

Distribuisci Security Connector con Intune

Sommario

[Introduzione](#)

[Panoramica](#)

[Procedura](#)

[Limitazioni](#)

[Risoluzione dei problemi](#)

[Log](#)

Introduzione

In questo documento viene descritto come distribuire il connettore di sicurezza utilizzando Intune.

Panoramica

Questa è una guida dettagliata su come ottenere il dispositivo iOS/iPadOS MDM-manage tramite Intune e spingere il profilo tramite Apple Configurator

È inoltre possibile fare riferimento alla documentazione di [registrazione di Intune](#) e alla [guida PDF](#) qui

Nota: questo metodo mostra come eseguire la MDM dei dispositivi tramite Intune e Apple Configurator

Note importanti:

Se stai eseguendo il MDM sui tuoi dispositivi sorvegliati tramite l'app Portale aziendale, puoi iniziare dal Passo 14.

Questo articolo viene fornito così com'è il 12/04/2023, il supporto Umbrella non garantisce che queste istruzioni rimarranno valide dopo questa data ed è soggetto a modifiche in base agli aggiornamenti di Microsoft Intune e Apple iOS.

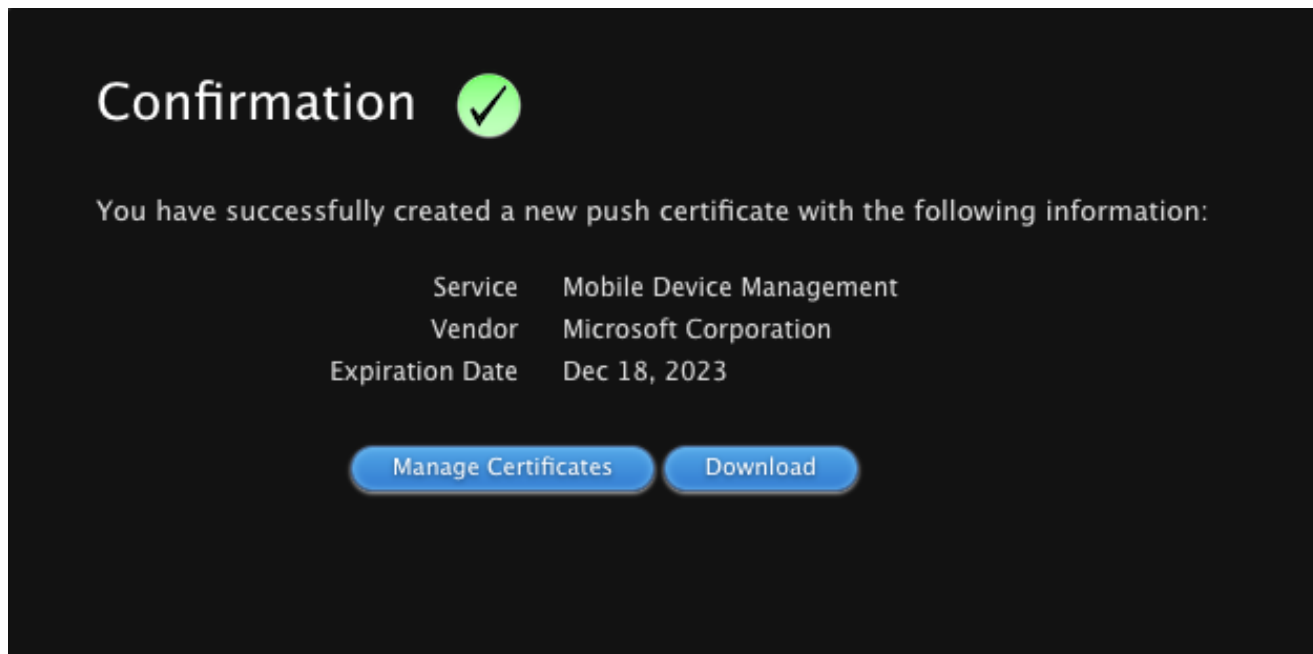
Procedura

1. Accedere al portale di Azure e cercare "Intune". In alternativa, accedere al sito https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/ ed effettuare il login
2. Nella home page di Intune, andare su Dispositivi —> iOS/iPadOS —> Registrazione di

iOS/iPadOS —> Certificato Apple MDM Push e fare clic su "Scarica CSR"

