Como configurar as definições da conta de e-mail seguro da Cisco para a API do Microsoft Azure (Microsoft 365)

Contents

Introduction

Este documento fornece um "como" passo a passo para registrar um novo aplicativo no Microsoft Azure (Azure Ative Diretory) para gerar as credenciais necessárias de ID do cliente, ID do espaço e Cliente e, em seguida, a configuração para Configurações de conta em um Cisco Secure Email Gateway ou Cloud Gateway. A configuração das configurações da conta e do perfil da conta associado são necessárias quando um administrador de e-mail configura a Mailbox Auto Remediation (MAR) para Advanced Malware Protection (AMP) ou a filtragem de URL ou utiliza a ação de correção do rastreamento de mensagens no Cisco Secure Email e Web Manager ou no Cisco Secure Gateway/Cloud Gateway.

Fluxo do processo de correção automática da caixa de correio

Um anexo (arquivo) em seu e-mail ou URL pode ser pontuado como mal-intencionado a qualquer momento, mesmo depois de ter alcançado a caixa de correio de um usuário. A AMP no Cisco Secure Email (via Cisco Secure Malware Analytics) pode identificar esse desenvolvimento à medida que novas informações surgem e enviará alertas retrospectivos para o Cisco Secure Email. O Cisco Talos oferece o mesmo com análise de URL, a partir do AsyncOS 14.2 para o Cisco Secure Email Cloud Gateway. Se sua empresa estiver usando o Microsoft 365 para gerenciar caixas de correio, você poderá configurar o Cisco Secure Email para executar ações de correção automática nas mensagens na caixa de correio do usuário quando esses vereditos de ameaça mudarem.

O Cisco Secure Email se comunica de forma segura e direta com o Microsoft Azure Ative Diretory para obter acesso às caixas de correio do Microsoft 365. Por exemplo, se um e-mail com um anexo for processado pelo gateway e digitalizado pela AMP, o anexo do arquivo (SHA256) será fornecido à AMP para obter a reputação do arquivo. A disposição da AMP pode ser marcada como Limpa (etapa 5, Figura 1) e então entregue à caixa de correio Microsoft 365 do destinatário final. Posteriormente, a disposição da AMP é alterada para Mal-intencionada, o Cisco Malware Analytics envia uma atualização de veredito retrospectivo (etapa 8, Figura 1) para *qualquer* gateway que processou esse SHA256 específico. Quando o gateway receber a atualização de veredito retrospectivo de mal-intencionado (se configurado), ele executará uma das seguintes ações de correção automática de caixa de correio (MAR): Encaminhar, Excluir ou Encaminhar e Excluir.

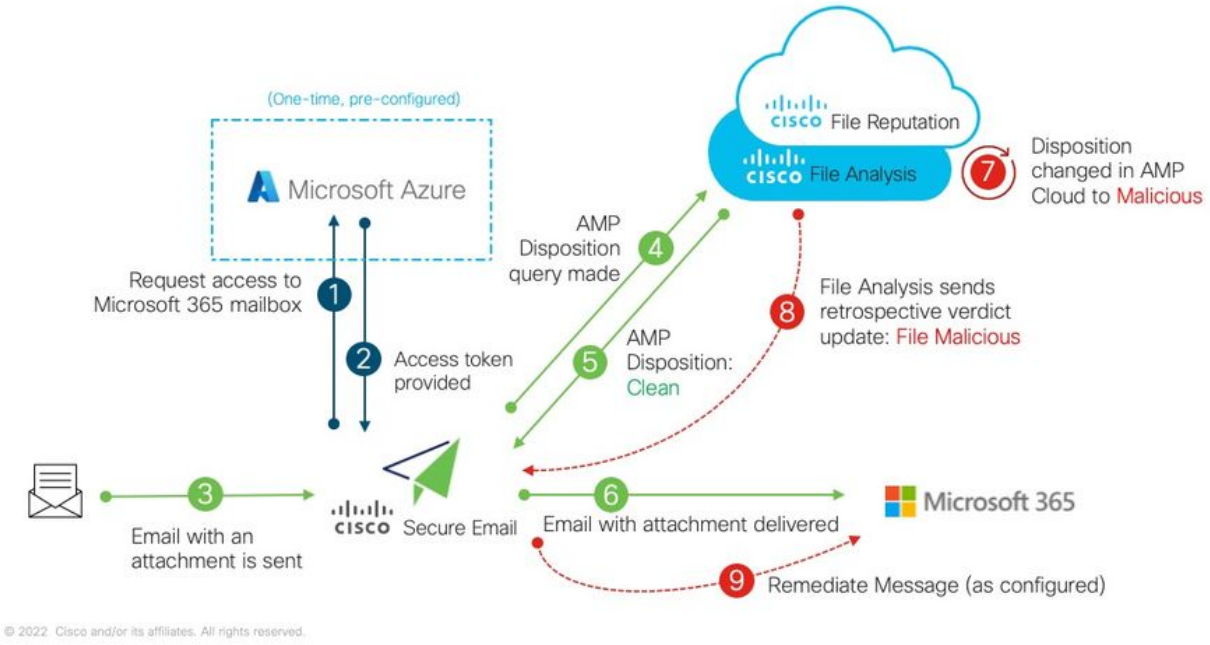

Figura 1: MAR (para AMP) no Cisco Secure Email

Este guia trata de como configurar o Cisco Secure Email com o Microsoft 365 somente para correção automática de caixa de correio. A AMP (File Reputation and File Analysis) e/ou a filtragem de URL no gateway já devem estar configuradas. Para obter mais detalhes sobre Reputação de arquivos e Análise de arquivos, consulte o Guia do usuário para obter a versão do AsyncOS que você implantou.

Prerequisites

1. Assinatura de conta do Microsoft 365 (Certifique-se de que a subscrição de conta do Microsoft 365 inclui acesso ao Exchange, como uma conta Enterprise E3 ou Enterprise E5.)

2. Conta de administrador do Microsoft Azure e acesso a http://portal.azure.com

3. As contas do Microsoft 365 e do Microsoft Azure AD estão vinculadas corretamente a um endereço de e-mail "user@domain.com" ativo e você pode enviar e receber e-mails por meio desse endereço de e-mail.

Você criará os seguintes valores para configurar a comunicação da API do gateway de e-mail seguro da Cisco para o Microsoft Azure AD:

- **ID do cliente**
- **ID do usuário**
- **Segredo do cliente**

  Note: A partir do AsyncOS 14.0, **Configurações de Conta** permite a configuração usando um segredo de Cliente ao criar o Registro de Aplicativo do Microsoft Azure. Esse é o método mais fácil e preferido.

Opcional - Se você NÃO estiver utilizando o segredo do cliente, precisará criar e ter pronto:

- **Impressão digital**
- **A chave privada (arquivo PEM)**

A criação da thumbprint e da chave privada é abordada no Apêndice deste guia:

1. Um certificado público (ou privado) ativo (CER) e a chave privada usada para assinar o certificado (PEM), ou a capacidade de criar um certificado público (CER) e a capacidade de salvar a chave privada usada para assinar o certificado (PEM). A Cisco fornece dois métodos neste documento para fazer isso com base na sua preferência de administração: Certificado: Unix/Linux/OS X (utilizando OpenSSL)Certificado: Windows (utilizando o PowerShell)

2. Acesso ao Windows PowerShell, geralmente administrado a partir de um Windows Host ou Servidor - ou- acesso ao aplicativo Terminal via Unix/Linux

Para criar esses valores necessários, você precisará concluir as etapas fornecidas neste documento.

