

# Como configurar o Microsoft Azure AD e o escritório 365 para o uso no ESA

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Configurar valores do certificado](#)

[Configurar o Microsoft Azure AD](#)

[Crie o aplicativo de web feito sob encomenda](#)

[Configurar o aplicativo de web feito sob encomenda](#)

[Crie o manifesto](#)

[Encontrando o inquilino ID](#)

[Revisão final dos valores a ser salvar](#)

[Configurar ajustes da caixa postal no ESA](#)

## Introdução

Este documento descreve como setup e configurar o Microsoft Azure AD e o escritório 365 para trabalhar com a ferramenta de segurança do email de Cisco (ESA).

## Pré-requisitos

As informações neste documento são baseadas nestas versões de software e hardware:

- AsyncOS para a Segurança 9.9.5-039 do email (Bellagio), ou mais novo.

Este documento igualmente exige o seguinte:

- Assinatura da conta do [escritório 365](#) (se certifique por favor de que sua [assinatura da conta do escritório 365](#) inclui o acesso para enviar por correio eletrônico, como uma conta da empresa E3 ou da empresa E5.)
- Conta do [Microsoft Azure](#)
- As contas do escritório 365 e do Microsoft Azure AD são amarradas corretamente a um endereço email ativo de *user@domain.com*, e você pode enviar e receber email através desses domínio e conta.
- Alcance a Windows PowerShell, administrado geralmente de Windows Server.
- Público ativo do domínio/certificado privado e a chave privada usada para assinar o certificado, ou a capacidade criar certificado público/privado e capacidade para salvar a chave privada usada para assinar o certificado.

## Configurar valores do certificado

Entre a Windows, e usando PowerShell termine os comandos seguintes traçar e obter *\$keyid*, *\$base64Thumbprint*, e *\$base64Value*:



Nota: O `$base64Value` é exigido ser editado para ser uma linha única.

Salvar o certificado da chave pública (.crt) e a chave privada usada para assinar localmente o certificado (.pem). A chave privada será precisada durante a configuração ESA.

## Configurar o Microsoft Azure AD

### Crie o aplicativo de web feito sob encomenda

1. Entre ao [Microsoft Azure](#).
2. Navegue a **TODOS OS ARTIGOS**.
3. Clique sobre o nome do recurso para seu domínio.
4. Das abas da ferramenta para o nome do recurso, selecione **APLICATIVOS**.

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

## cisco tac (content security)

USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS

LICENSES

Show Applications my company uses Search Application name or Client ID

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/outlo...
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	

+ NEW | ADD | VIEW ENDPOINTS | 1 ! ?

5. Da barra de ferramentas inferior, seleta **ADICIONAR**:

+ NEW | **ADD** | VIEW ENDPOINTS | 1 ! ?

6. Quando apresentado “*que você quer fazer?*”, seleta **adicionar um aplicativo que minha organização está desenvolvendo**.

7. Crie com um nome apropriado, e deixe o *tipo* como o **aplicativo de web e/ou a Web API**, e clique a seta para continuar:

# Tell us about your application

NAME

Type

- WEB APPLICATION AND/OR WEB API <sup>?</sup>
- NATIVE CLIENT APPLICATION <sup>?</sup>



8. Para terminar adicionar o aplicativo de web feito sob encomenda, incorporar os seguintes valores para seu domínio, e clicar a verificação para terminar: SINAL-NA URL: **https:// <your.domain.com>/ManualRegistration**ID DE APP URI: **https:// <your.domain.com>**

# App properties

SIGN-ON URL ?

APP ID URI ?



9. De Microsoft, em relação ao [App ID URI](#): “Porque o App ID URI é um identificador lógico, não precisa de resolver a um endereço do Internet. É apresentado por seu app ao enviar um único sinal-no pedido aos azuis celestes AD. O azul celeste AD identifica seu app e envia sinal-na resposta (um token de SAML) à resposta URL que foi fornecida durante o registro do app. Use o valor do App ID URI para ajustar a propriedade do wtrealm (para a WS-federação) ou a propriedade do expedidor (para SAML-P) ao fazer um pedido do login. O **App ID URI** deve ser um valor exclusivo nos azuis celestes AD da sua organização.”

