Come configurare le impostazioni dell'account di posta elettronica sicuro Cisco per l'API Microsoft Azure (Microsoft 365)

Sommario

Introduzione

In questo documento viene illustrato come eseguire la registrazione di una nuova applicazione in Microsoft Azure (Azure Active Directory) per generare l'ID client, l'ID tenant e le credenziali client necessari e quindi la configurazione delle impostazioni account in un gateway di posta elettronica sicura Cisco o in un gateway cloud. La configurazione delle impostazioni dell'account e del profilo dell'account associato è necessaria quando un amministratore della posta configura la funzione di monitoraggio e aggiornamento automatici delle cassette postali per Advanced Malware Protection (AMP) o il filtro URL o utilizza l'azione di monitoraggio dei messaggi su Cisco Secure Email e Web Manager o Cisco Secure Gateway/Cloud Gateway.

Flusso del processo di monitoraggio e aggiornamento automatici delle cassette

postali

È possibile che un allegato (file) presente nel messaggio di posta elettronica o in un URL venga classificato come dannoso in qualsiasi momento, anche dopo aver raggiunto la cassetta postale di un utente. AMP on Cisco Secure Email (tramite Cisco Secure Malware Analytics) può identificare questo sviluppo quando emergono nuove informazioni e inviare avvisi retrospettivi a Cisco Secure Email. Cisco Talos offre lo stesso livello di analisi degli URL di AsyncOS 14.2 per Cisco Secure Email Cloud Gateway. Se l'organizzazione utilizza Microsoft 365 per gestire le cassette postali, è possibile configurare Cisco Secure Email in modo da eseguire azioni di correzione automatica dei messaggi nella cassetta postale di un utente quando vengono modificati i verdetti delle minacce.

Cisco Secure Email comunica in modo sicuro e diretto con Microsoft Azure Active Directory per ottenere l'accesso alle cassette postali di Microsoft 365. Ad esempio, se un'e-mail con un allegato viene elaborata tramite il gateway e analizzata da AMP, l'allegato (SHA256) viene fornito ad AMP per la reputazione del file. La disposizione dell'AMP può essere contrassegnata come Pulita (passaggio 5, figura 1) e quindi consegnata alla cassetta postale Microsoft 365 del destinatario finale. In seguito, la disposizione dell'AMP viene modificata in Malicious (Dannosa), Cisco Malware Analytics invia un aggiornamento del verdetto retroattivo (passaggio 8, Figura 1) a *qualsiasi* gateway che abbia elaborato lo specifico SHA256. Quando il gateway riceve l'aggiornamento con verdetto retroattivo di Dannoso (se configurato), esegue una delle azioni di risoluzione automatica delle cassette postali (MAR) seguenti: Inoltra, Elimina o Inoltra ed Elimina.

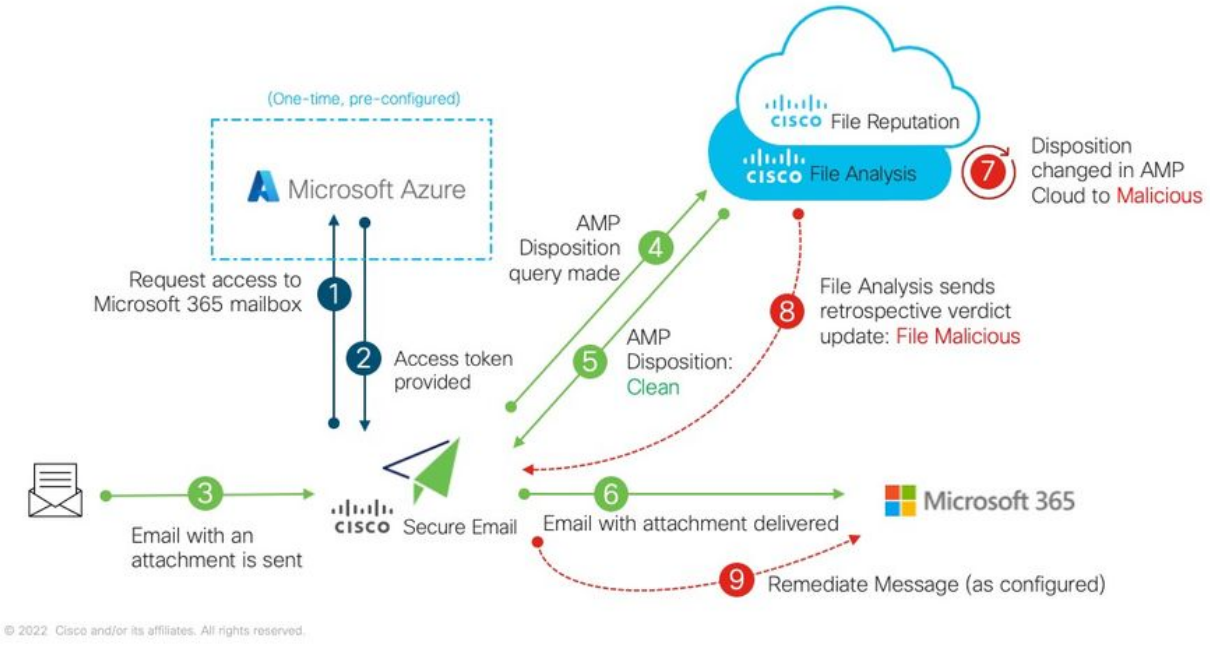

Figura 1: MAR (per AMP) su Cisco Secure Email

In questa guida viene illustrato come configurare Cisco Secure Email con Microsoft 365 solo per il monitoraggio e l'aggiornamento automatici delle caselle di posta. AMP (File Reputation and File Analysis) e/o il filtro URL sul gateway devono essere già configurati. Per ulteriori informazioni sulla reputazione e l'analisi dei file, consultare la Guida per l'utente della versione di AsyncOS distribuita.

Prerequisiti

1. Abbonamento all'account Microsoft 365 (verificare che l'abbonamento all'account Microsoft 365 includa l'accesso a Exchange, ad esempio un account Enterprise E3 o Enterprise E5).

2. Account amministratore di Microsoft Azure e accesso a http://portal.azure.com

3. Gli account Microsoft 365 e Microsoft Azure AD sono collegati correttamente a un indirizzo di posta elettronica "user@domain.com" attivo e l'utente può inviare e ricevere messaggi di posta elettronica tramite tale indirizzo.

I valori seguenti verranno creati per configurare la comunicazione dell'API del gateway di posta elettronica sicura Cisco con Microsoft Azure AD:

- **ID client**
- **ID tenant**
- **Segreto client**

  Nota: A partire da AsyncOS 14.0, **Impostazioni account** consente la configurazione tramite un segreto client durante la creazione della registrazione dell'app di Microsoft Azure. Questo è il metodo più facile e preferito.

Facoltativo - Se NON si utilizza il segreto client, è necessario creare e avere pronto:

- **Identificazione personale**
- **Chiave privata (file PEM)**

La creazione dell'identificazione personale e della chiave privata è illustrata nell'Appendice di questa guida:

1. Un certificato pubblico (o privato) attivo (CER) e la chiave privata utilizzata per firmare il certificato (PEM) oppure la possibilità di creare un certificato pubblico (CER) e di salvare la chiave privata utilizzata per firmare il certificato (PEM). In questo documento Cisco offre due metodi per eseguire questa operazione in base alle preferenze dell'amministratore: Certificato: Unix/Linux/OS X (con OpenSSL)Certificato: Windows (tramite PowerShell)

2. Accesso a Windows PowerShell, in genere amministrato da un host o un server Windows oppure accesso a un'applicazione terminal tramite Unix/Linux

Per creare i valori richiesti, completare la procedura descritta in questo documento.

