

Как настроить Microsoft Azure AD и офис 365 для использования на ESA

Содержание

[Введение](#)

[Предварительные условия](#)

[Настройте значения сертификата](#)

[Настройте Microsoft Azure AD](#)

[Создайте пользовательский Web - приложение](#)

[Настройте пользовательский Web - приложение](#)

[Создайте декларацию](#)

[Обнаружение ID арендатора](#)

[Заключительный обзор значений, которые будут сохранены](#)

[Настройте настройки почтового ящика на ESA](#)

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. `$keyid` = [Система. Гуйд]:: NewGuid ().ToString ()
8. `$base64Value` эха
9. `$base64Thumbprint` эха
10. `$keyid` эха

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

Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

```
PS C:\Users\Administrator> cd .\Desktop
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> $cer = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2
PS C:\Users\Administrator\Desktop>
$cer.Import('C:\Users\Administrator\Desktop\esatest.onmicrosoft.com_PEM.crt')
PS C:\Users\Administrator\Desktop> $bin = $cer.GetRawCertData()
PS C:\Users\Administrator\Desktop> $base64Value = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $bin = $cer.GetCertHash()
PS C:\Users\Administrator\Desktop> $base64Thumbprint = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $keyid = [System.Guid]::NewGuid().ToString()
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Value
MIIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxCAJBGnVBAyTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJYXjV
bGluYTEEMMAoGA1UEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxDVVEFDMSAwHgYDVQDEExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnAY2lzY28uY29tMBA4
XDTE2MDMyODE0NTYwMFoXDTE3MDMyODE0NTYwMFowZcxCAJBGnVBAyTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJYXjVbGluYTEEMMAoGA1UEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxDVVEFDMSAwHg
YDVQDEExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnAY2lzY28uY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB6r/Mt fKwG+86eHzdYk1CdyT+j
/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axulraQeZgY/dkyHkTE26vt6rpy5g611TLloTZG1F0nkzT5Gs+zLOuhPHaT1DMU70LCXh8CHs2cLsczpdWfb20sHxTV1ISVJ
qjdhYHM7vc6Vnf fMYIYxAE90ZE19QH0dU5n7spPyxUP0fp8z8gHsQ7HhRTsCNG
WbFyYb0Ib1RTOznmzMXaSONRKYaIpkLkOSwZurT0wyGJd+TzSw+RgsX1vKJNmKih/i11YlVMkyq+T7PjBPDwhU8uAGQIDAQA
Bo4HWMiHTMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAGwMHAGA1UdJQRpMGCcGCC
sGAQUFBwMBBggrBgEFBQcDAGYIKwYBBQUHAWQGCisGAQQBgjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgj
cKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQGA1UdEQQ9MDuCF2VzYXRlc
3Qub25taW9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnAY2lzY28uY29tMIIIBIjANBgkqhkiG9w0BAQUFAAOCAQEAR
/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625
f31o1kADPcK3ml0UarT35hH6f9abZSXM3mj3zMnuK5nW2ypDCVUiuA2C51+woEubSmvn980GHuSXOqfLMPtniUMTubp+SICD
rtCse212GkE1OCrmxFlwtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Z
xg8NKtiyEzV99OJ6+DokMn1fQOXDBPkgHI1mzFmVQogUGdCvbpvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj
1+guS0X0FMmhkDJOTyZWnAQ==
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Thumbprint
```

```
3DLH9EqnuMPdkMrUj/Fa1jxa+XU=  
PS C:\Users\Administrator\Desktop>  
PS C:\Users\Administrator\Desktop> echo $keyid  
89ed56fc-7fae-4d10-ad63-7ddaef8e737
```

Сохраните выходные данные, которые вы получаете за *\$keyid*, *\$base64Thumbprint* и *\$base64Value*, поскольку эти значения будут использоваться позже в *Создании 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**.