Registrar um aplicativo do Azure para uso com o Cisco Secure Email

Registro de aplicativos

Iniciar sessão no seu [Portal do Microsoft Azure]

1. Clique em **Azure Ative Diretory** (Figura 2)
2. Clique em **Registros de aplicativos**
3. Clique em **+ Novo registro**
4. Na página "Registrar um aplicativo":
    a. Nome: **Cisco Secure Email MAR** (ou o nome de sua escolha)
    b. Tipos de conta suportados: **Apenas contas neste diretório organizacional (Nome da conta)**
    c. URI de redirecionamento: (opcional)
    [Nota: Você pode deixar isso em branco ou ficar à vontade para usar https://www.cisco.com/sign-on para preencher]
    d. Na parte inferior da página, clique em **Registrar**

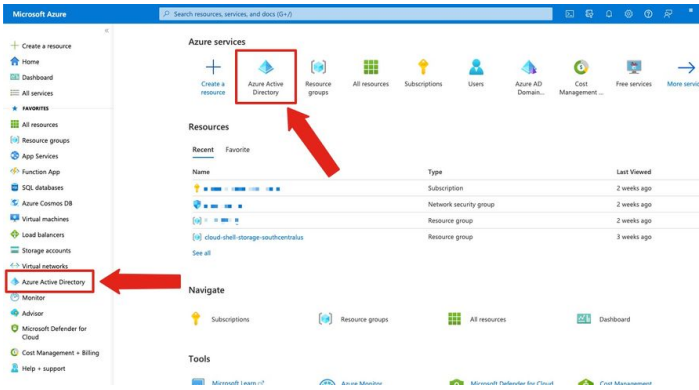

Figura 2: exemplo do Portal do Microsoft Azure

Depois de concluir as etapas acima, você verá seu aplicativo:

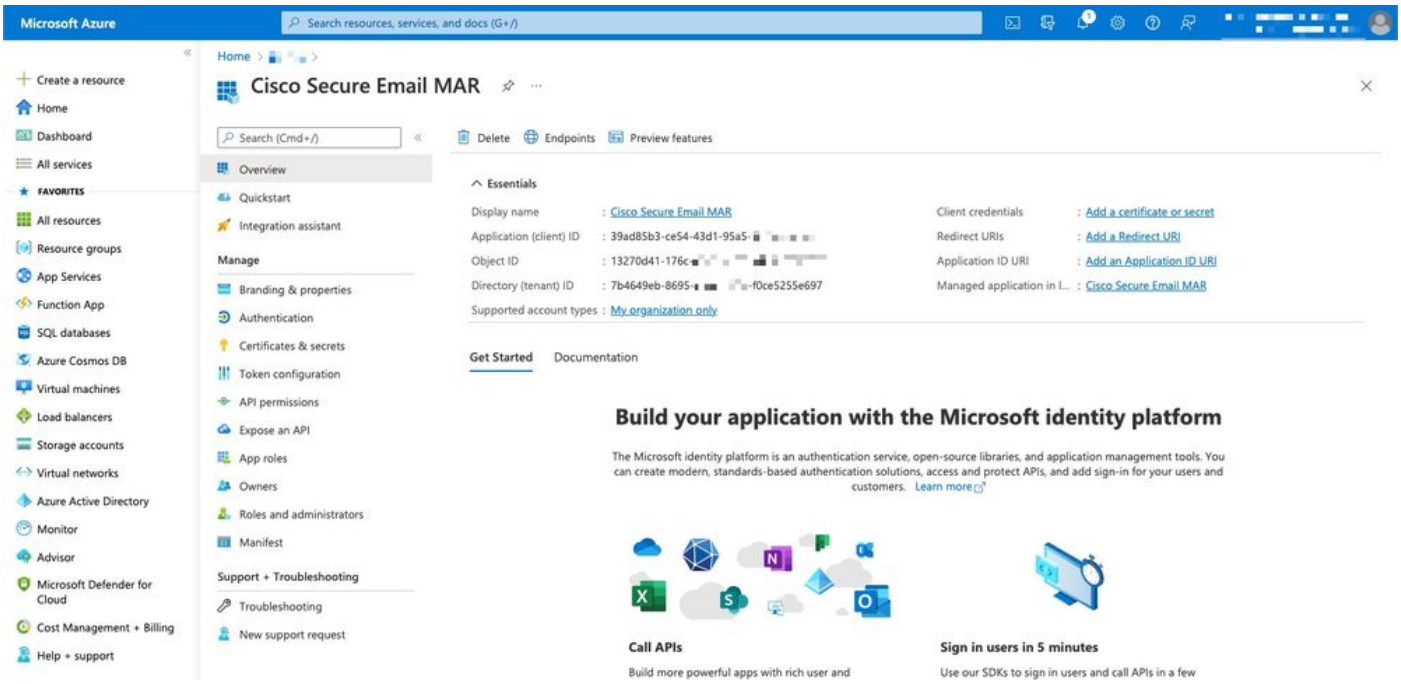

Figura 3: página do aplicativo do Microsoft Azure Ative Diretory

Certificados e segredos

Se você estiver executando o AsyncOS 14.0 ou posterior, a Cisco recomenda configurar seu aplicativo Azure para utilizar um segredo de cliente. No painel do aplicativo, nas opções Gerenciar:

1. Selecionar **certificados e segredos**

2. Na seção ***Segredos do cliente***, clique em **+ Novo segredo do cliente**

3. Adicione uma descrição para ajudar a identificar para que serve esse segredo de cliente, por exemplo "Correção de e-mail seguro da Cisco"

4. Selecionar um período de expiração

5. Clique em Add

6. Passe o mouse sobre à direita do valor gerado e clique no ícone **Copiar para a área de transferência**

7. Salve esse valor em suas anotações, observe isso como "segredo do cliente"

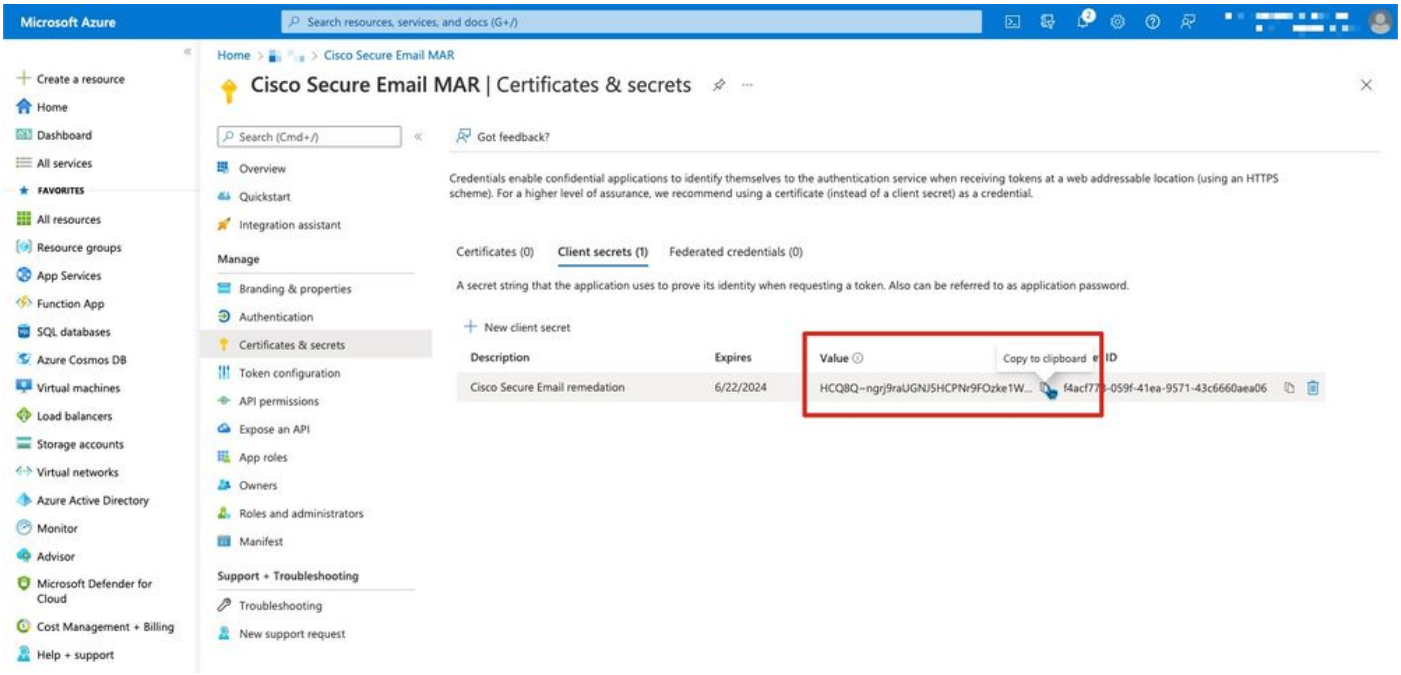

Figura 4: exemplo de criação de segredo de cliente do Microsoft Azure

> **Note**: Quando você sai da sessão ativa do Microsoft Azure, o valor do segredo do cliente que acabou de gerar *** sairá do valor. Se você não gravar e proteger o valor antes de sair, precisará recriar o segredo do cliente para ver a saída de texto claro.