Registra un'app di Azure per l'utilizzo con Cisco Secure Email

Registrazione applicazione

Accedere al portale di Microsoft Azure

1. Fare clic su **Azure Active Directory** (Figura 2)
2. Fai clic sulle **registrazioni dell'app**
3. Fare clic su **+ Nuova registrazione**
4. Nella pagina "Registra un'applicazione":
    r. Nome: **Cisco Secure Email MAR** (o il nome scelto)
    b. Tipi di conto supportati: **solo account in questa directory organizzativa (nome account)**
    c. URI di reindirizzamento: (facoltativo)
    [Nota: È possibile lasciare questo campo vuoto o utilizzare https://www.cisco.com/sign-on per compilare]
    d. Nella parte inferiore della pagina, fare clic su **Register**

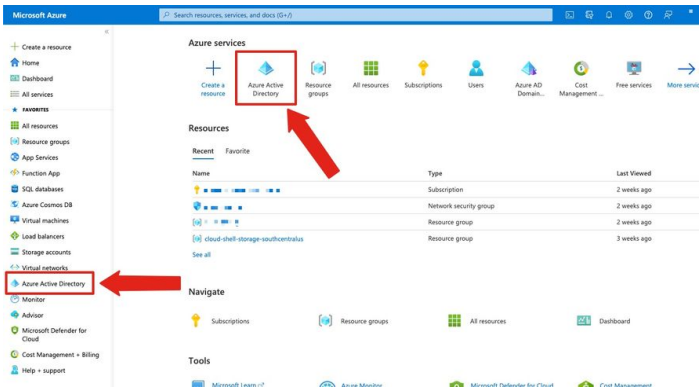

Figura 2: Esempio del portale di Microsoft Azure

Una volta completati i passaggi precedenti, verrà presentata la richiesta:

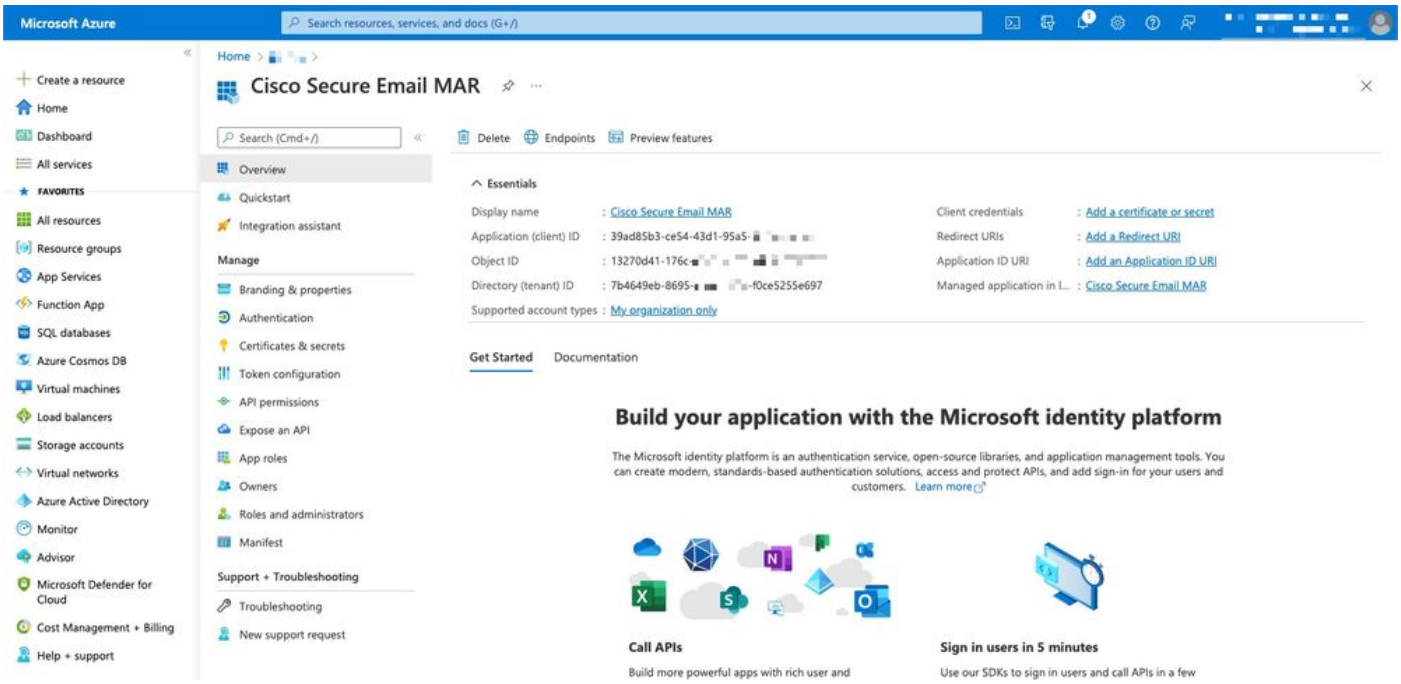

Figura 3: Pagina dell'applicazione Microsoft Azure Active Directory

Certificati e segreti

Se si esegue AsyncOS 14.0 o versione successiva, Cisco consiglia di configurare l'app Azure per utilizzare un segreto client. Nel riquadro dell'applicazione, in Opzioni di gestione:

1. Seleziona **certificati e segreti**

2. Nella sezione ***Segreti client***, fare clic su **+ Nuovo segreto client**

3. Aggiungi una descrizione per identificare lo scopo del segreto client, ad esempio "Monitoraggio e aggiornamento di Cisco Secure Email"

