目录

简介

本文描述如何设立和配置Microsoft天蓝色AD和办公室365与思科电子邮件安全工具(ESA)一起使用。

先决条件

本文档中的信息基于以下软件和硬件版本：

- 电子邮件安全的9.9.5-039 (贝拉焦) AsyncOS，或者更新。

本文也要求以下：

- 办公室365帐户订阅(请确保您的办公室365帐户订阅包括访问发电子邮件，例如企业E3或企业E5帐户。)
- Microsoft天蓝色帐户
- 办公室365和Microsoft天蓝色的AD帐户适当地附加对一个活动*user@domain.com*电子邮件地址，并且您能通过该域和帐户发送和收到电子邮件。
- 访问对Windows PowerShell，通常管理从Windows服务器。
- 域活动公共/Private证书和专用密钥曾经签署证书，或者能力创建一公共/Private证书和能力保存专用密钥曾经签署证书。

配置证书值

登陆对Windows，并且使用PowerShell请完成以下命令映射和获取*$keyid*、*$base64Thumbprint*和*$base64Value* ：

1. **$cer =新对象System.Security.Cryptography.X509Certificates.X509Certificate2**
2. **$cer. 导入('C:\path _to_cert \ PEM_certificate.crt')**
3. **$bin = $cer.GetRawCertData()**
4. **$base64Value = [System.Convert]::ToBase64String($bin)**
5. **$bin = $cer.GetCertHash()**
6. **$base64Thumbprint = [System.Convert]::ToBase64String($bin)**

7. **$keyid = [System.Guid] ： ：NewGuid().ToString()**
8. **响应**
9. **响应**
10. **响应$keyid**

为本文的目的，配置示例根据“esatest.onmicrosoft.com”。命令如运行通过PowerShell应该类似于以下示例：

保存您为*$keyid*收到的输出 *$base64Thumbprint*和*$base64Value*，因为这些值将是使用的以后在*创建*本文的*明显*部分。 *$base64Thumbprint*在ESA配置时将使用。

