Configurar Como ajustes da caixa postal dos azuis celestes AD e do escritório 365 para o ESA

Índice

Introdução

Este documento fornece um passo a passo “Como” registrando um aplicativo novo em Windows Azure e obtendo os valores necessários, a fim terminar a configuração para ajustes da caixa postal do escritório 365 em uma ferramenta de segurança do email de Cisco (ESA). Isto está exigido quando um administrador ESA configura a auto remediação da caixa postal (MARÇO) para a proteção avançada do malware (ampère) nos ajustes da política do correio do ESA.

Pré-requisitos

Produtos Relacionados

Este documento aplica-se ao seguinte:

- Todo o ESA, hardware e corredor virtual 10.x e mais novo
- Toda a Segurança do email da nuvem (CES) ESA, 10.x e mais novo running

Requisitos

Este documento 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 eletrónico, 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 um host ou de um server de Windows.
- 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.

Você estará criando os seguintes quatro valores a fim configurar o conector da caixa postal ESA de volta aos azuis celestes AD:

1. Identificação de cliente
2. Inquilino ID
3. Thumbprint
4. Chave privada do certificado no formato do .pem

A fim construir estes valores exigidos, você precisará de terminar as etapas neste documento. Antes de começar, você precisará de executar o seguinte através de Windows Powershell:

1. **$cer = Novo-objeto System.Security.Cryptography.X509Certificates.X509Certificate2**
2. **$cer. Importação (de "_to_cert 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. **eco $base64Value**
9. **eco $base64Thumbprint**
10. **eco $keyid**

    Nota: Para #2, substitua de **"o _to_cert C:\path \ PEM_certificate.crt" com o** trajeto a seu certificado.

$base64Thumbprint = *Thumbprint*. Adicionar este valor a sua lista das condições prévias de valores exigidos.

Dica: Tenha por favor a saída salvar localmente para *$base64Value*, *$base64Thumbprint*, e *$keyid*, porque serão exigidos mais tarde nas etapas de configuração. Neste tempo, você é

feito com o .crt do certificado. Tenha por favor o .pem associado de seu certificado em um disponível, pasta local em seu computador.

Informações de Apoio

Microsoft permite o acesso a duas versões do portal dos azuis celestes:

- https://manage.windowsazure.com (portal clássico)
- https://portal.azure.com (portal novo)

Você pode alcançar “o portal clássico” do portal novo pela barra de ferramentas da mão esquerda, dos “diretório ativo seleto azuis celestes” > portal clássico

Para fins deste documento, o registro e a configuração do aplicativo são feitos no portal novo. As etapas a usar “o portal clássico” são incluídas na extremidade deste documento. (Microsoft pode escolher em algum dia desabilitar o portal clássico dos azuis celestes.)

Configurar Como ajustes da caixa postal dos azuis celestes AD e do escritório 365 para o ESA

Registrar um aplicativo novo nos azuis celestes

1. Alcance a interface do utilizador dos azuis celestes: https://portal.azure.com/
2. A barra de menus da mão esquerda, clica **mais > SEGURANÇA dos serviços + IDENTIDADE: Registros do App**
3. Da placa dos registros do App, clique **+Add**
4. Crie um nome para seu app
5. Para o tipo de aplicativo, saa como a **Web app/API**
6. Para Sinal-na URL, use o seguinte formato: https://*<company_domain.com>/ManualRegistration*Nota: *<company_domain.com> é o* domínio de seu O365 onde os usuários de domínio podem ingressar e alcançar seu domínio O365.
7. O clique **cria**

Ajuste as permissões exigidas para o aplicativo

1. Clique sobre do “o nome indicador” associado para o app que você apenas se registrou
2. Na placa dos ajustes, para o acesso API, o clique **exigiu permissões**
3. Clique **+Add**
4. “Adicionar na placa do acesso API”, clique **selecionam um API**
5. “Na placa selecione e API”, **Online da troca do escritório 365 do** clique **(o Microsoft Exchange)**
6. Na parte inferior do clique da página **selecione**
7. Para permissões do aplicativo selecione:
   • Use serviços de Web da troca com acesso direto a todas as caixas postais
   • Envie o correio como todo o usuário
   • Leia e escreva o correio em todas as caixas postais
8. Para permissões Delegated selecione:

- Envie o correio como um usuário
- Leia e escreva o correio do usuário
- Leia o correio do usuário
- Alcance caixas postais como o usuário ingressado através dos serviços de Web da troca

9. Clique **seleto na** parte inferior da página, isto fechará “selecionam a placa API”
10. Clique **feito na** parte inferior da página, isto fechará “adicionam a placa do acesso API”
11. Clique **permissões de Grant**
12. Quando alertado “faça você querem conceder as permissões abaixo para o myESA para todas as contas no diretório atual? Esta ação atualizará todas as permissões que existentes este aplicativo já tiver que combinar o que está listado abaixo. ”, clique **sim**

Você agora deve ter dois API alistado, de “diretório ativo Windows Azure” e do “Online da troca escritório 365”.