4. Selezionare un periodo di scadenza

5. Fare clic su **Add**

6. Spostare il mouse a destra del valore generato e fare clic sull'icona **Copia negli Appunti**

7. Salvare questo valore nelle note, notarlo come "Segreto cliente"

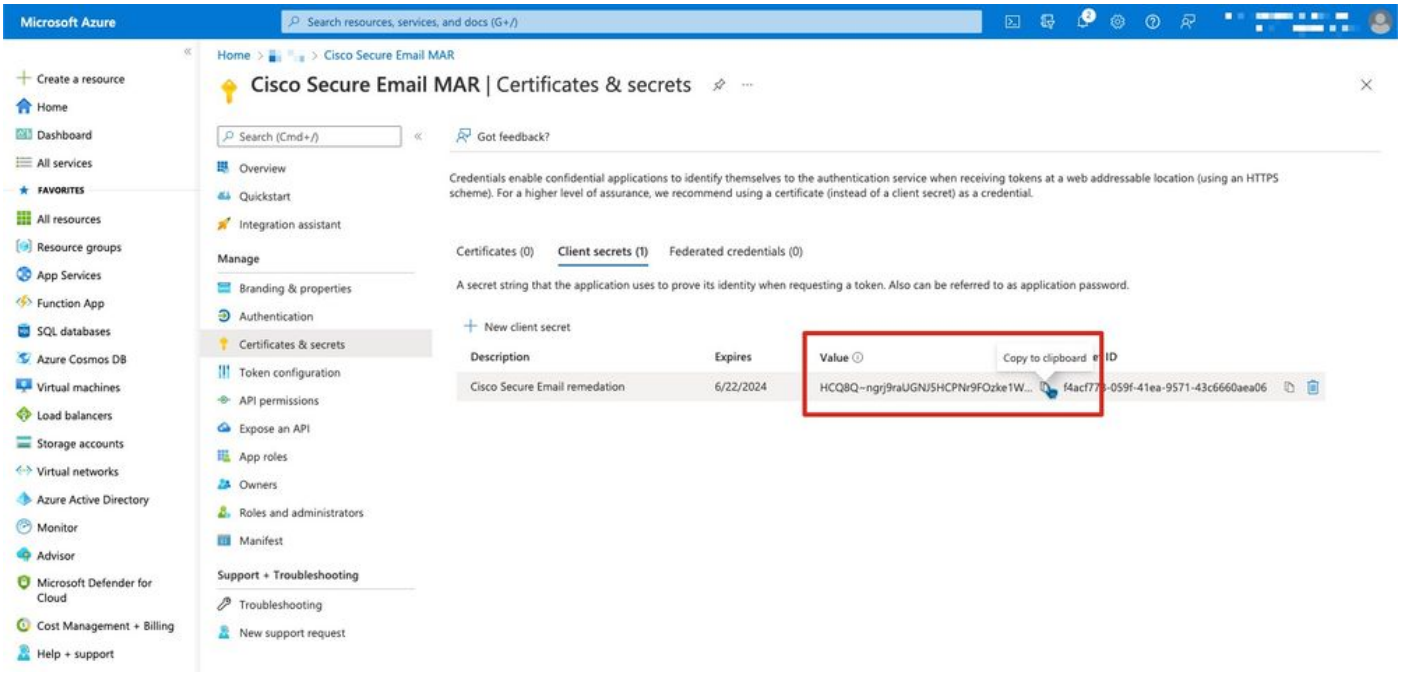

Figura 4: Esempio di creazione segreto client di Microsoft Azure

> **Nota:** Dopo aver chiuso la sessione di Microsoft Azure attiva, il valore della chiave privata client appena generata *** ne esce. Se non si registra e si salvaguarda il valore prima di uscire, sarà necessario ricreare il segreto client per visualizzare l'output in testo non crittografato.

Facoltativo - Se non si configura l'applicazione Azure con un segreto client, configurare l'app Azure per usare il certificato. Nel riquadro dell'applicazione, in Opzioni di gestione:

1. Seleziona **certificati e segreti**
2. Fare clic su **Carica certificato**
3. Selezionare il file CRT (creato in precedenza)
4. Fare clic su **Aggiungi**

Autorizzazioni API

Nota: A partire da AsyncOS 13.0 for Email Security, le autorizzazioni API per le comunicazioni di

posta elettronica da Microsoft Azure a Cisco Secure Email richieste sono cambiate da Microsoft Exchange a Microsoft Graph. Se è già stato configurato MAR e si sta aggiornando il gateway di posta elettronica sicuro Cisco esistente ad AsyncOS 13.0, è sufficiente aggiornare/aggiungere le nuove autorizzazioni API. Se si utilizza una versione precedente di AsyncOS, 11.x o 12.x, vedere l'Appendice B prima di continuare.

Nel riquadro dell'applicazione, in Opzioni di gestione:

1. Seleziona **autorizzazioni API**
2. Fare clic su **+ Aggiungi autorizzazione**
3. Seleziona **Microsoft Graph**
4. Selezionare le autorizzazioni seguenti per le ***autorizzazioni applicazione***: Mail > "Mail.Read" (Leggi posta in tutte le cassette postali)Mail > "Mail.ReadWrite" (Leggi e scrivi in tutte le cassette postali)Mail > "Mail.Send" (Invia posta come qualsiasi utente)Directory > "Directory.Read.All" (Leggi dati directory) [*Facoltativo: Se si utilizza la sincronizzazione LDAP Connector/LDAP, attivare. In caso contrario, non è necessario.]
5. *Facoltativo:* Per impostazione predefinita, Microsoft Graph è abilitato per le autorizzazioni "User.Read"; è possibile lasciare configurata questa opzione oppure fare clic su **Leggi** e fare clic su **Rimuovi autorizzazioni** per rimuoverla dalle autorizzazioni API associate all'applicazione.
6. Fare clic su **Aggiungi autorizzazioni** (o **Aggiorna autorizzazioni**, se Microsoft Graph era già presente nell'elenco)
7. Infine, fare clic su **Concedi consenso amministratore per...** per assicurarsi che le nuove autorizzazioni vengano applicate all'applicazione
8. Verrà visualizzato un messaggio che chiede:
   "*Concedere il consenso per le autorizzazioni richieste per tutti gli account in <Nome Azure>? In questo modo verranno aggiornati tutti i record di consenso amministratore esistenti che questa applicazione deve già corrispondere a quanto elencato di seguito.*"

   Fare clic su **Sì**

A questo punto, viene visualizzato un messaggio verde di operazione riuscita e nella colonna "Consenso amministratore richiesto" viene visualizzato il messaggio Concesso.

Recupero ID client e ID tenant

Nel riquadro dell'applicazione, in Opzioni di gestione:

1. Fare clic su **Panoramica**
2. Spostare il mouse a destra dell'ID applicazione (client) e fare clic sull'icona **Copia negli Appunti**
3. Salvare questo valore nelle note, notarlo come "ID client"
4. Spostare il mouse a destra dell'ID della directory (tenant) e fare clic sull'icona **Copia negli Appunti**
5. Salva questo valore nelle note, nota come "ID tenant"

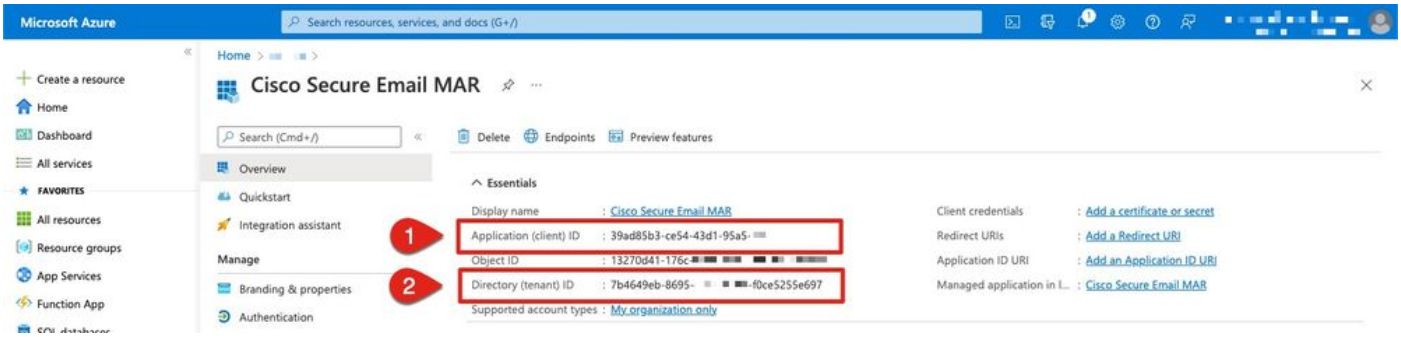

Figura 5: Microsoft Azure... Esempio di ID client e ID tenant

Configurazione di Cisco Secure Email Gateway/Cloud Gateway

A questo punto, è necessario preparare e salvare nelle note i seguenti valori:

- **ID client**
- **ID tenant**
- **Segreto client**

Facoltativo, se non si utilizza Client secret:

- **Identificazione personale**
- **Chiave privata (file PEM)**

Èpossibile usare i valori creati dalle note e configurare le impostazioni dell'account sul gateway Cisco Secure Email.

