

TIM PROTEZIONE DISPOSITIVI

Mobile Treath Defence

Configurazione dispositivi Apple con profilo BYOD

Non necessaria inizializzazione del dispositivo



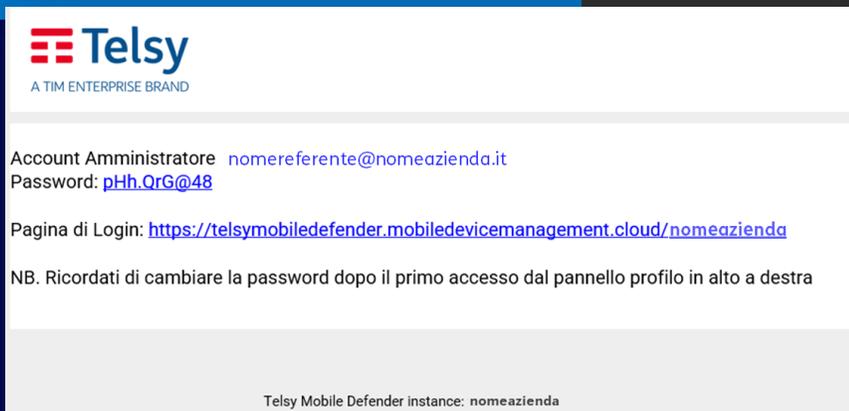
Powered by



STEP 1

Accedi alla console web **Mobile Threat Defence**

Le credenziali e il link di accesso alla piattaforma sono riportate nella mail di conferma di attivazione della licenza inviata in automatico dal sistema. Controlla la tua casella di posta.



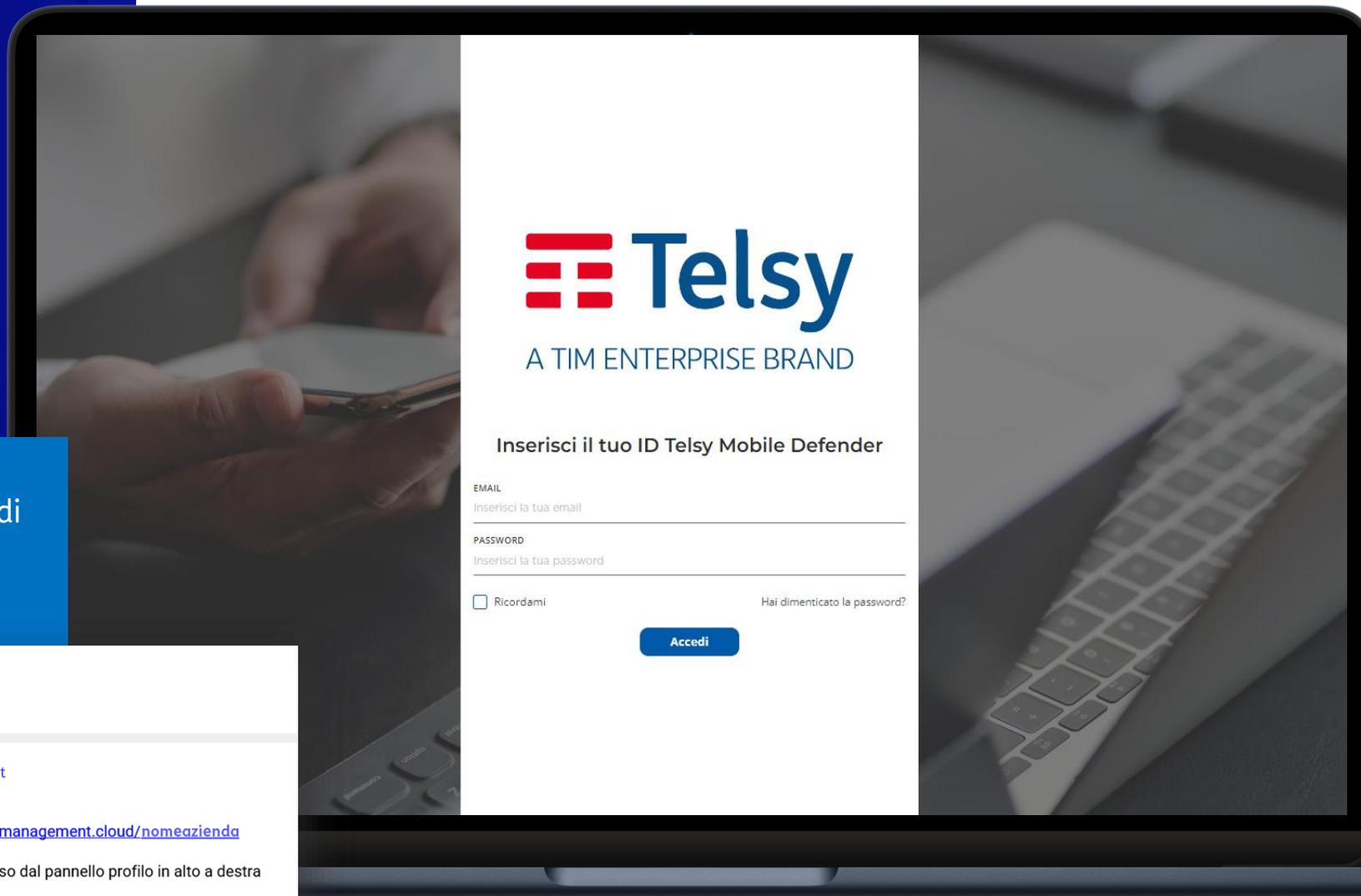

A TIM ENTERPRISE BRAND

Account Amministratore nomereferente@nomeazienda.it
Password: [pHh.QrG@48](#)

Pagina di Login: <https://telsymobiledefender.mobiledevicemanagement.cloud/nomeazienda>

NB. Ricordati di cambiare la password dopo il primo accesso dal pannello profilo in alto a destra

