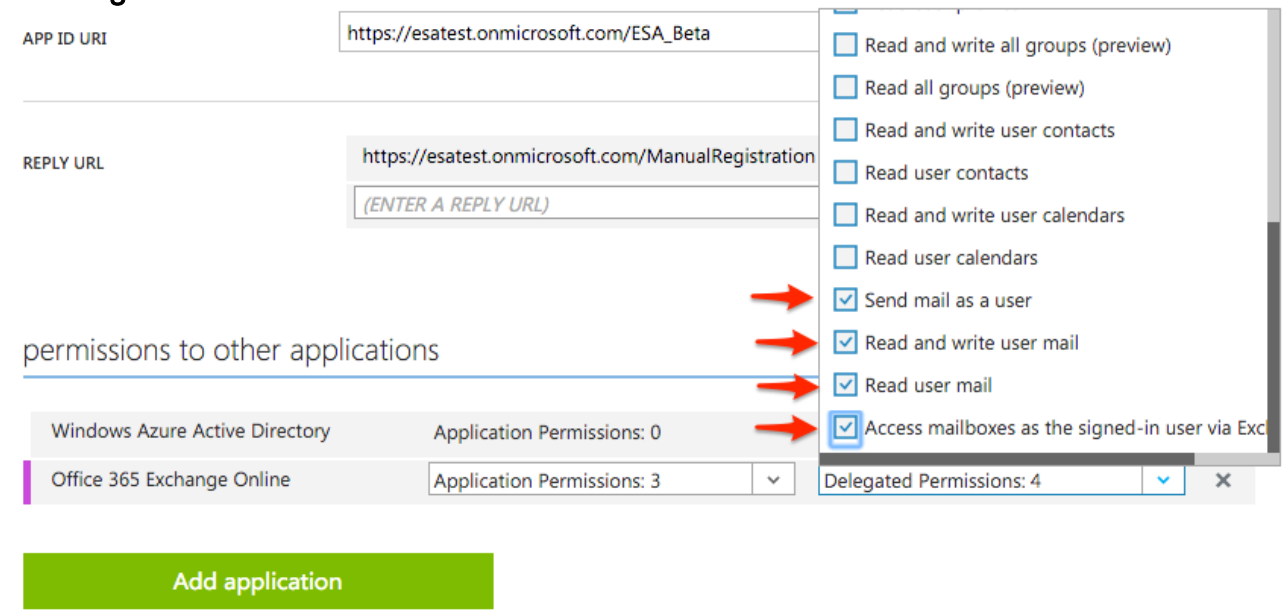


4. Выберите **Office 365 Exchange Online** и нажмите проверку для продолжения.
5. Для *разрешений Exchange OnlineApplication офиса 365* выберите **Read и почту записи**

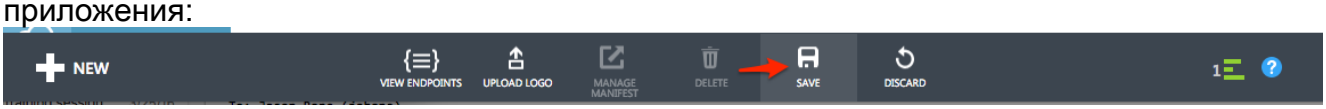
во всех почтовых ящиках, **Передайте почту как любого пользователя** и **веб-сервисы Exchange Использования с полным доступом...**:



6. Для *разрешений Exchange OnlineDelegated офиса 365* выберите **почту Send как пользователя**, **Рида и запишите пользовательскую почту**, **пользовательскую почту Рида** и **почтовые ящики Доступа как регистрировавшийся пользователь через Exchange**:



7. Нажмите **Save** от нижней панели инструментов для сохранения всех работают и конфигурация для пользовательского Web - приложения:



Создайте декларацию

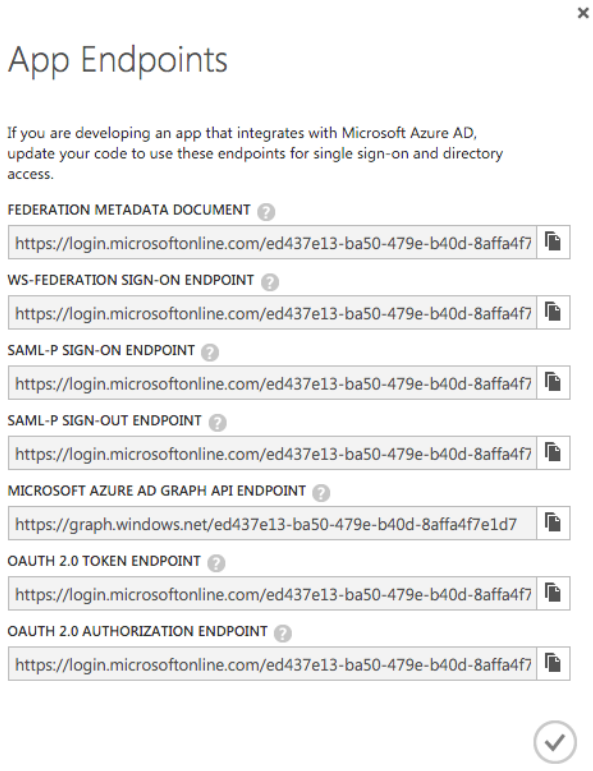
1. Как только пользовательский Web - приложение завершил сохранение и обновление, нажмите **MANAGE MANIFEST> Download Manifest** от нижней панели инструментов:

2. Перейдите посредством ответов и сохраните декларацию Web - приложения в формате .json к вашему локальному компьютеру.
3. Найдите этот .json файл и откройте этот .json файл с текстовым редактором. (Предпочтительный Блокнот ++, Atom, и т.д.)
4. Ищите и найдите "keyCredentials" линию.
5. Вы будете заменять этот отдельный канал следующими составными строками, и настраивать использование более ранних определенных учетных данных от *Настраивать* раздела Значений *Сертификата* (*$base64Thumbprint*, *$keyid* и *$base64Value*):
6. Как обращено внимание ранее, при вводе *$base64Value*, это требуется, чтобы быть отредактированным, чтобы быть значением отдельного канала.
7. Продолжая пример, как создано от запуска этого документа, модифицированный *keyCredentials* будет следующие:
8. Сохраните .json файл локально.
9. Возвратитесь к своему браузеру и порталу Microsoft Azure.
10. Нажмите **MANAGE MANIFEST> Upload Manifest**:

11. Просмотрите и найдите отредактированный .json файл и выберите метку выбора для завершения загрузки.

Обнаружение ID арендатора

1. Нажмите **on VIEW ENDPOINTS** для просмотра Оконечных точек, интегрированных в Microsoft Azure AD.
2. С в URL, заметьте подобное значение для каждой линии, "ed437e13-ba50-479e-b40d-8affa4f7e1d7", это - ***ID Арендатора***.



Это будет уникально для вашего приложения и конфигурации. Сделайте запись этого значения для более поздней конфигурации на ESA.

Заключительный обзор значений, которые будут сохранены

Следующие значения должны были быть зарегистрированы во время конфигурации Microsoft Azure AD для использования при настройке настроек почтового ящика на ESA:

От *настраивают значения сертификата*:

- Сертификат с закрытым ключом (.pem)
- $base64Thumbprint

От *Настраивают пользовательский Web - приложение*:

- Идентификатор клиента

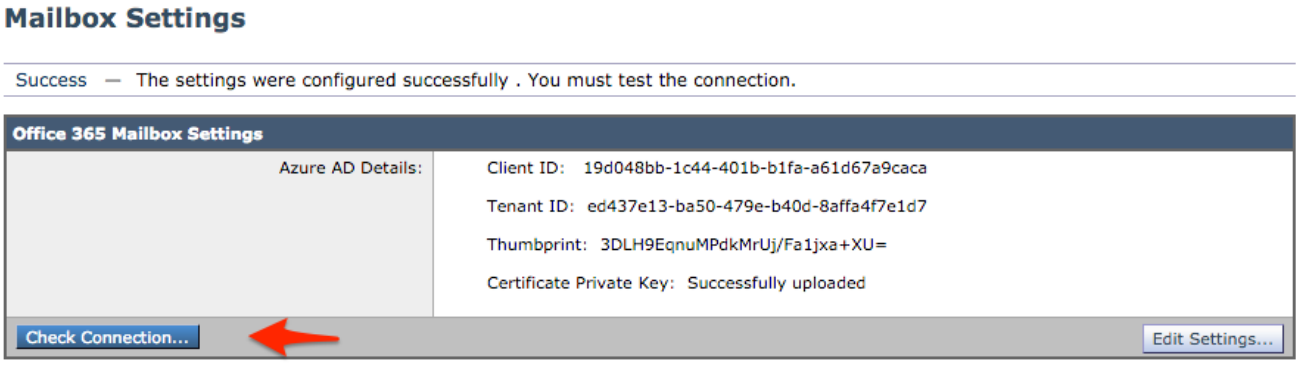
От *обнаружения ID арендатора*:

- ID арендатора

Настройте настройки почтового ящика на ESA

С завершенной конфигурацией Microsoft Azure AD вы готовы иметь ESA, передают и проверяют.

1. Вход в систему к устройству ESA через GUI.
2. **Включите** Настройки почтового ящика офиса 365 под **Администрированием системы> Настройки почтового ящика.**
3. Выбрать? **Включить Настройки почтового ящика офиса 365** флажок и предоставляет вашу подробную информацию Microsoft Azure AD (*Идентификатор клиента и ID Арендатора*) полученный при регистрации приложения ESA в Microsoft Azure AD наряду со *Следом большого пальца и Секретным ключом* сертификата.
4. Нажмите **Submit** для сохранения изменений к Настройкам почтового ящика.
5. Необходимо будет протестировать соединение с Microsoft Azure AD в это время для домена офиса 365 согласно конфигурации:



6. Используйте активный и допустимый адрес электронной почты на учетной записи, нажмите **Test Connection**: 

7. Как только статус соединения успешен, нажмите **Done** для завершения проверки соединения.
8. Наконец, нажмите **Commit** для сохранения всех изменений конфигурации на ESA.