Comment configurer l'AD de Microsoft Azure et le bureau 365 pour l'usage sur l'ESA

Contenu

Introduction

Ce document décrit comment installer et configurer l'AD et le bureau 365 de Microsoft Azure pour fonctionner avec l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- AsyncOS pour la sécurité du courrier électronique 9.9.5-039 (Bellagio), ou plus nouveau.

Ce document exige également ce qui suit :

- Abonnement de compte du bureau 365 (assurez-vous s'il vous plaît que votre abonnement de compte du bureau 365 inclut l'accès pour envoyer, comme un compte d'E3 d'entreprise ou d'entreprise E5.)
- Compte de Microsoft Azure
- Des comptes d'AD du bureau 365 et de Microsoft Azure sont attachés correctement à une adresse e-mail active d'*user@domain.com*, et vous pouvez envoyer et recevoir des emails par l'intermédiaire de ces domaine et compte.
- Accédez à Windows PowerShell, habituellement géré des Windows Server.
- Public actif de domaine/certificat privé et la clé privée utilisée pour signer le certificat, ou la capacité de créer certificat public/privé et capacité de sauvegarder la clé privée utilisée pour signer le certificat.

Configurez les valeurs de certificat

Ouvrez une session à Windows, et en utilisant PowerShell terminez-vous les commandes

suivantes de tracer et obtenir *$keyid*, *$base64Thumbprint*, et *$base64Value* :

1. $cer = Nouveau-objet System.Security.Cryptography.X509Certificates.X509Certificate2
2. $cer. Importation (« _to_cert de C:\path \ 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. écho $base64Value
9. écho $base64Thumbprint
10. écho $keyid

Afin de ce document, l'exemple de configuration sera basé sur « esatest.onmicrosoft.com. » Les commandes comme passage par l'intermédiaire de PowerShell devraient être semblables à l'exemple suivant :

```
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
MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJv
bGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEF
DMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMB4
XDTE2MDMyODE0NTYwMFoXDTE3MDMyODE0NTYwMFowgZcxCzAJBgNVBAYTAlVTMR
cwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHg
YDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYSc
m9ic2hlcndAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB6r/MtfKwG+86eHzdhYklCdyyT+j
/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZGlF0nkzT5Gs+zLOuhPHaT1DMU70LCXh8CHs2cLsczpDWfb2OsHxTVlISVJ
qjdhYHYM7vC6VNffMYIYxAE90ZEl9QHOdU5n7spPyxUP0fp8z8gHsQ7HhRTsCNg
WbFyYb0Ib1RTOznmzMXaSOnRKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/ii1YLvMKyq+T7PJbPDwhU8uAGQIDAQA
Bo4HWMIHTMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCC
sGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQBgjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgj
cKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQGA1UdEQQ9MDuCF2VzYXRlc
3Qub25taWNyb3NvZnQuY29tgSByb2JzaGVyd0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEAR
/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625
f31o1kADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSmvn980GHuSXOqfLMPtniUMTubp+SICD
rtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Z
xg8NKtiyEzV99OJ6+DOkMn1fQOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+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-ad63-7ddaeaf8e737
```

Sauvegardez la sortie que vous recevez pour *$keyid*, *$base64Thumbprint*, et *$base64Value*, car

ces valeurs seront utilisées plus tard dans la *création la* section *manifeste de* ce document. *Le $base64Thumbprint* sera utilisé pendant la configuration ESA.

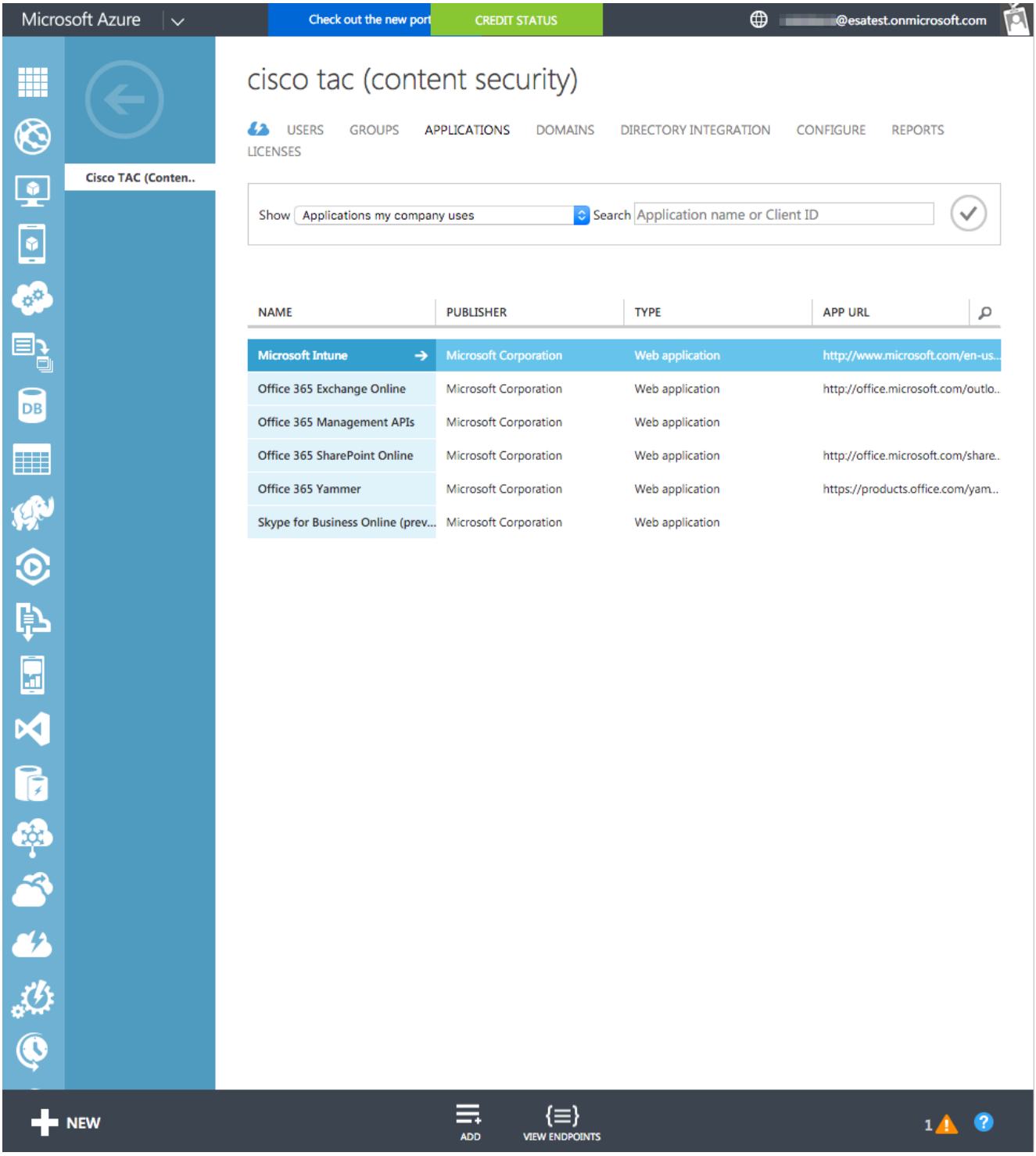
> Remarque: *Le $base64Value* est exigé pour être édité pour être une ligne simple.