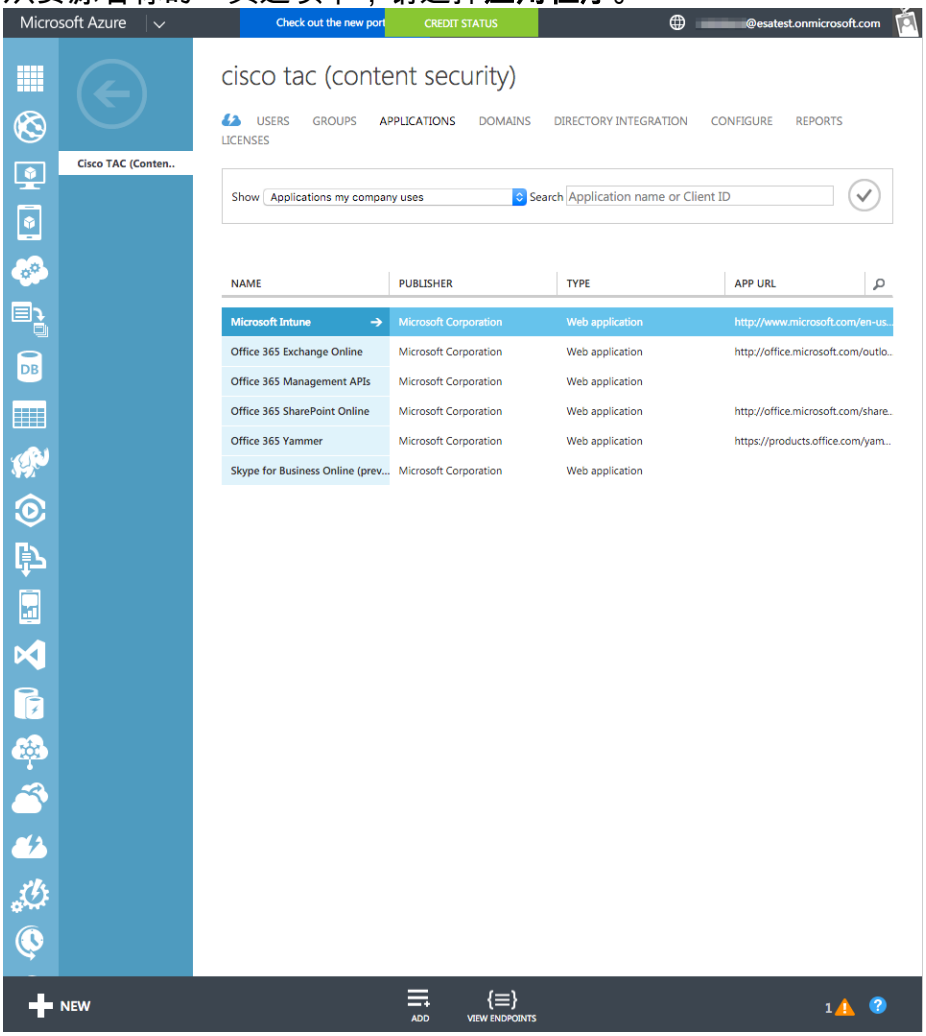
> **注意**：*$base64Value*要求编辑是单个线路。

保存用于的公开密钥认证(.crt)和专用密钥签署证书(.pem)本地。 专用密钥在ESA配置时将是需要的。

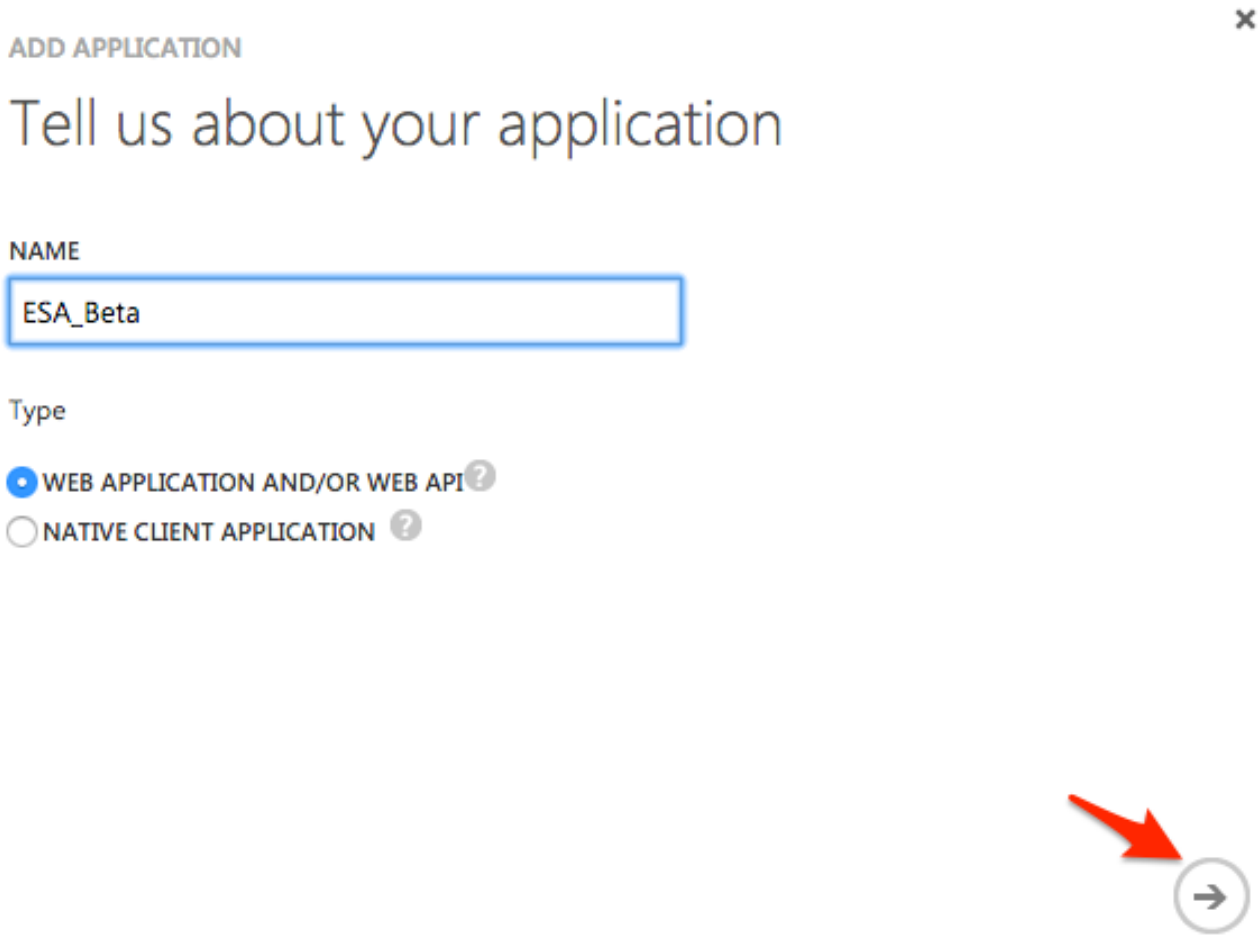