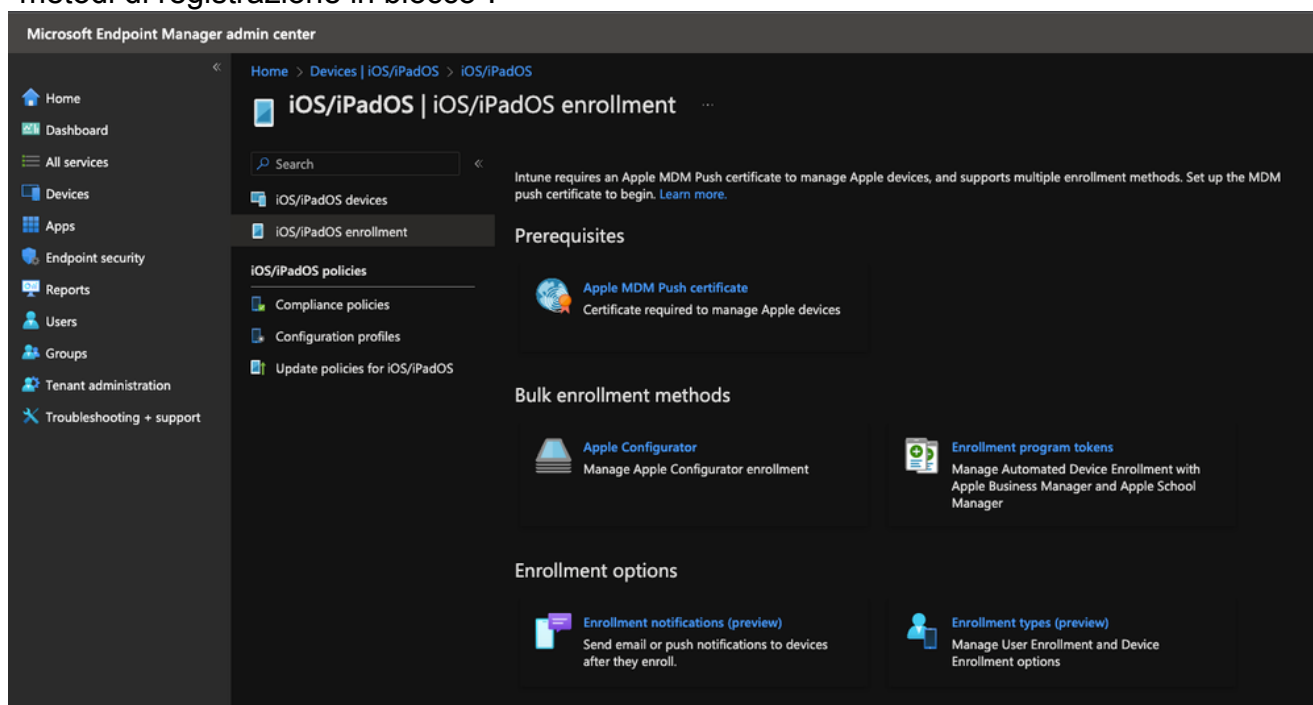


3. Fare quindi clic su "Create your MDM push Certificate" (Crea certificato push MDM), che reindirizza l'utente a <https://identity.apple.com/pushcert/>
4. Sul portale Apple Push Certificates, andare su "Crea certificato" e caricare il file IntuneCSR.csr appena scaricato. Una volta caricato correttamente il file CSR, fare clic su "Download" per scaricare il file Privacy Enhanced Mail (.pem) e procedere al passaggio successivo



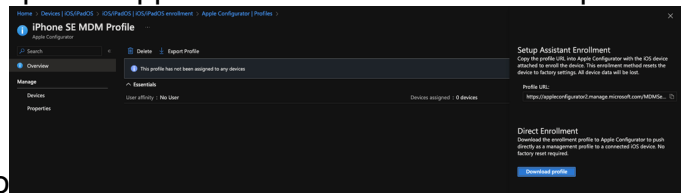
11752968667924

5. Immettere l'indirizzo e-mail dell'account Apple ID utilizzato per accedere al portale Apple Push Certificates e caricare il file .pem in "Apple MDM push certificate" e premere "Upload". Se il caricamento ha esito positivo, vengono visualizzate le altre opzioni per lo sblocco dei "metodi di registrazione in blocco".



