Comment-à des configurations configurez d'Azure AD et de bureau 365 boîte aux lettres pour l'ESA

Contenu

Introduction

Ce document fournit un pas à pas « comment-à » pour enregistrer une nouvelle application dans Windows Azure et obtenir les valeurs nécessaires, afin de se terminer la configuration pour des configurations de boîte aux lettres du bureau 365 sur une appliance de sécurité du courrier électronique de Cisco (ESA). Ceci est exigé quand un administrateur ESA configure la correction automatique de boîte aux lettres (MARS) pour la protection avancée de malware (AMP) sur les paramètres de la stratégie de la messagerie de l'ESA.

Conditions préalables

Produits connexes

Ce document s'applique à ce qui suit :

- Tous les ESA, matériel et exécution virtuelle 10.x et plus nouveau
- Tous opacifient la sécurité du courrier électronique (CES) ESA, 10.x et plus nouveau courants

Conditions requises

Ce document exige 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 permuter, 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 d'un hôte ou d'un serveur de Windows.
- 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.

Vous créerez les quatre valeurs suivantes afin de configurer le connecteur de boîte aux lettres ESA de nouveau à l'Azure AD :

1. ID de client
2. ID de locataire
3. Thumbprint
4. Clé privée de certificat dans le format .pem

Afin d'établir ces valeurs priées, vous devrez se terminer les étapes dans ce document. Avant de commencer, vous devrez exécuter le suivant par l'intermédiaire de Windows Powershell :

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**

    Note: Pour #2, remplacez le **« _to_cert de C:\path \ PEM_certificate.crt » par le** chemin à votre certificat.

$base64Thumbprint = *Thumbprint*. Ajoutez cette valeur à votre liste de conditions préalables de valeurs requises.

Conseil : Veuillez avoir la sortie enregistrée localement pour *$base64Value*,

$base64Thumbprint, et *$keyid*, car ils seront exigés plus tard dans les étapes de configuration. À ce moment, vous êtes fait avec le .crt du certificat. Veuillez avoir le .pem associé de votre certificat dans un répertoire disponible et local sur votre ordinateur.

Informations générales

Microsoft permet l'accès à deux versions du portail azuré :

- https://manage.windowsazure.com (portail classique)
- https://portal.azure.com (nouveau portail)

Vous pouvez accéder à « le portail classique » du nouveau portail par la barre d'outils de main gauche, « Répertoire actif azuré » choisi > portail classique

Aux fins de ce document, l'enregistrement et la configuration de l'application sont faits dans le nouveau portail. Les étapes à utiliser « le portail classique » sont incluses à la fin de ce document. (Microsoft peut choisir à un jour ou l'autre de désactiver le portail azuré classique.)

Comment-à des configurations configurez d'Azure AD et de bureau 365 boîte aux lettres pour l'ESA

Enregistrez une nouvelle application dans Azure

1. Accédez à l'interface utilisateur azurée : https://portal.azure.com/
2. La barre de menus gauche, cliquent sur **plus de services > de SÉCURITÉ + d'IDENTITÉ : Enregistrements d'app**
3. Du volet d'enregistrements d'app, clic **+Add**
4. Créez un nom pour votre app
5. Pour le type d'application, congé comme **Web app/API**
6. Pour l'URL d'ouverture de session, utilisez le format suivant : https://*<company_domain.com>/ManualRegistration***Note**: *<company_domain.com> est le* domaine de votre O365 où les utilisateurs de domaine mettent en boîte la connexion et accèdent à votre domaine O365.
7. Le clic **créent**

Placez les autorisations requises pour l'application

1. Cliquez sur en fonction le « nom d'affichage » associé pour l'app que vous vous êtes juste enregistré
2. Dans le volet de configurations, pour API Access, le clic **a exigé des autorisations**
3. Clic **+Add**
4. Dans le volet « ajoutez API accès », clic **sélectionnent un API**
5. Dans « sélectionnez et API », **échange du bureau 365 de** clic le volet **en ligne (Microsoft Exchange)**
6. Au clic de bas de page **choisi**
7. Pour l'application les autorisations sélectionnent :
   • Utilisez les services Web d'échange avec l'accès complet à toutes les boîtes aux lettres