Opcional - Se você não estiver configurando seu aplicativo do Azure com um segredo de cliente, configure seu aplicativo do Azure para usar seu certificado. No painel do aplicativo, nas opções Gerenciar:

1. Selecionar **certificados e segredos**
2. Clique em **Carregar certificado**
3. Selecione o arquivo CRT (conforme criado anteriormente)
4. Clique em Add

Permissões de API

Note: Começando no AsyncOS 13.0 para segurança de e-mail, as permissões de API para o Microsoft Azure para a comunicação de e-mail seguro da Cisco precisavam ser alteradas do uso do Microsoft Exchange para o Microsoft Graph. Se você já tiver configurado o MAR e estiver atualizando seu gateway de e-mail seguro da Cisco para o AsyncOS 13.0, basta atualizar/adicionar as novas permissões de API. (Se estiver executando uma versão mais antiga do AsyncOS, 11.x ou 12.x, consulte o Apêndice B antes de continuar.)

No painel do aplicativo, nas opções Gerenciar:

1. Selecionar **permissões de API**
2. Clique em **+ Adicionar uma permissão**
3. Selecionar **Microsoft Graph**
4. Selecione as permissões abaixo em ***Permissões de Aplicativo***: Email > "Mail.Read" (Leia o e-mail em todas as caixas de correio)E-mail > "Mail.ReadWrite" (E-mail de leitura e gravação em todas as caixas de correio)E-mail > "Mail.Send" (Enviar e-mail como qualquer usuário)Diretório > "Diretory.Read.All" (Ler dados do diretório) [*Opcional: Se estiver usando a sincronização LDAP Connector/LDAP, habilite. Caso contrário, isso não é obrigatório.]
5. *Opcional:* Você verá que o Microsoft Graph por padrão está habilitado para permissões "User.Read"; você pode deixá-lo configurado ou clicar em **Ler** e clicar em **Remover permissão** para removê-lo das permissões de API associadas ao aplicativo.
6. Clique em **Adicionar permissões** (ou **Atualizar permissões**, se o Microsoft Graph já estiver listado)
7. Finalmente, clique em **Conceder consentimento do administrador para...** para garantir que suas novas permissões sejam aplicadas ao aplicativo
8. Haverá um pop-up no painel que pergunta:
   "*Deseja conceder o consentimento para as permissões solicitadas para todas as contas no <Nome do Azure>? Isso atualizará todos os registros de consentimento do administrador existentes que este aplicativo já tiver que corresponder ao que está listado abaixo.*"

   Clique em Sim

Nesse ponto, você verá uma mensagem de êxito verde e a coluna "Admin Consent Required" será exibida.

Obtendo a ID do cliente e a ID do usuário

No painel do aplicativo, nas opções Gerenciar:

1. Clique em **Visão geral**
2. Passe o mouse à direita de sua ID do aplicativo (cliente) e clique no ícone **Copiar para a área de transferência**
3. Salve esse valor em suas anotações, observe isso como "ID do cliente"
4. Passe o mouse à direita da ID do diretório (locatário) e clique no ícone **Copiar para a área de transferência**
5. Salve esse valor em suas anotações, observe isso como "ID do espaço"

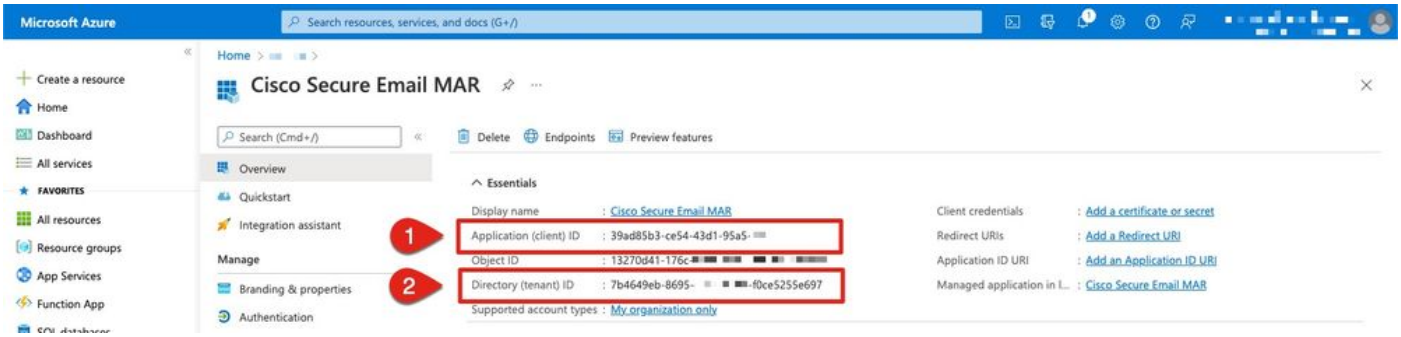

Figura 5: Microsoft Azure... ID do cliente, exemplo de ID do espaço

Configurando o Cisco Secure Email Gateway/Cloud Gateway

Neste momento, você deve ter os seguintes valores preparados e salvos em suas anotações:

- **ID do cliente**
- **ID do usuário**
- **Segredo do cliente**

Opcional, se não estiver usando o segredo do cliente:

- **Impressão digital**
- **A chave privada (arquivo PEM)**

Você está pronto para usar os valores criados das suas anotações e configurar as configurações da conta no gateway do Cisco Secure Email!

Criar perfil de conta

1. Faça login no seu gateway
2. Navegue até **Administração do sistema > Configurações da conta** Note: Se você estiver executando uma versão anterior ao AsyncOS 13.x, será **Administração do sistema > Configurações da caixa de correio**
3. Clique em **Ativar**
4. Clique na caixa de seleção Enable Account Settings (Ativar configurações da conta) e clique em **Submit (Enviar)**
5. Clique em **Criar perfil de conta**
6. Forneça um nome de perfil e uma descrição (algo que descreverá exclusivamente sua conta se você tiver vários domínios)
7. Àmedida que estiver definindo uma conexão com o Microsoft 365, deixe o tipo de perfil como **Office 365 / Hybrid (Graph API)**
8. Digite sua **ID do cliente**
9. Digite sua **ID do Espaço**
10. Para credenciais do Cliente, proceda de uma das seguintes maneiras, conforme

configurado no Azure: Clique em **Segredo do cliente** e cole no segredo do cliente configurado ou...Clique em **Certificado do cliente** e digite na Impressão digital e também forneça a PEM clicando em "Escolher arquivo"

11. Clique em Submit
12. Clique em **Confirmar alterações** no canto superior direito da interface do usuário
13. Insira qualquer comentário e conclua as alterações de configuração clicando em **Confirmar alterações**

Verificar conexão

A próxima etapa é verificar apenas a conexão API do gateway do Cisco Secure Email para o Microsoft Azure:

1. Na mesma página Detalhes da conta, clique em **Testar conexão**
2. Insira um endereço de e-mail válido para o domínio gerenciado na sua conta do Microsoft 365
3. Clique em **Testar conexão**
4. Você deve receber uma mensagem de êxito (Figura 6)
5. Clique em **Concluído** para concluir