Crea profilo account

1. Accedere al gateway
2. Selezionare **Amministrazione sistema > Impostazioni account** Nota: Se si esegue una versione precedente ad AsyncOS 13.x, sarà **Amministrazione del sistema > Impostazioni cassetta postale**
3. Fare clic su **Attiva**
4. Selezionare la casella di controllo Abilita impostazioni account e fare clic su **Invia**
5. Fare clic su **Crea profilo account**
6. Fornire un nome di profilo e una descrizione (qualcosa che descriva in modo univoco il tuo account se hai più domini)
7. Durante la definizione di una connessione a Microsoft 365, lasciare il tipo di profilo **Office 365 / Hybrid (Graph API)**
8. Immetti il tuo **ID client**
9. Immetti il tuo **ID tenant**
10. Per le credenziali client, eseguire una delle operazioni seguenti, come configurato in Azure: Fare clic su **Client Secret** e incollare il segreto client configurato oppure...Fare clic su

Certificato client e immettere l'identificazione personale, nonché fornire il modulo PEM facendo clic su "Scegli file"

11. Fare clic su **Submit (Invia).**
12. Fare clic su **Commit delle modifiche** nell'angolo superiore destro dell'interfaccia utente
13. Immettere eventuali commenti e completare le modifiche alla configurazione facendo clic su **Conferma modifiche**

Verifica connessione

Il passaggio successivo consiste solo nel verificare la connessione API dal gateway Cisco Secure Email a Microsoft Azure:

1. Dalla stessa pagina Dettagli account, fare clic su **Test connessione**
2. Immettere un indirizzo di posta elettronica valido per il dominio gestito nell'account Microsoft 365
3. Fare clic su **Test connessione**
4. Si dovrebbe ricevere un messaggio di riuscita (Figura 6)
5. Fate clic su **Fatto** (Done) per completare l'operazione

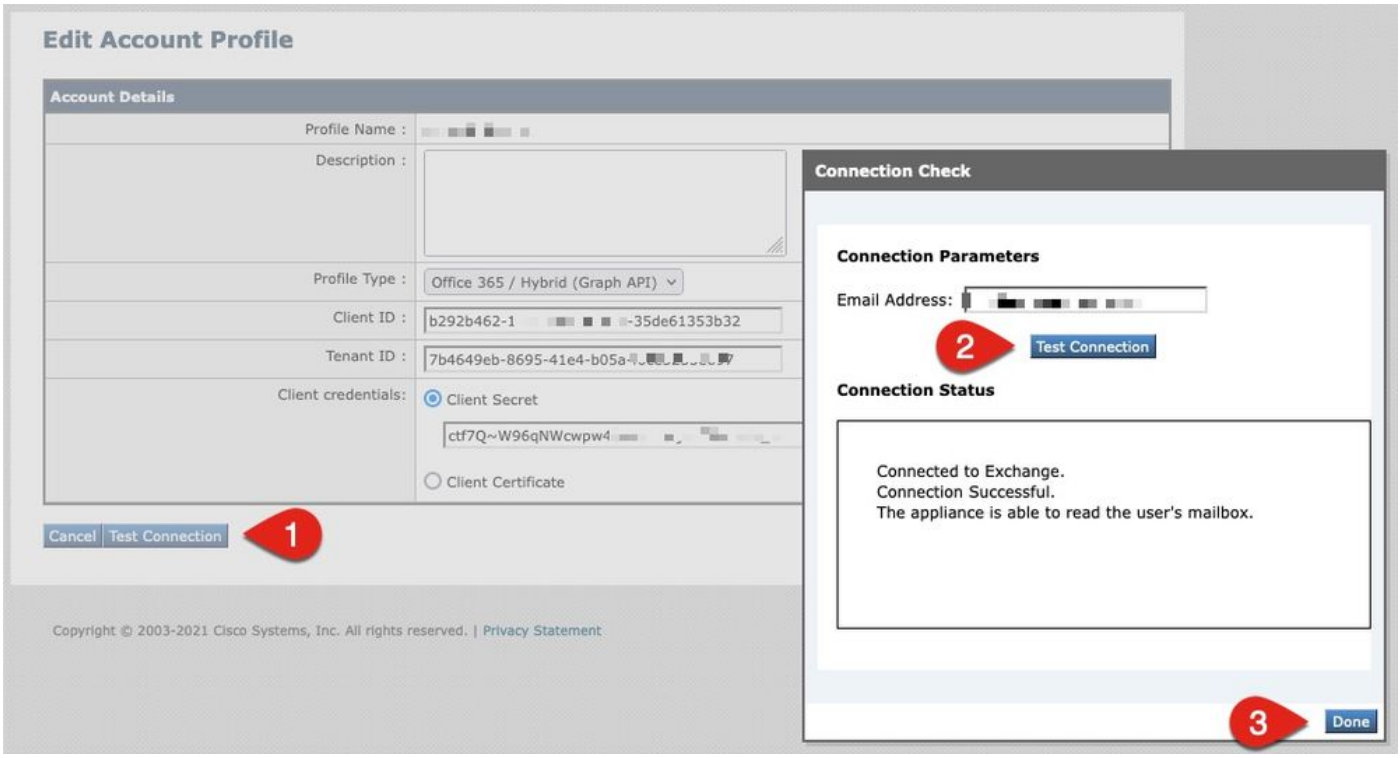

Figura 6: Esempio di verifica connessione/profilo account

6. Nella sezione *Mapping domini*, fare clic su **Crea mapping domini**

7. Inserire nei nomi di dominio associati all'account Microsoft 365 per il quale è stata appena convalidata la connessione API

Di seguito è riportato un elenco dei formati di dominio validi che è possibile utilizzare per mappare un profilo cassetta postale:

- Il dominio può essere la parola chiave speciale 'ALL' che identifica tutti i domini per creare un mapping di dominio predefinito.

- Nomi di dominio come 'example.com' - Corrisponde a qualsiasi indirizzo con questo dominio.

- Nomi di dominio parziali come '@.partial.example.com' - Corrisponde a qualsiasi indirizzo che termina con questo dominio

- È possibile immettere più domini utilizzando un elenco di domini separati da virgole.

8. Fare clic su **Sottometti**

9. Fare clic su **Commit modifiche** nell'angolo superiore destro dell'interfaccia utente

10. Inserire eventuali commenti e completare le modifiche alla configurazione facendo clic su **Conferma modifiche**

Abilita Monitoraggio e aggiornamento automatici cassette postali per la protezione avanzata da malware nei criteri di posta

Completare questo passaggio per abilitare MAR nella configurazione AMP per i criteri di posta.

1. Selezionare **Mail Policies > Incoming Mail Policies > (Policy di posta in arrivo)**
2. Fare clic sulle impostazioni nella colonna Advanced Malware Protection per il nome del criterio che si desidera configurare (ad esempio, Figura 7):

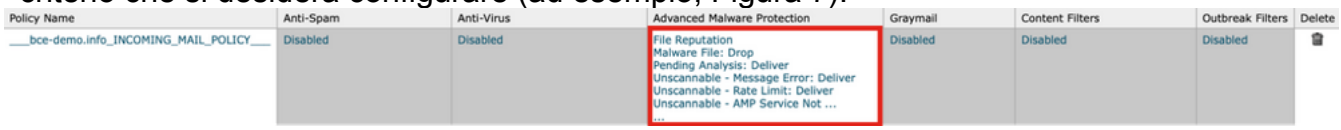

Figura 7: Abilita MAR (criteri posta in arrivo)

3. Scorri fino alla fine della pagina
4. Fare clic sulla casella di controllo Abilita correzione automatica cassetta postale (MAR)
5. Selezionare una delle seguenti azioni da eseguire per MAR (ad esempio, Figura 8): Inoltra a: <*immettere l'indirizzo di posta elettronica*>EliminaInoltra a: <*immettere l'indirizzo di posta elettronica*> ed eliminare

Figura 8: Esempio di abilitazione di MAR per la configurazione di AMP

6. Fare clic su **Submit (Invia).**
7. Fare clic su **Commit delle modifiche** nell'angolo superiore destro dell'interfaccia utente
8. Immettere eventuali commenti e completare le modifiche alla configurazione facendo clic su **Conferma modifiche**

Abilita correzione automatica cassetta postale (MAR) per il filtro URL

A partire da AsyncOS 14.2 per Cisco Secure Email Cloud Gateway, il filtro URL include ora il verdetto retrospettivo e la correzione degli URL.

