Инструкция настраивает AD Azure и настройки почтового ящика офиса 365 для ESA

Содержание

Введение

Этот документ предоставляет пошаговое "практическое руководство" для регистрации нового приложения в Windows Azure и получении необходимых значений для завершения конфигурации для настроек почтового ящика офиса 365 на Cisco Email Security Appliance (ESA). Когда администратор ESA настраивает Почтовый ящик автоматическое исправление (MAR) для Усовершенствованной вредоносной защиты (AMP) на почтовых параметрах настройки политики ESA, это требуется.

Предварительные условия

Родственные продукты

Этот документ применяется к придерживающемуся:

- Весь ESA, аппаратные средства и действительное выполнение 10.x и более новый
- Весь ESA Облачной безопасности электронной почты (CES), работая 10.x и более новый

Требования

Этот документ 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 Host или Сервера.
- 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.

Вы будете создавать следующие четыре стоимости для настройки разъёма почтового ящика ESA назад к AD Azure:

1. Идентификатор клиента
2. ID арендатора
3. След большого пальца
4. Секретный ключ сертификата в формате .pem

Для построения этих требуемых значений необходимо будет выполнить шаги в этом документе. До начала необходимо будет выполнить придерживающееся через Windows Powershell:

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. **$base64Value эха**
9. **$base64Thumbprint эха**
10. **$keyid эха**

Примечание: Для #2, замена **'C:\path_to_cert\PEM_certificate.crt'** с путем к вашему сертификату.

$base64Thumbprint = *След большого пальца*. Добавьте это значение к своему списку

предварительных условий требуемых значений.

> **Совет:** Сохраните выходные данные локально за *$base64Value*, *$base64Thumbprint* и *$keyid*, поскольку они будут требоваться позже в действиях настройки. В это время вы сделаны с .crt сертификата. Имейте связанный .pem своего сертификата в доступном, локальном каталоге на вашем компьютере.

Общие сведения

Microsoft предоставляет доступ к двум версиям Портала Azure:

- https://manage.windowsazure.com (Классический портал)
- https://portal.azure.com (Новый портал)

Вы в состоянии обратиться к "Классическому порталу" от Нового портала левой панелью инструментов, выбрать "Azure Active Directory"> Classic Portal

В целях этого документа регистрация и конфигурация приложения сделаны в Новом портале. Шаги в использование "Классического портала" включены в конце этого документа. (Microsoft может принять решение в когда-то отключить Классический портал Azure.)

Инструкция настраивает AD Azure и настройки почтового ящика офиса 365 для ESA

Зарегистрируйте новое приложение в Azure

1. Обратитесь к интерфейсу пользователя Azure: https://portal.azure.com/
2. Левая строка меню, нажмите **More Services> SECURITY + ИДЕНТИЧНОСТЬ: Регистрации приложений**
3. От области Регистраций приложений нажмите **+Add**
4. Создайте название для своего приложения
5. Для типа приложения, выход как **Веб-приложение / API**
6. Для URL Входа в систему используйте следующий формат: https://*<company_domain.com>/ManualRegistration***Примечание:** *<company_domain.com>* является доменом вашего O365, где пользователи домена могут войти в систему и обратиться к вашему домену O365.
7. **Нажмите кнопку Create**

Установите требуемые разрешения для приложения

1. Щелкните по 'Названию Показа', привязанному для приложения, которое вы просто зарегистрировали
2. В области Settings, для Доступа API, нажимают **разрешения Required**
3. Нажмите **+Add**
4. В области "Add API access" нажмите **Select an API**
5. В области "Select and API" нажмите **Office 365 Exchange Online (Microsoft Exchange)**

6. Внизу страницы нажмите **Select**
7. Для Приложения Разрешения выбирают:
   • Используйте веб-сервисы Exchange с полным доступом ко всем почтовым ящикам
   • Передайте Почту как любого пользователя
   • Считайте и запишите почту во всех почтовых ящиках
8. Поскольку Делегированные Разрешения выбирают:
   • Передайте почту как пользователя
   • Считайте и запишите пользовательскую почту
   • Считайте пользовательскую почту
   • Почтовые ящики доступа как регистрировавшийся пользователь через веб-сервисы Exchange
9. Нажмите **Select** внизу страницы, это закроет область "Select an API"
10. Нажмите **Done** внизу страницы, это закроет область "Add API access"
11. Нажмите **Grant Permissions**
12. Когда предложено "Вы хотите дать разрешения ниже для myESA для всех учетных записей в текущем каталоге? Это действие обновит любые существующие разрешения, это приложение уже должно совпасть с тем, что упомянуто ниже. **Нажмите кнопку YES**

У вас теперь должно быть два перечисленные API, "Windows Azure Active Directory" и "Exchange офиса 365 Онлайн".