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

cisco tac (content security)

USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS

LICENSES

Show Applications my company uses Search Application name or Client ID

| NAME | PUBLISHER | TYPE | APP URL |
|------------------------------------|-----------------------|-----------------|-------------------------------------|
| Microsoft Intune | Microsoft Corporation | Web application | http://www.microsoft.com/en-us... |
| Office 365 Exchange Online | Microsoft Corporation | Web application | http://office.microsoft.com/outlo.. |
| Office 365 Management APIs | Microsoft Corporation | Web application | |
| Office 365 SharePoint Online | Microsoft Corporation | Web application | http://office.microsoft.com/share.. |
| Office 365 Yammer | Microsoft Corporation | Web application | https://products.office.com/yam.. |
| Skype for Business Online (prev... | Microsoft Corporation | Web application | |

+ NEW | ADD | VIEW ENDPOINTS | 1 ! ?

5. От нижней панели инструментов выберите **ADD**:

+ NEW |  ADD | VIEW ENDPOINTS | 1 ! ?

6. Когда представлено, "Что вы хотите сделать?", выберите, **добавляю 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:

Tell us about your application

NAME

Type

- WEB APPLICATION AND/OR WEB API [?]
- NATIVE CLIENT APPLICATION [?]



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>/ManualRegistrationURI> ИДЕНТИФИКАТОРА ПРИЛОЖЕНИЯ: <https://<your.domain.com>>**

App properties

SIGN-ON URL ?

APP ID URI ?



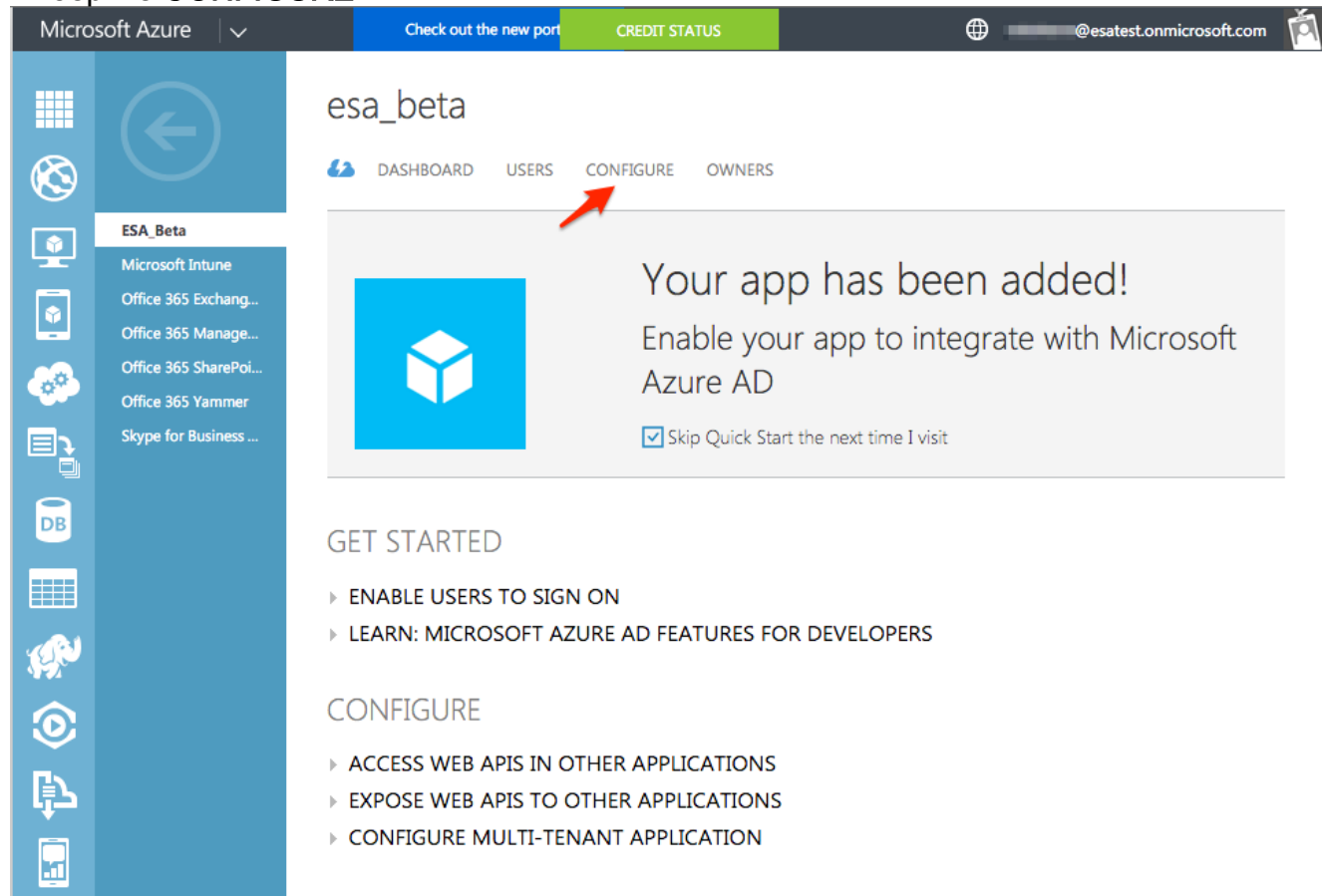
9. От Microsoft, относительно [URI Идентификатора приложения](#): "Поскольку URI Идентификатора приложения является логическим идентификатором, он не должен решать к интернет-адресу. Это представлено вашим приложением при отправлении запроса единой точки входа к AD Azure. AD Azure определяет ваше приложение 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 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 тцеславие), 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".