11752971407380

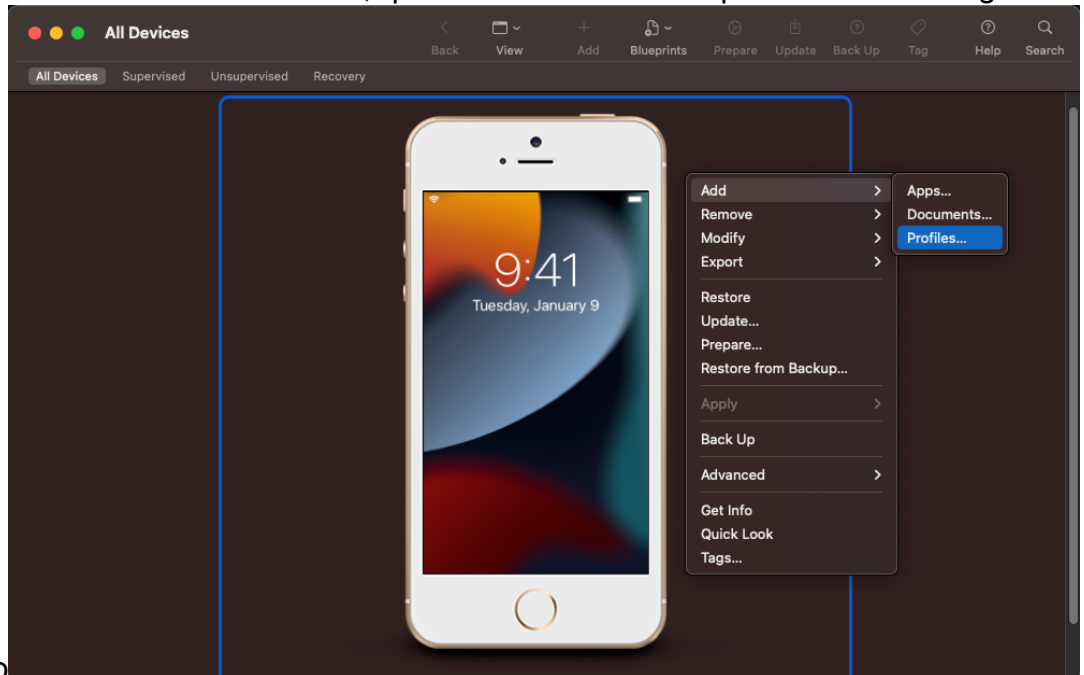
6. Selezionare Apple Configurator —> Profiles —> Create (Crea) e creare un nuovo profilo. Assegnare un nome significativo e per Affinità utente selezionare "Registra senza affinità utente". Una volta creato il profilo, fare clic sul profilo appena creato e selezionare "Esporta



profilo", quindi "Scarica profilo" sul lato destro

11753020728596

7. Scaricare e avviare "Apple Configurator" sul macOS dall'App Store e collegare il telefono tramite cavo Lightning. Fare clic con il pulsante destro del mouse sul dispositivo in Apple Configurator, selezionare Add —> Profiles, quindi selezionare il file profile.mobileconfig



appena scaricato

11753024446100

Windows alternativo: Utilità di configurazione iPhone

8. Al termine della sincronizzazione, sul dispositivo iOS/iPadOS passare all'app Impostazioni e passare a Generale —> Gestione VPN e dispositivi —> Profilo di gestione

No SIM 

4:25 PM

@ 69% 



VPN & Device Management



VPN

Not Connected >

[Sign In to Work or School Account...](#)

DOWNLOADED PROFILE



Management Profile



Cancel

Install Profile

Install



Management Profile

Signed by IOSProfileSigning.manage.microsoft.com

Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrollment Challenge

More Details



Remove Downloaded Profile

Profile Installed

[Done](#)



Management Profile

Default Directory

Signed by IOSProfileSigning.manage.microsoft.com

Verified ✓

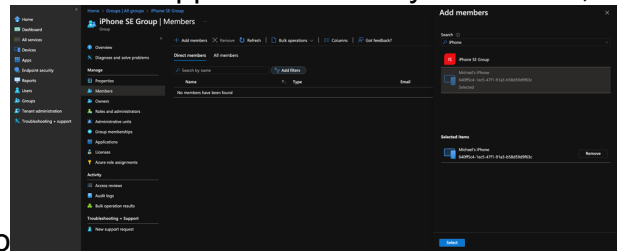
Description Install this profile to get access to your company apps