Nota: “Ao permitir um app para usuários externos, o valor do App ID URI do app deve ser um endereço em um dos domínios verificados do seu diretório. Em consequência, não pode ser uma URNA. Esta proteção impede que outras organizações especifiquem (e a tomem) a propriedade original que pertence a sua organização. Durante o desenvolvimento, você pode mudar seu App ID URI a um lugar no domínio inicial da sua organização (se você não verificou um domínio feito sob encomenda/vaidade), e atualiza seu app para usar este valor novo. O domínio inicial é o domínio 3-level que você cria durante assina acima, como contoso.onmicrosoft.com.”

## Configurar o aplicativo de web feito sob encomenda

1. Uma vez que o aplicativo de web feito sob encomenda foi criado, você está navegado automaticamente no aplicativo de web feito sob encomenda próprio. De aqui, nas abas da ferramenta, seletas **CONFIGURAR**:

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

esa\_beta

DASHBOARD USERS **CONFIGURE** OWNERS

**Your app has been added!**  
Enable your app to integrate with Microsoft Azure AD  
 Skip Quick Start the next time I visit

GET STARTED

- ▶ ENABLE USERS TO SIGN ON
- ▶ LEARN: MICROSOFT AZURE AD FEATURES FOR DEVELOPERS

CONFIGURE

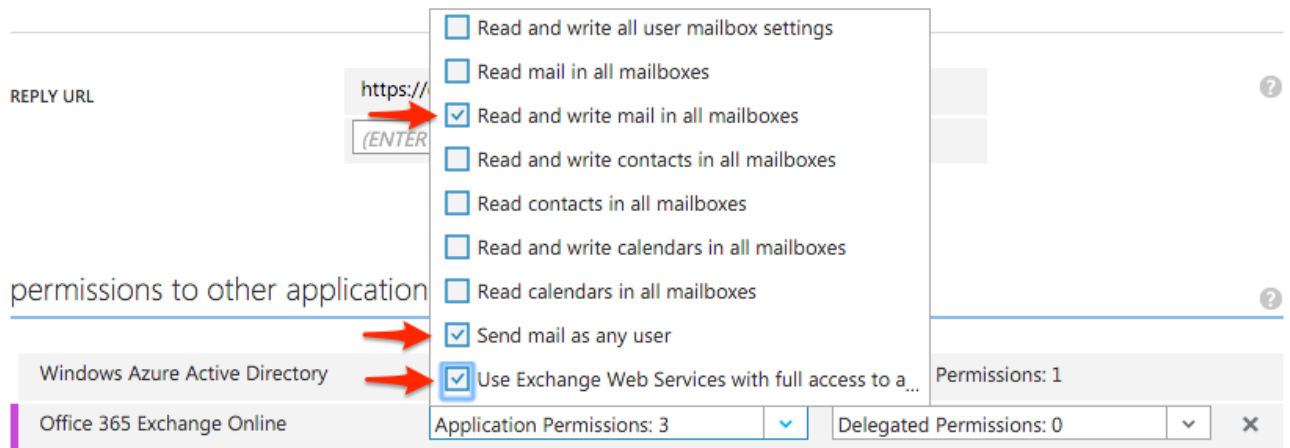
- ▶ ACCESS WEB APIS IN OTHER APPLICATIONS
- ▶ EXPOSE WEB APIS TO OTHER APPLICATIONS
- ▶ CONFIGURE MULTI-TENANT APPLICATION

2. Desta tela, você pode ver Sinal-na URL e nos outros detalhes de configuração como criado. Nota: **A identificação de cliente** é alistada nesta tela. Este valor será precisado durante a configuração ESA.