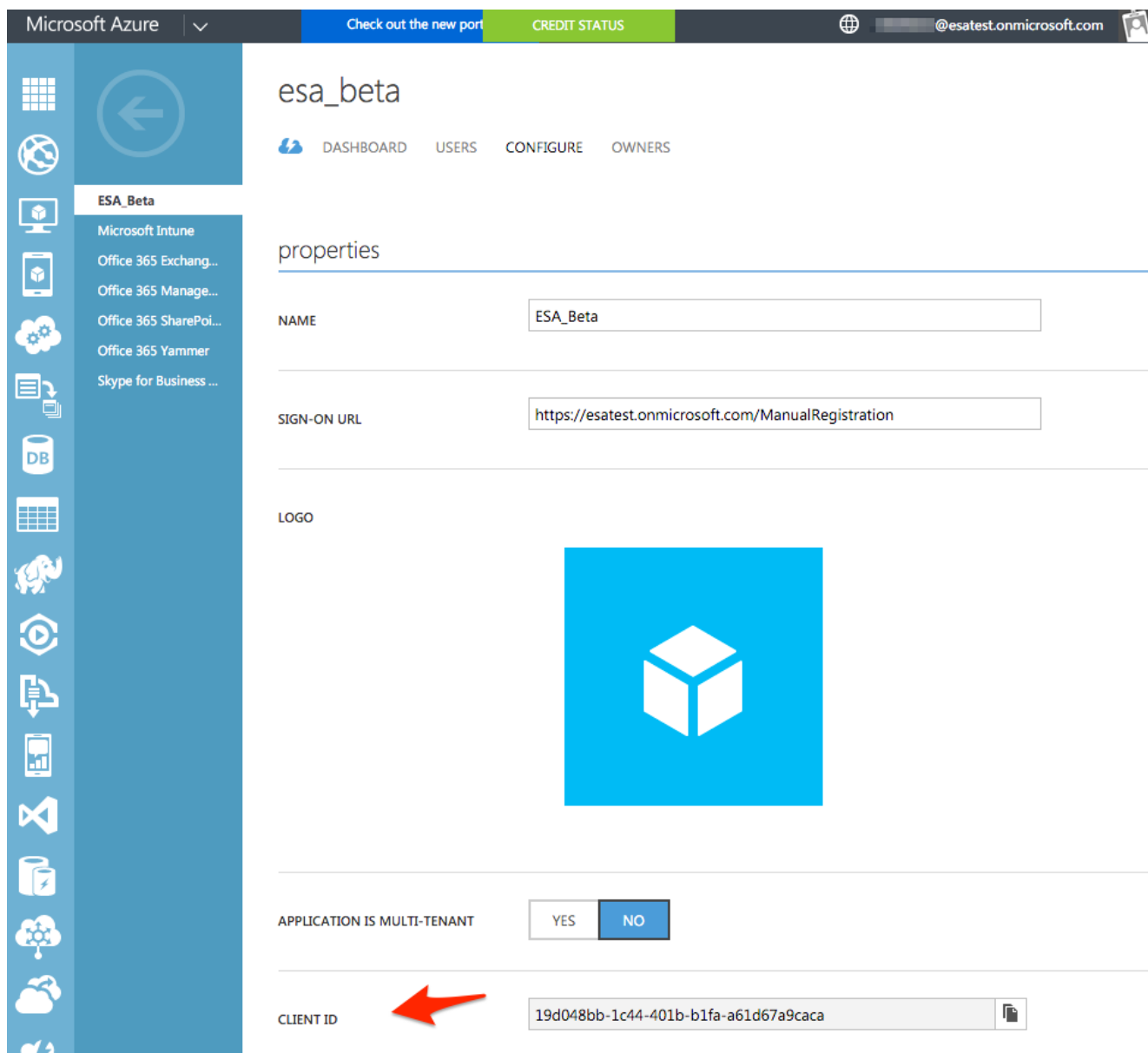
Настройте пользовательский Web - приложение