Contains Mobile Device Management
Device Identity Certificate
2 Certificates

More Details



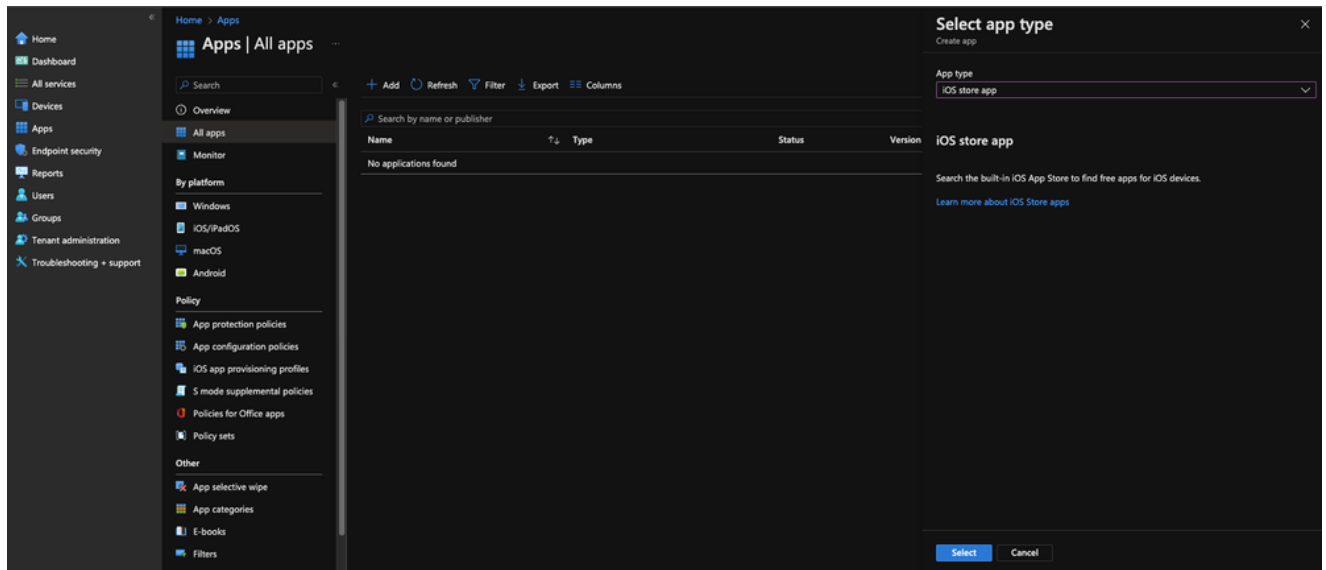
. Individuare il dispositivo MDM su cui si desidera installare l'app Cisco Security Connector,



nell'elenco e aggiungerlo al gruppo appena creato

11753692550036

14. Vai ad Apps —> All apps —> Add. Quindi per il tipo di app, selezionare "iOS store app" e confermare facendo clic su "Seleziona"



11753797372436

15. Selezionare "Cerca App Store" e immettere "Cisco Security Connector" nella barra di ricerca e selezionare l'app "Cisco Security Connector" facendo clic su "Seleziona"

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

Select app * ⓘ Search the App Store

Name * ⓘ Cisco Security Connector

Description * ⓘ This application requires licenses for Cisco Clarity and/or Cisco Umbrella.

Publisher * ⓘ Cisco

Appstore URL https://apps.apple.com/us/app/cisco-security-connector/id1282518969?uo=4

Minimum operating system * ⓘ iOS 8.0

Applicable device type * ⓘ 2 selected

Category ⓘ 0 selected

Show this as a featured app in the Company Portal ⓘ Yes No

Information URL ⓘ Enter a valid url

Privacy URL ⓘ Enter a valid url

Developer ⓘ

Owner ⓘ

Previous Next

11753844054420

16. In Assegnazioni, aggiungere il gruppo creato nei passaggi precedenti che contiene il dispositivo MDM, quindi procedere con Revisione e creazione