• Envoyez la messagerie en tant que n'importe quel utilisateur
• Lisez et écrivez la messagerie dans toutes les boîtes aux lettres

8. Pour Delegated les autorisations sélectionnent :
   • Envoyez la messagerie en tant qu'utilisateur
   • Lisez et écrivez la messagerie d'utilisateur
   • Lisez la messagerie d'utilisateur
   • Accédez aux boîtes aux lettres en tant qu'utilisateur connecté par l'intermédiaire des services Web d'échange
9. Le clic **choisi au** bas de page, ceci fermera le volet « sélectionnent API »
10. Cliquez sur **fait au** bas de page, ceci fermera le volet « ajoutent API accès »
11. **Autorisations de Grant de** clic
12. Une fois incité « faites vous veulent accorder les autorisations ci-dessous pour le myESA pour tous les comptes dans le répertoire courant ? Cette action mettra à jour toutes les autorisations existantes que cette application déjà doit apparier ce qui est répertorié ci-dessous. », cliquez sur **oui**

Vous maintenant devriez faire répertorier deux API, « Répertoire actif de Windows Azure » et « échange du bureau 365 en ligne ».

Vous devrez retourner au volet enregistré d'app pour poursuivre la section suivante :

1. Cliquez sur « X » pour fermer le volet « a exigé autorisations »
2. Cliquez sur le « X pour fermer « volet de configurations le »

Vous êtes maintenant de retour au volet enregistré d'app.

Préparez le manifeste pour l'application

Éditez manifeste

1. Du volet enregistré d'app, clic manifeste dans la barre d'outil
2. Vous êtes présenté le complet vous manifestez dans l'éditeur. Trouvez la ligne exisiting de « keyCredentials ». Vous remplacerez SEULEMENT des « keyCredentials » par ce qui suit :

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

3. Vous devrez remplacer $base64Thumbprint, $keyid, et $base64Value par vos valeurs Laissez les devis ("") autour de TOUTES LES valeurs, comme affichéPrêtez la particulière attention que chaque valeur est SEULEMENT 1 ligne, y compris le $base64Thumbprint
4. **Sauvegarde de** clic pour mettre à jour votre application. Vous devriez voir l'avis « d'application avec succès à jour » dans la zone de barre d'outils.

Vous devrez retourner au volet enregistré d'app pour poursuivre la section suivante :

Le clic « X » pour clôturer « éditent » le volet manifeste.

(Facultatif) téléchargez le manifeste

> **Conseil** : Vous pouvez ignorer le téléchargement manifeste et télécharger manifeste si vous pouviez avec succès utiliser l'éditeur de dans-Azure pour le manifeste. Sinon, et vous devez éditer manuellement le manifeste, poursuivez s'il vous plaît.

1. Du volet enregistré d'app, clic manifeste dans la barre d'outil
2. Dans le menu manifeste d'éditer cliquez sur Download
3. Sauvegardez le manifeste au répertoire contenant votre certificat. Ceci sauvegardera le manifeste dans le format .json localement à votre ordinateur.
4. Utilisant un éditeur local (Wordpad++, atome, etc.), étapes complètes 2 et 3 de « éditent » la section manifeste de ce document
5. Sauvegardez le fichier manifeste .json localement

(Facultatif) téléchargez le manifeste

Si vous choisissiez de télécharger et éditiez le manifeste manuellement, vous devrez télécharger le manifeste édité :

1. Revenez à votre navigateur et au portail d'Azure
2. Cliquez sur Upload du « éditent » le volet manifeste

Vous devrez retourner au volet enregistré d'app pour poursuivre la section suivante :

Le clic « X » pour clôturer « éditent » le volet manifeste.