Sauvegardez le certificat de clé publique (.crt) et la clé privée utilisée pour signer le certificat (.pem) localement. La clé privée sera nécessaire pendant la configuration ESA.

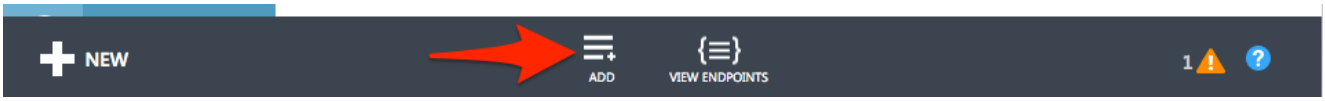
Configurez l'AD de Microsoft Azure

Créez l'application Web faite sur commande

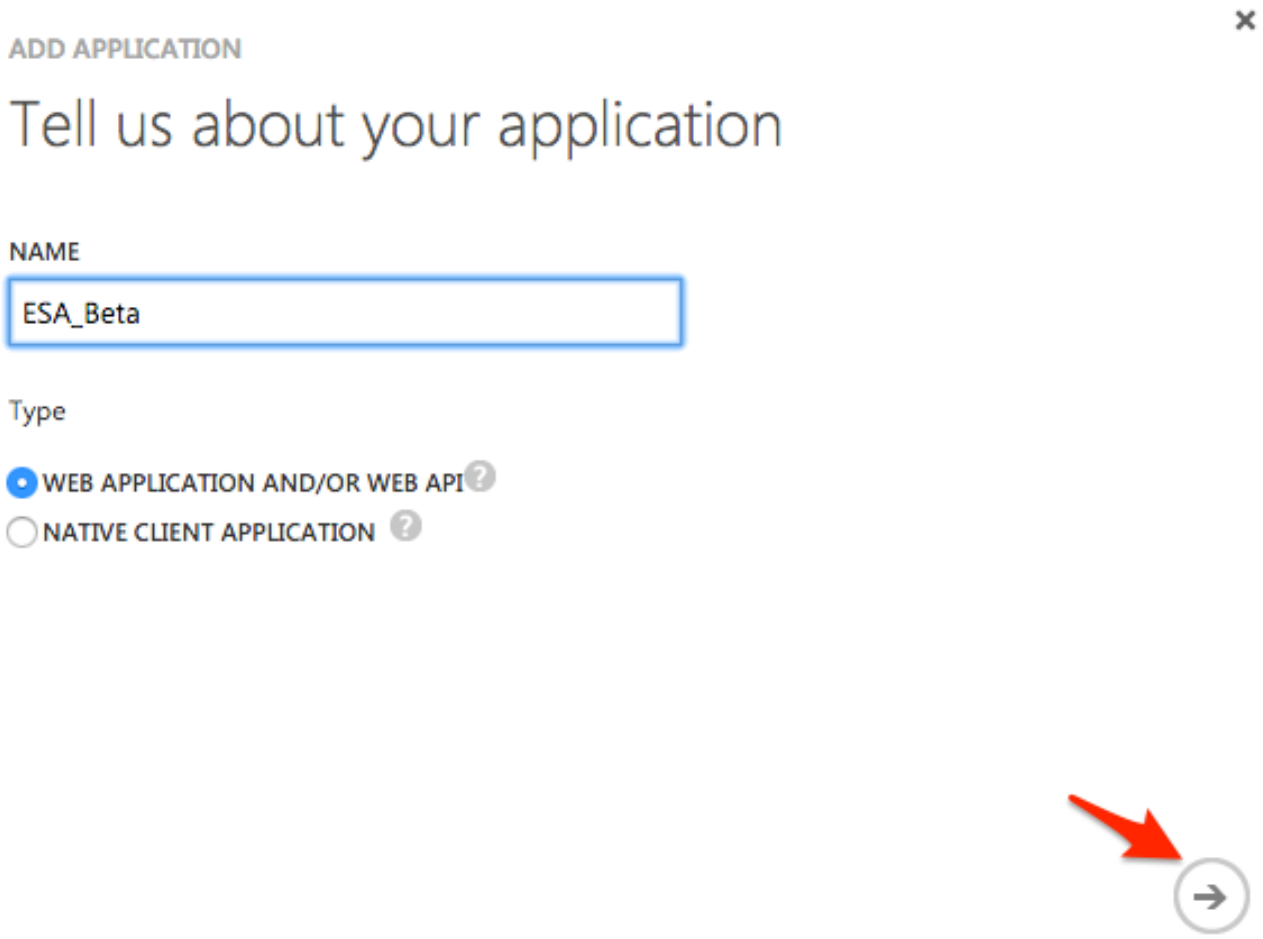
1. Procédure de connexion au Microsoft Azure.
2. Naviguez vers **TOUS LES ÉLÉMENTS**.
3. Cliquez sur en fonction le nom des ressources pour votre domaine.
4. Des onglets d'outil pour le nom des ressources,
   APPLICATIONS choisies.



