

Contenu

[Introduction](#)

[Conditions préalables](#)

[Configurez les valeurs de certificat](#)

[Configurez l'AD de Microsoft Azure](#)

[Créez l'application Web faite sur commande](#)

[Configurez l'application Web faite sur commande](#)

[Créez le manifeste](#)

[Trouver l'ID de locataire](#)

[Examen final des valeurs à enregistrer](#)

[Configurez les configurations de boîte aux lettres sur l'ESA](#)

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
9. écho
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 :

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,

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Licenses' page for 'cisco tac (content security)'. A search bar is visible with the text 'Applications my company uses'. Below the search bar is a table listing various applications:

| 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/out... |
| 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 | |

The 'Microsoft Intune' application is highlighted in blue. The left sidebar shows navigation options, and the bottom of the screen has a dark blue bar with icons for 'NEW', 'ADD', and 'VIEW ENDPOINTS'.

APPLICATIONS choisies.

5. De la barre d'outils inférieure, choisissez **AJOUTEZ** : 
6. Une fois présenté « *que voulez-vous faire ?* », choisissez **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 :

ADD APPLICATION x

Tell us about your application

NAME

ESA_Beta

Type

WEB APPLICATION AND/OR WEB API ?

NATIVE CLIENT APPLICATION ?




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

ADD APPLICATION x

App properties

SIGN-ON URL ?

https://esatest.onmicrosoft.com/ManualRegistration 

APP ID URI ?

https://esatest.onmicrosoft.com 



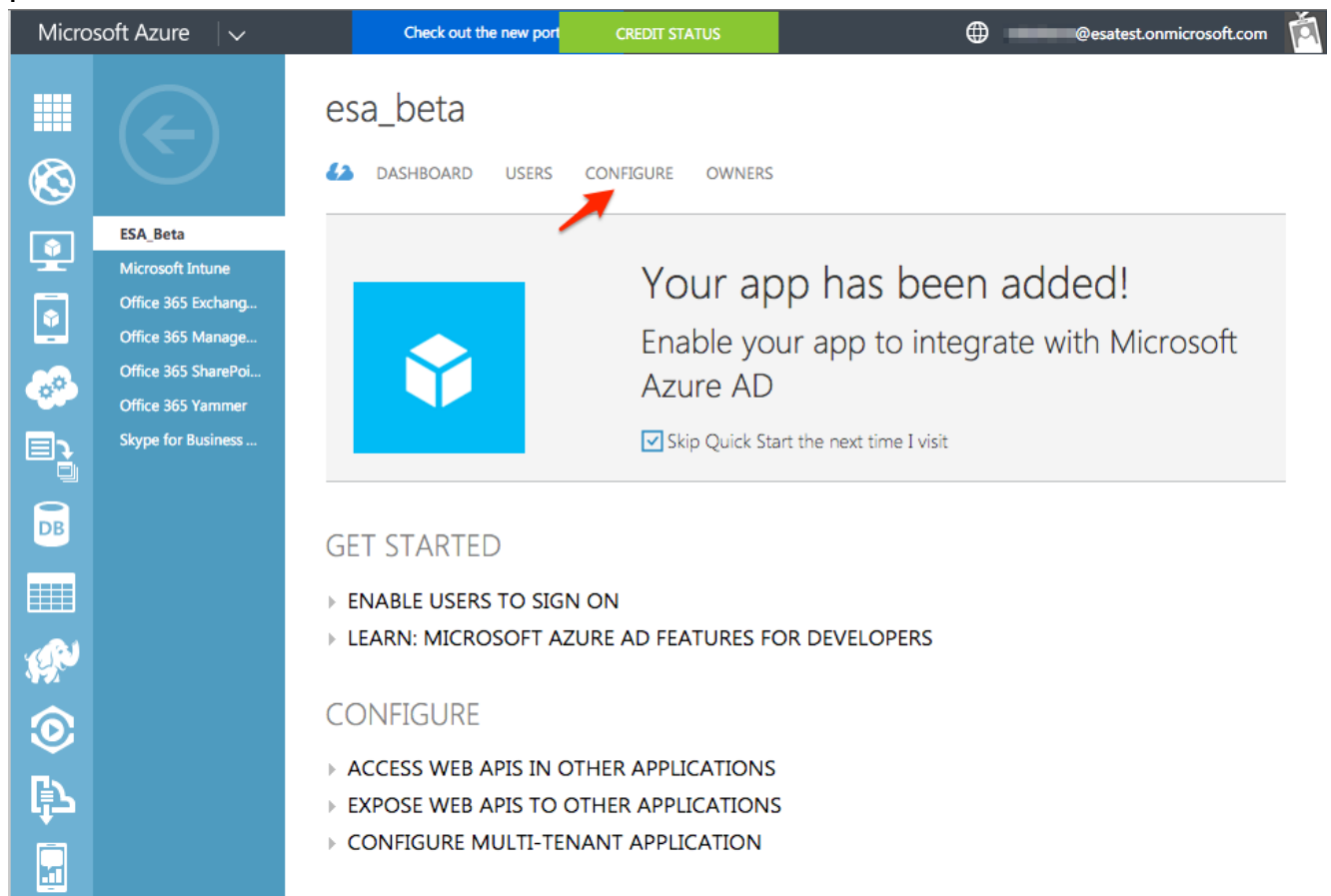
9. De Microsoft, concernant l'[URI d'ID d'app](#) : « Puisque l'URI d'ID d'app est un identifiant logique, il n'a pas besoin de le résoudre à une adresse Internet. Il est présenté par votre app en envoyant une demande simple d'ouverture de session à l'AD azuré. L'AD azuré identifie votre app et envoie 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 wrealm (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, choisissez **CONFIGUREZ**