Telsy Mobile Defender instance: nomeazienda



STEP 2

Nella sezione 'Impos. Globali' > 'Generale', controlla che siano attive le voci evidenziate nell'immagine

La voce '**Consenti accesso amministratore al rivenditore Telsy S.p.A.**' abilita la possibilità di accesso all'Help Desk Telsy in caso di supporto

Una volta completata la registrazione dei dispositivi, la voce '**Consenti Registrazione Dispositivi Ospite**' potrà essere disattivata

The screenshot displays the Telsy Mobile Defender Admin interface. The left sidebar contains a navigation menu with the following items: Dashboard, Sicurezza, Licenza, Gestione, Catalogo privato, and Impos. globali (expanded to show Generale, Apple, Google, Samsung Knox, Single Sign On, and Directory Sync). The main content area is titled 'IMPOSTAZIONI SERVER' and contains several settings:

- Attenzione: Per registrare e gestire i dispositivi iOS configura [Apple Push Certificate](#)
- Attenzione: Per gestire nuovi dispositivi Android configura [Android Enterprise](#)
- Telsy Mobile Defender Admin > Impos. Globali > Generale
- IMPOSTAZIONI SERVER
 - Presto il consenso all'invio di newsletter per finalità di promozione commerciale. (Toggle: ON)
 - Consenti accesso amministratore al rivenditore Telsy S.p.A.** (Toggle: ON) - This item is highlighted with a green box and a green arrow.
 - Consenti Registrazione Dispositivi Ospite (Toggle: ON)
 - Controllo integrità per gli enroll Android Enterprise (Toggle: OFF)
 - Chiudi Telsy Mobile Defender Agent (Android) al termine della registrazione (Toggle: OFF)
 - Intervallo di aggiornamento info dispositivi (Dropdown: 72 Ore)
 - Installa automaticamente le app pre-associate alla registrazione del dispositivo (Toggle: OFF)

STEP
3

Effettua il download del file CSR dalla sezione **‘Impos. Globali’ > ‘Apple’ > ‘PUSH CERTIFICATE’**

Questo step è necessario ad ottenere il certificato Apple Push e consentire la registrazione dei dispositivi Apple

Telsy
A TIM ENTERPRISE BRAND

Attenzione: Per registrare e gestire i dispositivi iOS configura Apple Push Certificate

TELSYPUSH MOBILE DEFENDER ADMIN > IMPOS. GLOBALI > APPLE > **PUSH CERTIFICATE**

PUSH CERTIFICATE DEPLOYMENT PROGRAM VOLUME PURCHASE PROGRAM

Per gestire i tuoi dispositivi mobili iOS, devi utilizzare un certificato per le notifiche push di Apple. Questo certificato stabilisce, mediante il servizio Apple Push mobili Apple e il server.

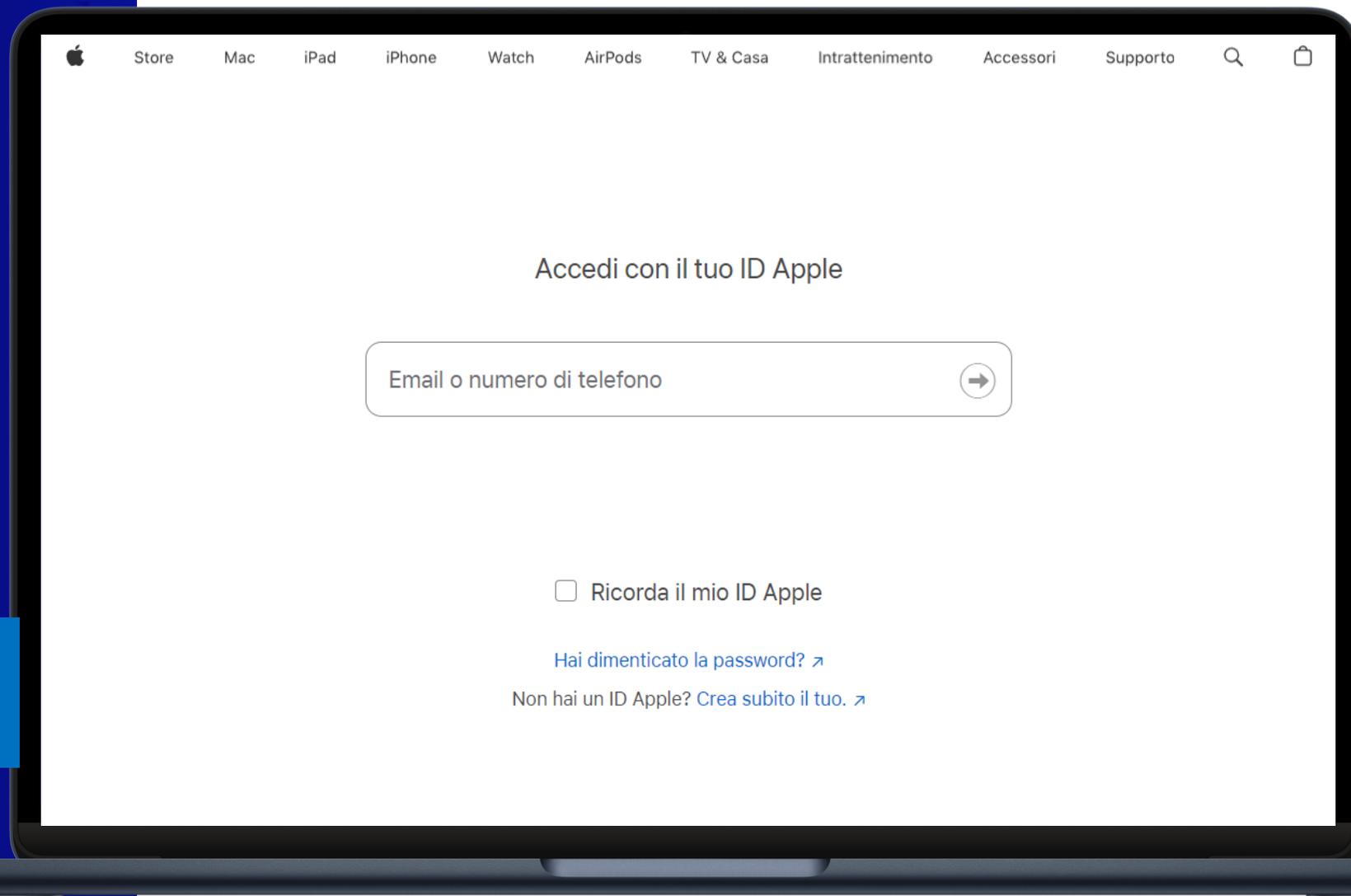
Scarica CSR
Per ottenere il certificato, scarica il file CSR ed esegui l'accesso nel Portale dei Certificati Apple Push.