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

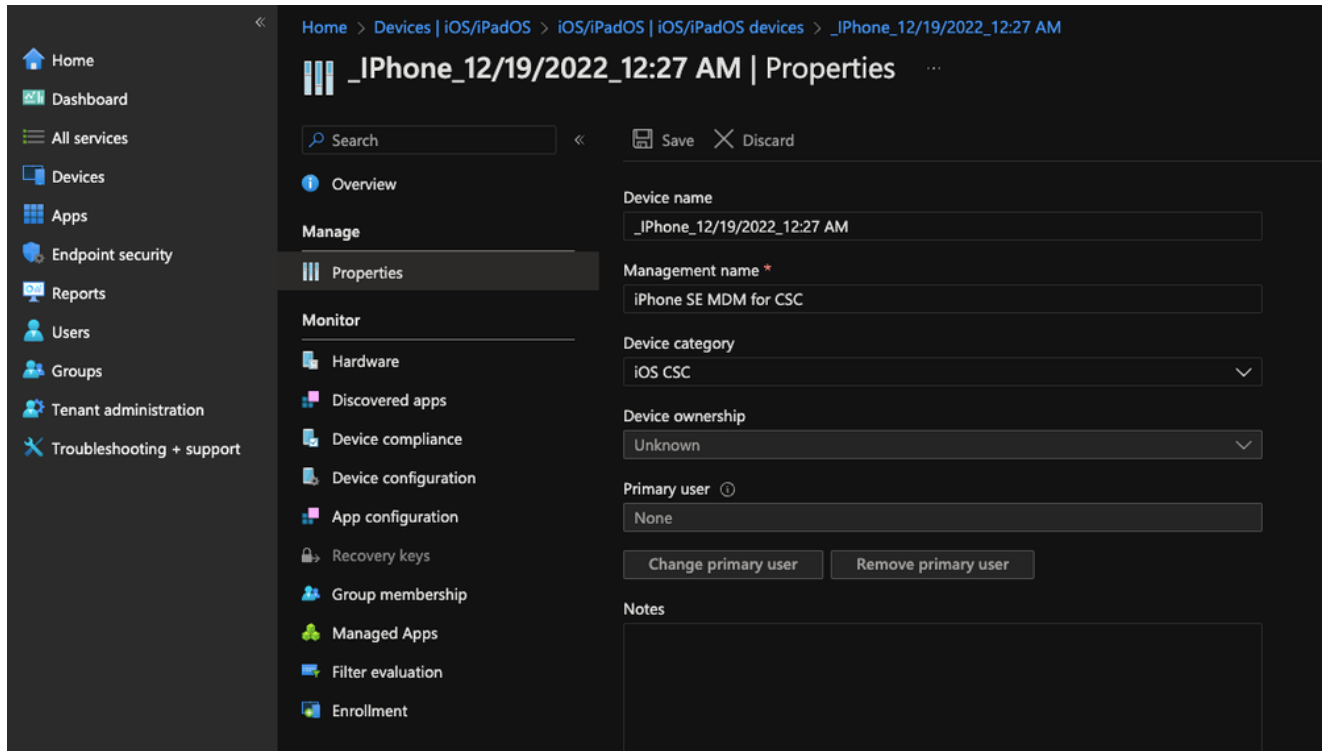
Required ⓘ

Group mode	Group	Filter mode	Filter	VPN	Uninstall on device re...	Install as removable
⊕ Included	iPhone SE Group	None	None	None	No	Yes

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

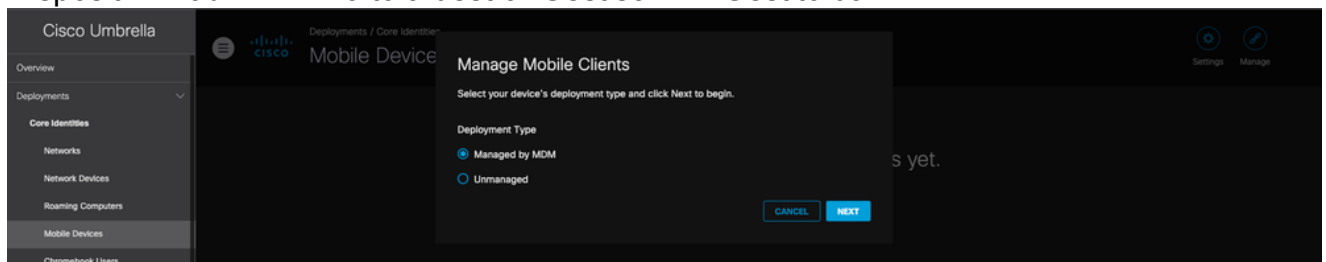
11753839516692

17. [Passaggio facoltativo] Vai a Dispositivi —> iOS/iPadOS —> Dispositivi iOS/iPadOS —> Proprietà —> Categoria dispositivo, crea un profilo e assegna al dispositivo



11753916236820

18. Accedere al dashboard di Cisco Umbrella, in Implementazioni —> Identità principali —> Dispositivi mobili —> in alto a destra: Gestisci —> Gestito da MDM



11753923081492

19. Quindi andare su iOS —> Download della configurazione di Microsoft Intune. Immetti il tuo indirizzo e-mail a cui desideri che gli utenti passino quando selezionano "Segnala un problema" nell'app Cisco Security Connector

Managed Mobile Clients

To deploy Umbrella mobile coverage, download a configuration data file and use it to configure your MDM. For more information, see Umbrella's [iOS](#) and [Android](#) Help.

iOS

Android

iOS Configuration File

Cisco Meraki

[Link MDM](#)

Apple

[Apple Config](#) 

IBM Maas360

[IBM Maas360 Config](#) 