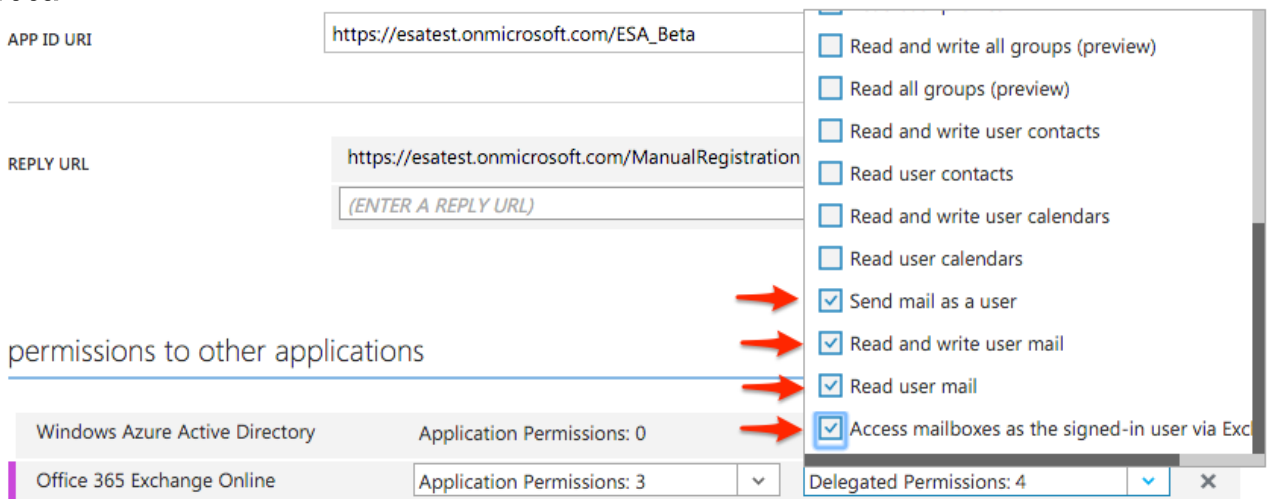
3. Desta mesma tela para a configuração de aplicativo de web feita sob encomenda, o rolo à parte inferior e o clique **adicionam o aplicativo**:

4. O Online seleta da **troca do escritório 365** e clica a verificação para continuar.
5. Para as **permissões de OnlineApplication da troca do escritório 365**, selecione **lido e escreva o correio em todas as caixas postais, envie o correio como todo o usuário, e use serviços de Web da troca com acesso direto...**:





6. Para as *permissões de OnlineDelegated da troca do escritório 365*, seletor **envie o correio como um usuário, leu e escreveu o correio do usuário, leu o correio do usuário, e alcançou caixas postais como o usuário ingressado através da troca**:

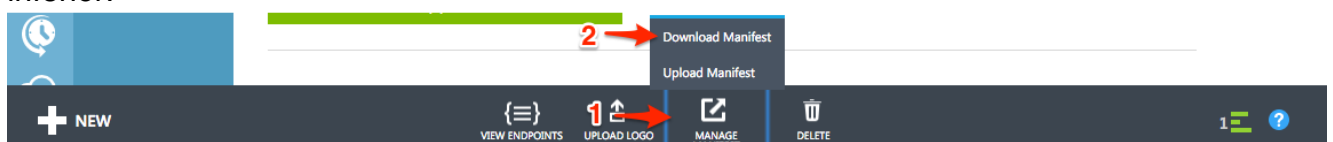


7. Clique a **salvaguarda da barra de ferramentas inferior** para salvar todo o trabalho e configuração para o aplicativo de web feito sob encomenda:



## Crie o manifesto

1. Uma vez que o aplicativo de web feito sob encomenda terminou a economia e a atualização, o clique **CONTROLA MANIFESTO > transferência manifesta da barra de ferramentas inferior**:



2. Navegue com as respostas, e salvar o aplicativo de web manifesto no formato .json a seu computador local.
3. Encontre este arquivo .json e abra este arquivo .json com um editor de texto. (Notepad++ preferível, átomo, etc.)
4. Procure e encontre a linha dos "keyCredentials".
5. Você estará substituindo esta linha única com as seguintes múltiplas linhas, e personaliza-a usando as credenciais identificadas mais adiantadas da seção dos valores do *certificado configurar* (*\$base64Thumbprint*, *\$keyid*, e *\$base64Value*):
6. "keyCredentials": [
 

```

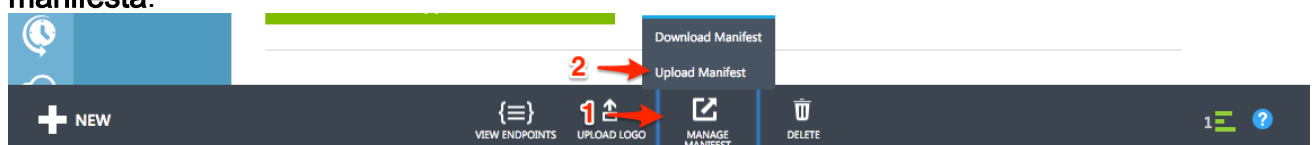
{
  "customKeyIdentifier": "$base64Thumbprint",
  "keyId": "$keyid",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "$base64Value"
}
],

```
7. Como notável mais cedo, ao incorporar o *\$base64Value*, isto é exigido ser editado para ser um valor da linha única.
8. Continuando com o exemplo como criado desde o início deste documento, os *keyCredentials* alterados serão como segue:
9. "keyCredentials": [
 

```

{
  "customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Faljxa+XU=",
  "keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value":
  "MIIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxzCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aC
  BDYXJvbGluYTEEMMAoGA1UEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMMDVEFDMSAwHgYDVQQDEXd1c2F0Z
  XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2lzY28uY29tMB4XDTE2MDMyODE0NTYw
  MFoXDTE3MDMyODE0NTYwMFowZcxzCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEEMMAoGA1UEBxM
  DU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMMDVEFDMSAwHgYDVQQDEXd1c2F0ZXXN0Lm9ubWljcm9zb2Z0LmNvbT
  EhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2lzY28uY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEaz
  B6r/MtFkWG+86eHzdHyklCdyT+j/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
  axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZG1F0nkzT5Gs+zL0uhPHaT1DMU70LCXh8CHS2cLsczpDwf20sHxTV
  lISVJqjdhYHYM7vC6VNfMYIYxAE90ZE19QH0dU5n7spPyxUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSon
  RKYaIpkLkOSwZurT0wyGJd+TzSw+RgsX1vKJNmKih/i1YLvMKYq+T7PJbPDwhU8uAGQIDAQABo4HWMIHMAwGA1UdE
  wQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAGYIKwYBBQUHAWQCisGAQQB
  gjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
  GA1UdEQQ9MDuCF2VzYXRlc3Qub25taWNyb3NvZnQuY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29tY29t
  ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBrIYK8fet0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
  31o1kADPcK3ml0UarT35hH6f9abZSxm3mj3zMnuK5nW2ypDCVUiuA2C51+woEubSsmvn980GHuSXOqfLMPtniUMTubp+
  SICDrtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV990J6+DokMnlf
  QOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj1+guS0X0FMmhkDJOtyZ
  WnAQ== "
}
],

```
10. Salvar o arquivo .json localmente.
11. Retorne a seu navegador e ao portal do Microsoft Azure.
12. O clique **CONTROLA MANIFESTO > transferência de arquivo pela rede manifesta:**



13. Consulte e encontre o arquivo editado .json, e selecione a marca de verificação para

terminar a transferência de arquivo pela rede.

## Encontrando o inquilino ID

1. Clique sobre **VALORES-LIMITE da VISTA** para ver os valores-limite integrados no Microsoft Azure AD.
2. Com nas URL, observe o valor similar para cada linha, "ed437e13-ba50-479e-b40d-8affa4f7e1d7," que este é o *inquilino ID*.



# 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>



Isto será original a seus aplicativo e configuração. Grave este valor para uma configuração mais atrasada no ESA.

## Revisão final dos valores a ser salvar

Os seguintes valores devem ter sido gravados durante a configuração do Microsoft Azure AD para o uso ao configurar os ajustes da caixa postal no ESA:

De *configurar valores do certificado*:

- Certificado da chave privada (.pem)
- \$base64Thumbprint

De *configurar o aplicativo de web feito sob encomenda*:

- Identificação de cliente

De *encontrar o inquilino ID*:

- Inquilino ID

## Configurar ajustes da caixa postal no ESA


Com a configuração do Microsoft Azure AD completa, você está pronto para mandar o ESA comunicar-se e validar.

1. Início de uma sessão ao dispositivo ESA através do GUI.
2. **Permita** ajustes da caixa postal do escritório 365 sob **ajustes da administração do sistema > da caixa postal**.
3. “**Permita** caixa de verificação seleta dos **ajustes da caixa postal do escritório 365**” & forneça seus detalhes do Microsoft Azure AD (*identificação de cliente & inquilino ID*) obtidos ao registrar o aplicativo ESA o Microsoft Azure AD junto com Thumbprint & *chave privada do certificado*.
4. O clique **submete-se** para salvar as mudanças aos ajustes da caixa postal.
5. Você precisará de testar neste tempo a conexão ao Microsoft Azure AD para seu domínio do escritório 365 como configurado:

### 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. Use um endereço email ativo e válido na conta, **conexão de teste do**

## Connection Check

### Connection Parameters

Office 365 Email Address:

[Test Connection](#)



### Connection Status

Connected to Azure AD.  
Connection Successful.  
Inbox count of Messages are 0

[Done](#)

clique:

7. Uma vez que o status de conexão é bem sucedido, clique **feito** para terminar a verificação da conexão.
8. Finalmente, o clique **compromete** para salvar todas as alterações de configuração no ESA.