Carica certificato
File: nessun file caricato
Seleziona il certificato che hai scaricato dal Portale dei Certificati Apple Push

STEP
4

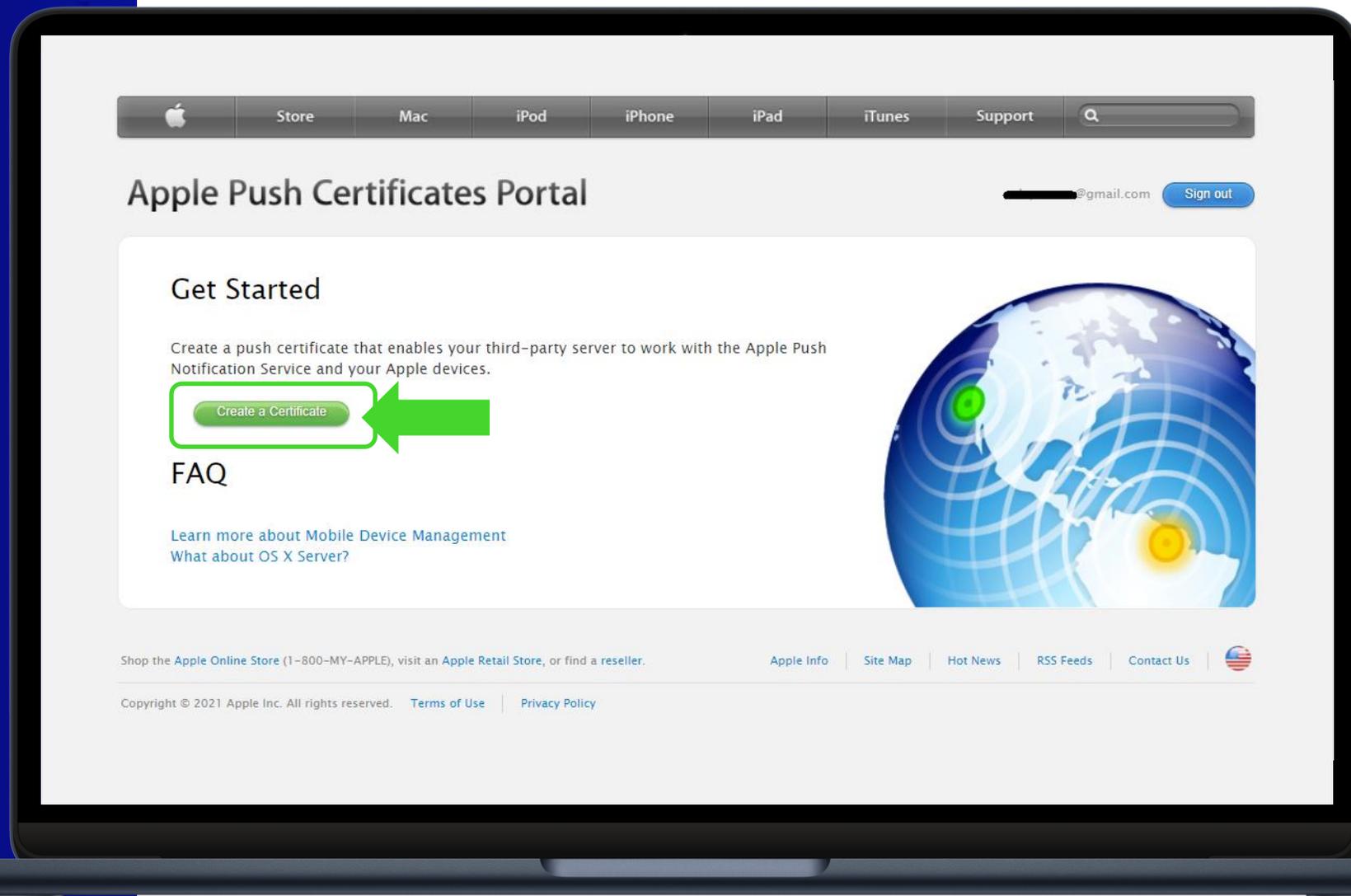
Accedere al Portale
Apple Push al
seguente link
<https://identity.apple.com/pushcert/>
utilizzando un Apple
ID dell'organizzazione

In caso non si disponga di un account
Apple (anche base e non business) può
esserne creato uno nuovo