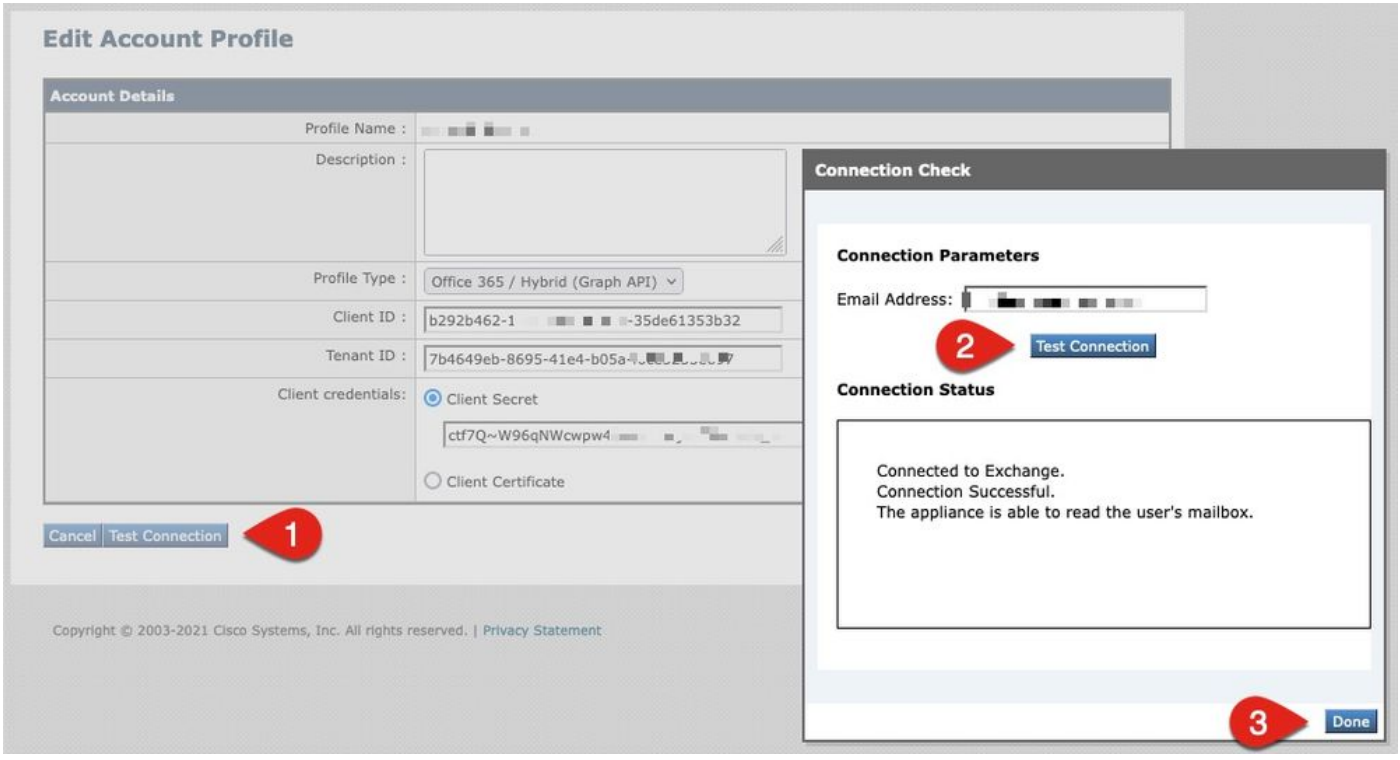

Figura 6: Exemplo de verificação de perfil/conexão da conta

6. Na seção *Mapeamento de domínio*, clique em **Criar mapeamento de domínio**

7. Digite o(s) nome(s) de domínio associado(s) à conta Microsoft 365 para a qual você acabou de validar a conexão API

A seguir, uma lista de formatos de domínio válidos que podem ser usados para mapear um perfil de caixa de correio:

- O domínio pode ser a palavra-chave especial 'ALL' para corresponder todos os domínios a fim de criar um mapeamento de domínio padrão.

- Nomes de domínio como 'example.com' - Corresponde a qualquer endereço com este domínio.

- Nomes de domínio parciais como '@.partial.example.com' - Corresponde a qualquer endereço que termine com este domínio

- Vários domínios podem ser inseridos usando uma lista separada por vírgulas de domínios.

8. Clique em Submit

9. Clique em **Confirmar alterações** no canto superior direito da interface do usuário

10. Insira qualquer comentário e conclua as alterações de configuração clicando em **Confirmar alterações**

Ativar a correção automática de caixa de correio (MAR) para proteção avançada contra malware na política de correio

Conclua esta etapa para ativar o MAR na configuração do AMP para políticas de e-mail.

1. Navegue até **Políticas de e-mail > Políticas de recebimento de e-mail**
2. Clique nas configurações na coluna Proteção avançada contra malware para o nome da política que deseja configurar (ex., Figura 7):

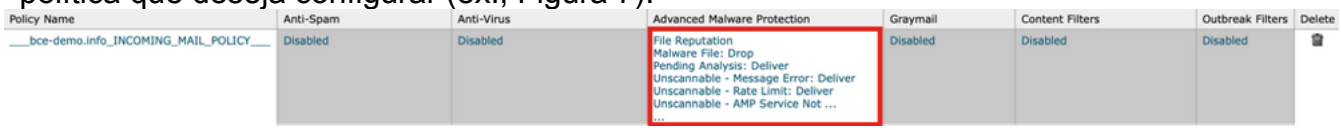

Figura 7: Habilitar MAR (políticas de e-mail de entrada)

3. Role até a parte inferior da página
4. Clique na caixa de seleção para Ativar a correção automática da caixa de correio (MAR)
5. Selecione uma das seguintes ações que deseja executar para MAR (ex., Figura 8): Encaminhar para: <*inserir no endereço de email*>excluirEncaminhar para: <*digite o endereço de email*> e exclua

Figura 8: Ativar MAR para exemplo de configuração de AMP

6. Clique em Submit
7. Clique em **Confirmar alterações** no canto superior direito da interface do usuário
8. Insira qualquer comentário e conclua as alterações de configuração clicando em **Confirmar alterações**

Ativar a correção automática de caixa de correio (MAR) para filtragem de URL

Começando com AsyncOS 14.2 para o Cisco Secure Email Cloud Gateway, a filtragem de URL agora inclui URL Retrospectiva Veredito e correção de URL.

1. Navegue até **Serviços de segurança > Filtragem de URL**
2. Se ainda não tiver a Filtragem de URL configurada, clique em **Ativar**
3. Clique na caixa de seleção "Habilitar categoria de URL e filtros de reputação"
4. As *configurações avançadas* com as configurações padrão
5. Clique em Submit

A filtragem de URL deve ser semelhante à seguinte:

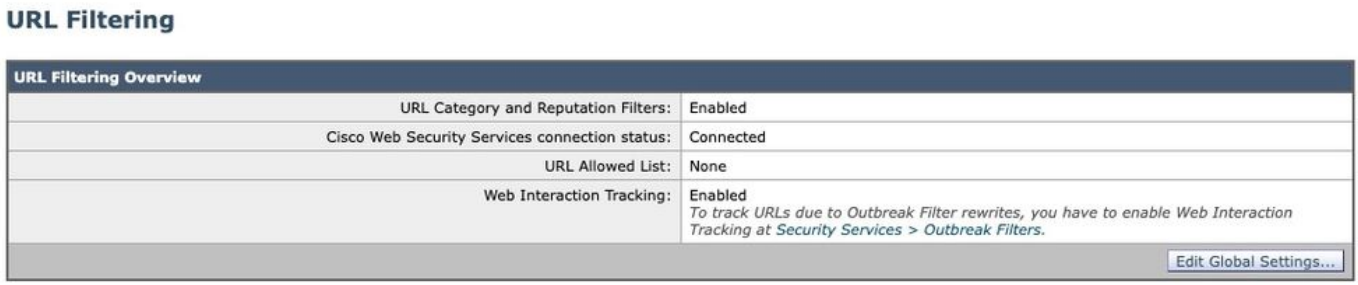

Figura 9: Exemplo de filtragem de URL pós-ativação

Para ver a retrospecção de URL com filtragem de URL interna, execute o seguinte procedimento ou abra um caso de suporte para que a Cisco execute:

```
esa1.hcxxyy-zz.iphmx.com> urlretroservice enable

URL Retro Service is enabled.

esa1.hcxxyy-zz.iphmx.com> websecurityconfig

URL Filtering is enabled.
No URL list used.
```

```
Web Interaction Tracking is enabled.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Unavailable

Disable URL Filtering? [N]>

Do you wish to disable Web Interaction Tracking? [N]>

Do you wish to add URLs to the allowed list using a URL list? [N]>


Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.

Do you wish to enable Mailbox Auto Remediation action? [N]> y

URL Retrospective service based Mail Auto Remediation is enabled.

Please select a Mailbox Auto Remediation action:
1. Delete
2. Forward and Delete
3. Forward
[1]> 1

esa1.hcxxyy-zz.iphmx.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Mar 29 19:43:48 2022 EDT
```