Microsoft Intune

[Microsoft Intune Config](#) 

Jamf

[Jamf Config](#) 

MobiConnect

[MobiConnect Config](#) 

MobileIron

[MobileIron Config](#) 

Workspace ONE

[Workspace ONE Config](#) 

Common Config 

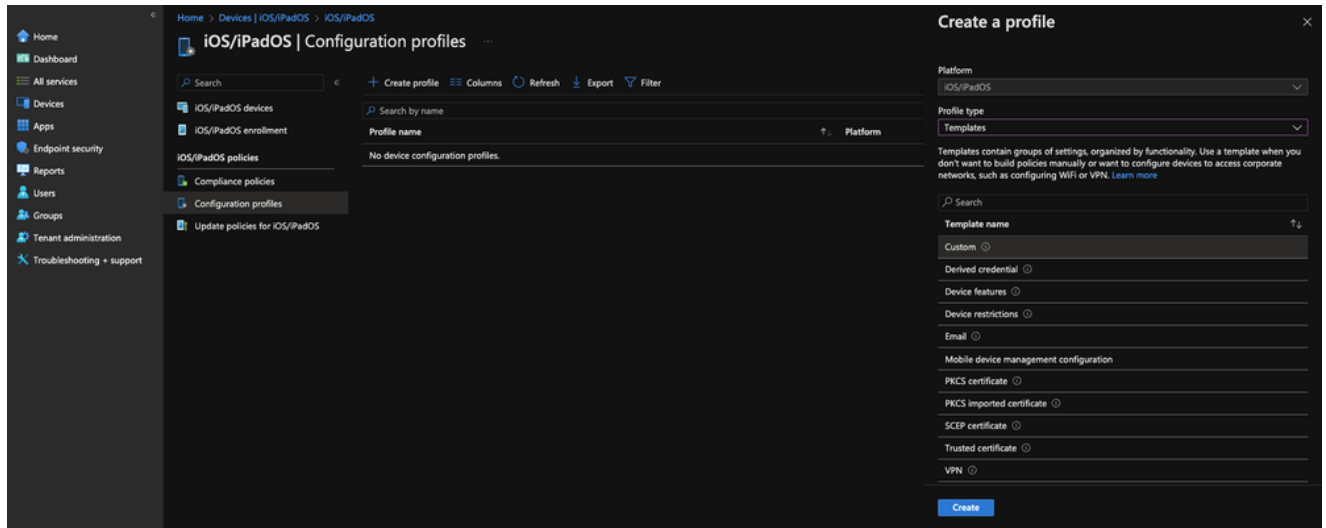
[iOS Config](#) 

BACK

DONE

11753924523540

20. Tornare al portale di Intune, in Dispositivi —> iOS/iPadOS —> Profili di configurazione —> Crea profilo —> Modelli —> Personalizzati



11753988354964

21. Assegnare un nome significativo al profilo di configurazione. Nel Passaggio 2 - Impostazioni di configurazione, caricare il file XML appena scaricato dal dashboard Cisco Umbrella

11754000962196

22. In Assegnazioni, assegnare il gruppo creato in precedenza che contiene il dispositivo MDM e selezionare "Revisione e creazione".
23. Tornare ai dispositivi iOS/iPadOS, selezionare il dispositivo MDM e fare clic su Sincronizza nella parte superiore. Verrà visualizzata una schermata popup sul dispositivo MDM iOS/iPadOS per installare l'app Cisco Security Connector