配置Microsoft天蓝色AD

创建自定义Web应用程序

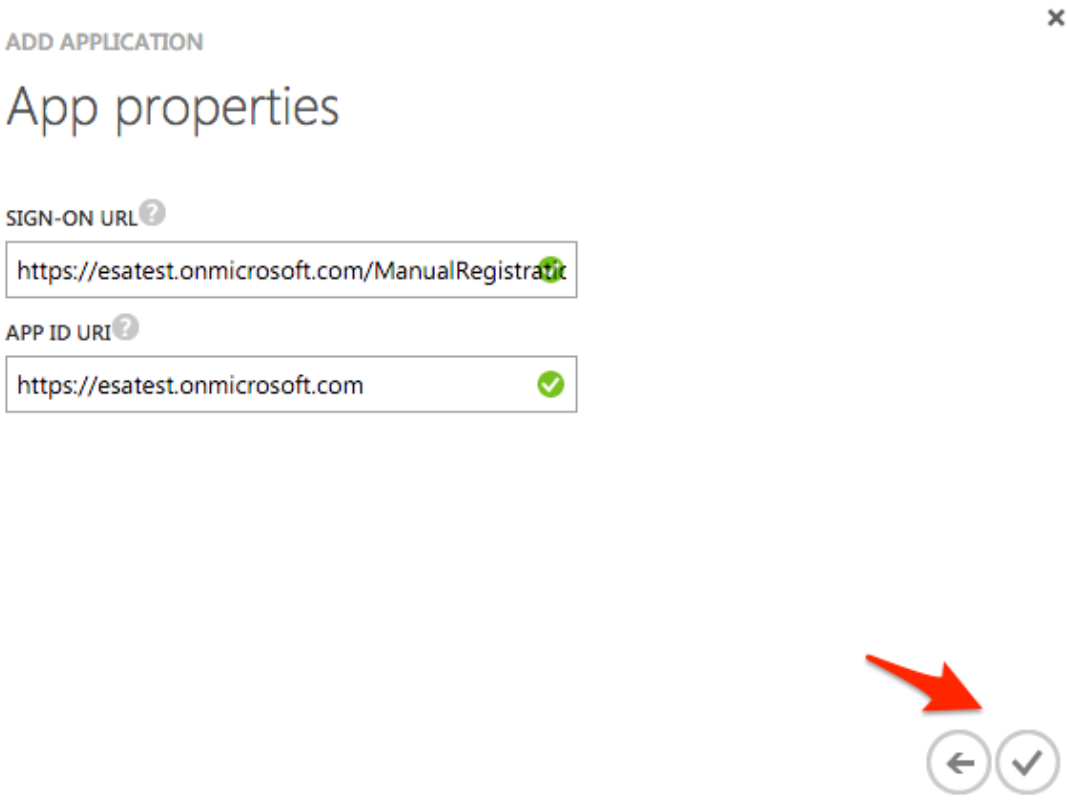
1. 登陆对Microsoft天蓝色。
2. 导航对**所有ITEM**。
3. 点击资源名称对于您的域。
4. 从资源名称的工具选项卡，请选择**应用程序**。