Depois de concluir, atualize sua IU na página Filtragem de URLs e você deverá ver o seguinte:

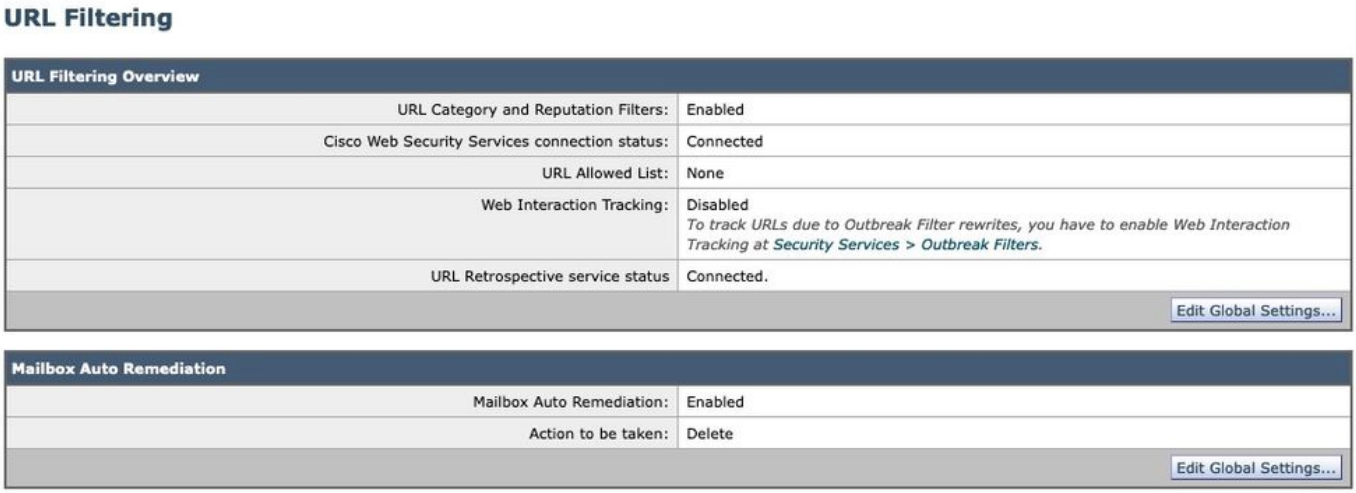

Figura 10: Filtragem de URL (AsyncOS 14.2 para Cisco Secure Email Cloud Gateway)

A proteção de URL agora está pronta para executar ações corretivas quando um veredito altera a pontuação. Para obter mais informações, consulte Proteção contra URLs mal-intencionados ou indesejáveis no Guia do usuário do AsyncOS 14.2 para Cisco Secure Email Cloud Gateway.

Configuração concluída!

Neste momento, o Cisco Secure Email está pronto para avaliar continuamente ameaças emergentes à medida que novas informações se tornam disponíveis e notificar você sobre os arquivos que são considerados ameaças depois que eles entrarem na sua rede.

Quando um veredito retrospectivo é produzido a partir da Análise de arquivo (Cisco Secure Malware Analytics), uma mensagem de informação é enviada ao administrador do Email Security (se configurado). Exemplo:

```
The Info message is:

Retrospective verdict received for Book1.xls.

SHA256: 7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b
Timestamp: 2019-06-03T23:40:36Z
Verdict: MALICIOUS
Spyname: W32.7D06FD224E-95.SBX.TG

Total users affected: 1
----------- Affected Messages ---------------


Message 1
   MID              : 348938
   Subject          : [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]test Mon, 03 Jun 2019 16:50:18 -0400
   From             :
   To               :
   File name        : Book1.xls
   Parent SHA256    : unknown
   Parent File name : unknown
   Date             : 2019-06-03T20:52:33Z

------------------------------------------------


Version: 12.1.0-087
Serial Number: 420DE3B51AB744C7F092-9F0
Timestamp: 04 Jun 2019 04:40:36 +0500
```

A correção automática de caixa de correio será considerada como configurada se for configurada em relação à política de correio.

Exemplos de relatório de correção automática de caixa de correio

Os relatórios para qualquer SHA256 que tenha sido corrigido estarão no relatório de correção automática de caixa de correio disponível no gateway de e-mail seguro da Cisco e no Cisco Secure Email e Web Manager.

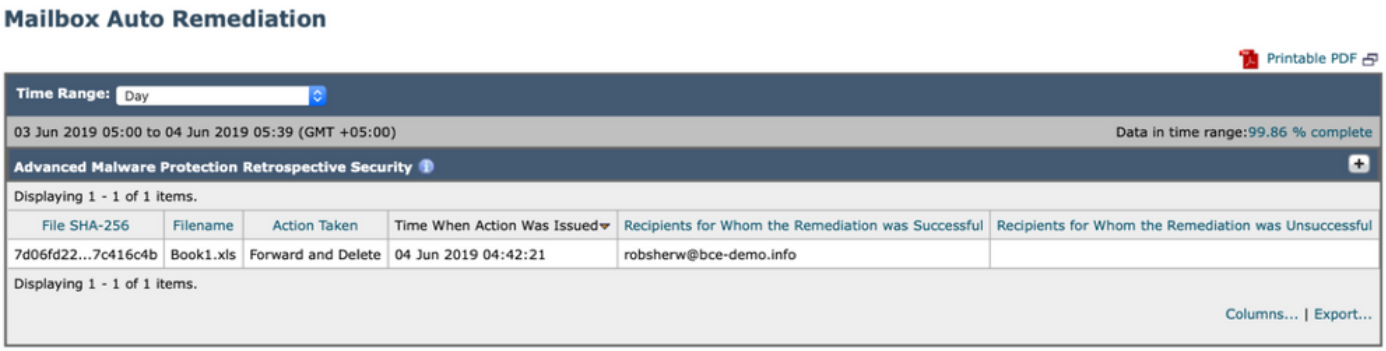

Figura 11: Relatório de correção automática de caixa de correio (IU antiga)