:



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', a search icon, and a user profile. Below that, a blue sidebar contains various service icons. The main content area is titled 'esa_beta' and has a navigation menu with 'DASHBOARD', 'USERS', 'CONFIGURE', and 'OWNERS'. The 'CONFIGURE' tab is active and highlighted with a red arrow. The main content area displays a message: 'Your app has been added! Enable your app to integrate with Microsoft Azure AD' with a checkbox for 'Skip Quick Start the next time I visit'. Below this, there are sections for 'GET STARTED' and 'CONFIGURE' with various options.

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

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


esa_beta

DASHBOARD | USERS | CONFIGURE | OWNERS

properties

NAME: ESA_Beta

SIGN-ON URL: https://esatest.onmicrosoft.com/ManualRegistration

LOGO: 

APPLICATION IS MULTI-TENANT: YES NO

CLIENT ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca

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

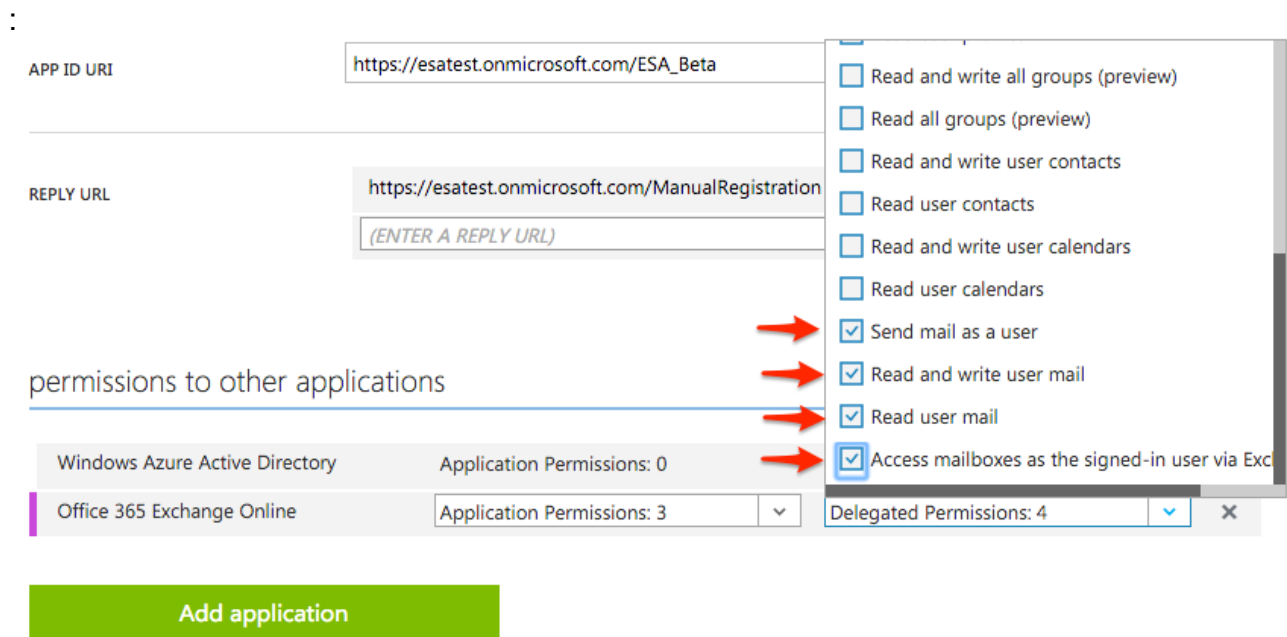
permissions to other applications

Windows Azure Active Directory | Application Permissions: 0 | Delegated Permissions: 1

Add application

- L'échange** choisi du **bureau 365 en ligne** et cliquent sur le contrôle pour continuer.
- 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. Comme remarquable plus tôt, en écrivant le $\$base64Value$, ceci est exigé pour être édité pour être une ligne simple valeur.
7. Continuant l'exemple comme créé dès le début de ce document, les *keyCredentials* modifiés seront comme suit :

8. Sauvegardez le fichier .json localement.
9. Revenez à votre navigateur et au portail de Microsoft Azure.
10. Le clic **GÈRENT MANIFESTE** > téléchargement manifeste



11. 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**.



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>



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. Choisi ? Configurations de boîte aux lettres du bureau 365 d'enable ? la case 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

:

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. 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.