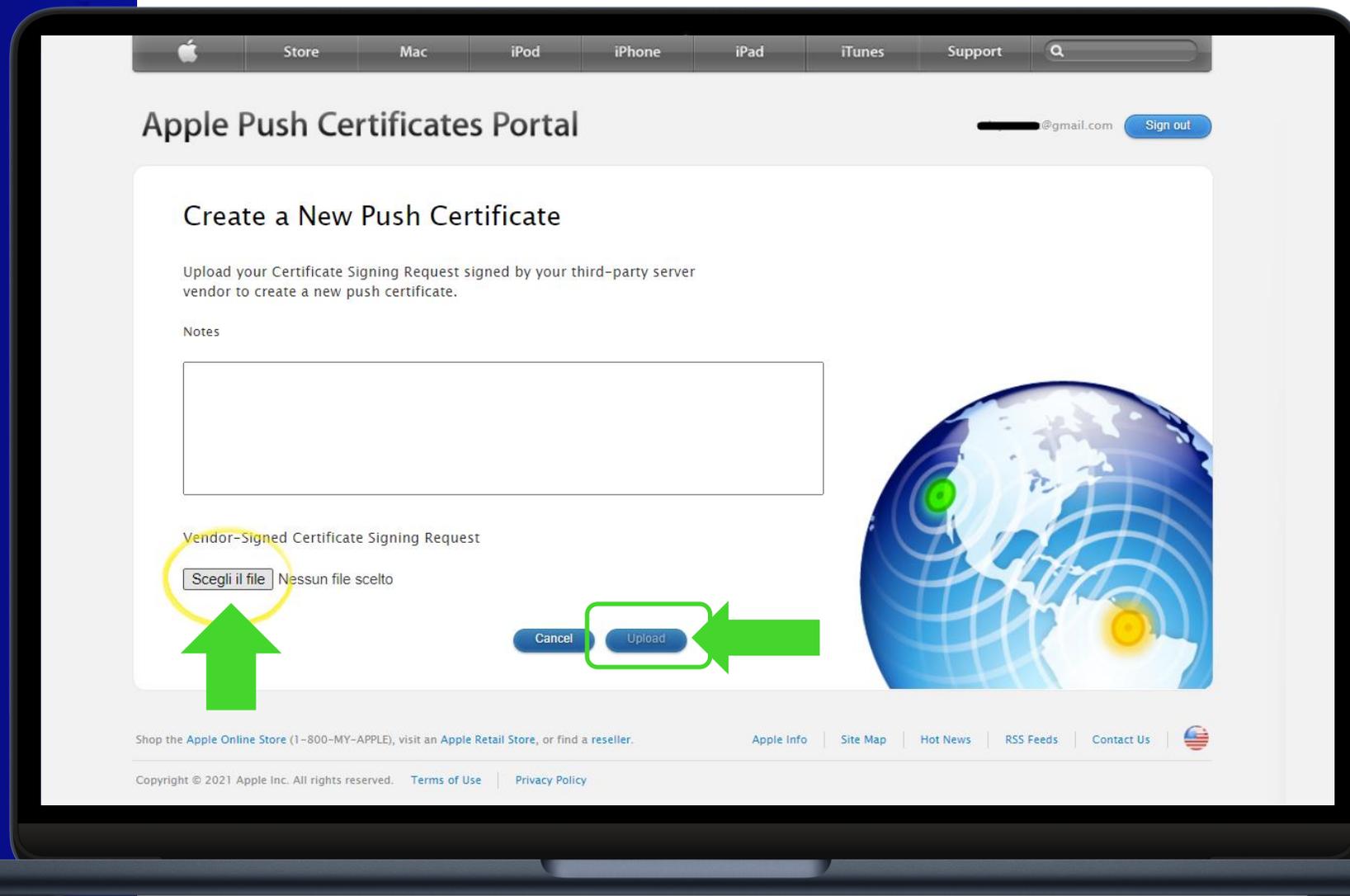
STEP 5

Dall'Apple Push Certificate Portal clicca su 'Create a Certificate'