No SIM



4:30 AM



VPN & Device Management

VPN

VPN

Not Connected



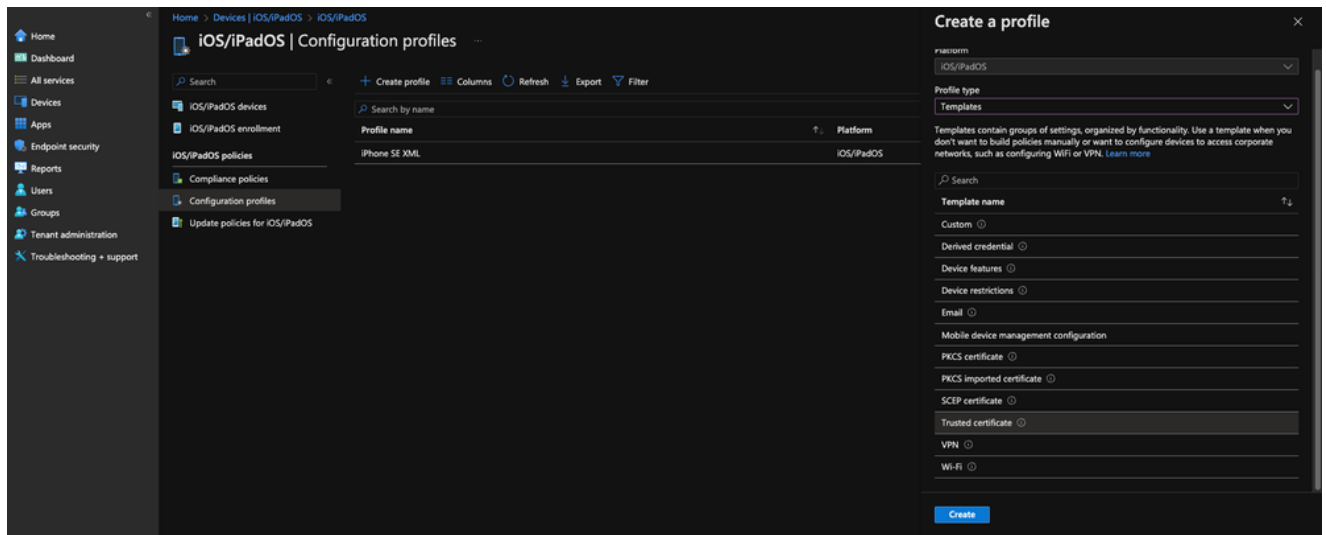
MOBILE DEVICE MANAGEMENT

App Installation

Default Directory is about to install and manage the app "Cisco Security Connector" from the App Store. Your iTunes account will not be charged for this app.

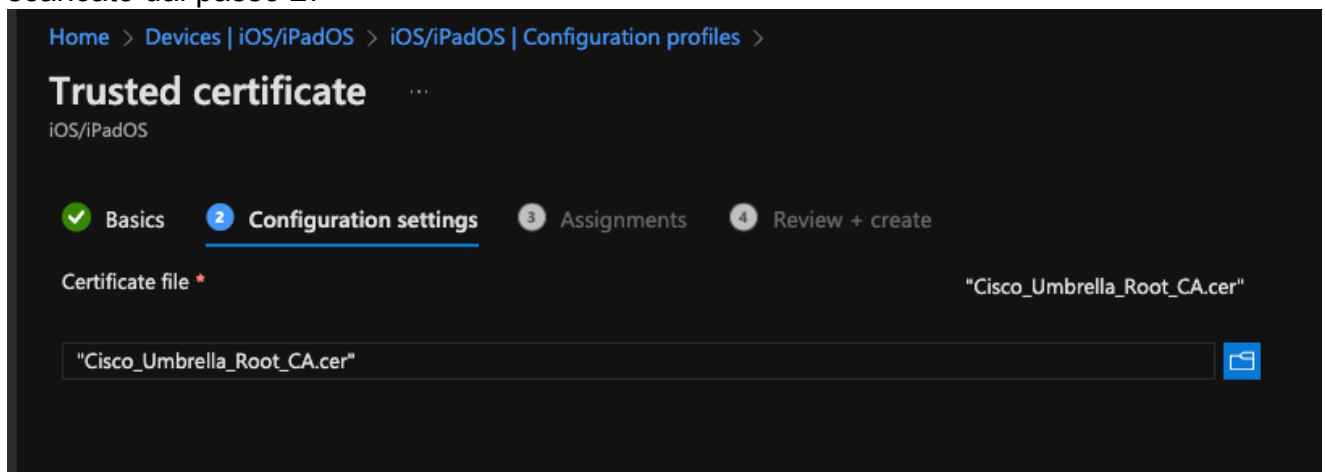
Cancel

Install



11754159037460

29. Nel passo 2 - Impostazioni di configurazione, caricare il certificato radice Umbrella appena scaricato dal passo 27



11754204605460

30. Per Passaggio 3 - Assegnazioni, selezionare il gruppo che contiene il dispositivo MDM iOS/iPadOS e fare clic su "Avanti" e su "Crea"
31. Tornare ai dispositivi iOS/iPadOS e selezionare il dispositivo MDM e premere di nuovo sync nella parte superiore (come al punto 24)
32. Chiudere e riavviare l'app Cisco Security Connector. Lo stato visualizzato è "Protetto da Umbrella"

No SIM 

4:41 AM



Status

DNS SECURITY



Protected by Umbrella



ENDPOINT VISIBILITY



Clarity Not Configured

No SIM



4:48 AM



Cisco Umbrella



Welcome to Umbrella!

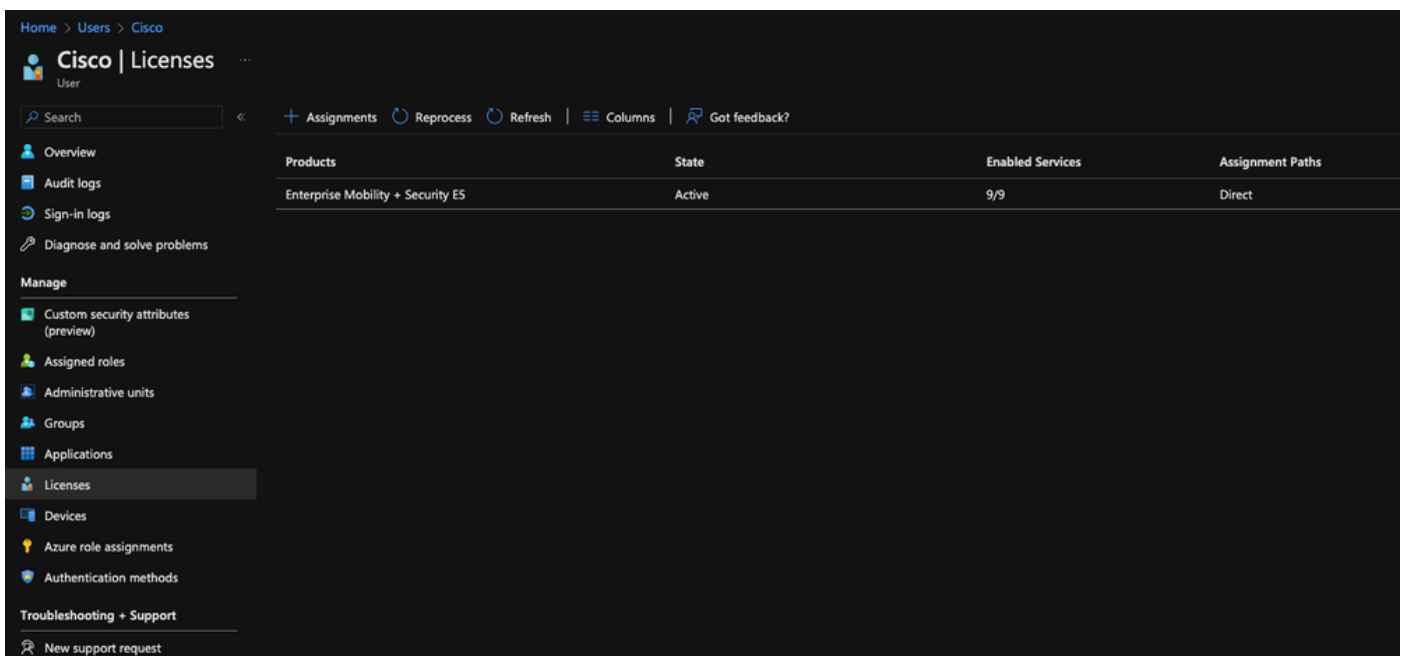
Your internet is faster,
more reliable and better
protected because
you're using Cisco
Umbrella.

- Non è possibile avere alcuna impostazione "Applicazioni limitate" che limiti l'app Umbrella e/o qualsiasi impostazione "Mostra o nascondi" per nascondere l'app Umbrella applicata nel profilo di configurazione del dispositivo.(In Amministrazione Intune > Dispositivi > iOS/iPadOS > Configurazione)

Risoluzione dei problemi

- Come raccogliere i log di diagnostica di Cisco Security Connector
- Errore funzione "Nessun messaggio di posta elettronica amministratore" nel registro CSC
- CSC Stato "Non protetto" sulle reti mobili

In caso di errore: "Nome utente non riconosciuto. L'utente non è autorizzato a usare Microsoft Intune, passare al portale di Azure, in "Utenti" e selezionare il nome utente o l'account che si sta utilizzando per configurare Intune, passare a "Licenze" e verificare che all'utente sia stata assegnata una licenza Intune attiva



The screenshot shows the 'Cisco | Licenses' page in the Microsoft Intune portal. The page has a dark theme. On the left is a navigation pane with options like Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Manage (with sub-options like Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods), and Troubleshooting + Support. The main area displays a table with license information.

Products	State	Enabled Services	Assignment Paths
Enterprise Mobility + Security ES	Active	9/9	Direct

11754557401748

Log

Per impostazione predefinita, la password dei log è `bypass_email_filters`. È inoltre possibile trovare il file `UmbrellaProblemReport.txt`

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).