1. Как только пользовательский Web - приложение был создан, по вам автоматически

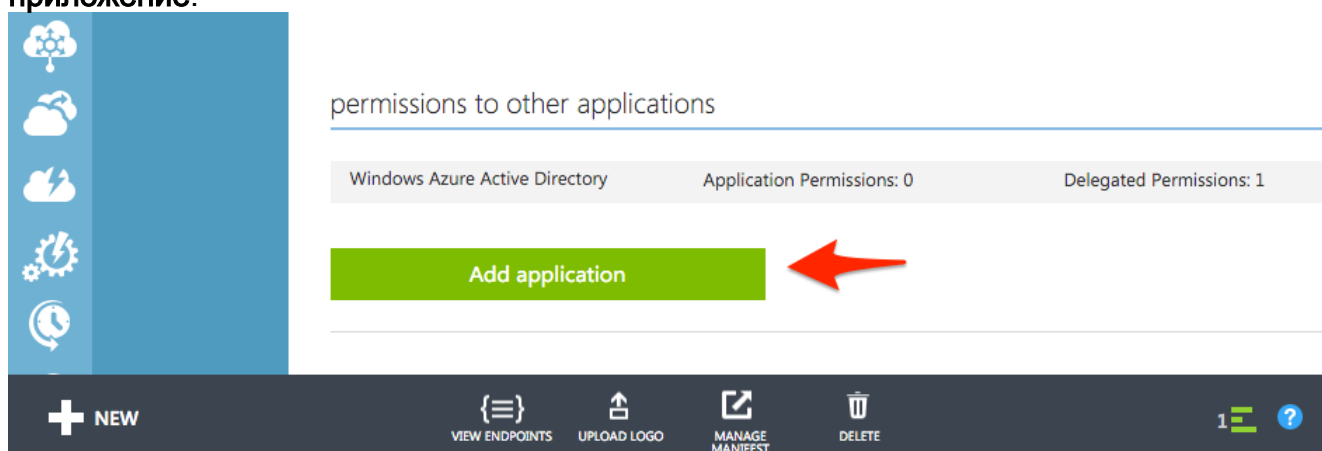
проводят в сам пользовательский Web - приложение. Отсюда, во вкладках программного средства, выберите **CONFIGURE**:



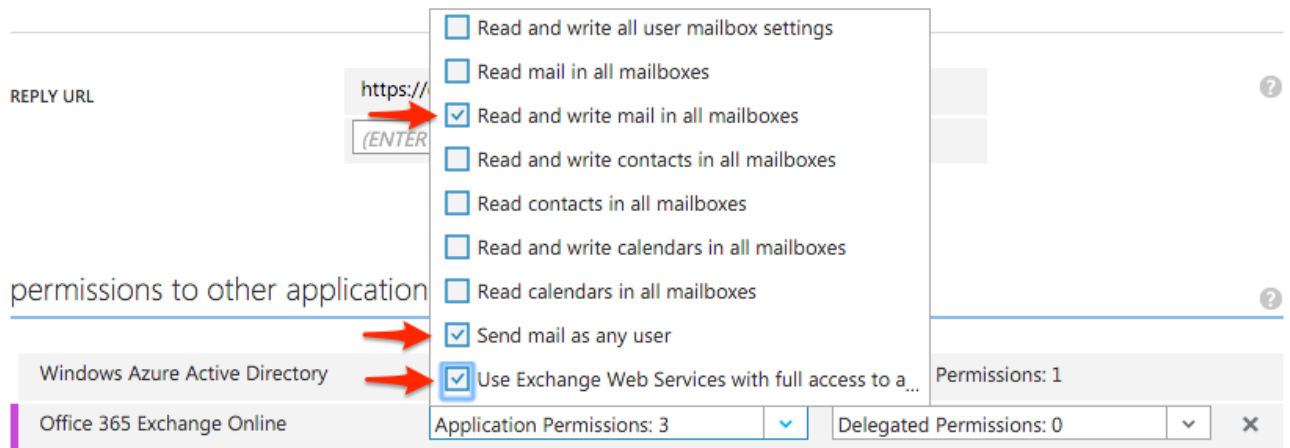
2. С этого экрана можно просмотреть URL Входа в систему и другие элементы конфигурации, как создано. **Примечание:** *Идентификатор клиента* перечислен на этом экране. Это значение будет необходимо во время конфигурации ESA.