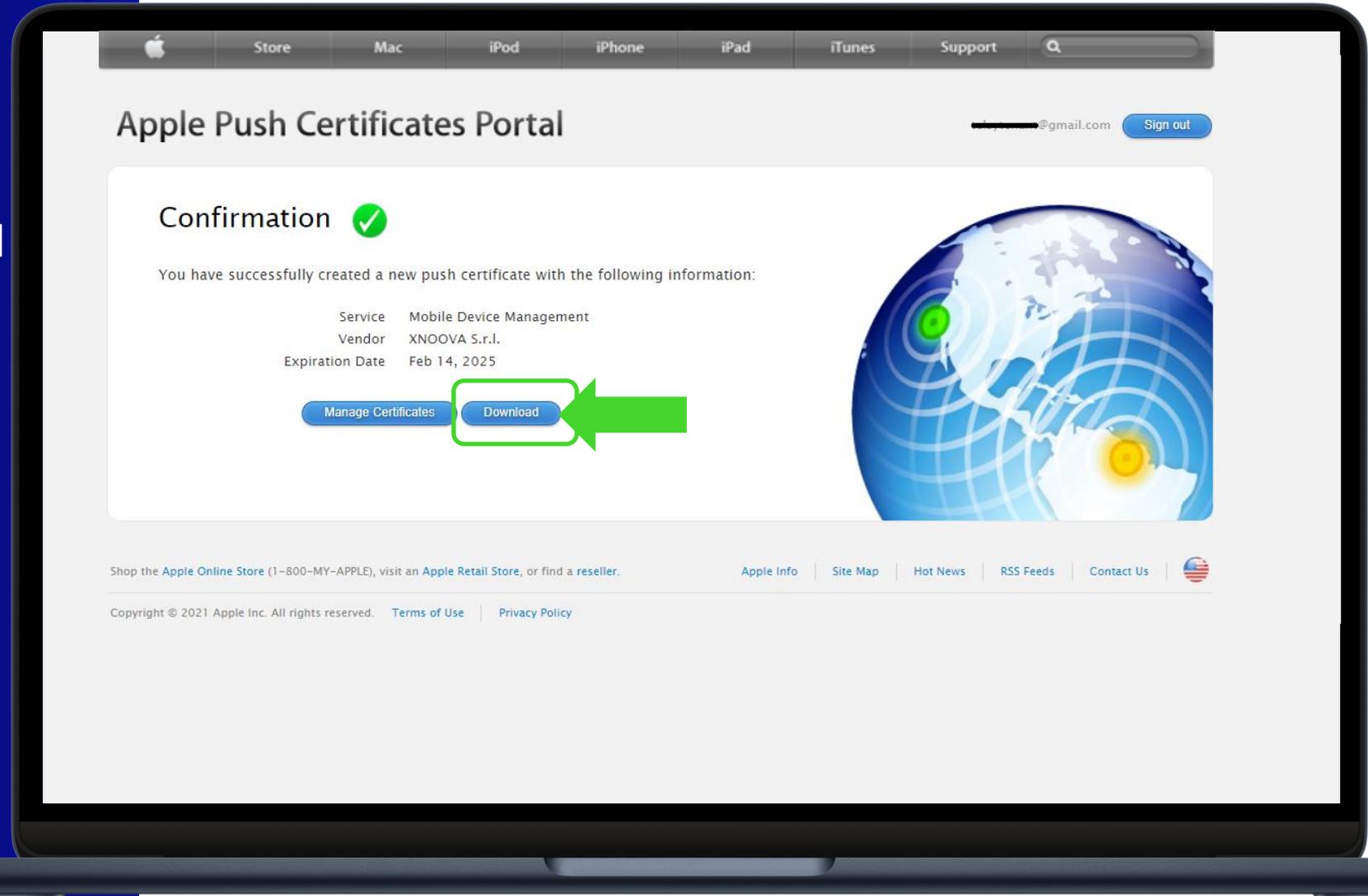
STEP 6

Da 'Scegli file'
caricare il file CSR
precedentemente
scaricato dalla
console web **Mobile
Threat Defence** e
clicca poi su 'Upload'



STEP 7

Il certificato così creato dovrà essere scaricato cliccando su 'Download' per poi essere caricato sulla console **Mobile Threat Defence**



STEP
8

Torna sulla web console **Mobile Threat Defence** nella sezione 'Impos. Globali' > 'Apple' > '**PUSH CERTIFICATE**' e carica il certificato appena scaricato

Telsy
A TIM ENTERPRISE BRAND

Attenzione: Per registrare e gestire i dispositivi iOS configura **Apple Push Certificate**

TELSY MOBILE DEFENDER ADMIN > IMPOS. GLOBALI > APPLE > **PUSH CERTIFICATE**

PUSH CERTIFICATE | DEPLOYMENT PROGRAM | VOLUME PURCHASE PROGRAM

Per gestire i tuoi dispositivi mobili iOS, devi utilizzare un certificato per le notifiche push di Apple. Questo certificato stabilisce, mediante il servizio Apple Push mobili Apple e il server.

Scarica CSR

Per ottenere il certificato, scarica il file CSR ed esegui l'accesso nel [Portale dei Certificati Apple Push](#).

Carica certificato
File: nessun file caricato

Seleziona il certificato che hai scaricato dal [Portale dei Certificati Apple Push](#)

STEP 9

Il certificato Apple Push risulta caricato correttamente

NB: il certificato Apple Push deve essere aggiornato ogni 12 mesi e per farlo sarà sufficiente ripetere gli step dal 3 all'8 di questa guida

Telsy
A TIM ENTERPRISE BRAND

Attenzione: Per registrare e gestire i dispositivi iOS configura [Apple Push Certificate](#)

TELSY MOBILE DEFENDER ADMIN > IMPOS. GLOBALI > APPLE > **PUSH CERTIFICATE**

PUSH CERTIFICATE DEPLOYMENT PROGRAM VOLUME PURCHASE PROGRAM

Per gestire i tuoi dispositivi mobili iOS, devi utilizzare un certificato per le notifiche push di Apple. Questo certificato stabilisce, mediante il servizio Apple Push mobili Apple e il server.

Scarica CSR

Per ottenere il certificato, [scarica il file CSR](#) ed esegui l'accesso nel [Portale dei Certificati Apple Push](#).

Sovrascrivi certificato

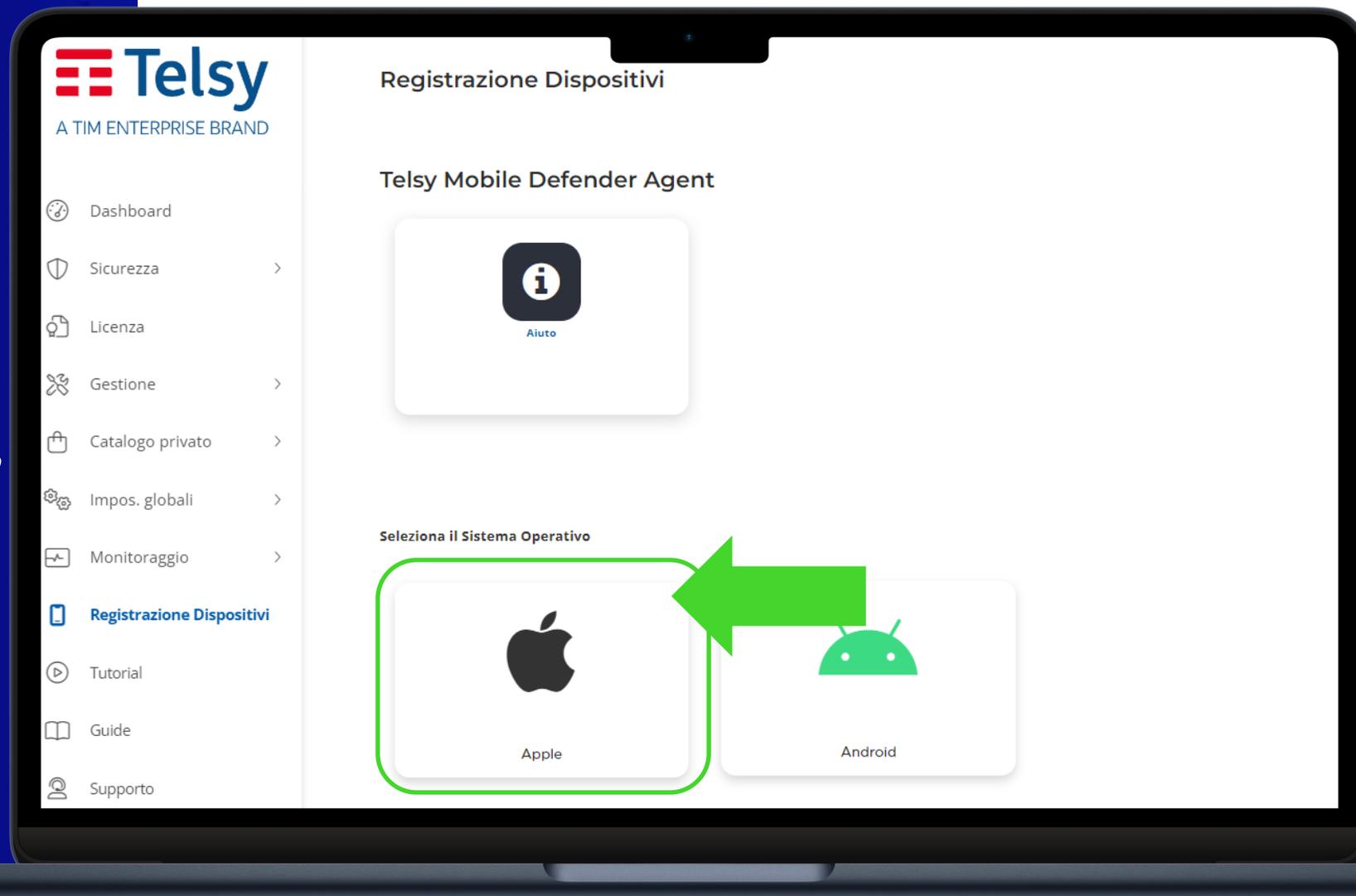
File: UEM_Push_Certificate.pem
Certificate Name: APSP:735e8a73-dfb4-450b-a9e7-0e0587658b7c
Apple ID: [redacted]@gmail.com

Valido fino al: 16:31:04 14-02-2025
Seleziona il certificato che hai scaricato dal Portale dei Certificati Apple Push

STEP 10

Procediamo ora con il creare il profilo di registrazione da caricare poi sul dispositivo.

Vai alla sezione 'Registrazione dispositivi', scorri fino a 'Seleziona il Sistema Operativo' e clicca su **Apple**

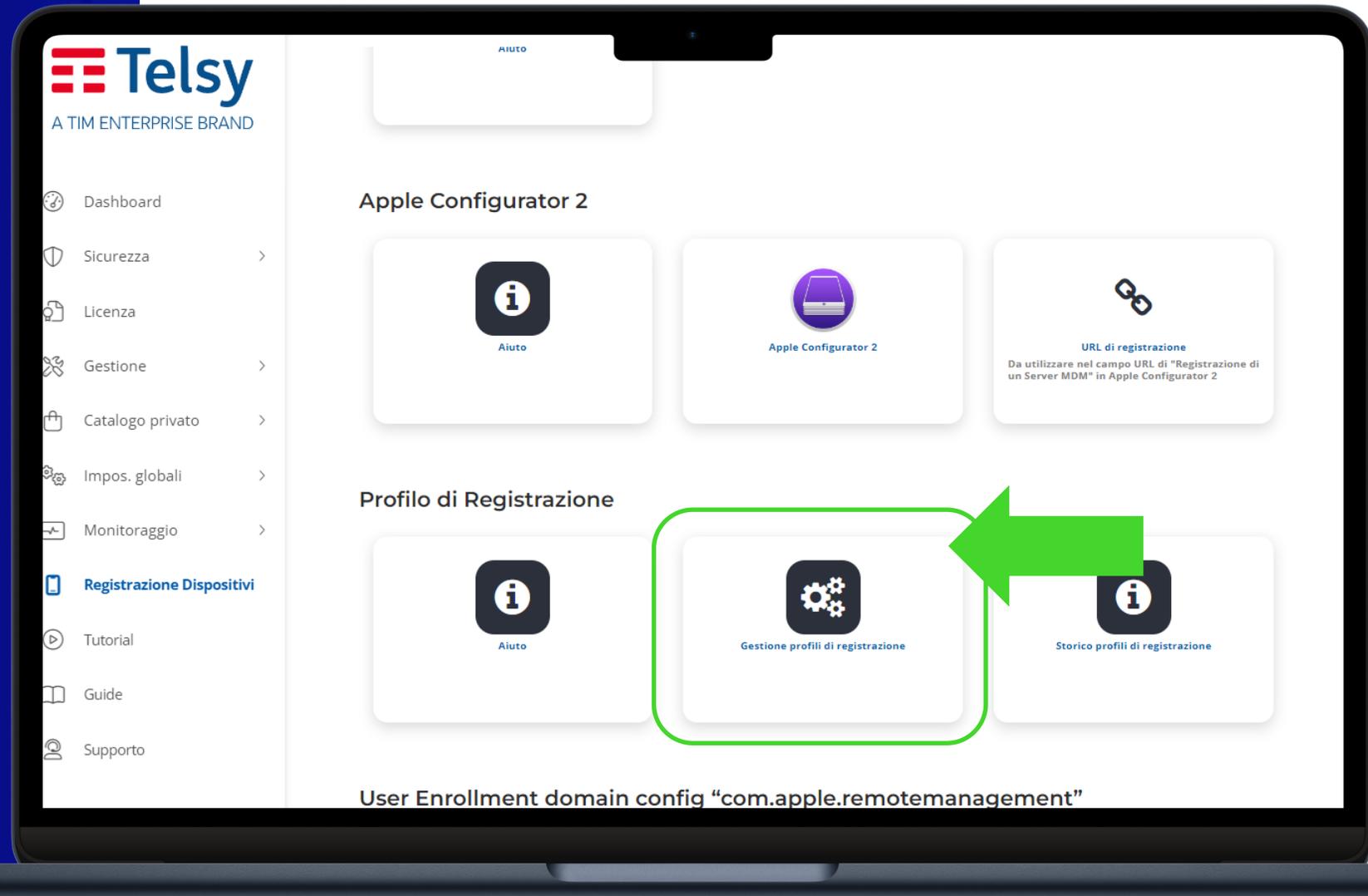


STEP 11

Scorri poi fino a **‘Profilo di Registrazione’** e clicca su **‘Gestione profilo di registrazione’**.