Você precisará de retornar à placa registrada do app para continuar com a próxima seção:

1. Clique “X” para fechar “exigiu a placa das permissões”
2. Clique o “X para fechar placa “dos ajustes a”

Você está agora para trás na placa registrada do app.

Prepare o manifesto para o aplicativo

Edite manifesto

1. Da placa registrada do app, clique manifesto na barra de ferramentas
2. Você é apresentado o completo manifesta no editor. A linha 12 deve ser “keyCredentials”. Você estará substituindo SOMENTE a linha 12 com o seguinte: `"keyCredentials": [`

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

3. Você precisará de substituir $base64Thumbprint, $keyid, e $base64Value com seus valores Deixe as citações ("") em torno de TODOS OS valores, como mostradoPague a atenção especial que cada valor é SOMENTE 1 linha, incluindo o $base64Thumbprint
4. Clique a **salvaguarda** para atualizar seu aplicativo. Você deve ver “a observação do aplicativo com sucesso actualizado” na área da barra de ferramentas.

Você precisará de retornar à placa registrada do app para continuar com a próxima seção:

O clique “X” para fechar “edita” a placa manifesta.

(Opcional) transfira o manifesto

> Dica: Você pode saltar a transferência manifesta e a transferência de arquivo pela rede manifesta se você podia com sucesso usar o editor dos em-azuis celestes para o manifesto. Se não, e você precisa de editar manualmente o manifesto, continue por favor.

1. Da placa registrada do app, clique manifesto na barra de ferramentas
2. **Na transferência** manifesta do clique do menu da edição
3. Salvar o manifesto ao diretório que contém seu certificado. Isto salvar o manifesto no formato .json localmente a seu computador.
4. Usando um editor local (Wordpad++, átomo, etc.), termine etapas 2 e 3 do “editam” a seção manifesta deste documento
5. Salvar o arquivo manifesto .json localmente

(Opcional) transfira arquivos pela rede o manifesto

Se você escolheu transferir e editou o manifesto manualmente, você precisará de transferir arquivos pela rede o manifesto editado:

1. Retorne a seu navegador e ao portal dos azuis celestes
2. **A transferência de arquivo pela rede do** clique do “edita” a placa manifesta

Você precisará de retornar à placa registrada do app para continuar com a próxima seção:

O clique “X” para fechar “edita” a placa manifesta.

Obtenha a identificação de cliente para o aplicativo

1. Do app registrado encontre o “ID de aplicativo”
2. Copie o ID de aplicativo (ID de aplicativo = a *identificação de cliente*)
3. Adicionar este valor a sua lista das condições prévias de valores exigidos.

Obtenha o valor do inquilino ID para o aplicativo

1. Do “da placa dos registros App”, clique sobre “valores-limite” e selecione a primeira linha para o DOCUMENTO dos METADATA da FEDERAÇÃO
2. A cópia e cola a linha a um editor externo
3. Você quererá recuperar o *inquilino ID*, que é o string de ID após “https://login.windows.net/”
4. Adicionar este valor a sua lista das condições prévias de valores exigidos.

Exemplo:

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

Para este exemplo, o inquilino ID será "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Verifique os valores exigidos

Seus valores são terminados agora. Você deve poder preencher os seguintes valores:

- Identificação de cliente

- Inquilino ID
- Thumbprint (veja condições prévias)
- Certificate a chave privada no formato do .pem (veja condições prévias)

Você está pronto para terminar os ajustes da caixa postal do escritório 365 configurando estes valores no ESA.

Configurar o ESA

1. No ESA GUI: **Os ajustes da administração do sistema > da caixa postal > editam ajustes…**
2. Entre em seus valores da seção anterior (identificação de cliente, inquilino ID, Thumbprint)
3. Carregue o certificado salvar (o .pem)
4. O clique **submete-se**
5. Você verá que “os ajustes estiveram configurados com sucesso. Você deve comprometer as mudanças e testar a conexão.”
6. Do canto superior do assistente, o clique **compromete mudanças** antes de todos os testes
7. Clique da “conexão verificação…” e entre em um bom, endereço email trabalhando conhecido associado com seu domínio O365
8. Clique a “conexão de teste”

Você deve receber resultados do sucesso no status de conexão:

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

Pesquisando defeitos o ESA

Se você não está vendo que os resultados bem sucedidos para o status de conexão testam, você pode desejar rever o registro do aplicativo executado dos azuis celestes AD.

Do ESA, ajuste os logs de MARÇO ao nível de rastreamento e reexamine a conexão.