Obtenez l'ID de client pour l'application

1. De l'app enregistré trouvez le « ID de la demande »
2. Copiez l'ID de la demande (l'*ID d*'ID de la demande = de *client*)
3. Ajoutez cette valeur à votre liste de conditions préalables de valeurs requises.

Obtenez la valeur d'ID de locataire pour l'application

1. Du volet « d'enregistrements d'app », cliquez sur en fonction les « points finaux » et sélectionnez la première ligne pour le DOCUMENT de MÉTADONNÉES de FÉDÉRATION
2. Copiez et collez la ligne à un éditeur externe
3. Vous voudrez récupérer l'*ID de locataire*, qui est la chaîne d'ID après « https://login.windows.net/ »
4. Ajoutez cette valeur à votre liste de conditions préalables de valeurs requises.

Exemple :

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

```
}
],
```

Pour cet exemple, l'ID de locataire sera "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Vérifiez les valeurs requises

Vos valeurs sont maintenant terminées. Vous devriez pouvoir compléter les valeurs suivantes :

- ID de client
- ID de locataire
- Thumbprint (voir les conditions préalables)
- Clé privée de certificat dans le format .pem (voir les conditions préalables)

Vous êtes prêt à se terminer les configurations de boîte aux lettres du bureau 365 en configurant ces valeurs sur l'ESA.

Configurez l'ESA

1. Sur le GUI ESA : **Les configurations d'administration système > de boîte aux lettres > éditent des configurations…**
2. Entrez en vos valeurs de la section précédente (ID de client, ID de locataire, Thumbprint)
3. Chargez le certificat enregistré (.pem)
4. Cliquez sur Submit
5. Vous verrez que « les configurations ont été configurées avec succès. Vous devez commettre les modifications et tester la connexion. »
6. Du coin supérieur droit, la **validation de** clic **change** avant n'importe quel test
7. Clic « connexion de contrôle… » et entrez dans un bon connu, en fonctionnant l'adresse e-mail associée avec votre domaine O365
8. Clic « connexion de test »

Vous devriez recevoir des résultats de succès dans l'état de la connexion :

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

Dépannage de l'ESA

Si vous ne voyez pas que les résultats positifs pour l'état de la connexion testent, vous pouvez souhaiter passer en revue l'enregistrement d'application exécuté de l'Azure AD.

De l'ESA, placez les logs de MARS au niveau de suivi et retestez la connexion.

Pour les connexions infructueuses, les logs peuvent afficher semblable à :

```
"keyCredentials": [
```

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

Confirmez l'ID de la demande, l'ID de répertoire (qui est identique que l'ID de locataire), ou d'autres identificateurs associés du log avec votre application dans l'Azure AD. Si vous êtes incertain des valeurs, supprimez la demande du portail d'Azure AD et recommencez.

Pour la connexion réussie, les logs devraient être semblables à :

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

Dépannage de l'Azure AD

> **Note**: Cisco TAC et le support de Cisco ne sont pas autorisés à dépanner des questions de côté client avec l'AD de Microsoft Exchange, de Microsoft Azure, ou le bureau 365.

Pour des questions de côté client avec l'AD de Microsoft Azure, vous devrez engager le support de Microsoft. Veuillez voir l'option de « aide + de support » de votre tableau de bord de Microsoft Azure. Vous pouvez pouvoir ouvrir des demandes de support direct au support de Microsoft du tableau de bord.