1. Selezionare **Security Services > URL Filtering** (Servizi di sicurezza > Filtro URL)
2. Se il filtro URL non è ancora stato configurato, fare clic su **Enable** (Abilita)
3. Fare clic sulla casella di controllo "Abilita filtri categorie e reputazione URL"
4. *Impostazioni avanzate* con le impostazioni predefinite
5. Fare clic su Submit (Invia).

Il filtro URL dovrebbe essere simile al seguente:

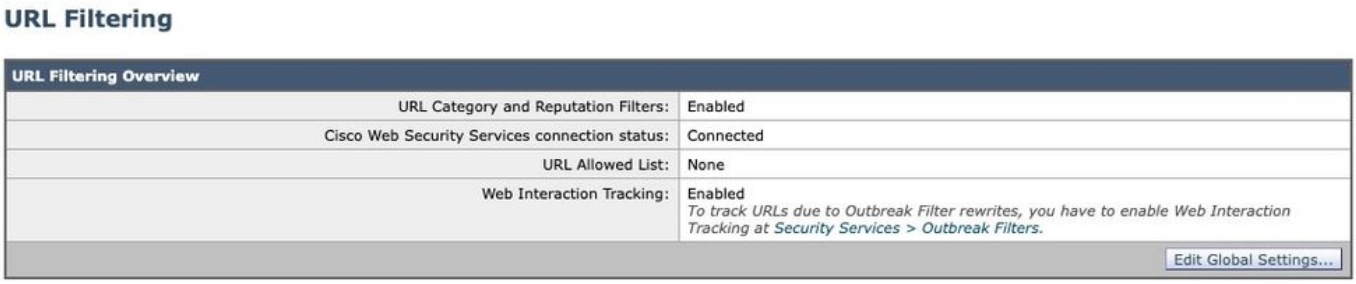

Figura 9: Esempio di post-abilitazione del filtro URL

Per verificare la retrospettiva degli URL con il filtro URL interno, eseguire le operazioni seguenti o aprire una richiesta di assistenza per consentire a Cisco di effettuare le operazioni:

```
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
```

Al termine, aggiornare l'interfaccia utente nella pagina del filtro URL in modo da visualizzare quanto segue:

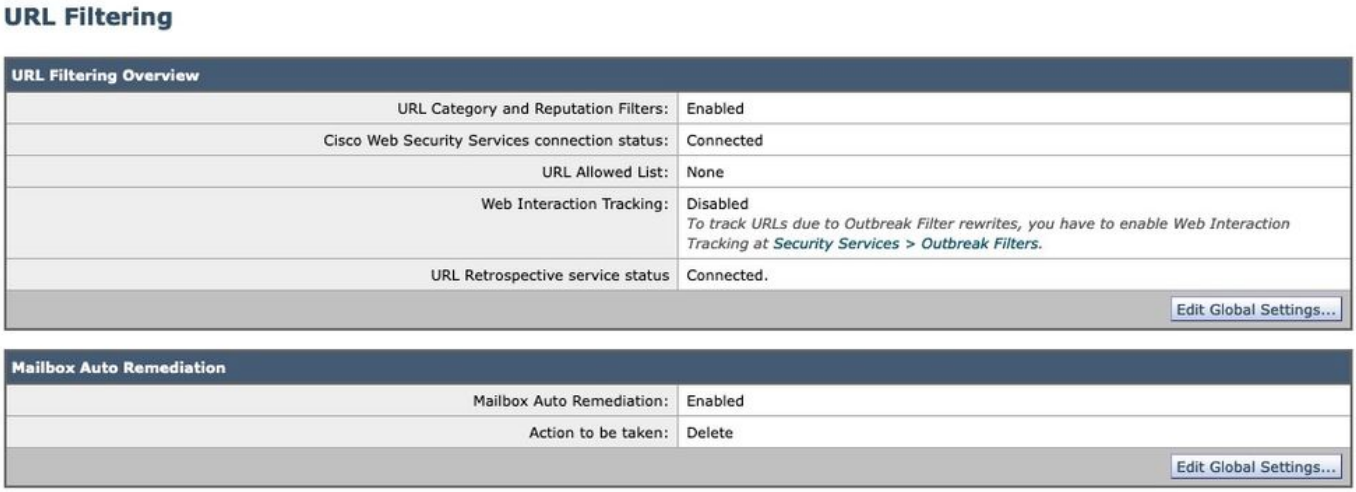

Figura 10: Filtro URL (AsyncOS 14.2 per Cisco Secure Email Cloud Gateway)

La protezione URL è ora pronta per eseguire azioni correttive quando un verdetto cambia punteggio. Per ulteriori informazioni, vedere la sezione relativa alla protezione da URL dannosi o indesiderati nel manuale dell'utente di AsyncOS 14.2 for Cisco Secure Email Cloud Gateway.

Configurazione completata.

A questo punto Cisco Secure Email è pronta a valutare continuamente le minacce emergenti man

mano che si rendono disponibili nuove informazioni e a inviare all'utente notifiche sui file che sono considerati minacce dopo essere entrati nella rete.

Quando si genera un verdetto retrospettivo da Analisi file (Cisco Secure Malware Analytics), viene inviato un messaggio informativo all'amministratore di Sicurezza e-mail (se configurato). Esempio:

```
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             : [redacted]
   To               : [redacted]
   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[redacted]
Timestamp: 04 Jun 2019 04:40:36 +0500
```

Il monitoraggio e l'aggiornamento automatici delle cassette postali verrà eseguito come configurato se configurato in base ai criteri di posta.

Esempi di report di risoluzione automatica delle cassette postali

La segnalazione di qualsiasi SHA256 per cui è stato eseguito il monitoraggio e l'aggiornamento è disponibile nel report di monitoraggio e aggiornamento automatici delle cassette postali sia sul gateway Cisco Secure Email che su Cisco Secure Email e Web Manager.

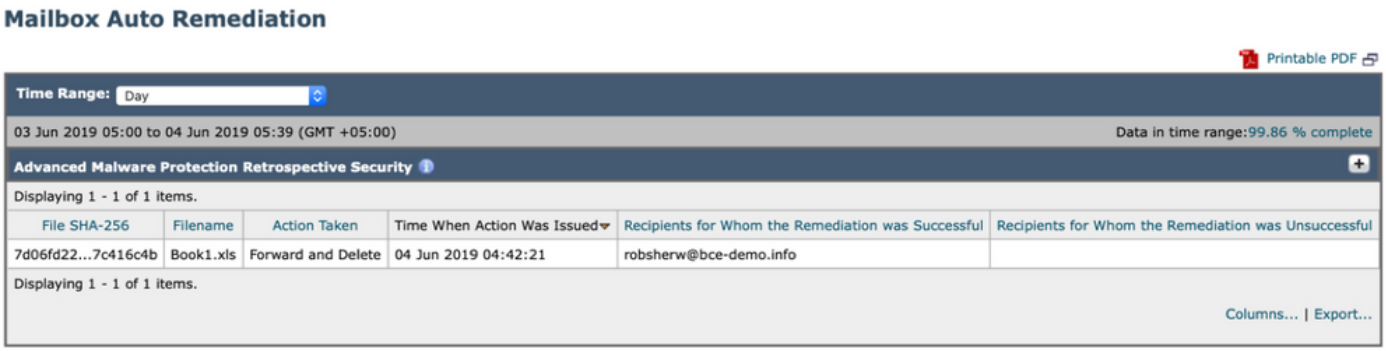

Figura 11: Rapporto di correzione automatica cassetta postale (interfaccia utente legacy)

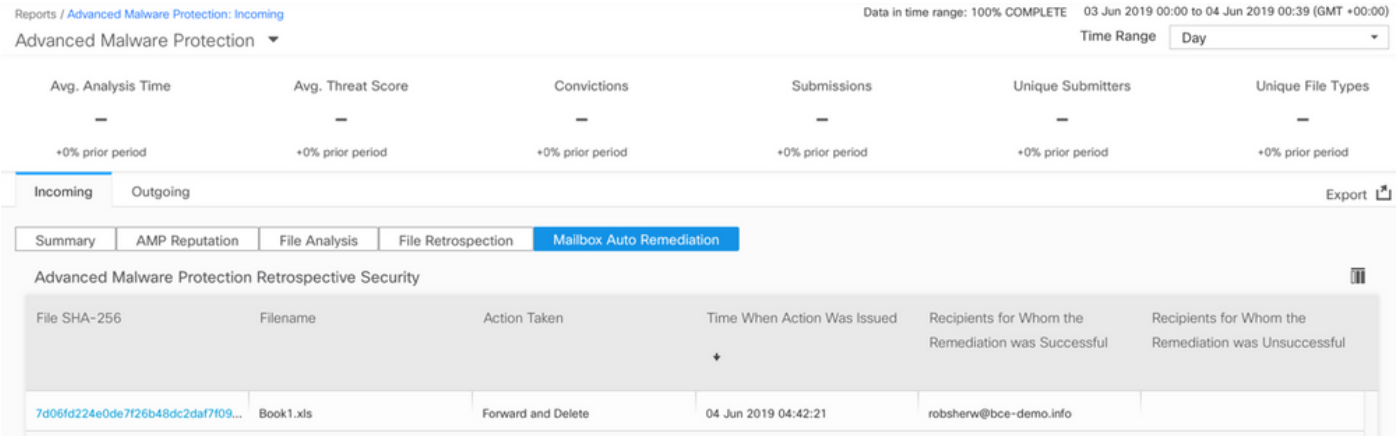

Figura 12: (NG UI) Rapporto di risoluzione automatica delle cassette postali

Registrazione correzione automatica cassetta postale

Il monitoraggio e l'aggiornamento automatici delle cassette postali ha un singolo registro, "mar". I log di monitoraggio e aggiornamento automatici delle cassette postali conterranno tutte le attività di comunicazione tra il gateway Cisco Secure Email e Microsoft Azure, Microsoft 365.

Un esempio di log dei marchi:

```
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.
```

Risoluzione dei problemi di Cisco Secure Email Gateway

Se non vengono visualizzati risultati positivi per il test dello stato della connessione, è possibile esaminare la registrazione dell'applicazione eseguita da Microsoft Azure AD.

Dal gateway Cisco Secure Email, impostare i log MAR sul livello 'trace' e verificare nuovamente la connessione.

Per le connessioni non riuscite, i registri potrebbero essere simili a:

```
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
```

Confermare l'ID applicazione, l'ID directory (che corrisponde all'ID tenant) o altri identificatori associati dal log con l'applicazione in Azure AD. Se non si è certi dei valori, eliminare l'applicazione dal portale di Azure AD e ricominciare.

Per una connessione riuscita, i registri devono essere simili 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.
```

Risoluzione dei problemi di Azure AD

Nota: il supporto Cisco TAC e Cisco non sono autorizzati a risolvere i problemi del lato cliente con Microsoft Exchange, Microsoft Azure AD o Office 365.

Per i problemi relativi al cliente in Microsoft Azure AD, è necessario contattare il supporto tecnico Microsoft. Vedere l'opzione "Guida + supporto" dal dashboard di Microsoft Azure. È possibile aprire richieste di supporto diretto al supporto tecnico Microsoft dal dashboard.

Appendice A

Nota: questo argomento è obbligatorio SOLO se NON si utilizza il segreto client per la configurazione dell'applicazione Azure.

Creazione di un certificato pubblico e privato e di una coppia di chiavi

Suggerimento: salvare l'output localmente per *$base64Value*, *$base64Thumbprint* e *$keyid*, poiché saranno necessari in seguito nei passaggi di configurazione. Memorizzare il file .crt e il file .pem associato del certificato in una cartella locale disponibile nel computer.

Nota: Se si dispone già di un certificato (formato x509/standard) e di una chiave privata, ignorare questa sezione. Accertarsi di disporre di entrambi i file CRT e PEM, in quanto saranno necessari nelle sezioni successive.

Certificato: Unix/Linux (con openssl)

Valori da creare:

- **Identificazione personale**
- **Certificato pubblico (file CRT)**
- **Chiave privata (file PEM)**

Gli amministratori che utilizzano Unix/Linux/OS X, ai fini e dell'esecuzione dello script fornito, presuppongono che sia installato OpenSSL.

Nota: Eseguire i comandi 'which openssl' e 'openssl version' per verificare l'installazione di OpenSSL. Installare OpenSSL se non è presente.

Per assistenza, vedere il documento seguente: Script di configurazione di Azure AD per Cisco Secure Email

Dall'host (UNIX/Linux/OS X):

1. Da un'applicazione terminale, un editor di testo (o comunque si stia creando uno script shell), creare uno script copiando quanto segue: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. Incollare lo script
3. Assicurarsi di rendere eseguibile lo script. Eseguire il comando seguente: **chmod u+x my_azure.sh**
4. Eseguire lo script: **./my_azure.sh**

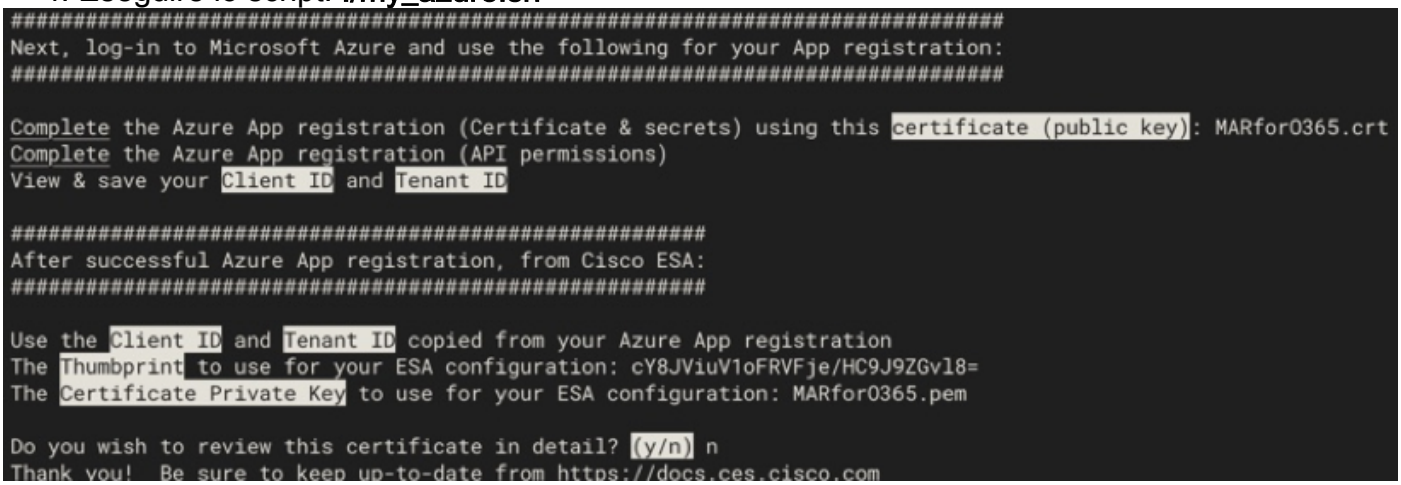

Figura 13: output dello schermo da my_azure.sh

Come illustrato nella Figura 2, lo script genera e chiama il **certificato pubblico (file CER)**necessario per la registrazione dell'app di Azure. Lo script richiama anche la***Identificazione personale***e***Chiave privata del certificato (file PEM)***da utilizzare nella sezione Configurazione di Cisco Secure Email.

sono disponibili i valori necessari per registrare l'applicazione in Microsoft Azure.

[Salta la sezione successiva! Procedere a "Registrazione di un'app di Azure per l'utilizzo con Cisco Secure Email"]

Certificato: Windows (tramite PowerShell)

Per gli amministratori che utilizzano Windows, è necessario utilizzare un'applicazione o disporre delle conoscenze necessarie per creare un certificato autofirmato. Questo certificato viene usato per creare l'applicazione Microsoft Azure e associare la comunicazione API.

Valori da creare:

- **Identificazione personale**
- **Certificato pubblico (file CRT)**
- **Chiave privata (file PEM)**

L'esempio di questo documento per la creazione di un certificato autofirmato è l'utilizzo di XCA (https://hohnstaedt.de/xca/,https://sourceforge.net/projects/xca/).

Nota: XCA può essere scaricato per Mac, Linux o Windows.

1. Creare un database per il certificato e le chiavi:
   r. Selezionare **File** dalla barra degli strumenti
   b. Seleziona **nuovo database**
   c. Creare una password per il database (sarà necessario in passaggi successivi, quindi ricordatelo!)
2. Fare clic sulla scheda Certificati, quindi su **Nuovo certificato**
3. Fare clic sulla scheda Oggetto e compilare quanto segue:
   r. Nome interno
   b. NomePaese
   c. StateOrProvinceName
   d. NomeLocalità
   e. NomeOrganizzazione
   f. NomeUnitàOrganizzativa (OU)
   g. commonName (CN)
   h. IndirizzoPostaElettronica
4. Fare clic su **Generate a New Key (Genera una nuova chiave)**
5. Nel popup, verificare le informazioni fornite (modifica in base alle esigenze):
   r. Nome
   b. Tipo chiave: RSA
   c. Dimensione chiave: 2048 bit
   d. Fare clic su Crea
   e. Confermare la creazione della chiave privata RSA 'Nome' " facendo clic su **OK.**
6. Fare clic sulla scheda Uso chiave e selezionare quanto segue:
   r. In Utilizzo chiave X509v3:

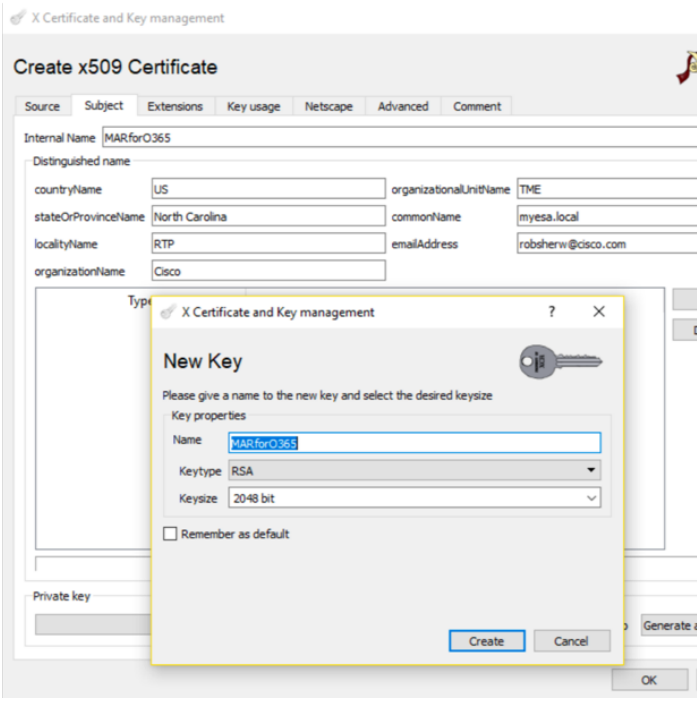

Figura 14: Uso di XCA (punti 3-5)

Firma digitale, cifratura chiave

b. In Utilizzo chiave esteso X509v3: **Protezione posta elettronica**

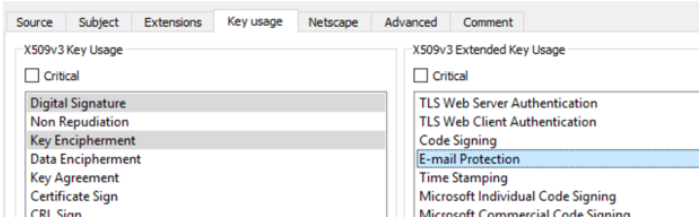

Figura 15: Utilizzo di XCA (passaggio 6)

7. Fare clic su **OK** per applicare le modifiche al certificato
8. Confermare la creazione del certificato *'Nome*' " facendo clic su **OK**

Successivamente, si desidera esportare sia il **file del certificato pubblico (CER)** che la ***chiave privata del certificato (PEM)*** per l'utilizzo nei comandi PowerShell successivi e nei passaggi della configurazione di Cisco Secure Email:

1. Fare clic ed evidenziare il Nome interno del certificato appena creato.
2. Fare clic su **Esporta**
    r. Impostazione della directory di salvataggio per facilitare l'accesso (modifica in base alle esigenze)
    b. Assicurarsi che il formato di esportazione sia impostato su **PEM (.crt)**
    c. Fare clic su **OK.**

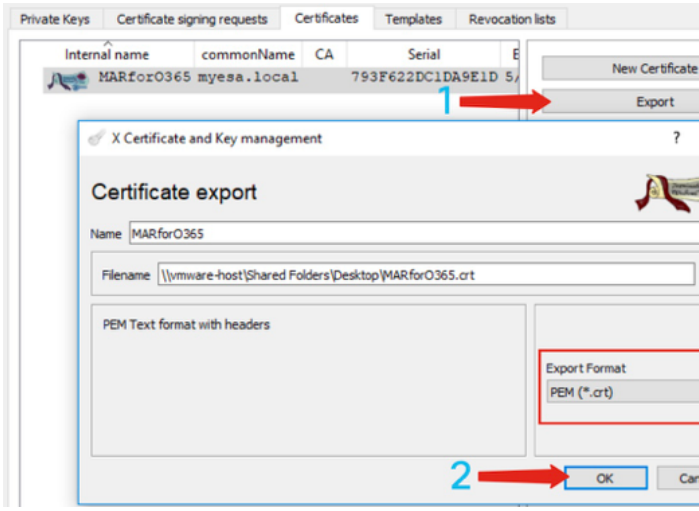

Figura 16: Uso di XCA (esportazione CRT) (fasi 1-2)

3. Fare clic sulla scheda **Chiavi private**
4. Fare clic ed evidenziare il Nome interno del certificato appena creato.
5. Fare clic su **Esporta**
    r. Impostazione della directory di salvataggio per facilitare l'accesso (modifica in base alle esigenze)
    b. Assicurarsi che il formato di esportazione sia impostato su **PEM private (.pem)**
    c. Fare clic su **OK.**
6. Uscire e chiudere XCA

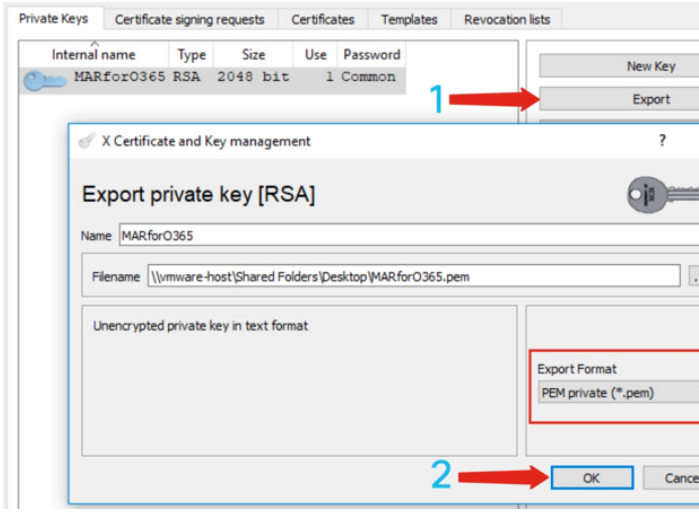

Figura 17: Utilizzo di XCA (esportazione PEM) (passaggi 3-5)

Infine, si prenderà il certificato creato ed estrarrà l'**identificazione personale**, necessaria per configurare Cisco Secure Email.

1. Utilizzando Windows PowerShell, eseguire quanto segue:

```
$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. Per ottenere i valori per i passaggi successivi, salvare in un file o copiare negli Appunti:

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

Nota: “c:\Users\joe\Desktop..." è il percorso del PC in cui si sta salvando l'output.

L'output previsto durante l'esecuzione del comando PowerShell dovrebbe essere simile al seguente:

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

Come si vede, il comando PowerShell chiama l'identificazione personale *base64Thumbprint*, che è l'**identificazione personale** necessaria per la configurazione del gateway Cisco Secure Email.

Èstata inoltre completata la creazione del **certificato pubblico (file CER)** necessario per la registrazione dell'app di Azure. Inoltre, è stata creata la ***chiave privata del certificato (file PEM)*** che verrà utilizzata nella sezione Configurazione di Cisco Secure Email.

Sono disponibili i valori necessari per registrare l'applicazione in Microsoft Azure.

[Procedere con "Registrazione di un'app Azure per l'utilizzo con Cisco Secure Email"]

Appendice B

Nota: questa operazione è necessaria SOLO se sul gateway è in esecuzione AsyncOS 11.x o 12.x for Email.

Autorizzazioni API (AsyncOS 11.x, 12.x)

Nel riquadro dell'applicazione, in Opzioni di gestione...

1. Seleziona **autorizzazioni API**
2. Fare clic su **+ Aggiungi autorizzazione**
3. Scorrere verso il basso fino a **API legacy supportate** e selezionare **Exchange**
4. Selezionare le autorizzazioni seguenti per le autorizzazioni delegate: EWS > "EWS.AccessAsUser.All" (accedere alle cassette postali come utente connesso tramite i servizi Web di Exchange)Mail > "Mail.Read" (Leggi posta utente)Mail > "Mail.ReadWrite" (Lettura e scrittura posta utente)Mail > "Mail.Send" (Invia posta come utente)
5. Scorrere fino alla parte superiore del riquadro...
6. Selezionare le autorizzazioni seguenti per le autorizzazioni applicazione: "full_access_as_app" (Usa i servizi Web di Exchange con accesso completo a tutte le cassette postali)Mail > "Mail.Read" (Leggi posta utente)Mail > "Mail.ReadWrite" (Lettura e scrittura posta utente)Mail > "Mail.Send" (Invia posta come utente)
7. *Facoltativo:* Per impostazione predefinita, Microsoft Graph è abilitato per le autorizzazioni "User.Read"; è possibile lasciare configurata questa opzione oppure fare clic su **Leggi** e fare clic su **Rimuovi autorizzazioni** per rimuoverla dalle autorizzazioni API associate all'applicazione.
8. Fare clic su **Aggiungi autorizzazioni** (o **Aggiorna autorizzazioni**, se Microsoft Graph era già presente nell'elenco)
9. Infine, fare clic su **Concedi consenso amministratore per...** per assicurarsi che le nuove autorizzazioni vengano applicate all'applicazione
10. Verrà visualizzato un messaggio che chiede:
    "*Concedere il consenso per le autorizzazioni richieste per tutti gli account in <Nome Azure>? In questo modo verranno aggiornati tutti i record di consenso amministratore esistenti che questa applicazione deve già corrispondere a quanto elencato di seguito.*"

    Fare clic su **Sì**

A questo punto, viene visualizzato un messaggio verde di esito positivo e nella colonna "Consenso amministratore richiesto" viene visualizzato il messaggio Concesso, simile al seguente:

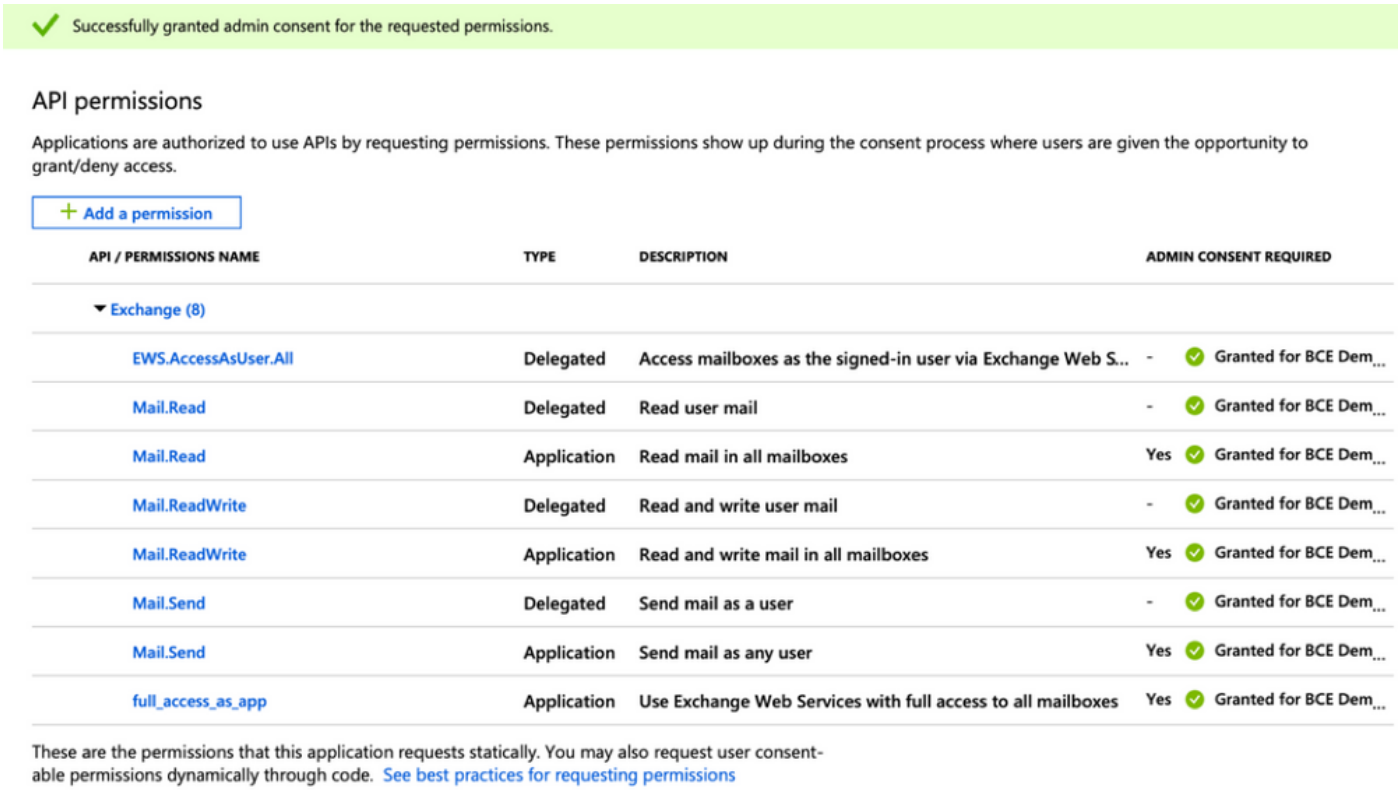

Figura 18: Registrazione dell'app di Microsoft Azure (sono necessarie le autorizzazioni API)

[Procedere con "Registrazione di un'app Azure per l'utilizzo con Cisco Secure Email"]

Informazioni correlate

- Cisco Email Security Appliance - Supporto dei prodotti
- Cisco Email Security Appliance - Note di rilascio
- Cisco Email Security Appliance - Guida per l'utente