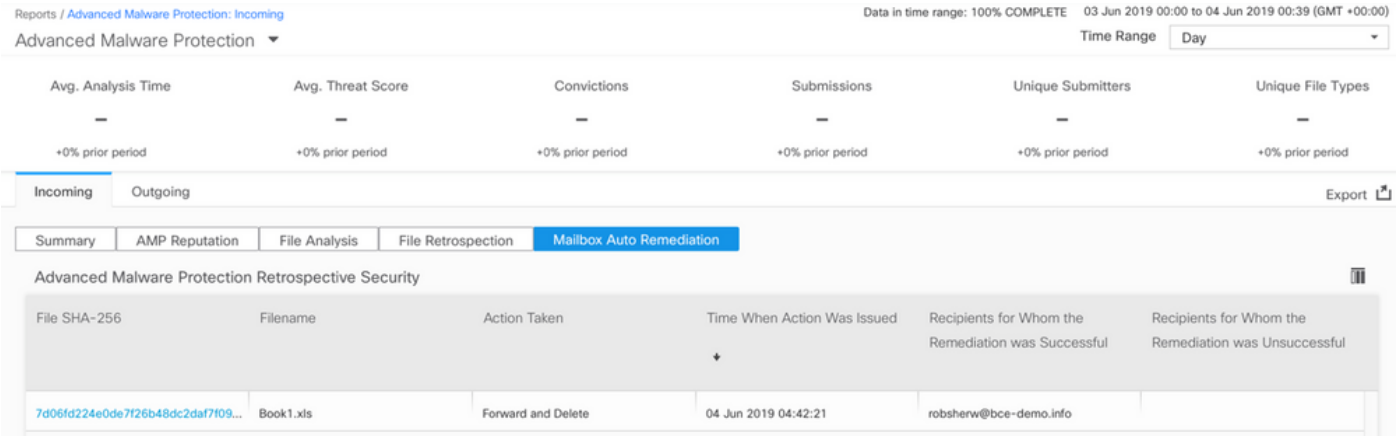

Figura 12: (UI NG) Relatório de correção automática de caixa de correio

Registro de correção automática da caixa de correio

A correção automática da caixa de correio tem um registro individual, "mar". Os registros de Correio Automático da Caixa de Correio conterão todas as atividades de comunicação entre o gateway do Cisco Secure Email e o Microsoft Azure, Microsoft 365.

Um exemplo dos registros de marca:

```
Mon May 27 02:24:28 2019 Info: Version: 12.1.0-087 SN: 420DE3B51AB744C7F092-9F0000000000
Mon May 27 02:24:28 2019 Info: Time offset from UTC: 18000 seconds
Fri May 31 01:11:53 2019 Info: Process ready for Mailbox Auto Remediation
Fri May 31 01:17:57 2019 Info: Trying to connect to Azure AD.
Fri May 31 01:17:57 2019 Info: Requesting token from Azure AD.
Fri May 31 01:17:58 2019 Info: Token request successful.
Fri May 31 01:17:58 2019 Info: The appliance is able to read the user's(robsherw@bce-demo.info)
mailbox.
Fri May 31 04:41:54 2019 Info: Trying to perform the configured action on MID:312391
SHA256:de4dd03acda0a24d0f7e375875320538952f1fa30228d1f031ec00870ed39f62 Recipient:robsherw@bce-
demo.info.
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938
SHA256:7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b Recipient:robsherw@bce-
demo.info.
```

```
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
```

Solução de problemas do Cisco Secure Email Gateway

Se você não estiver vendo resultados bem-sucedidos para o teste de status da conexão, talvez queira revisar o registro do aplicativo executado no Microsoft Azure AD.

A partir do gateway de e-mail seguro da Cisco, defina seus registros MAR para o nível 'trace' e teste novamente a conexão.

Para conexões malsucedidas, os registros podem mostrar como:

```
Thu Mar 30 16:08:49 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 16:08:49 2017 Info: Requesting token from Azure AD.
Thu Mar 30 16:08:50 2017 Info: Error in requesting token: AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
Thu Mar 30 16:08:50 2017 Info: Error while requesting token AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
```

Confirme a ID do aplicativo, a ID do diretório (que é igual à ID do espaço) ou outros identificadores associados do log com seu aplicativo no Azure AD. Se você não tiver certeza dos valores, exclua o aplicativo do portal do Azure AD e comece novamente.

Para uma conexão bem-sucedida, os registros devem ser semelhantes a:

```
Thu Mar 30 15:51:58 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 15:51:58 2017 Info: Requesting token from Azure AD.
Thu Mar 30 15:51:58 2017 Trace: command session starting
Thu Mar 30 15:52:00 2017 Info: Token request successful.
Thu Mar 30 15:52:00 2017 Info: The appliance is able to read the
user's(myuser@mydomain.onmicrosoft.com) mailbox.
```

Solução de problemas do Azure AD

Observação: o Cisco TAC e o Suporte da Cisco não têm o direito de solucionar problemas do lado do cliente com o Microsoft Exchange, o Microsoft Azure AD ou o Office 365.

Para problemas do lado do cliente com o Microsoft Azure AD, você precisará envolver o Suporte da Microsoft. Consulte a opção "Ajuda + suporte" no Painel do Microsoft Azure. Você pode abrir solicitações de suporte direto para o Suporte da Microsoft no painel.

Apêndice A

Observação: isso é obrigatório SOMENTE se você NÃO estiver utilizando o segredo do cliente para configurar seu aplicativo do Azure.

Criação de um certificado público e privado e um par de chaves

Dica: Salve a saída localmente para *$base64Value*, *$base64Thumbprint* e *$keyid*, pois elas serão necessárias posteriormente nas etapas de configuração. Tenha o .crt e o .pem associado do certificado em uma pasta local disponível no computador.

Note: Se já tiver um certificado (formato/padrão x509) e uma chave privada, ignore esta seção. Certifique-se de que você tenha arquivos CRT e PEM, pois eles serão necessários nas próximas seções!

Certificado: Unix/Linux (utilizando openssl)

Valores a serem criados:
Impressão digital •
Certificado • **público (arquivo CRT)**
Chave privada • **(arquivo PEM)**

Administradores que usam Unix/Linux/OS X, para a finalidade e a execução do script fornecido, é suposto que você tenha o OpenSSL instalado.

Note: Execute os comandos 'which openssl' e 'openssl version' para verificar a instalação do OpenSSL. Instale o OpenSSL se ele não estiver presente!

Consulte o seguinte documento para obter assistência: [Script de configuração do Azure AD para o Cisco Secure Email]

Do seu host (UNIX/Linux/OS X):

1. A partir de um aplicativo terminal, editor de texto (ou, no entanto, se estiver confortável em criar um script shell), crie um script copiando o seguinte: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. Colar o script
3. Certifique-se de tornar o script executável! Execute o seguinte comando: **chmod u+x my_azure.sh**
4. Executar o script: **./my_azure.sh**

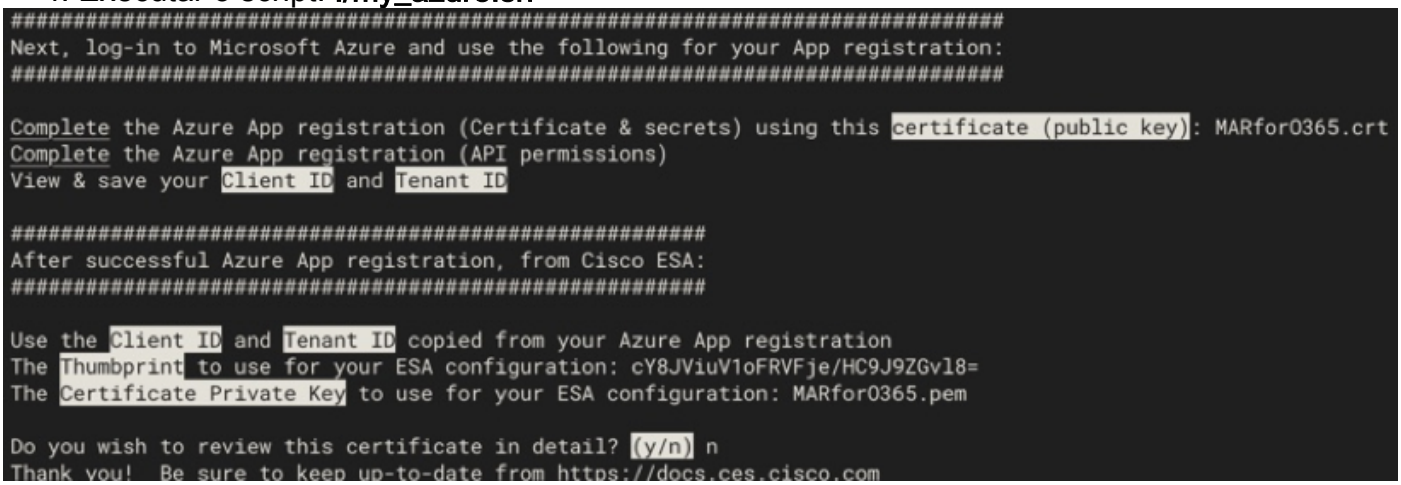

Figura 13: saída de tela do my_azure.sh

Como você vê na Figura 2, o script cria e chama o **Certificado Público (arquivo CER)** necessário para o registro do Aplicativo do Azure. O script também chama o comando***Impressão digital***e***Chave privada do certificado (arquivo PEM)***você usará a seção Configuração do Cisco Secure Email.

você tem os valores necessários para registrar nosso aplicativo no Microsoft Azure!