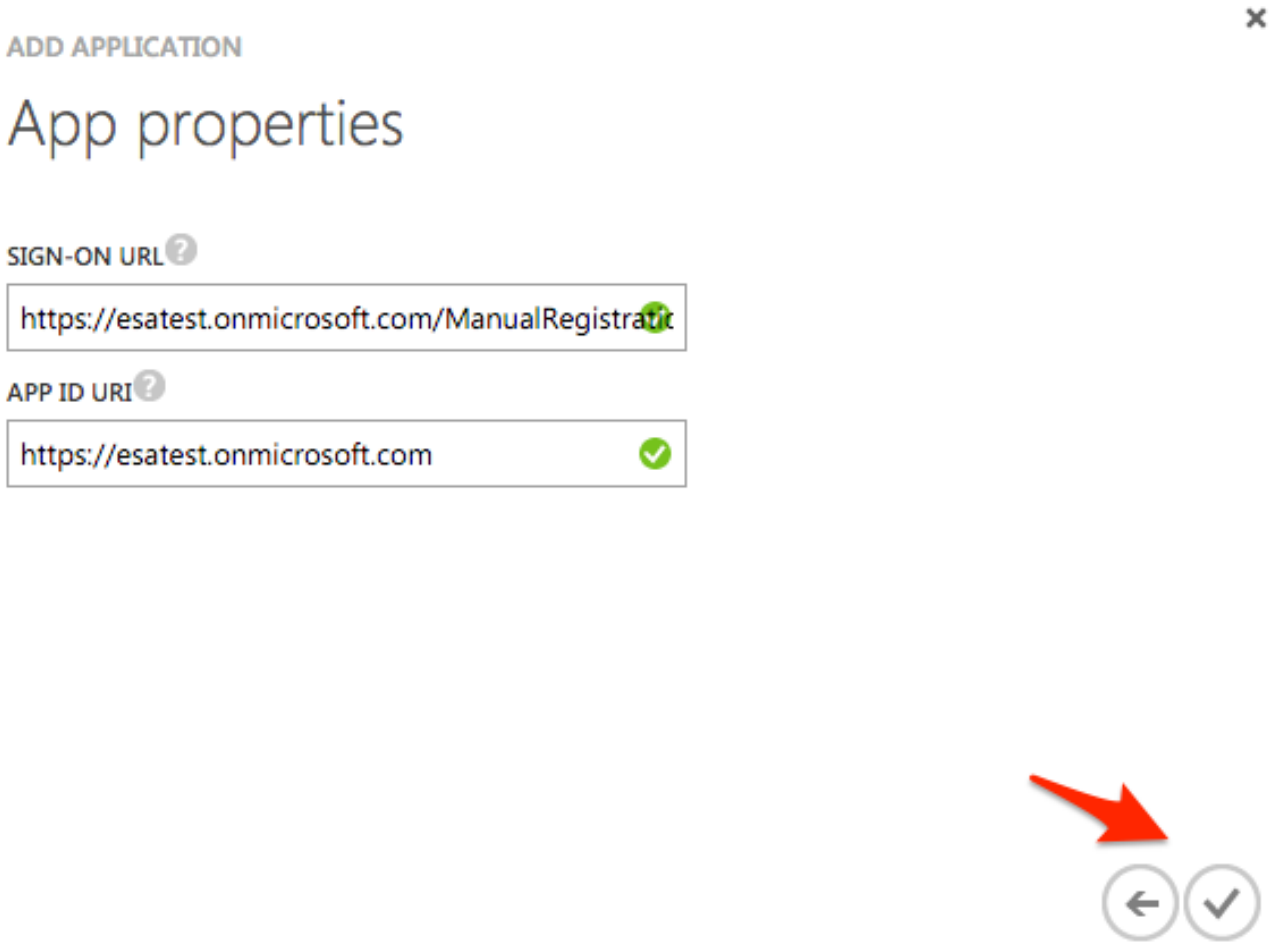
5. De la barre d'outils inférieure, choisie **AJOUTEZ** :



6. Une fois présenté *« que voulez-vous faire ? »*, choisi **ajoutez une application que mon organisation développe**.
7. Créez avec un nom approprié, et laissez le *type* comme **application Web et/ou Web API**, et cliquez sur la flèche pour continuer :



8. Pour terminer ajouter l'application Web faite sur commande, écrire les valeurs suivantes pour votre domaine, et cliquer sur le contrôle pour terminer : URL D'OUVERTURE DE SESSION : **https:// *<your.domain.com>/ManualRegistration***URI D'ID D'APP : **https:// *<your.domain.com>***

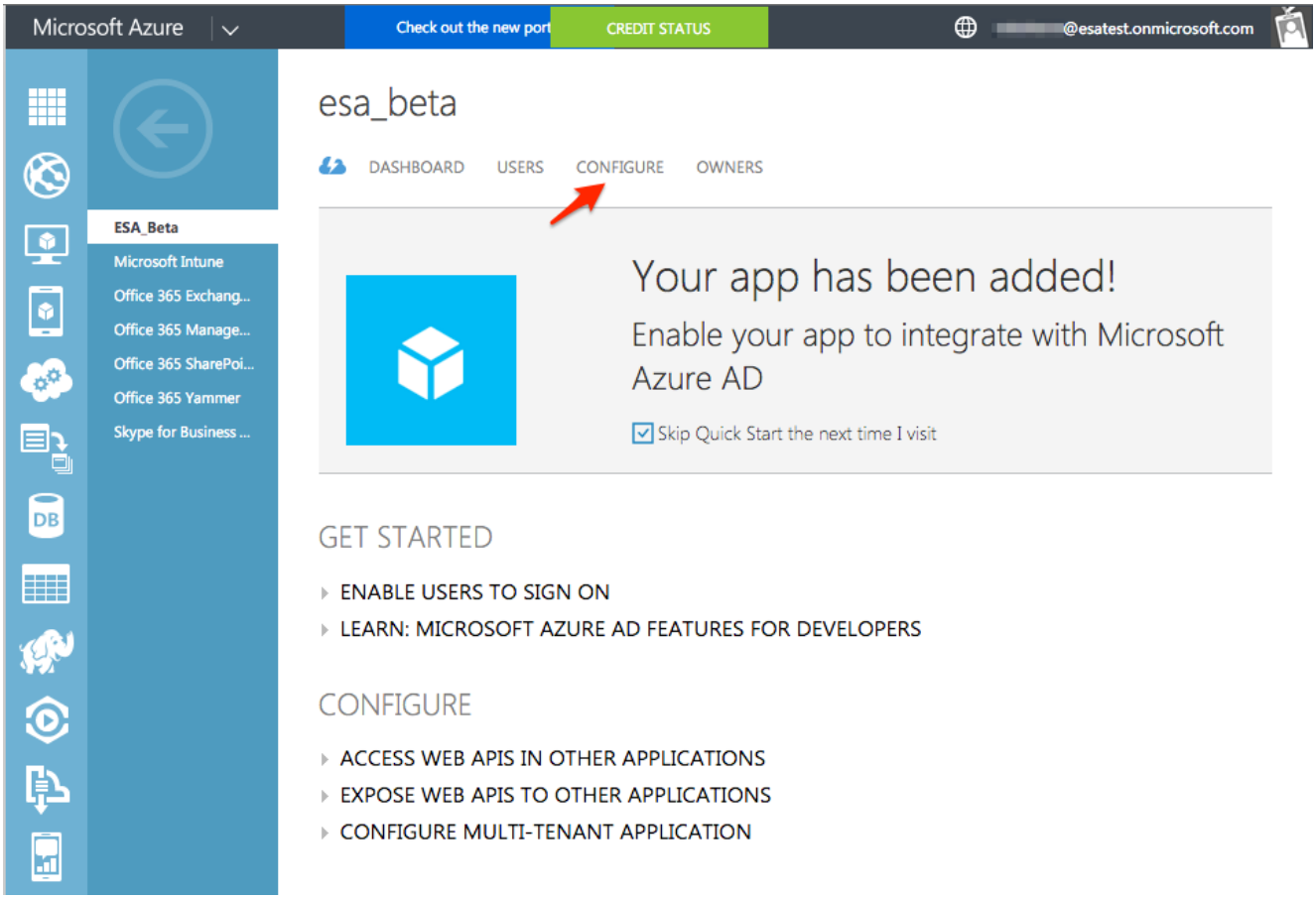


9. De Microsoft, concernant l'URI d'ID d'app : « Puisque l'URI d'ID d'app est un identifiant logique, il n'a pas besoin de le résoudre à une adresse Internet. Il est présenté par votre app en envoyant une demande simple d'ouverture de session à l'AD azuré. L'AD azuré identifie votre app et envoie la réponse d'ouverture de session (un jeton SAML) à l'URL de réponse qui a été fourni pendant l'enregistrement d'app. Employez la valeur d'URI d'ID d'app pour placer la propriété de wtrealm (pour la WS-fédération) ou la propriété d'émetteur (pour SAML-P) en faisant une demande de connexion. **L'URI d'ID d'app** doit être une seule valeur dans l'AD azuré de votre organisation. »

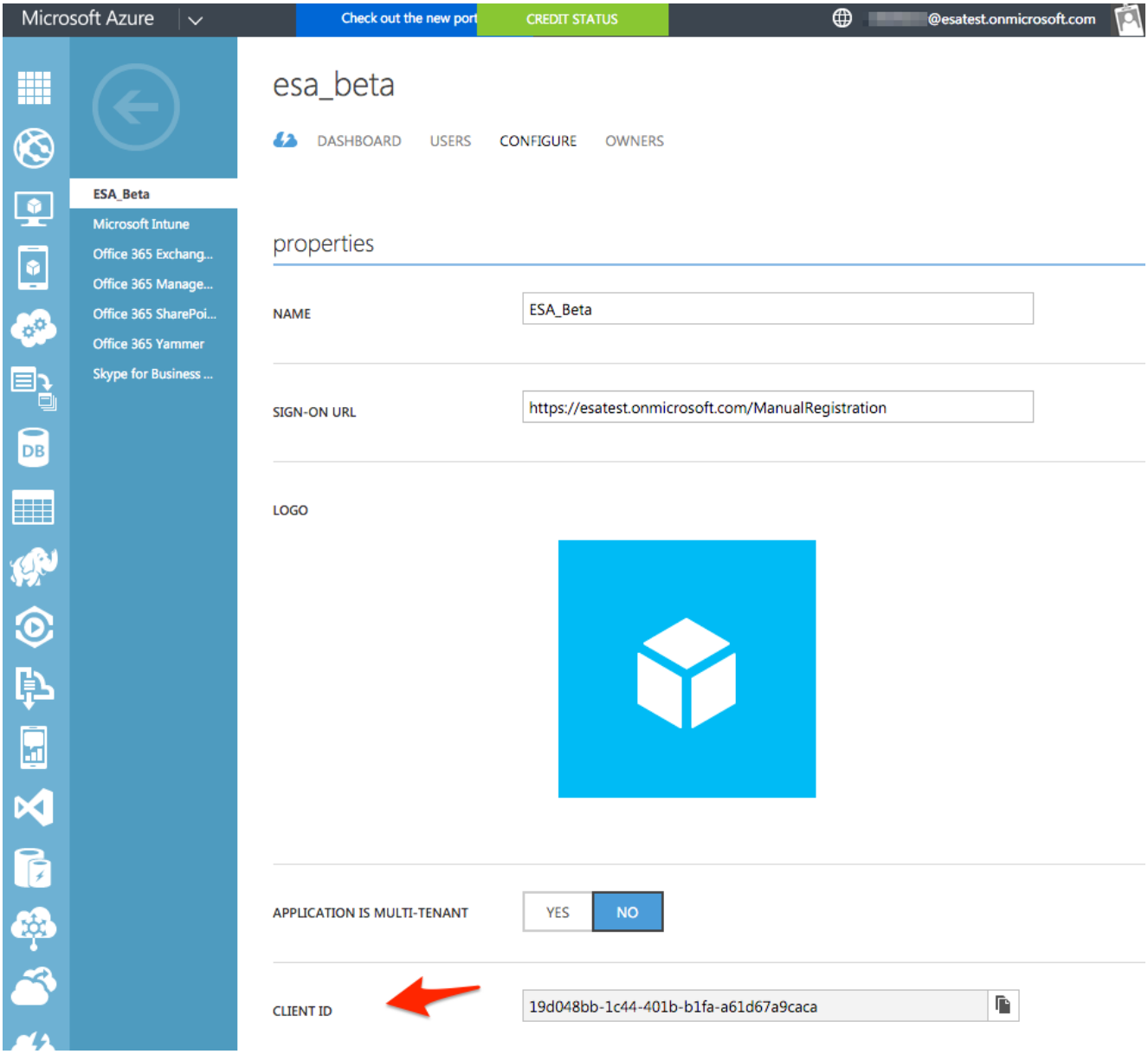
   Remarque: « En activant un app pour des utilisateurs externes, la valeur de l'URI d'ID d'app de l'app doit être une adresse dans un des domaines vérifiés de votre répertoire. En conséquence, ce ne peut pas être une URNE. Cette sauvegarde empêche d'autres organismes de spécifier (et de prendre) la seule propriété qui appartient à votre organisation. Pendant le développement, vous pouvez changer votre URI d'ID d'app à un emplacement dans le domaine initial de votre organisation (si vous n'avez pas vérifié un domaine fait sur commande/vanité), et mettez à jour votre app pour utiliser cette nouvelle valeur. Le domaine initial est le domaine 3-level pendant lequel vous créez vous inscrivez, comme contoso.onmicrosoft.com. »

Configurez l'application Web faite sur commande

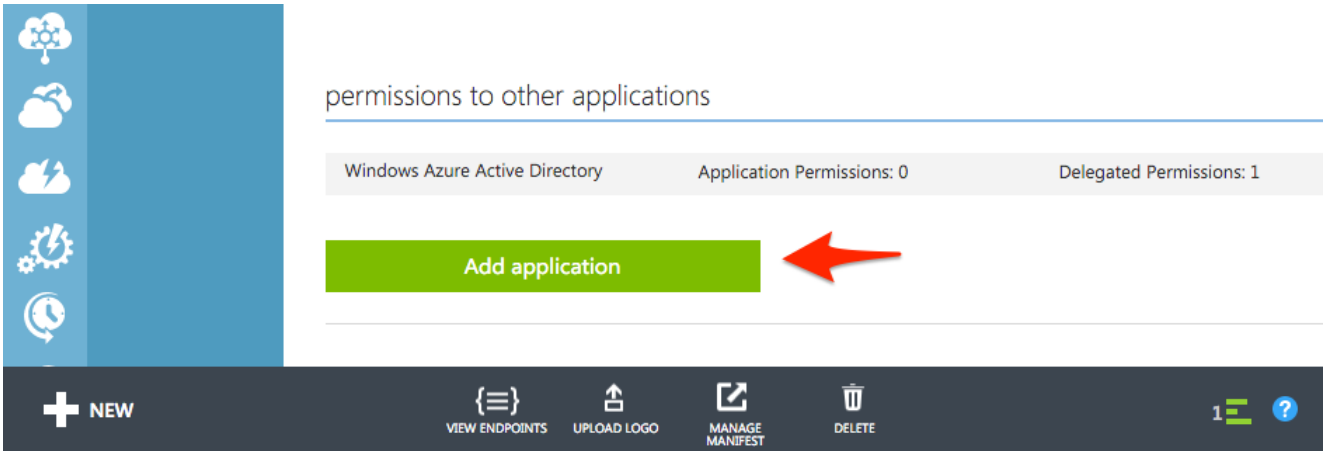
1. Une fois que l'application Web faite sur commande a été créée, vous êtes automatiquement navigué dans l'application Web faite sur commande elle-même. D'ici, dans les onglets d'outil, choisis **CONFIGUREZ**
   :



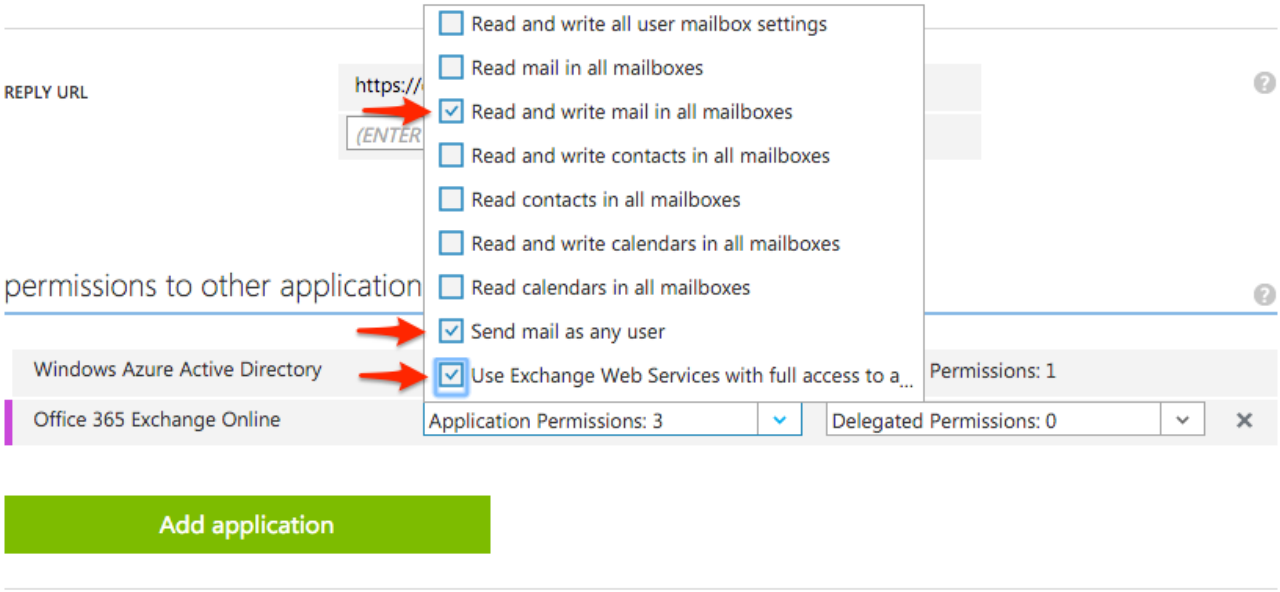
2. De cet écran, vous pouvez visualiser l'URL d'ouverture de session et d'autres détails de configuration comme créé. Remarque: ***L'ID de client*** est répertorié sur cet écran. Cette valeur sera nécessaire pendant la configuration
ESA.



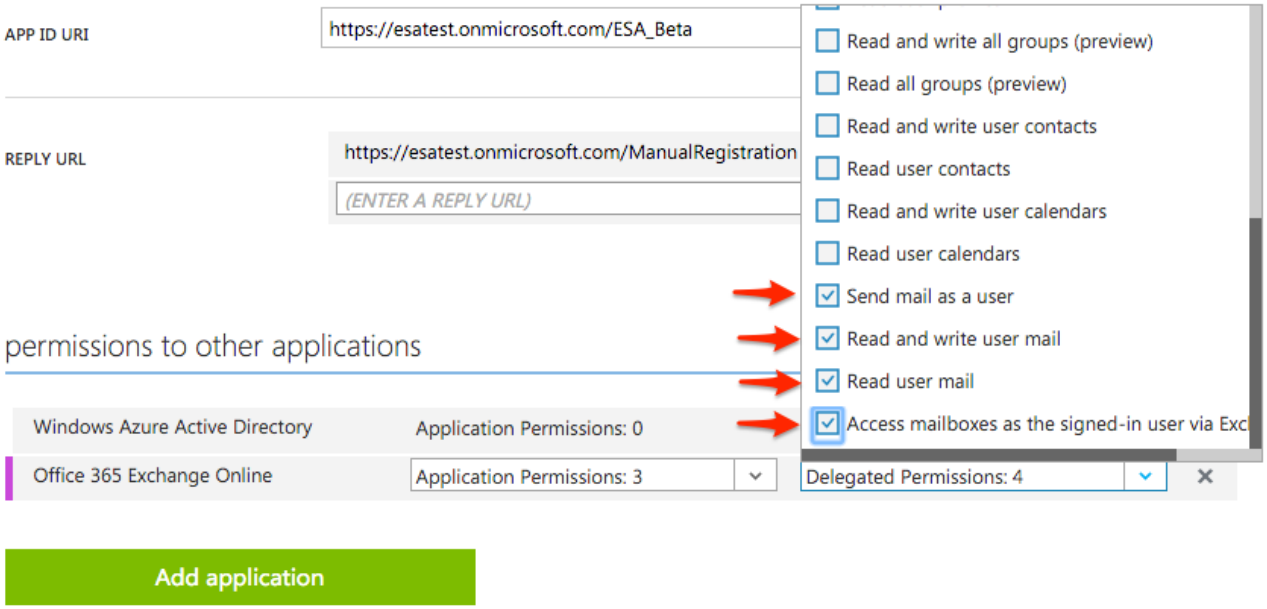
3. De cet même écran pour la configuration d'application Web faite sur commande, faites défiler au bas et cliquez sur Add l'**application**
:



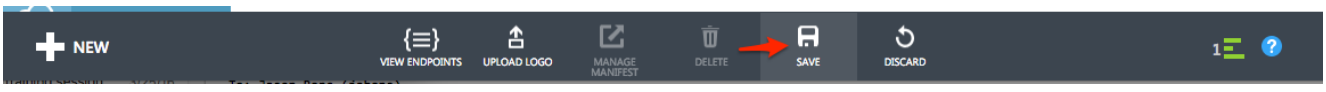
4. **L'échange** choisi du **bureau 365 en ligne** et cliquent sur le contrôle pour continuer.
5. Pour les *autorisations d'OnlineApplication d'échange du bureau 365*, sélectionnez **lu et écrivez la messagerie dans toutes les boîtes aux lettres**, **envoyez la messagerie en tant que n'importe quel utilisateur**, et **utilisez les services Web d'échange avec l'accès complet…**
:



6. Pour les *autorisations d'OnlineDelegated d'échange du bureau 365*, choisi **envoyez la messagerie comme un utilisateur**, **a lu et écrit la messagerie d'utilisateur**, **a lu la messagerie d'utilisateur**, et **accède à des boîtes aux lettres en tant qu'utilisateur connecté par l'intermédiaire de l'échange**
:



7. **Sauvegarde de** clic de la barre d'outils inférieure pour sauvegarder tous les travail et configuration pour l'application Web faite sur commande
:



Créez le manifeste

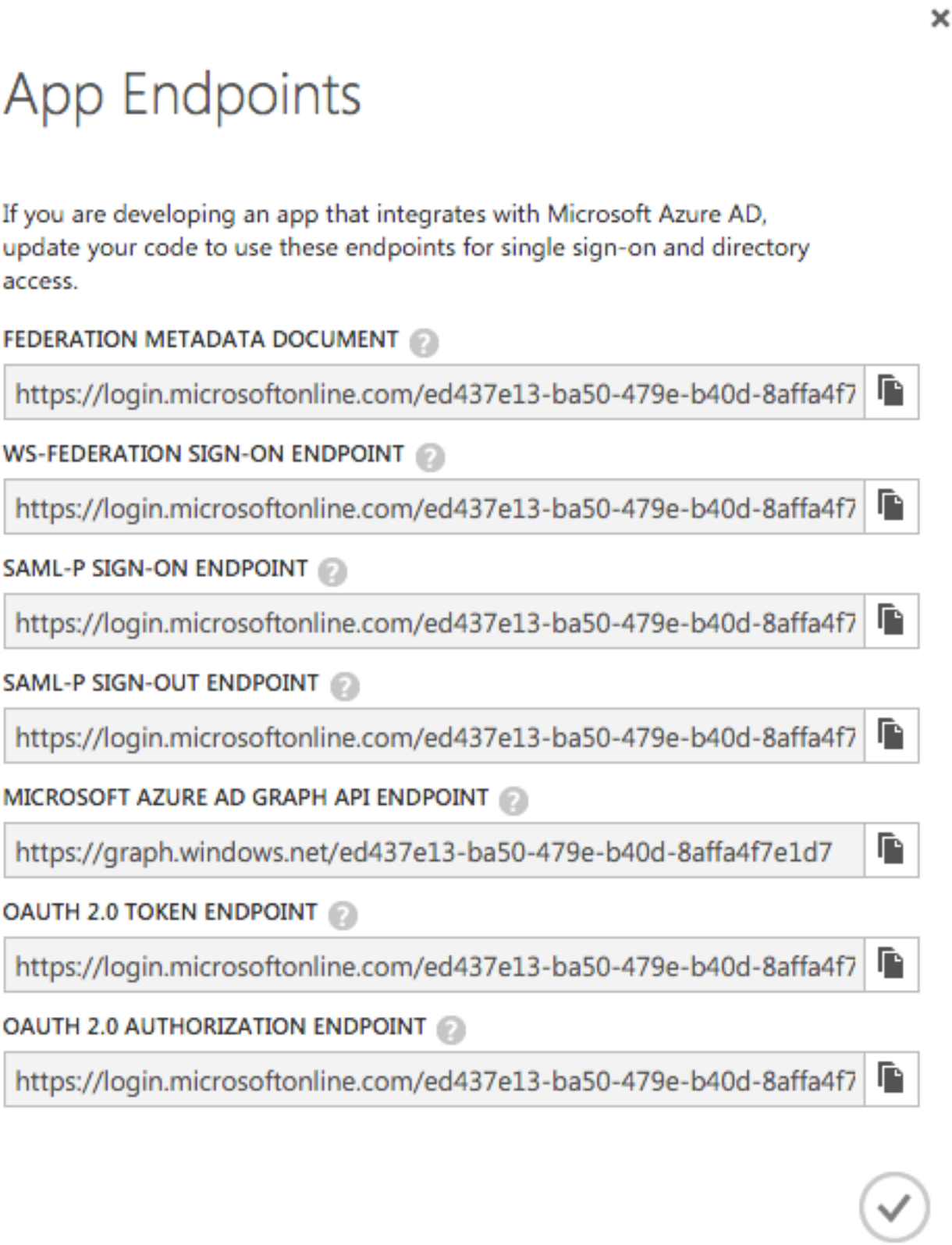
1. Une fois que l'application Web faite sur commande s'est terminée l'économie et la mise à jour, le clic **GÈRENT MANIFESTE > téléchargement manifeste de la** barre d'outils inférieure
:

2. Naviguez par les réponses, et sauvegardez l'application Web manifeste dans le format .json à votre ordinateur local.
3. Trouvez ce fichier .json et ouvrez ce fichier .json avec un éditeur de texte. (Notepad++ préférable, atome, etc.)
4. Recherchez et trouvez la ligne de « keyCredentials ».
5. Vous remplacerez cette ligne simple par les plusieurs lignes suivantes, et personnalisez utilisant les qualifications identifiées plus tôt de la section de valeurs de *certificat de configurer* (*$base64Thumbprint*, *$keyid*, et *$base64Value*) :
6. ```
   "keyCredentials": [
   {
   "customKeyIdentifier": "$base64Thumbprint",
   "keyId": "$keyid",
   "type": "AsymmetricX509Cert",
   "usage": "Verify",
   "value": "$base64Value"
   }
   ],
   ```
7. Comme remarquable plus tôt, en écrivant le *$base64Value*, ceci est exigé pour être édité pour être une ligne simple valeur.
8. Continuant l'exemple comme créé dès le début de ce document, les *keyCredentials* modifiés seront comme suit :
9. ```
   "keyCredentials": [
   {
   "customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Fa1jxa+XU=",
   "keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
   "type": "AsymmetricX509Cert",
   "usage": "Verify",
   "value":
   "MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aC
   BDYXJvbGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHgYDVQQDExdlc2F0Z
   XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMB4XDTE2MDMyODE0NTYw
   MFoXDTE3MDMyODE0NTYwMFowgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBxM
   DUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbT
   EhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz
   B6r/MtfKwG+86eHzdhYklCdyyT+j/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
   axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZGlF0nkzT5Gs+zLOuhPHaT1DMU70LCXh8CHs2cLsczpDWfb2OsHxTV
   lISVJqjdhYHYM7vC6VNffMYIYxAE90ZEl9QHOdU5n7spPyxUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSOn
   RKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/ii1YLvMKyq+T7PJbPDwhU8uAGQIDAQABo4HWMIHTMAwGA1UdE
   wQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQB
   gjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
   GA1UdEQQ9MDuCF2VzYXRlc3Qub25taWNyb3NvZnQuY29tgSByb2JzaGVyd0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbT
   ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
   31o1kADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSmvn980GHuSXOqfLMPtniUMTubp+
   SICDrtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV99OJ6+DOkMn1f
   QOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj1+guS0X0FMmhkDJOTyZ
   WnAQ=="
   }
   ],
   ```
10. Sauvegardez le fichier .json localement.
11. Revenez à votre navigateur et au portail de Microsoft Azure.
12. Le clic **GÈRENT MANIFESTE > téléchargement manifeste** :

13. Parcourez et trouvez le fichier édité .json, et sélectionnez le coche pour se terminer le téléchargement.

Trouver l'ID de locataire

1. Cliquez sur en fonction les **POINTS FINAUX de VUE** pour visualiser les points finaux intégrés dans l'AD de Microsoft Azure.
2. Avec dans l'URLs, notez la valeur semblable pour chaque ligne, "ed437e13-ba50-479e-b40d-8affa4f7e1d7," que c'est l'***ID de locataire***.



Ce sera seul à votre application et configuration. Enregistrez cette valeur pour une configuration plus récente sur l'ESA.

Examen final des valeurs à enregistrer

Les valeurs suivantes devraient avoir été enregistrées pendant la configuration d'AD de Microsoft Azure pour l'usage en configurant les configurations de boîte aux lettres sur l'ESA :

De *configurez les valeurs de certificat* :

- Certificat de clé privée (.pem)
- $base64Thumbprint

De *configurez l'application Web faite sur commande* :

- ID de client

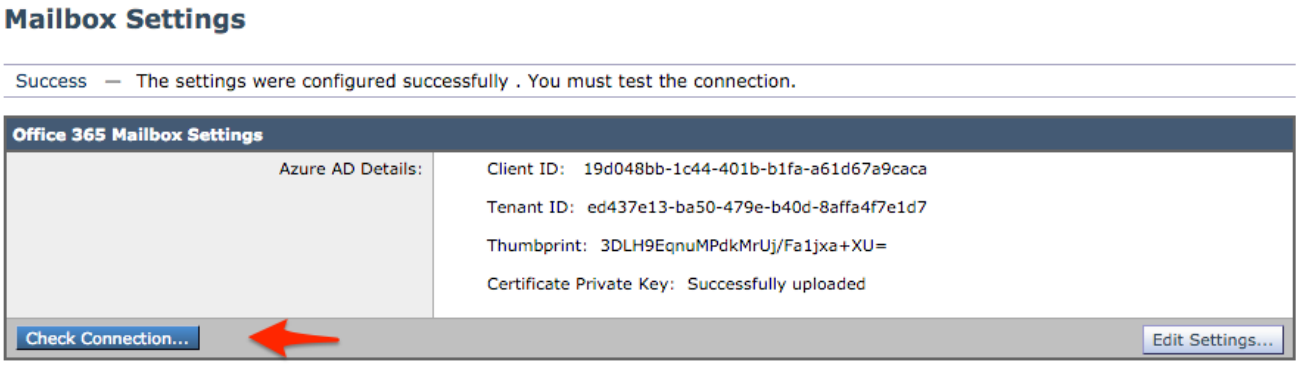
De trouver l'ID de locataire :

- ID de locataire

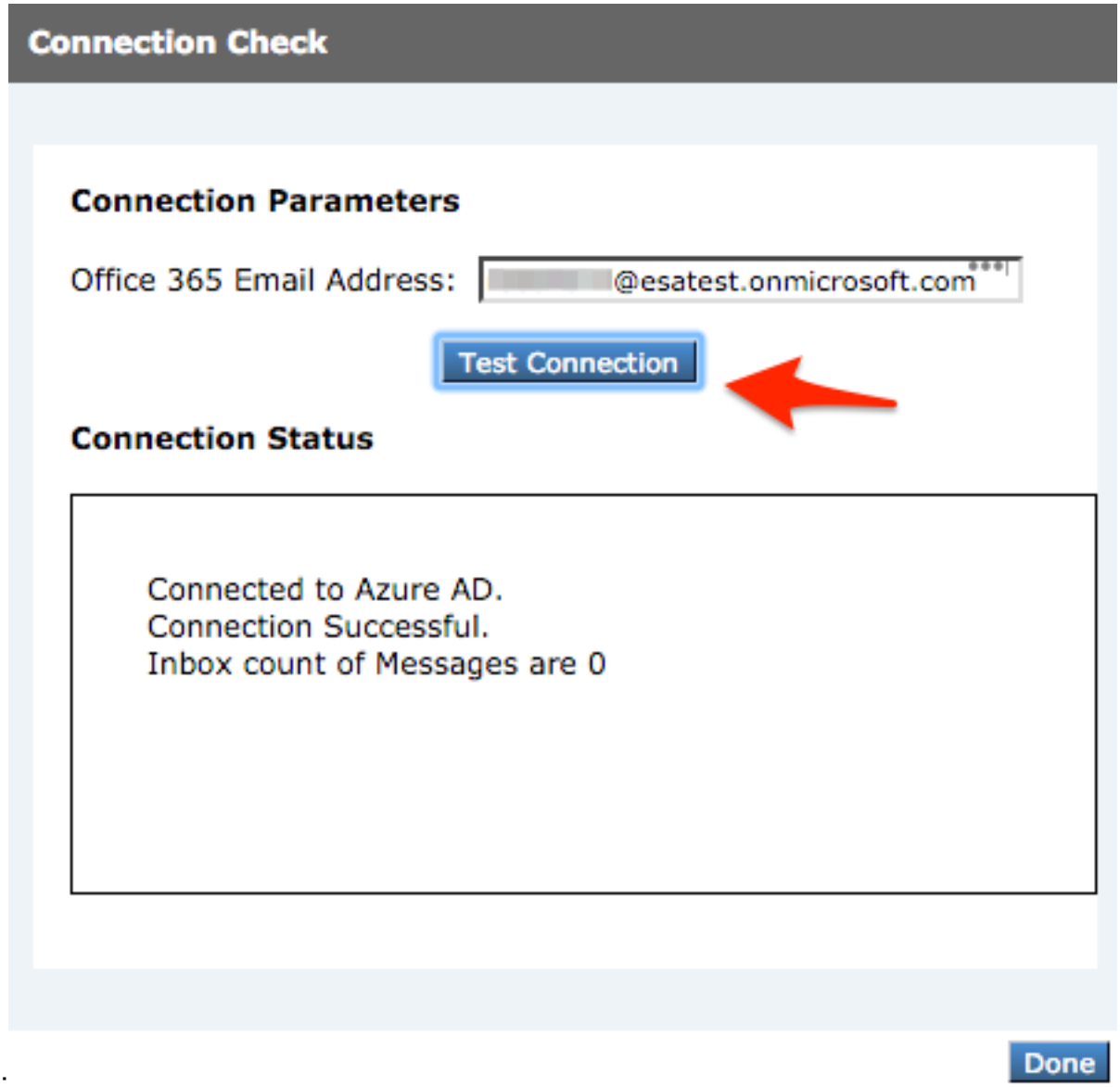
Configurez les configurations de boîte aux lettres sur l'ESA

Avec la configuration d'AD de Microsoft Azure complète, vous êtes prêt à faire valider l'ESA communiquer et.

1. Procédure de connexion à l'appliance ESA par l'intermédiaire du GUI.
2. Configurations de boîte aux lettres du bureau 365 d'**enable** sous des **configurations d'administration système > de boîte aux lettres.**
3. « La case choisie de **configurations de boîte aux lettres du bureau 365 d'enable »** et fournissent à vos détails d'AD de Microsoft Azure (*ID de client et ID de locataire*) obtenus tout en enregistrant l'application ESA L'AD de Microsoft Azure avec Thumbprint *et clé privée du* certificat.
4. Cliquez sur Submit pour sauvegarder les modifications aux configurations de boîte aux lettres.
5. Vous devrez tester la connexion à l'AD de Microsoft Azure à cette heure pour votre domaine du bureau 365 comme configuré
   :



6. Utilisez une adresse e-mail active et valide sur le compte, **connexion de test de** clic



:

7. Une fois que l'état de la connexion est réussi, cliquez sur **fait** pour se terminer le contrôle de connexion.
8. En conclusion, **validation de** clic pour sauvegarder toutes les modifications de configuration sur l'ESA.