Ti si aprirà la finestra **‘Gestione profilo di registrazione’** dove saranno elencati tutti i profili che andrai a creare.

In questa finestra clicca sul tasto **‘Aggiungi +’** per creare un profilo di registrazione.



STEP 12

Compila i campi richiesti dando un nome al profilo e specificando per quanti dispositivi sarà utilizzato. Questo profilo potrà essere infatti associato a più dispositivi. Clicca poi su **Salva**

L'opzione **'Limita a placeholder'** indica che è possibile registrare il dispositivo solo se è stato specificato un Segnaposto (placeholder). Per definire un placeholder andare in **Gestione > Dispositivi** e cliccare su **'Aggiungi segnaposto'**. Se non vuoi aggiungere un segnaposto, disattiva l'opzione.

Gestione profili di registrazione

Nome:
Nome identificativo del profilo.
Nome

Numero utilizzi consentiti:
Numero massimo di registrazione dispositivi consentito con questo profilo.
Numero utilizzi consentiti

Limita a placeholders:
Se selezionato, il profilo può essere utilizzato esclusivamente se il dispositivo è inserito come placeholder.

Utilizzo singolo:
Se selezionato, il profilo può essere utilizzato una sola volta (questo valore prevale sul campo numero di utilizzi consentiti).

Scadenza:
Indica la data di scadenza del profilo. Una volta scaduto, non può più essere scaricato, inviato e/o utilizzato per la registrazione di dispositivi.
gg/mm/aaaa

Indietro

Telsa
A TIM ENTERPRISE B...

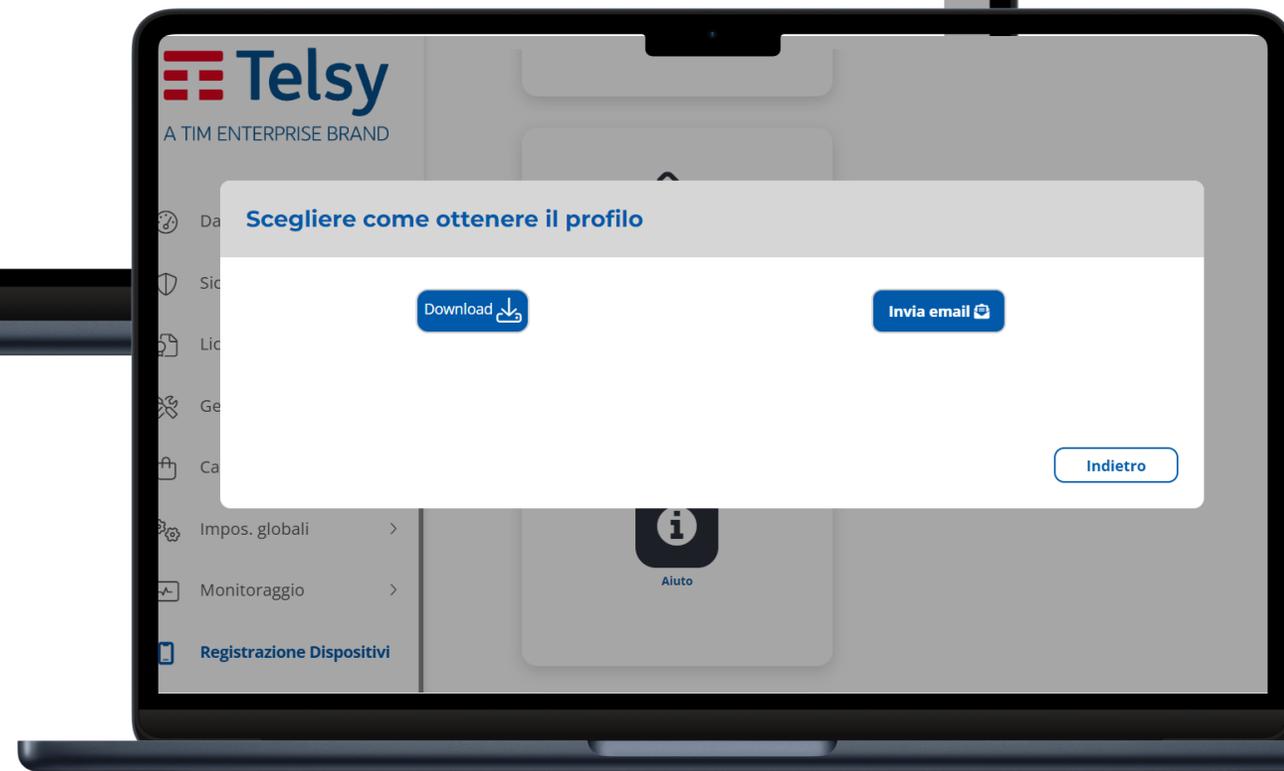
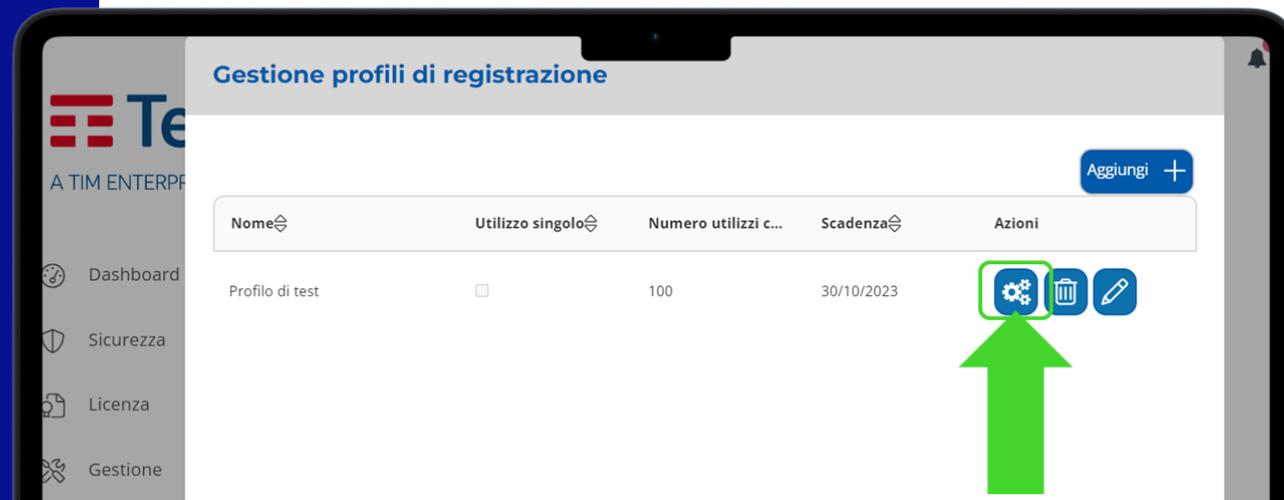
- Dashboard
- Sicurezza
- Licenza
- Gestione
- Catalogo privato
- Impos. globali
- Monitoraggio
- Registrazione Dispositivi**
- Tutorial