[Ignore a próxima seção! Prossiga para "Registrar um aplicativo do Azure para uso com o Cisco Secure Email"]

Certificado: Windows (utilizando o PowerShell)

Para administradores que usam o Windows, você precisará utilizar um aplicativo ou ter o conhecimento para criar um certificado autoassinado. Este certificado é usado para criar o aplicativo do Microsoft Azure e a comunicação de API associada.

Valores a serem criados:
Impressão digital •
Certificado • **público (arquivo CRT)**
Chave privada • **(arquivo PEM)**

Nosso exemplo para este documento criar um certificado autoassinado está usando XCA (https://hohnstaedt.de/xca/,https://sourceforge.net/projects/xca/).

Note: O XCA pode ser baixado para Mac, Linux ou Windows.

1. Crie um banco de dados para seu certificado e chaves:
    a. Selecione **Arquivo** na barra de ferramentas
    b. Selecionar **Nova Base de Dados**
    c. Criar uma senha para o banco de dados (será necessário em etapas posteriores, lembre-se disso!)
2. Clique na guia Certificados e, em seguida, clique em **Novo certificado**
3. Clique na guia Assunto e preencha o seguinte:
    a. Nome interno
    b. nome do país
    c. EstadoOuNomeDaProvíncia
    d. nome da localidade
    e. nome da organização
    f. organizationalUnitName (OU)
    g. CommonName (CN)
    h. endereço de email
4. Clique em **Gerar uma nova chave**
5. Na janela pop-up, verifique as informações fornecidas (alterando conforme desejado):
    a. Nome
    b. Tipo de chave: RSA
    c. Tamanho da chave: 2048 bit
    d. Clique em Criar
    e. Confirme o pop-up "Nome da chave privada RSA" criado com êxito clicando em **OK**
6. Clique na guia de uso da chave e selecione o seguinte:
    a. Em X509v3 Key Usage:

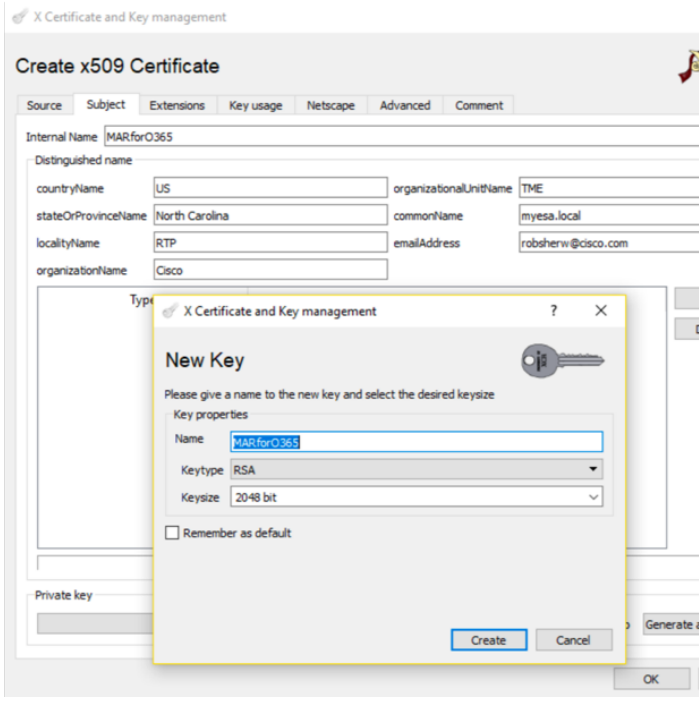

Figura 14: Usando XCA (etapas 3 a 5)

Assinatura digital, elemento chave

b. Em X509v3 Extended Key Usage: **Proteção de e-mails**

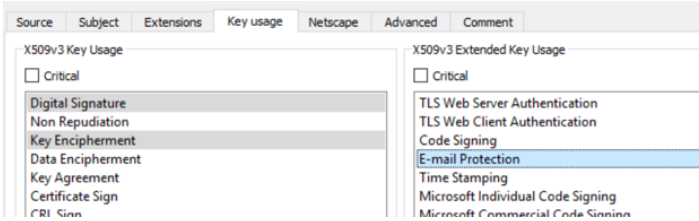

Figura 15: Usando XCA (etapa 6)

7. Clique em **OK** para aplicar alterações ao certificado
8. Confirme o pop-up "Nome do certificado criado com êxito" clicando em **OK**

Em seguida, você deverá exportar o **certificado público (arquivo CER)** e a ***chave privada do certificado (arquivo PEM)*** para uso nos comandos do PowerShell em seguida e para uso nas etapas de configuração do Cisco Secure Email:

1. Clique e realce o Nome interno do certificado recém-criado.
2. Clique em **Exportar**
    a. Defina o diretório save para facilidade de acesso (alterando conforme desejado)
    b. Verifique se o formato de exportação está definido como **PEM (.crt)**
    c. Clique em OK.

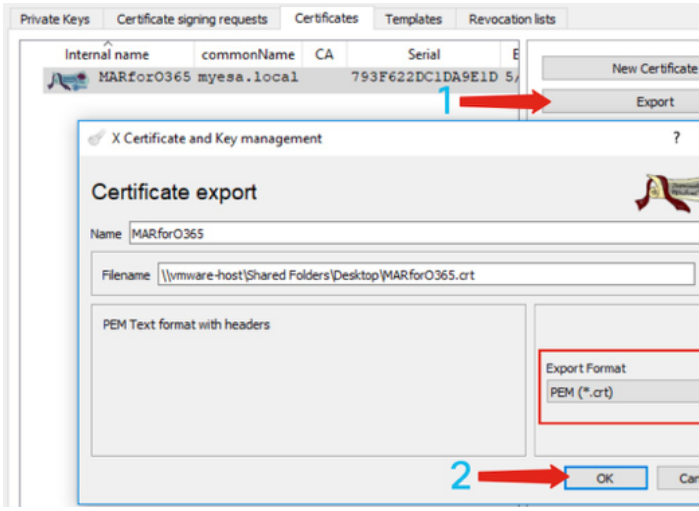

Figura 16: Usando XCA (exportar CRT)(etapas 1-2)

3. Clique na guia **Chaves privadas**
4. Clique e realce o Nome interno do certificado recém-criado.
5. Clique em **Exportar**
    a. Defina o diretório save para facilidade de acesso (alterando conforme desejado)
    b. Verifique se o formato de exportação está definido como **PEM private (.pem)**
    c. Clique em OK.
6. Sair e fechar XCA

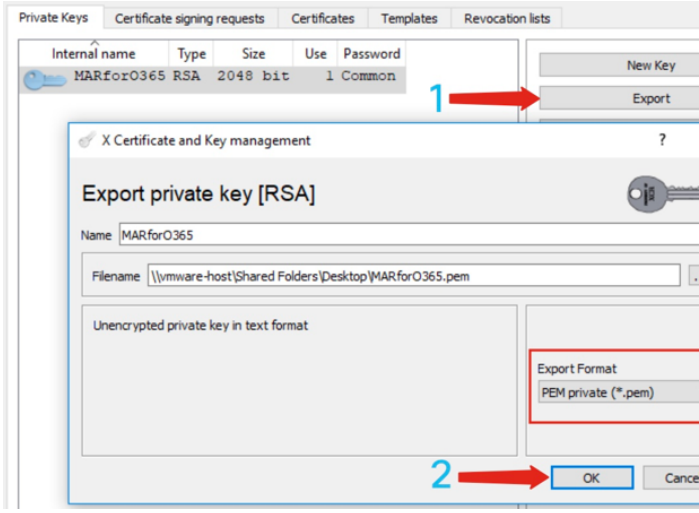

Figura 17: Usando XCA (exportar PEM) (etapas 3-5)

Finalmente, você pegará o certificado criado e extrairá a **impressão digital**, necessária para

configurar o Cisco Secure Email.