5. 从底下工具栏，精选请**添加**：
6. 提交“什么时候*要执行什么？*”，请选择**添加我的组织开发的应用程序。**
7. 创建与适当的名称，并且留下*类型*作为**Web应用程序和Web API**，并且点击箭头继续：



8. 完成添加自定义Web应用程序，输入以下值您的域的和点击检查完成： 登录URL ：**https://*<your.domain.com>/ManualRegistration***APP ID URI ：**https://*<your.domain.com>***

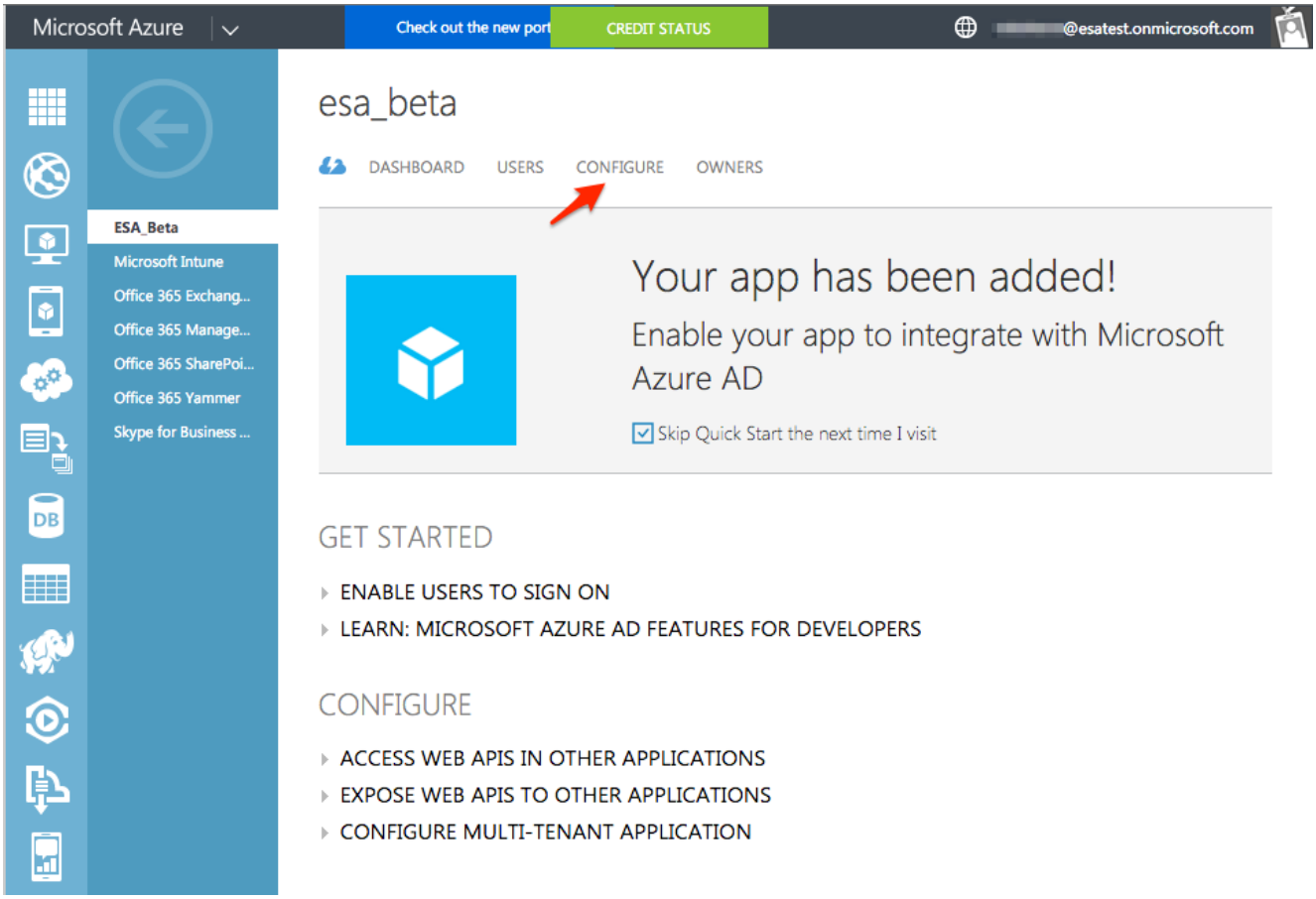