Para conexões mal sucedidas, os logs podem mostrar similar a:

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

Confirme o ID de aplicativo, o diretório ID (que é o mesmo que o inquilino ID), ou outros identificadores associados do log com seu aplicativo nos azuis celestes AD. Se você é un-certo dos valores, suprima do aplicativo do portal dos azuis celestes AD e comece-o sobre.

Para a conexão bem sucedida, os logs devem ser similares a:

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

Pesquisando defeitos os azuis celestes AD

> Nota: O tac Cisco e o apoio de Cisco não são autorizados a pesquisar defeitos edições de lado do cliente com Microsoft Exchange, Microsoft Azure AD, ou escritório 365.

Para edições de lado do cliente com Microsoft Azure AD, você precisará de contratar Microsoft apoia. Veja por favor da “a opção ajuda + do apoio” de seu painel do Microsoft Azure. Você pode poder abrir pedidos do suporte direto ao apoio de Microsoft do painel.

(Opcional) como criar e configurar um aplicativo nos azuis celestes usando o portal clássico

> Nota: Você não precisa de terminar este se você podia com sucesso usar o portal dos azuis celestes por https://portal.azure.com de acesso (portal novo). Isto é provido somente para o administrador dos azuis celestes que escolhe usar ainda “o portal clássico”. Se você deseja usar esta versão do portal dos azuis celestes AD, encontre por favor as seguintes instruções passo a passo para terminar os valores exigidos:

Adicionar um aplicativo

1. Entre ao Microsoft Azure.
2. Da barra de menus da mão esquerda, navegue a **TODOS OS ARTIGOS**
3. Clique sobre o nome do recurso para seu domínio
4. Das abas da ferramenta sob seu nome do recurso, selecione **APLICATIVOS**
5. Da área inferior da barra de ferramentas, o clique **ADICIONA**
6. Quando apresentado *“que você quer fazer? ”*, seleto **adicionar um aplicativo que minha organização está desenvolvendo**
7. Termine “*dizem-nos sobre a* informação do *seu aplicativo*”: Crie um nome para seu appPara o tipo de aplicativo, saa como o **aplicativo de web e/ou a Web API**Clique sobre a seta para continuar
8. Termine as propriedades do App: Para SINAL-na URL, use o seguinte formato: https:// *<company_domain.com>/ManualRegistration*Nota: *<company_domain.com> é o* domínio de seu O365 onde os usuários de domínio podem ingressar e alcançar seu domínio O365.Para o ID de APP URI, use o seguinte formato:
   https:// <company_domain.com>Clique o sinal para terminar

Configurar seu aplicativo

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**
2. **A identificação de cliente** é alistada nesta tela. Copie e adicionar este valor a sua lista das condições prévias de valores exigidos.
3. Rolo à parte inferior da tela para ver “permissões a outros aplicativos”.
4. O clique **adiciona o aplicativo O Online** seleto da **troca do escritório 365** e clica a verificação para continuarPara **permissões do aplicativo**, seleto: **Leia e escreva o correio em todas as caixas postaisEnvie o correio como todo o usuárioUse serviços de Web da troca com acesso direto…**Para permissões Delegated, seleto: **Envie o correio como um usuárioLeia e escreva o correio do usuárioLeia o correio do usuárioAlcance caixas postais como o usuário ingressado através da troca**
5. Clique a **salvaguarda da** barra de ferramentas inferior para salvar todo o trabalho e configuração para o aplicativo de web feito sob encomenda

Controle 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. Localmente, encontre o arquivo .json e abra-o com um editor de texto. (Notepad++ preferível, átomo, etc.)
4. Procure e encontre a linha dos “keyCredentials”
5. Substituindo esta linha única com as seguintes múltiplas linhas, personalizando usando o *$base64Thumbprint*, o *$keyid*, e o *$base64Value*: `"keyCredentials": [`
```
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```
6. Ao incorporar o *$base64Value*, isto é exigido ser editado a um valor da linha única
7. Salvar o arquivo .json localmente
8. Retorne a seu navegador e ao portal do Microsoft Azure
9. O clique **CONTROLA MANIFESTO > transferência de arquivo pela rede manifesta**
10. Consulte e encontre o arquivo editado .json
11. Selecione a marca de verificação para terminar a transferência de arquivo pela rede

Encontrando o inquilino ID

1. Da barra de ferramentas inferior, clique sobre **VALORES-LIMITE da VISTA** para ver os valores-limite integrados no Microsoft Azure AD
2. Selecione a primeira linha para o DOCUMENTO dos METADATA da FEDERAÇÃO
3. A cópia e cola a linha a um editor externo
4. Você quererá recuperar o *inquilino ID*, que é o string de ID após “https://login.windows.net/”

5. Adicionar este valor a sua lista das condições prévias de valores exigidos

Exemplo:

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

Para este exemplo, o inquilino ID será "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Informações Relacionadas

- Automaticamente mensagens de Remediating em caixas postais do escritório 365