STEP 13

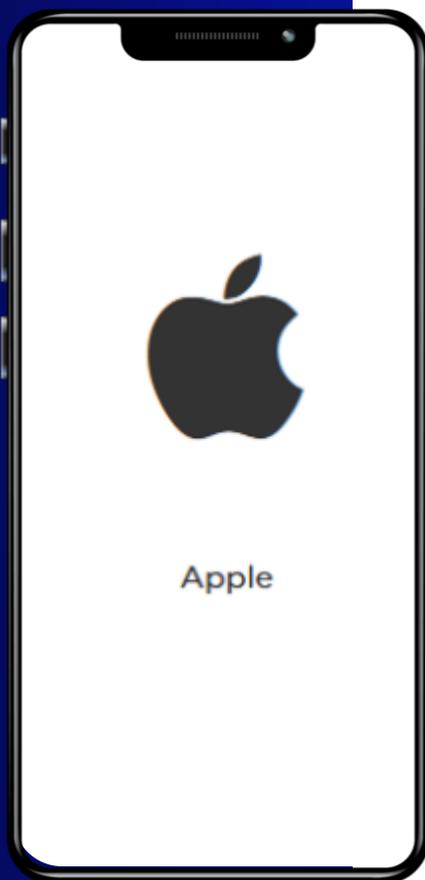
Clicca sul pulsante con l'icona degli ingranaggi sulla riga del profilo appena creato e scegli come ottenere/ condividere il profilo.

È possibile selezionare 'Download' per scaricare il profilo creato oppure 'Invia e-mail' per inviare il profilo all'indirizzo mail configurato sul dispositivo da registrare.

Si consiglia di scegliere l'opzione 'Invia e-mail' così da poter inviare il profilo a tutti gli utenti i cui dispositivi dovranno essere registrati nella piattaforma.



Passiamo al dispositivo mobile da configurare



#01

Ricezione mail

L'utente riceverà una mail con le istruzioni da seguire per impostare il profilo di registrazione.

#02

Scaricare il file

allegato alla mail



L'amministratore di sistema di [redacted] ti ha inviato il profilo per attivare il monitoraggio e la protezione dei dati e degli strumenti aziendali sul tuo dispositivo Apple.
Apri l'allegato sul dispositivo Apple da configurare, vai in Impostazioni > Generale > VPN e Gestione remota > Profilo di registrazione di Chimpa e segui la procedura accettando i termini.
Se non riesci ad aprire direttamente il profilo dal tuo client di posta elettronica, puoi provare a salvarlo in File, aprire File, aprire il profilo salvato e poi procedere in Impostazioni > Generale > VPN e Gestione remota > Profilo di registrazione di Chimpa e segui la procedura accettando i termini.

Telsy Mobile Defender instance: adtelsy

#03

Installare il Profilo

Apri le 'Impostazioni' del dispositivo e clicca su 'Generali' > 'VPN e gestione dispositivi'.
Seleziona il profilo di gestione per procedere all'installazione. Terminata l'installazione il dispositivo sarà registrato.

ANNULLARE LA GESTIONE DI UN DISPOSITIVO

Dalla sezione **'Gestione'** > **'Dispositivi'** individua il dispositivo di interesse e clicca sull'icona indicata nell'immagine per aprire il menu delle azioni. Scorri fino alla voce **'Annulla Gestione ed Elimina'**

Eseguendo questa operazione il dispositivo sarà rimosso dalla lista dei dispositivi gestiti e non sarà più possibile averne il controllo da remoto.

TELSY MOBILE DEFENDER ADMIN > GESTIONE > DISPOSITIVI

A TIM ENTERPRISE BRAND

Importa Aggiungi Segnaposto Cerca...

NOME	SERIALE	PRODOTTO	STATO	ATTIVO
Galaxy A32	RZ8T4	Samsung S...	✓ SUPERVISIONATO	●
Tab A7	R9WW1008RXX	Samsung S...		
Tab A7 - R	JYFF-Q66	..Samsung S...		
Cl	F17RK	IPhone SE		
Device	22X022C	...Huawei VO...		
Device	R9WW1008RXX			

Dashboard
Sicurezza >
Licenza
Gestione >
Utenti
Dispositivi
Gruppi
Apps & Media >
Smart Workflows
Catalogo privato >
Impos. globali >
Monitoraggio >

Riavvia
Installa Certificato
Rimuovi Certificato
Abilita Protezione Ripristino dati Fabbrica
Abilita Modalità Emergenza
Pulisci Dati Utilizzo
Inizializza
Annulla Gestione
Annulla Gestione ed Elimina