9. 从Microsoft，关于App ID URI ：“由于App ID URI是一个逻辑标识符，不需要解决到互联网地址。当发送单一登录请求对天蓝色AD时，您的app提交它。天蓝色AD识别您的app并且发送在app注册时提供的登录答复(SAML标记)对回复URL。请使用App ID URI值设置wtrealm属性(WS联合身份验证)或发布者属性(SAML-P)，当进行签到请求。**App ID URI**必须是在您的组织的天蓝色AD的一一个唯一值”。

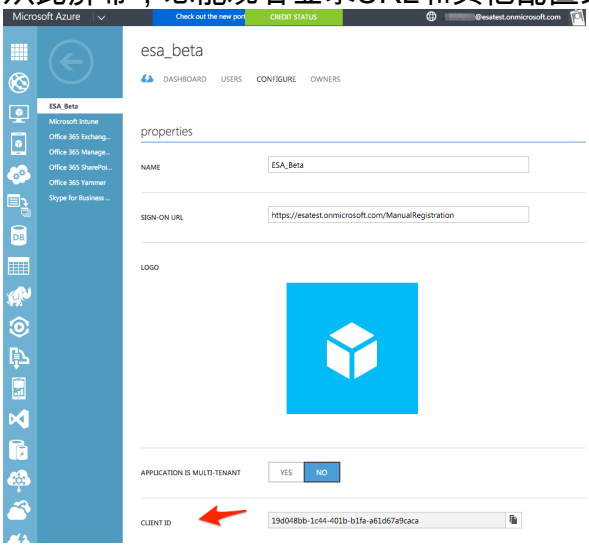
   注意：

配置自定义Web应用程序

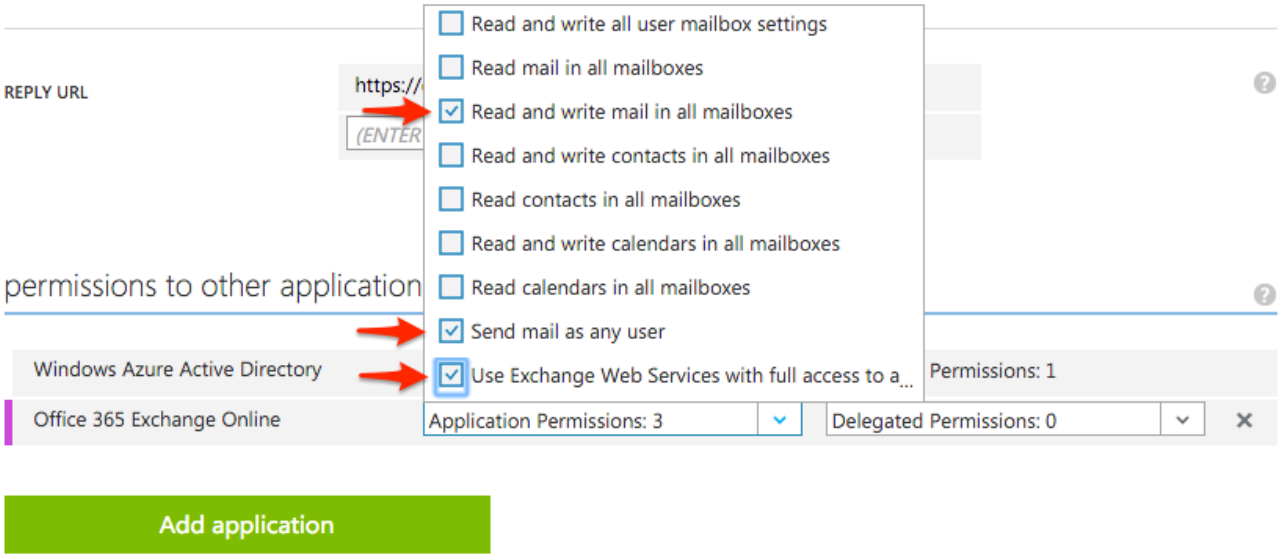
1. 一旦自定义Web应用程序创建，您自动地导航到自定义Web应用程序。 从这里，在工具选项卡，精选请**配置**
   ：



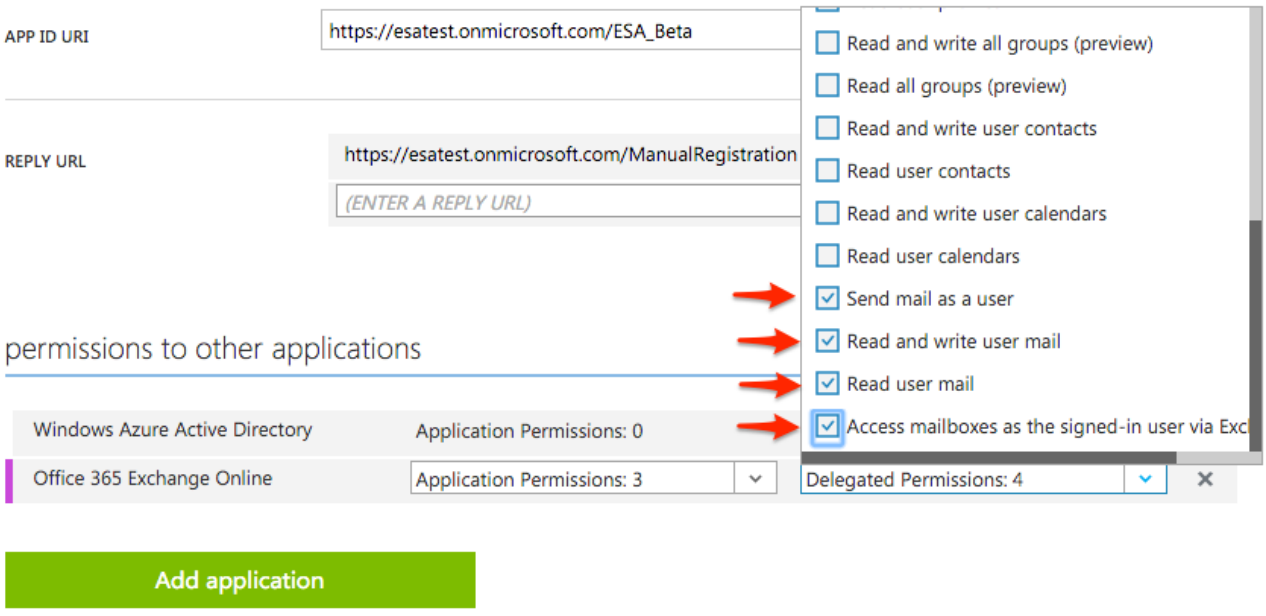
2. 从此屏幕，您能观看登录URL和其他配置细节如创建。**注意**： ***客户端ID***在此屏幕列出。 此值



3. 从自定义Web应用程序配置的此同样屏幕，请移动到底部并且单击**添加应用程序**：
4. 选择**办公室365联机的Exchange**并且点击检查继续。
5. 对于*办公室365 Exchange OnlineApplication权限*，请选择**读并且写在所有邮箱的邮件**，**发送邮件作为所有用户**和**使用Exchange与完全权限的网站服务…**
   ：



6. 对于*办公室365 Exchange OnlineDelegated权限*，请选择**发送邮件，用户**，**读了并且写入用户邮件**，**读了用户邮件**，并且**访问邮箱作为签署在用户通过Exchange**
   ：



7. 点击从底下工具栏的**"Save"**保存所有工作和配置自定义Web应用程序的
   ：

创建明显

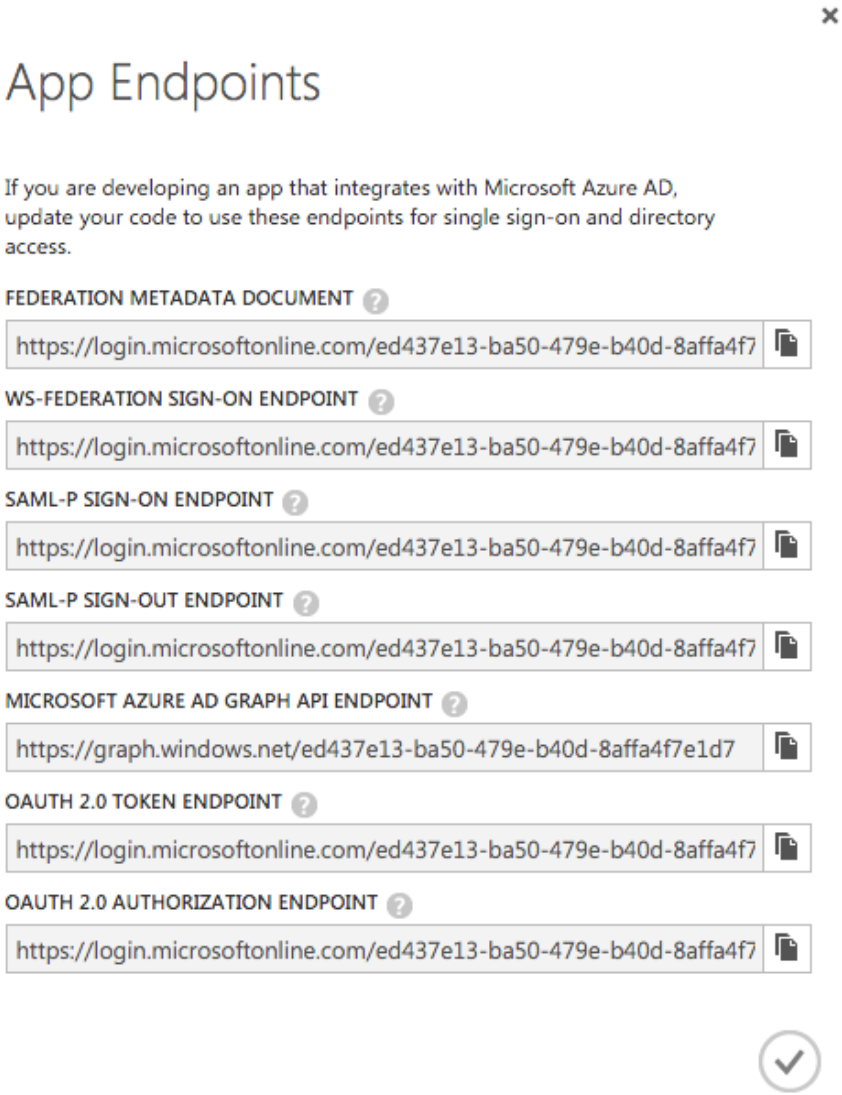
1. 一旦自定义Web应用程序完成保存和更新，请单击**管理明显>下载明显**从底下工具栏
   ：

2. 通过答复导航，并且保存Web应用程序明显在.json格式对您的本地计算机。
3. 查找此.json文件并且打开有文本编辑的此.json文件。 (更可取的Notepad++、原子等等)
4. 搜索并且查找“keyCredentials”线路。
5. 您替换此单个线路用以下多条线路，并且自定义使用从*配置证书的更*早的已确定凭证重视部分 (*$base64Thumbprint*、*$keyid*和*$base64Value*) ：
6. 如注释前，当输入*$base64Value*，这要求编辑是单个线路值时。
7. 继续与示例如从开始创建本文，已修改*keyCredentials*如下：
8. 保存.json文件本地。
9. 返回到您的浏览器和Microsoft天蓝色的门户。
10. 单击**管理明显>明显的加载**
    :

11. 浏览并且查找编辑的.json文件，并且选择复选标记完成加载。

查找承租人ID

1. 点击**视图终端**查看在Microsoft天蓝色AD集成的终端。
2. 使用在URL，请注意每条线路的相似的值， "ed437e13-ba50-479e-b40d-8affa4f7e1d7,"这是的***承租人ID***。



这对您的应用程序和配置将是唯一。 记录新配置的此值在ESA。

将保存的值最终审查

应该在Microsoft天蓝色的AD配置时记录了以下值为使用，当配置在ESA时的邮箱设置：

从请*配置证书值*：

- 专用密钥证书(.pem)
- $base64Thumbprint

从请*配置自定义Web应用程序*：

- 客户端ID

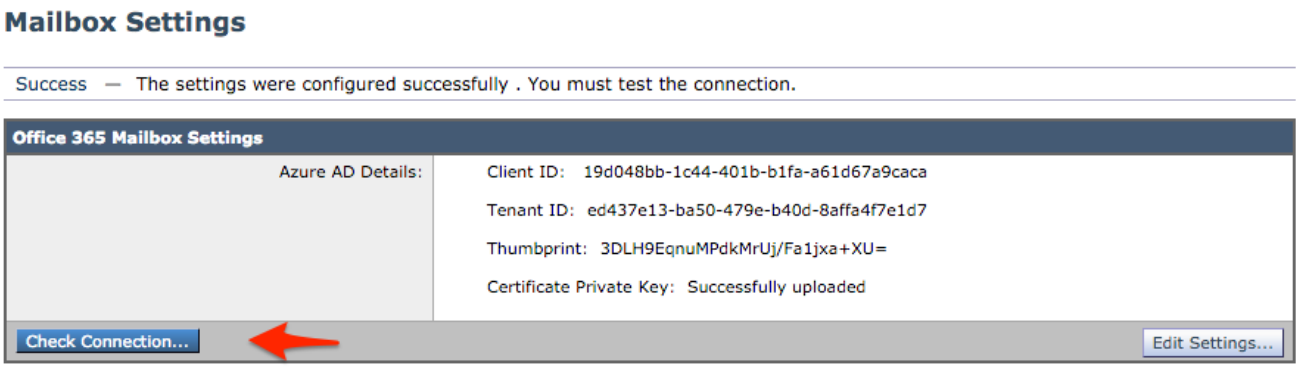
从*查找承租人ID* ：

- 承租人ID

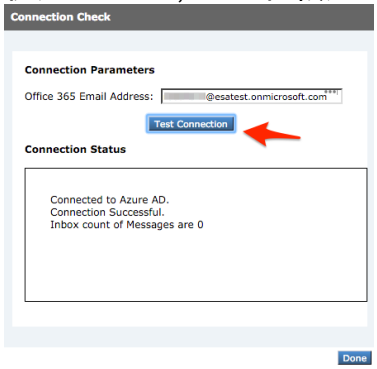
配置在ESA的邮箱设置

使用完整Microsoft天蓝色的AD的配置，您准备安排ESA通信和验证。

1. ESA设备的洛金通过GUI。
2. **Enable (event)**办公室365在**系统管理>邮箱设置下的**邮箱设置。
3. 精选？**Enable (event)办公室365邮箱设置？**复选框&提供您的(*客户端ID &承租人ID*)得到的Microsoft天蓝色的AD细节，当注册ESA应用程序Microsoft天蓝色AD与证书的Thumbprint *&专用密钥一起时*。
4. 单击**提交**保存对邮箱设置的更改。
5. 您将需要测试对Microsoft天蓝色AD的连接在您的办公室365域的此时刻如配置：



6. 请使用一活动，并且在帐户的有效电子邮件地址，点击**测试连接**：



7. 一旦连接状态是成功的，请单击**完成**完成连接检查。
8. 最后，请点击**进行**保存在ESA的所有配置更改。