Необходимо будет возвратиться к Зарегистрированной области приложения для перехода следующий раздел:

1. Нажмите "X" для закрытия области "Required Permissions"
2. Нажмите "X' для закрытия области "Settings"

Вы теперь вернулись в Зарегистрированной области приложения.

Подготовьте декларацию к приложению

Отредактируйте декларацию

1. От Зарегистрированной области приложения нажмите Manifest в строке инструментов
2. Вы представлены завершенная декларация в редакторе. Линия 12 должна быть "keyCredentials". Вы будете заменять линию ONLY 12 придерживающимся:

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

3. Необходимо будет заменить $base64Thumbprint, $keyid и $base64Value со значениями Оставьте кавычки ("") вокруг значений ALL, как показаноОбратите особое внимание, что каждое значение является линией ONLY 1, включая $base64Thumbprint
4. Нажмите **Save** для обновления приложения. Необходимо видеть "Успешно

обновленное приложение" предупреждение в области панели инструментов.

Необходимо будет возвратиться к Зарегистрированной области приложения для перехода следующий раздел:

Нажмите "X" для закрытия области "Edit Manifest".

(Необязательно) загрузите декларацию

> **Совет:** Если вы успешно смогли использовать редактора в Azure для декларации, можно пропустить декларацию Загрузки и декларацию Загрузки. В противном случае и необходимо вручную отредактировать декларацию, продолжитесь.

1. От Зарегистрированной области приложения нажмите Manifest в строке инструментов
2. В Edit Manifest меню нажимают **Download**
3. Сохраните декларацию к каталогу, содержащему ваш сертификат. Это сохранит декларацию в формате .json локально к вашему компьютеру.
4. Использование локального редактора (Wordpad ++, Atom, и т.д.), завершенные шаги 2 и 3 от "Редактирует декларацию" раздел этого документа
5. Сохраните декларацию .json файл локально

(Необязательно) загрузите декларацию

Если вы приняли решение загрузить и отредактировали декларацию вручную, необходимо будет загрузить отредактированную декларацию:

1. Возвратитесь к своему браузеру и порталу Azure
2. Нажмите **Upload** от области "Edit Manifest"

Необходимо будет возвратиться к Зарегистрированной области приложения для перехода следующий раздел:

Нажмите "X" для закрытия области "Edit Manifest".

Получите Идентификатор клиента для приложения

1. Из Зарегистрированного приложения находят "Идентификатор приложения"
2. Скопируйте идентификатор приложения (идентификатор приложения = *идентификатор клиента*)
3. Добавьте это значение к своему списку предварительных условий требуемых значений.

Получите Значение идентификатора Арендатора для приложения

1. От области "App registrations" щелкните по "Endpoints" и выберите первую линию для FEDERATION ДОКУМЕНТ METADATA
2. Скопируйте и вставьте линию внешнему редактору
3. Вы захотите получить *ID Арендатора*, который является Строкой идентификатора после "https://login.windows.net /"

4. Добавьте это значение к своему списку предварительных условий требуемых значений.

Пример:

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

Для данного примера ID Арендатора будет "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Проверьте требуемые значения

Ваши значения теперь завершены. Должна существовать возможность заполнить следующие значения:

- Идентификатор клиента
- ID арендатора
- След большого пальца (см. предварительные условия),
- Секретный ключ сертификата в формате .pem (см. Предварительные условия),

Вы готовы завершить настройки почтового ящика офиса 365 путем настройки этих значений на ESA.

Настройте ESA

1. На GUI ESA: **Администрирование системы> Настройки почтового ящика> Редактирует Параметры настройки...**
2. Войдите в своих значениях от предыдущего раздела (Идентификатор клиента, ID Арендатора, След большого пальца)
3. Загрузите сохраненный сертификат (.pem)
4. **Нажмите кнопку Submit (Отправить)**
5. Вы будете видеть , что "Параметры настройки были настроены успешно. Необходимо передать изменения и протестировать соединение".
6. От верхнего правого угла нажмите **Commit Changes** до любого тестирования
7. Нажмите "Check Connection..." и войдите в известном хорошем, рабочем адресе электронной почты, привязанном к вашему домену O365
8. Нажмите "Test Connection"

Необходимо получить результаты успеха в Статусе соединения:

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

Устранение проблем ESA

Если вы не видите успешные результаты для теста статуса соединения, можно хотеть рассмотреть регистрацию приложений , выполненную от AD Azure.

От ESA, устанавливает журналы MAR в уровень трассировки и перетест соединение.

Для неуспешных соединений журналы могут показать подобный:

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

Подтвердите Идентификатор приложения, каталог ID (который совпадает с ID Арендатора), или другой связанный идентификатор (идентификаторы) от журнала с вашим приложением в AD Azure. Если вы не уверены в значениях, удаляете приложение из портала AD Azure и запускаетесь.

Для успешного подключения журналы должны быть подобны:

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

Устранение проблем AD Azure

> **Примечание:** Центр технической поддержки Cisco и Поддержка Cisco не названы для решения проблем абонентской стороны с Microsoft Exchange, Microsoft Azure AD или офисом 365.

Поскольку абонентская сторона выходит с Microsoft Azure AD, необходимо будет нанять Microsoft Support. Посмотрите опцию "Help + support" от своей Microsoft Azure Dashboard. Можно быть в состоянии открыть запросы непосредственной поддержки для Microsoft Support от информационной панели.

(Необязательно), Как создать и настроить приложение в Azure с помощью Классического портала

> **Примечание:** Если вы успешно смогли использовать портал Azure путем доступа https://portal.azure.com (Новый портал), вы не должны завершать это. На это только ссылаются для администратора Azure, кто принимает решение все еще использовать

"Классический портал". Если вы хотите использовать эту версию портала AD Azure, найдите следующие пошаговые инструкции для завершения требуемых значений:

Добавьте приложение

1. Вход в систему к Microsoft Azure.
2. От левой строки меню перейдите к **ЭЛЕМЕНТАМ ALL**
3. Щелкните по названию ресурса для своего домена
4. От вкладок программного средства под вашим названием ресурса выберите **APPLICATIONS**
5. От нижней области панели инструментов **нажмите Add**
6. Когда представлено*, "Что вы хотите сделать?"*, выберите**, добавляют приложение, которое разрабатывает моя организация**
7. Завершите, "*Говорят нам о вашем приложении*" информацию: Создайте название для своего приложенияДля типа приложения, выход как **Web - приложение и/или веб-API**Щелкните по стрелке для продолжения
8. Завершите Свойства приложения: Для ВХОДЯТ В СИСТЕМУ URL, используют следующий формат: https://*<company_domain.com>/ManualRegistration***Примечание:** *<company_domain.com>* является доменом вашего O365, где пользователи домена могут войти в систему и обратиться к вашему домену O365.Для URI ИДЕНТИФИКАТОРА ПРИЛОЖЕНИЯ используйте следующий формат: https://<company_domain.com>Нажмите галочку для завершения

Настройте свое 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. **Идентификатор клиента** перечислен на этом экране. Скопируйте и добавьте это значение к своему списку предварительных условий требуемых значений.
3. Перейдите в нижнюю часть экрана для наблюдения "разрешений к другим приложениям".
4. **Нажмите Add приложение** Выберите **Office 365 Exchange Online** и нажмите проверку для продолженияДля **Разрешений Приложения** выберите: **Считайте и запишите почту во всех почтовых ящикахПередайте почту как любого пользователяИспользуйте веб-сервисы Exchange с полным доступом...**Для Делегированных Разрешений выберите: **Передайте почту как пользователяСчитайте и запишите пользовательскую почтуСчитайте пользовательскую почтуПочтовые ящики доступа как регистрировавшийся пользователь через Exchange**
5. Нажмите **Save** от нижней панели инструментов для сохранения всех работают и конфигурация для пользовательского Web - приложения

Управляйте декларацией

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. Локально, найдите .json файл и открытый с текстовым редактором. (Предпочтительный Блокнот ++, Atom, и т.д.)
4. Ищите и найдите "keyCredentials" линию
5. Заменяя этот отдельный канал следующими составными строками, настраивая при помощи *$base64Thumbprint*, *$keyid* и *$base64Value*: `"keyCredentials": [`
   ```
   {
   "customKeyIdentifier": "$base64Thumbprint",
   "keyId": "$keyid",
   "type": "AsymmetricX509Cert",
   "usage": "Verify",
   "value": "$base64Value"
   }
   ],
   ```
6. При вводе *$base64Value* это требуется, чтобы быть отредактированным к значению отдельного канала
7. Сохраните .json файл локально
8. Возвратитесь к своему браузеру и порталу Microsoft Azure
9. Нажмите **MANAGE MANIFEST> Upload Manifest**
10. Просмотрите и найдите отредактированный .json файл
11. Выберите метку выбора для завершения загрузки

Обнаружение ID арендатора

1. От нижней панели инструментов нажмите **on VIEW ENDPOINTS** для просмотра Оконечных точек, интегрированных в Microsoft Azure AD
2. Выберите первую линию для FEDERATION ДОКУМЕНТ METADATA
3. Скопируйте и вставьте линию внешнему редактору
4. Вы захотите получить *ID Арендатора*, который является Строкой идентификатора после "https://login.windows.net /"
5. Добавьте это значение к своему списку предварительных условий требуемых значений

Пример:

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

Для данного примера ID Арендатора будет "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Дополнительные сведения

- Автоматически перепосреднические сообщения в Office 365 почтовых ящиков