1. Usando o Windows PowerShell, execute o seguinte:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("c:\Users\joe\Desktop\myCert.crt")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()[Note: “c:\Users\joe\Desktop...” is the location on
your PC where your CRT file is saved.]
```

2. Para obter valores para as próximas etapas, salvar em um arquivo ou copiar para a área de transferência:

```
$base64Thumbprint | Out-File c:\Users\joe\Desktop\base64Thumbprint.txt
$base64Thumbprint
```

Note: “c:\Users\joe\Desktop..." é o local no PC onde você está salvando a saída.

A saída esperada ao executar o comando PowerShell deve ser semelhante à seguinte:

```
PS C:\Users\joe\Desktop> $base64Thumbprint
75fA1XJEJ4I1ZVFOB2xqkoCIh94=
```

Como você pode ver, o comando PowerShell chama a *base64Thumbprint*, que é a **Thumbprint** necessária para a configuração do gateway do Cisco Secure Email.

Você também concluiu a criação do **Certificado Público (arquivo CER)** necessário para o registro do Aplicativo do Azure. E você criou a ***Chave privada do certificado (arquivo PEM)***que será usada na seção Configuração do Cisco Secure Email.

Você tem os valores necessários para registrar seu aplicativo no Microsoft Azure!

[Prossiga para "Registrar um aplicativo do Azure para uso com o Cisco Secure Email"]

Apêndice B

Observação: isso é obrigatório SOMENTE se você estiver executando o AsyncOS 11.x ou 12.x para e-mail em seu gateway.

Permissões de API (AsyncOS 11.x, 12.x)

No painel do aplicativo, nas opções Gerenciar...

1. Selecionar **permissões de API**
2. Clique em **+ Adicionar uma permissão**
3. Role para baixo até **APIs antigas suportadas** e selecione **Exchange**
4. Selecione as permissões abaixo em permissões delegadas: EWS > "EWS.AccessAsUser.All" (Acessar caixas de correio como o usuário conectado via Serviços Web do Exchange)Email > "Mail.Read" (Ler email do usuário)E-mail > "Mail.ReadWrite" (Leitura e gravação de e-mail de usuário)E-mail > "Mail.Send" (Enviar e-mail como usuário)
5. Role até a parte superior do painel...
6. Selecione as permissões abaixo em Permissões do aplicativo: "full_access_as_app" (Use os Serviços Web do Exchange com acesso total a todas as caixas de correio)Email > "Mail.Read" (Ler email do usuário)E-mail > "Mail.ReadWrite" (Leitura e gravação de e-mail de usuário)E-mail > "Mail.Send" (Enviar e-mail como usuário)
7. *Opcional:* Você verá que o Microsoft Graph por padrão está habilitado para permissões "User.Read"; você pode deixá-lo configurado ou clicar em **Ler** e clicar em **Remover permissão** para removê-lo das permissões de API associadas ao aplicativo.
8. Clique em **Adicionar permissões** (ou **Atualizar permissões**, se o Microsoft Graph já estiver listado)
9. Finalmente, clique em **Conceder consentimento do administrador para...** para garantir que suas novas permissões sejam aplicadas ao aplicativo
10. Haverá um pop-up no painel que pergunta:
"*Deseja conceder o consentimento para as permissões solicitadas para todas as contas no <Nome do Azure>? Isso atualizará todos os registros de consentimento do administrador existentes que este aplicativo já tiver que corresponder ao que está listado abaixo.*"

    Clique em Sim

Nesse ponto, você verá uma mensagem de êxito verde e a coluna "Admin Consent Required" (Consentimento do administrador obrigatório), concedida, semelhante à mostrada:

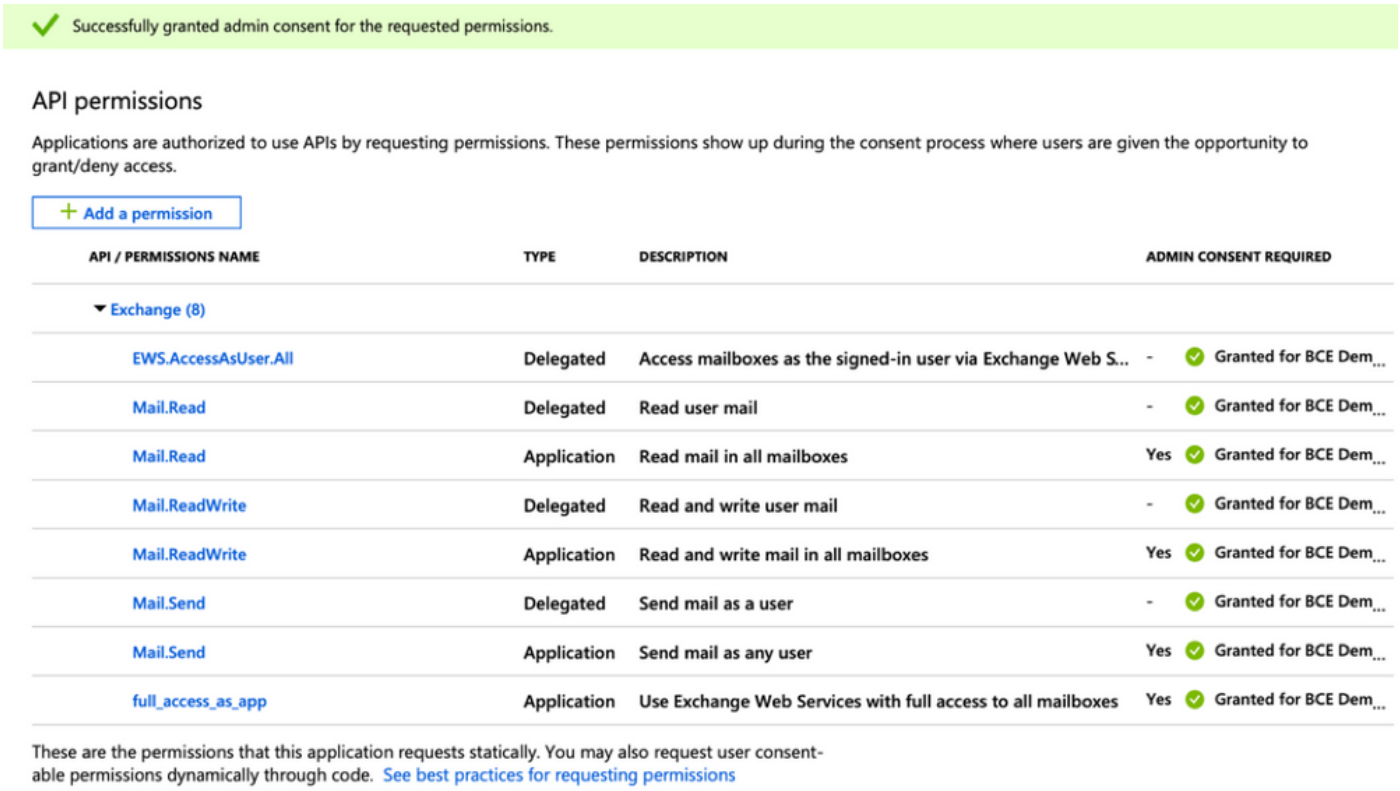

Figura 18: Registro de Aplicativo do Microsoft Azure (permissões de API necessárias)

[Prossiga para "Registrar um aplicativo do Azure para uso com o Cisco Secure Email"]

Informações Relacionadas

- Cisco Email Security Appliance - Suporte ao produto
- Cisco Email Security Appliance - Notas da versão
- Cisco Email Security Appliance - Guia do usuário final