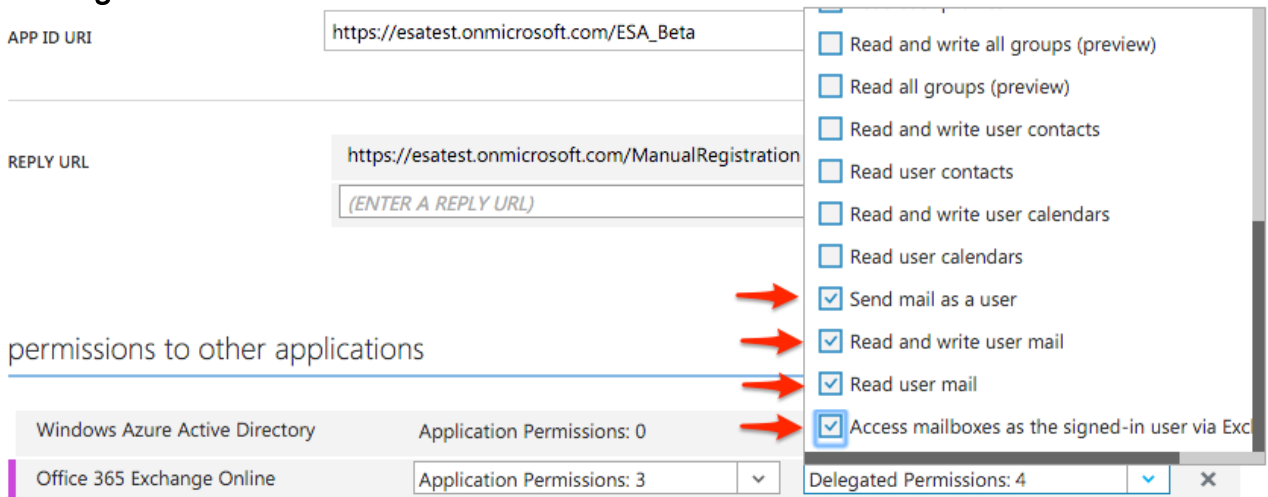
3. С этого того же экрана для пользовательской конфигурации Web - приложения перейдите к нижней части и **нажмите Add приложение:**



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 Исползования с полным доступом....:



6. Для разрешений Exchange Online Delegated офиса 365 выберите почту Send как пользователя, Риды и запишите пользовательскую почту, пользовательскую почту Риды и почтовые ящики Доступа как зарегистрировавшийся пользователь через Exchange:

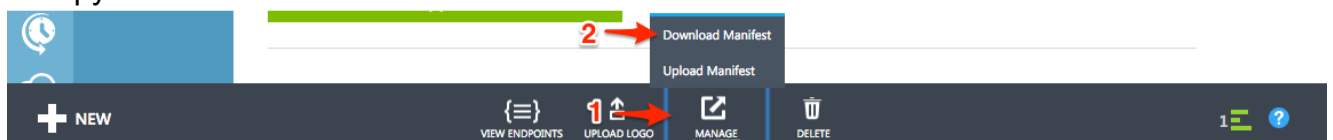


7. Нажмите **Save** от нижней панели инструментов для сохранения всех работают и конфигурация для пользовательского Web - приложения:



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 *Настроить* раздела Значений *Сертификата* (*\$base64Thumbprint*, *\$keyid* и *\$base64Value*):
6. "keyCredentials": [


```

{
  "customKeyIdentifier": "$base64Thumbprint",
  "keyId": "$keyid",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "$base64Value"
}
],

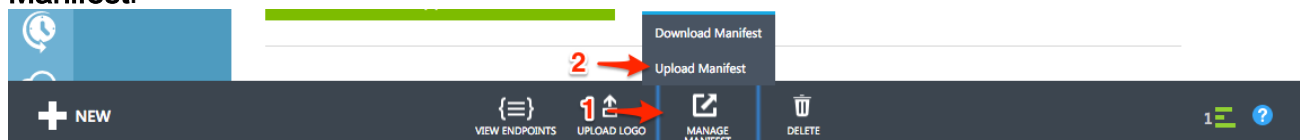
```
7. Как обращено внимание ранее, при вводе *\$base64Value*, это требуется, чтобы быть отредактированным, чтобы быть значением отдельного канала.
8. Продолжая пример, как создано от запуска этого документа, модифицированный *keyCredentials* будет следующие:
9. "keyCredentials": [


```

{
  "customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Faljxa+XU=",
  "keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value":
  "MIIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxZAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aC
  BDYXJvbGluYTEEMMAoGA1UEBxMDU1RQMq4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdVEFDMSAwHgYDVQQDEXd1c2F0Z
  XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY21zY28uY29tMB4XDTE2MDMyODE0NTYw
  MFoXDTE3MDMyODE0NTYwMFowZCcxZAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEEMMAoGA1UEBxM
  DU1RQMq4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdVEFDMSAwHgYDVQQDEXd1c2F0ZlXN0Lm9ubWljcm9zb2Z0LmNvbT
  EhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY21zY28uY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz
  B6r/MtFkKg+86eHzdhYklCdyT+j/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
  axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZG1F0nkzT5Gs+zL0uhPHaT1DMU70LCXh8CHs2cLsczpDwf20sHxTV
  lISVJqjdhYHYM7vC6VNfMYIYxAE90ZE19QH0dU5n7spPyxUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSON
  RKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/i1YLvMKYq+T7PjBpDwhU8uAGQIDAQABo4HwMIHTMAwGA1UdE
  wQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAWQCisGAQQB
  gjcCARUGCisGAQQBgjcCARYGcisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
  GA1UdEQQ9MDuCF2VzYXRlc3Qub25taWNyb3NvZnQuY29tSByb2JzaGVyY29tY29tY29tY29tY29tY29tY29tY29tY29t
  ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBrIYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
  31o1kADPcK3ml0UarT35hH6f9abZSxm3mj3zMnuK5nW2ypDCVUiuA2C51+woEubSvmn980GHuSXOqfLMPtniUMTubp+
  SICDrCse212GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV99OJ6+DokMn1f
  QOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj1+guS0X0FmMhkDJOTyZ
  WnAQ=="
}
],

```
10. Сохраните .json файл локально.
11. Возвратитесь к своему браузеру и порталу Microsoft Azure.
12. Нажмите **MANAGE MANIFEST> Upload**

Manifest:



13. 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**.



App Endpoints

If you are developing an app that integrates with Microsoft Azure AD, update your code to use these endpoints for single sign-on and directory access.

FEDERATION METADATA DOCUMENT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



WS-FEDERATION SIGN-ON ENDPOINT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-ON ENDPOINT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-OUT ENDPOINT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



MICROSOFT AZURE AD GRAPH API ENDPOINT ?

<https://graph.windows.net/ed437e13-ba50-479e-b40d-8affa4f7e1d7>



OAuth 2.0 TOKEN ENDPOINT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



OAuth 2.0 AUTHORIZATION ENDPOINT ?

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



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. Установите флажок '**Enable Office 365 Mailbox Settings**' и предоставьте свою 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:

Mailbox Settings

Success — The settings were configured successfully . You must test the connection.

| Office 365 Mailbox Settings | |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure AD Details: | Client ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca Tenant ID: ed437e13-ba50-479e-b40d-8affa4f7e1d7 Thumbprint: 3DLH9EqnuMPdkMrUj/Fa1jxa+XU= Certificate Private Key: Successfully uploaded |
| Check Connection... | Edit Settings... |



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

Connection Check

Connection Parameters

Office 365 Email Address:

Test Connection



Connection Status

Connected to Azure AD.
Connection Successful.
Inbox count of Messages are 0

Done

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