(Facultatif) comment créer et configurer une application dans Azure utilisant le portail classique

> **Note**: Vous n'avez pas besoin de se terminer ceci si vous pouviez avec succès utiliser le portail d'Azure en accédant à https://portal.azure.com (nouveau portail). Ceci est seulement mis en référence pour l'administrateur azuré qui choisissent d'utiliser toujours « le portail classique ». Si vous souhaitez utiliser cette version du portail d'Azure AD, veuillez trouver les instructions pas à pas suivantes pour se terminer les valeurs requises :

Ajoutez une application

1. Procédure de connexion au Microsoft Azure.
2. De la barre de menus gauche, naviguez vers **TOUS LES ÉLÉMENTS**
3. Cliquez sur en fonction le nom des ressources pour votre domaine
4. Des onglets d'outil sous votre nom des ressources, **APPLICATIONS** choisies
5. De la zone inférieure de barre d'outils, cliquez sur Add

6. Une fois présenté *« que voulez-vous faire ? »*, choisi **ajoutez une application que mon organisation développe**
7. Remplissez « *nous disent les* informations *au sujet de votre application* » : Créez un nom pour votre appPour le type d'application, le congé comme **application Web et/ou le Web API**Cliquez sur en fonction la flèche pour continuer
8. Terminez-vous les propriétés d'app : Pour l'URL d'OUVERTURE DE SESSION, utilisez le format suivant : https://*<Office365_assigned_company_domain.com>/ManualRegistration***Note**: *<company_domain.com> est le* domaine de votre O365 où les utilisateurs de domaine mettent en boîte la connexion et accèdent à votre domaine O365.Pour l'URI d'ID d'APP, utilisez le format suivant :
https:// < *Office365_assigend_company_domain.com* >Cliquez sur le coche pour se terminer

Configurez votre application

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. **L'ID de client est répertorié sur cet écran. Copiez et ajoutez** cette valeur à votre liste de conditions préalables de valeurs requises.
3. Défilement au bas de l'écran pour voir des « autorisations à d'autres applications ».
4. Cliquez sur Add l'**application L'échange** choisi du **bureau 365 en ligne** et cliquent sur le contrôle pour continuerPour des **autorisations d'application**, choisi : **Lisez et écrivez la messagerie dans toutes les boîtes aux lettresEnvoyez la messagerie en tant que n'importe quel utilisateurServices Web d'échange d'utilisation avec l'accès complet…**Pour des autorisations Delegated, choisi : **Envoyez la messagerie en tant qu'utilisateurLisez et écrivez la messagerie d'utilisateurLisez la messagerie d'utilisateurAccédez aux boîtes aux lettres en tant qu'utilisateur connecté par l'intermédiaire de l'échange**
5. **Sauvegarde de clic de la barre d'outils inférieure pour sauvegarder tous les travail et configuration pour l'application Web faite sur commande**

Gérez 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. Localement, trouvez le fichier .json et ouvrez-vous avec un éditeur de texte. (Notepad++ préférable, atome, etc.)
4. Recherchez et trouvez la ligne de « keyCredentials »
5. Remplacer cette ligne simple par les plusieurs lignes suivantes, personnalisant à l'aide du *$base64Thumbprint*, du *$keyid*, et du *$base64Value* :

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

```
}
],
```

6. En écrivant le *$base64Value*, ceci est exigé pour être édité à une ligne simple valeur
7. Sauvegardez le fichier .json localement
8. Revenez à votre navigateur et au portail de Microsoft Azure
9. Le clic **GÈRENT MANIFESTE > téléchargement manifeste**
10. Parcourez et trouvez le fichier édité .json
11. Sélectionnez le coche pour se terminer le téléchargement

Trouver l'ID de locataire

1. De la barre d'outils inférieure, cliquez sur en fonction les **POINTS FINAUX de VUE** pour visualiser les points finaux intégrés dans l'AD de Microsoft Azure
2. Sélectionnez la première ligne pour le DOCUMENT de MÉTADONNÉES de FÉDÉRATION
3. Copiez et collez la ligne à un éditeur externe
4. Vous voudrez récupérer l'*ID de locataire*, qui est la chaîne d'ID après « https://login.windows.net/ »
5. Ajoutez cette valeur à votre liste de conditions préalables de valeurs requises

Exemple :

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

Pour cet exemple, l'ID de locataire sera "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Support produit
- Appliance de sécurité du courrier électronique de Cisco - Notes de mise à jour
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur