FDM integrato per Defense Orchestrator

Sommario

Introduzione

In questo documento viene descritto come integrare un dispositivo gestito da Firepower Device Manager (FDM) in Cisco Defense Orchestrator (CDO) utilizzando una chiave di registrazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Device Manager (FDM) Azure in esecuzione versione 7.4.1

Per un elenco completo delle versioni e dei prodotti compatibili, consultare la Guida alla compatibilità di Secure Firewall Threat Defense per ulteriori informazioni.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

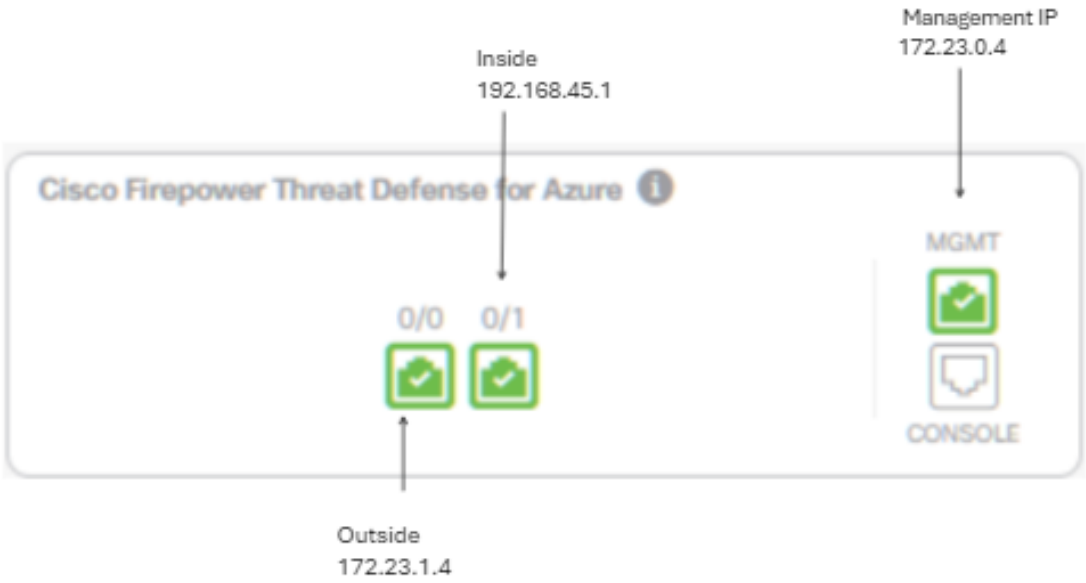
Prima di iniziare il processo di caricamento di un dispositivo gestito da FDM in Cisco Defense Orchestrator (CDO) tramite una chiave di registrazione, verificare che siano soddisfatti i seguenti prerequisiti:

1. Versione compatibile: sul dispositivo deve essere in esecuzione la versione 6.6 o successiva.
2. Requisiti di rete: connessione di Cisco Defense Orchestrator ai dispositivi gestiti
3. Software di gestione: il dispositivo deve essere gestito tramite Secure Firewall Device Manager (FDM).
4. Licenze: il dispositivo può utilizzare una licenza di valutazione valida 90 giorni o una licenza Smart.
5. Registrazioni esistenti: verificare che il dispositivo non sia già registrato con i servizi cloud Cisco per evitare conflitti durante il processo di caricamento.
6. Modifiche in sospeso: verificare che non vi siano modifiche in sospeso nel dispositivo.
7. Configurazione DNS: le impostazioni DNS devono essere configurate correttamente nel dispositivo gestito da FDM.
8. Servizi ora: i servizi ora sul dispositivo possono essere configurati accuratamente per garantire la sincronizzazione con i protocolli ora della rete.
9. Requisito per l'attivazione del supporto FDM. Il supporto di Firewall Device Manager (FDM) e la relativa funzionalità sono concessi in esclusiva su richiesta. Gli utenti che non dispongono del supporto FDM abilitato sul tenant non sono in grado di gestire o distribuire le configurazioni nei dispositivi gestiti da FDM. Per attivare questa piattaforma, gli utenti devono inviare una richiesta al team di supporto per l'attivazione del supporto FDM.

Configurazione

Esempio di rete

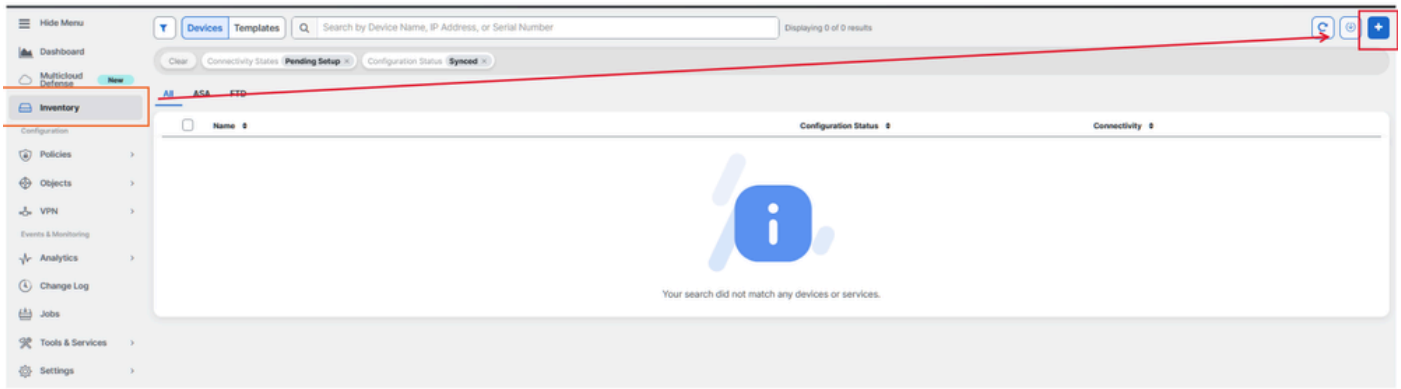
In questo documento viene illustrato un dispositivo FDM (Firepower Device Manager) controllato tramite la relativa interfaccia di gestione. Questa interfaccia ha un accesso a Internet che è essenziale per registrare il dispositivo con Cisco Defense Orchestrator (CDO).



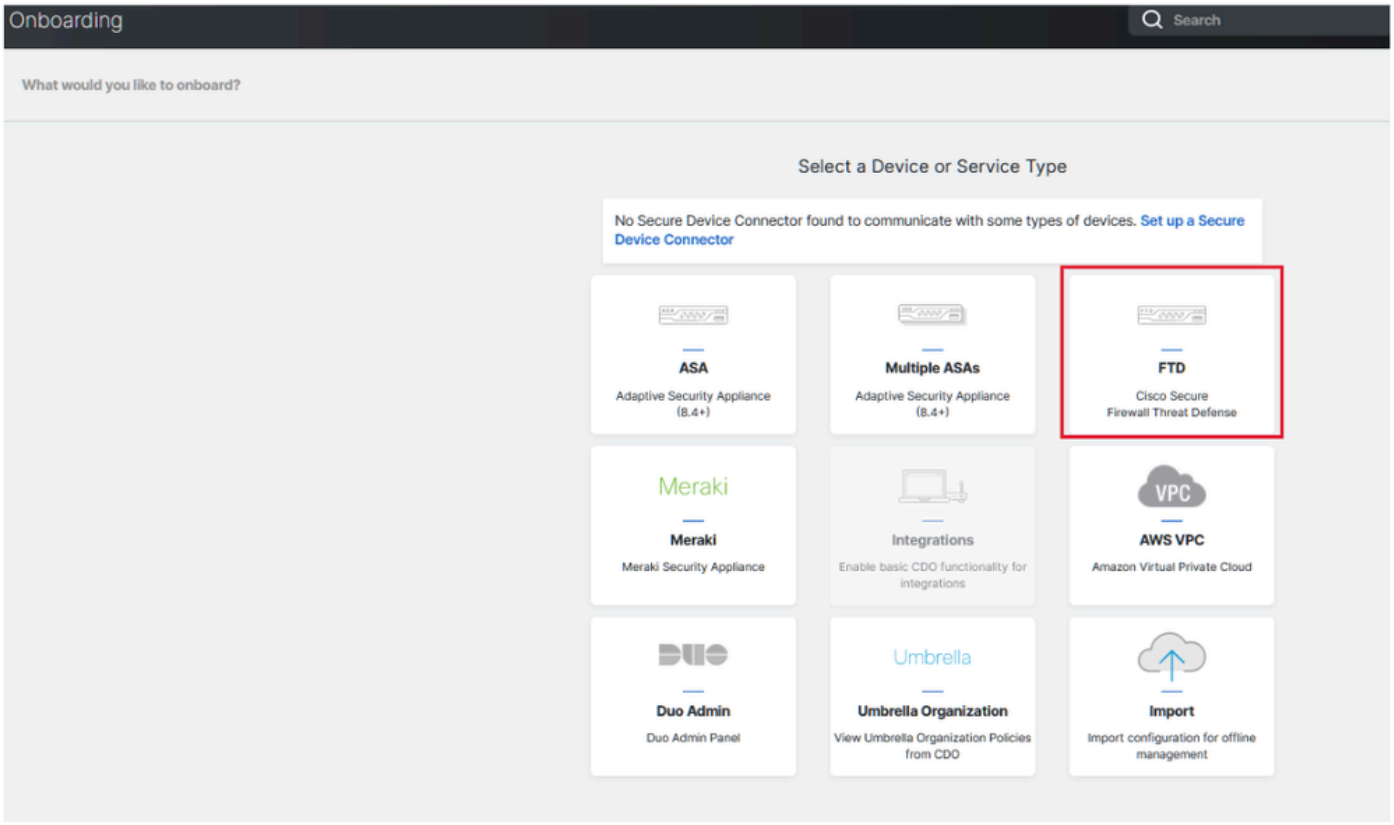
Configurazioni

Passaggio 1. Accedere a Cisco Defense Orchestrator (CDO).

Passaggio 2. Passare al riquadro Inventory e selezionare il pulsante blu più per caricare un dispositivo.



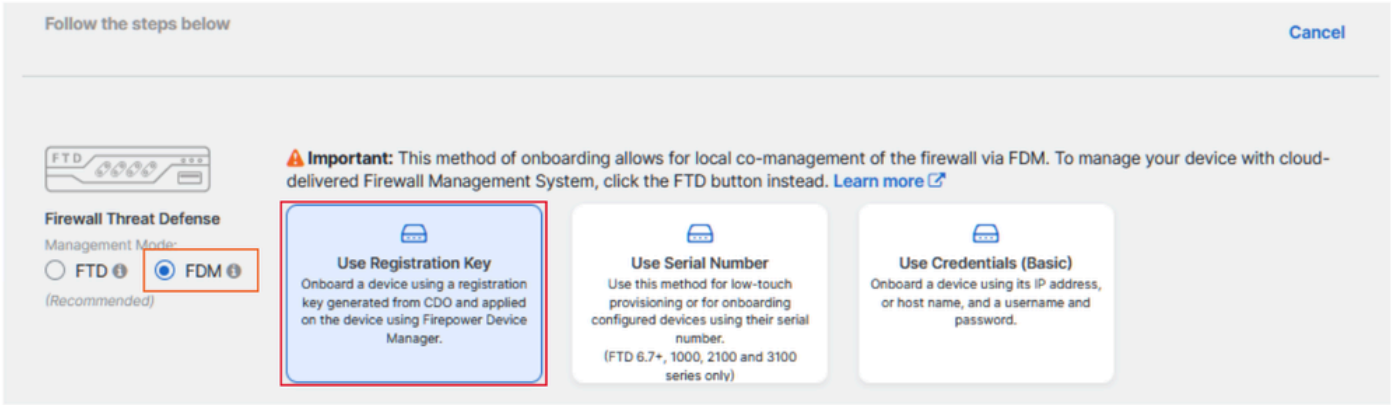
Passaggio 3. Selezionate l'opzione FTD.



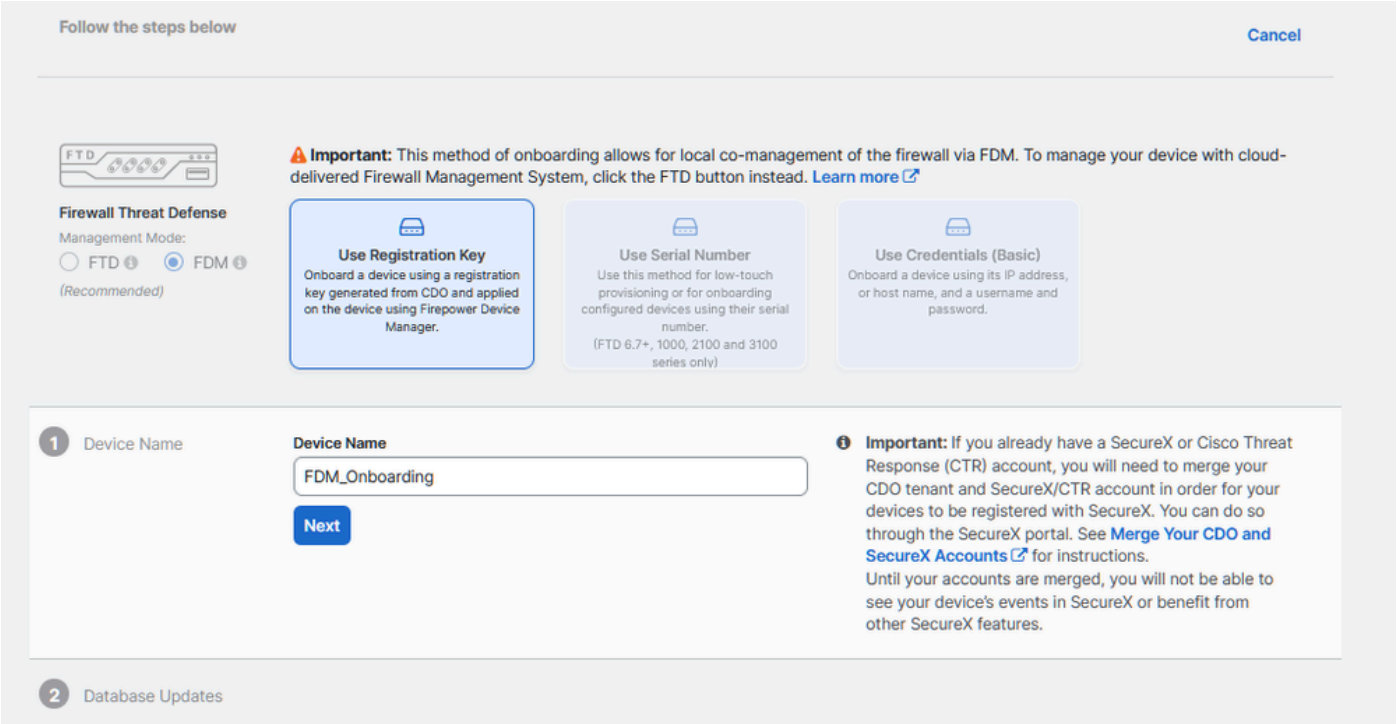
4. Procedere alla sezione "Dispositivo FTD integrato" per avviare il processo di registrazione. È importante notare i metodi disponibili per caricare un dispositivo di difesa dalle minacce:

- Per numero di serie: questo metodo è valido per i dispositivi fisici come Firepower serie 1000, Firepower serie 2100 o Secure Firewall serie 3100 con versioni software supportate. Richiede il numero di serie dello chassis o dell'APC e una connessione di rete a Internet.
- Per chiave di registrazione: questo è il metodo preferito per l'onboarding, particolarmente vantaggioso per i dispositivi che ricevono indirizzi IP tramite DHCP, in quanto aiuta a mantenere la connettività con CDO anche se c'è una modifica nell'indirizzo IP del dispositivo.
- Utilizzo delle credenziali: questa alternativa comporta l'immissione delle credenziali del dispositivo e dell'indirizzo IP della relativa interfaccia esterna, interna o di gestione, in base alla configurazione del dispositivo all'interno della rete.

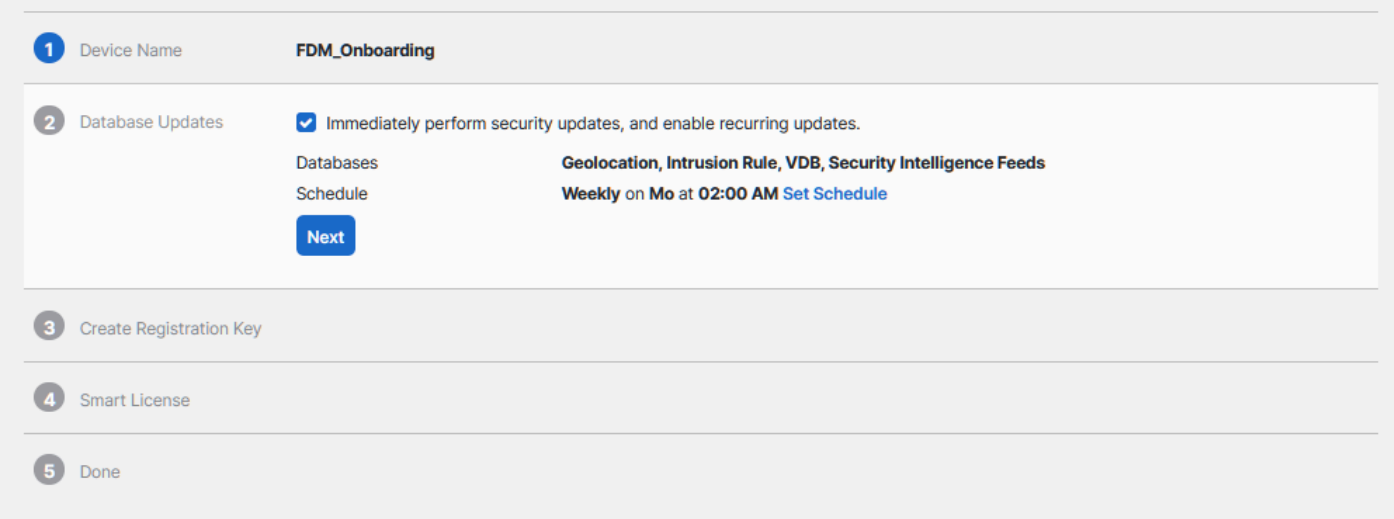
Per questo processo, selezionare l'opzione FDM e quindi l'opzione Use Registration Key per garantire una connettività coerente al CDO, indipendentemente dalle potenziali modifiche dell'indirizzo IP del dispositivo.



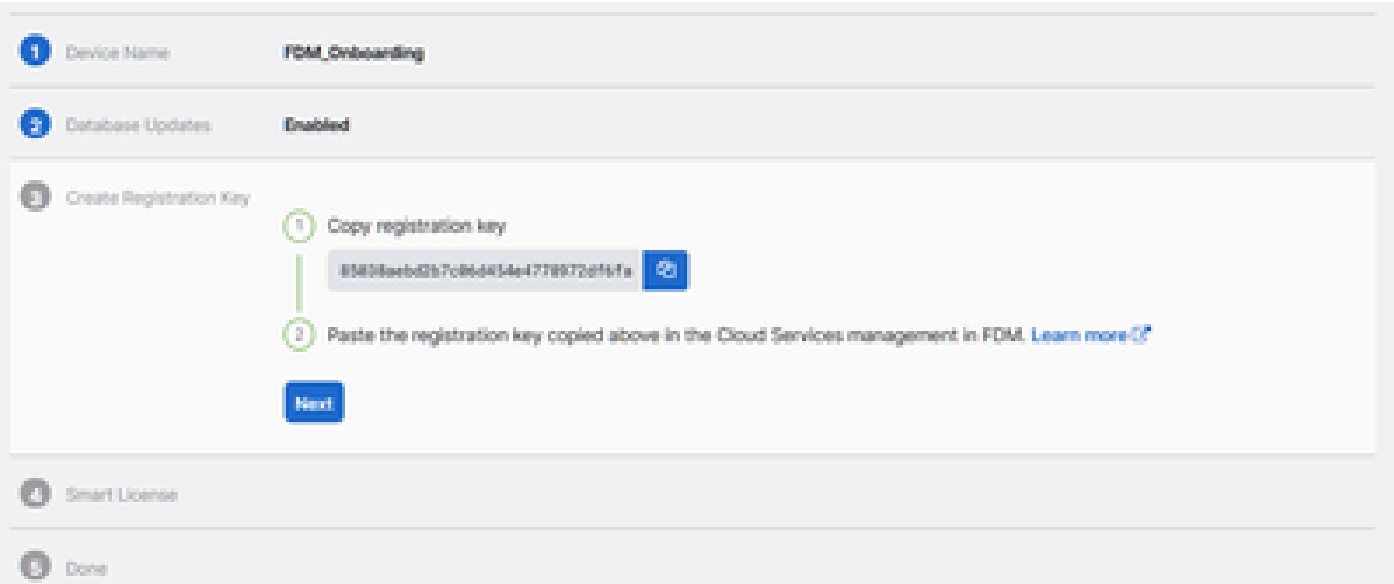
Passaggio 5. Immettere il nome del dispositivo desiderato nel campo Nome dispositivo e specificare l'assegnazione dei criteri. Inoltre, scegliere la licenza di sottoscrizione che deve essere associata al dispositivo.



Passaggio 6. Per impostazione predefinita, la sezione Aggiornamenti del database è configurata in modo da eseguire immediatamente gli aggiornamenti per la protezione e impostare aggiornamenti ricorrenti. La modifica di questa impostazione non altera le pianificazioni di aggiornamento esistenti stabilite tramite Gestione periferiche di Secure Firewall.



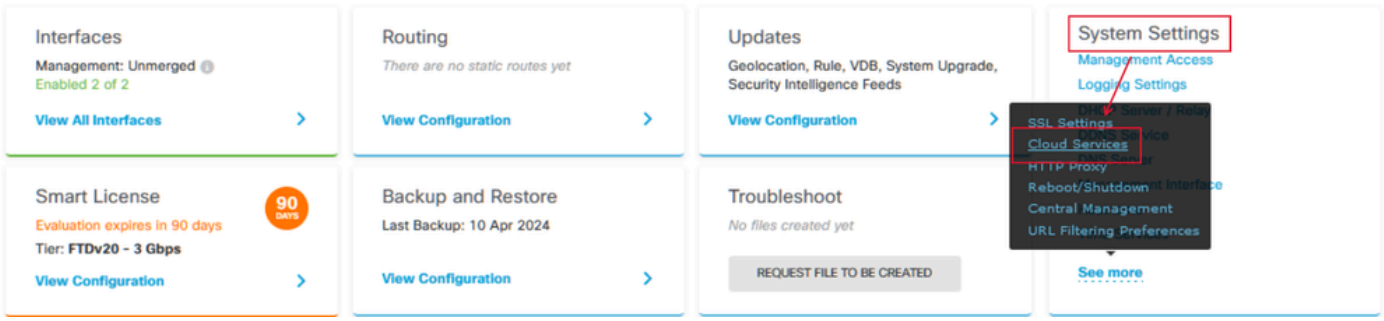
Passaggio 7. Nella sezione CLI Registration Key, CDO genera automaticamente una chiave di registrazione. Se si esce dall'interfaccia di caricamento prima del completamento, viene creato un segnaposto per il dispositivo nell'inventario. La chiave di registrazione può essere recuperata da questo percorso in un secondo momento, se necessario.



Passaggio 8. Utilizzare l'icona Copia per copiare la chiave di registrazione generata.

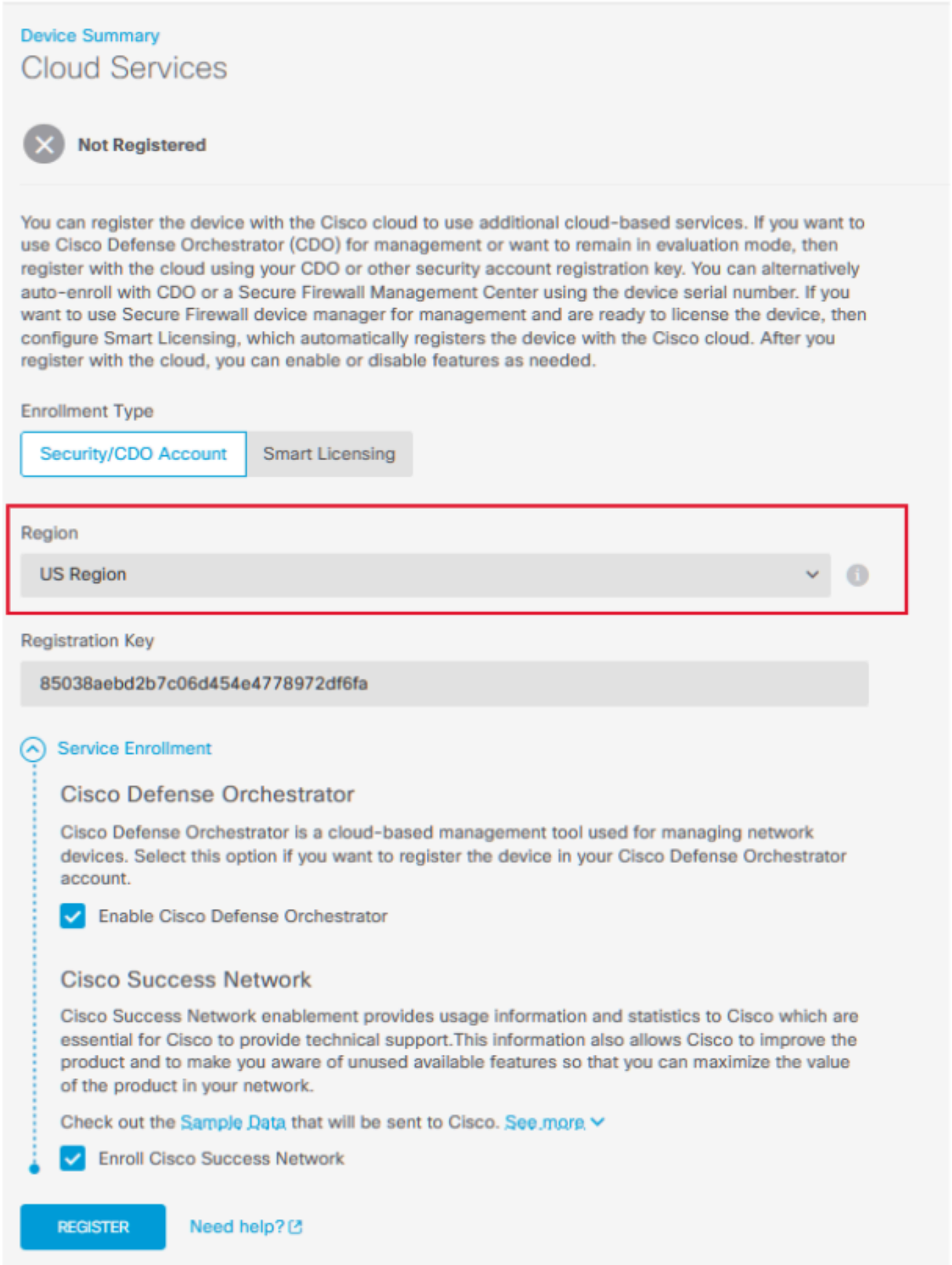
Passaggio 9. Accedere alla periferica Secure Firewall Device Manager destinata all'onboarding in CDO.

Passaggio 10. Selezionare Servizi cloud dal menu Impostazioni di sistema.

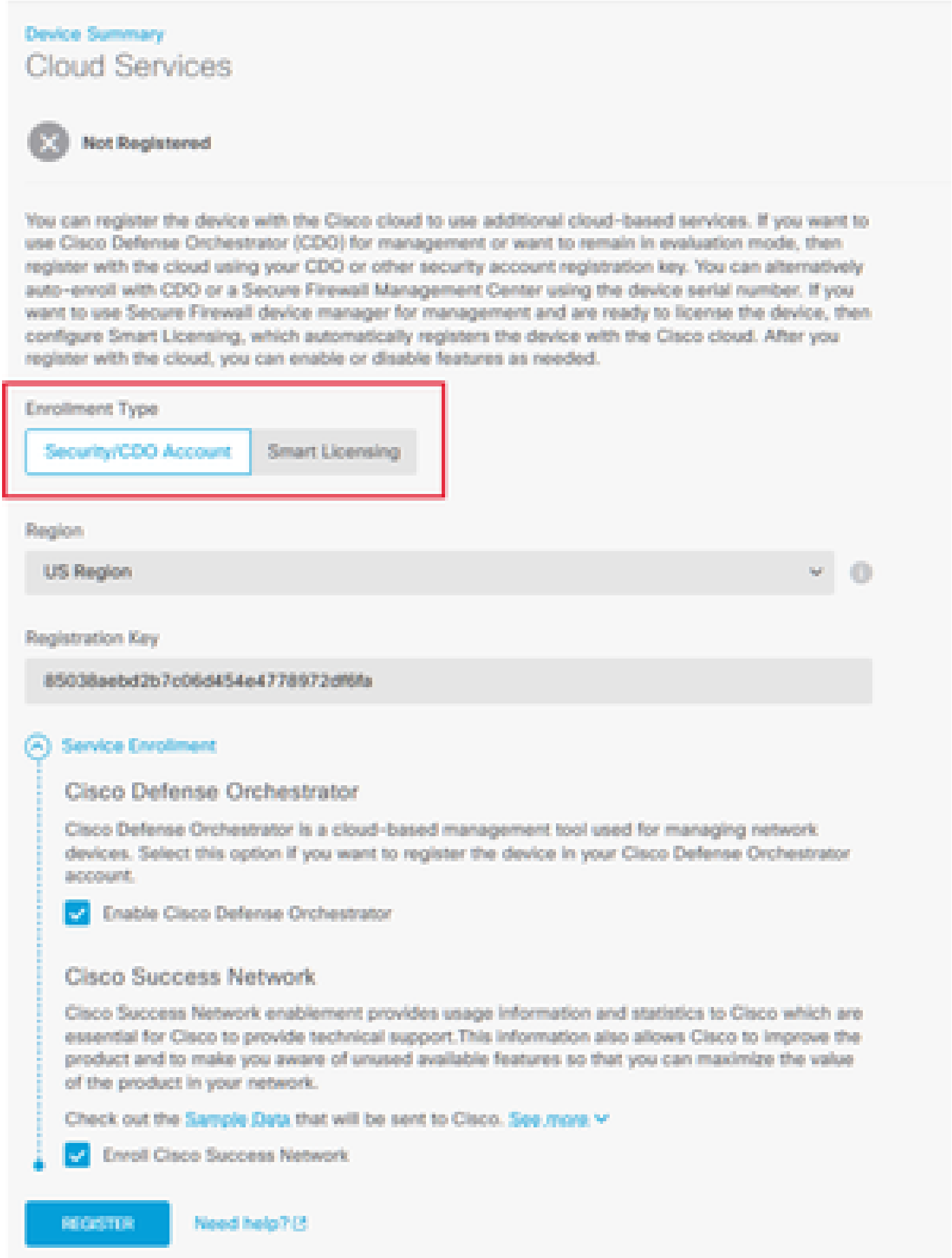


Passaggio 11. Designare l'area cloud Cisco corretta nell'elenco a discesa Area, allineando la posizione geografica del tenant:

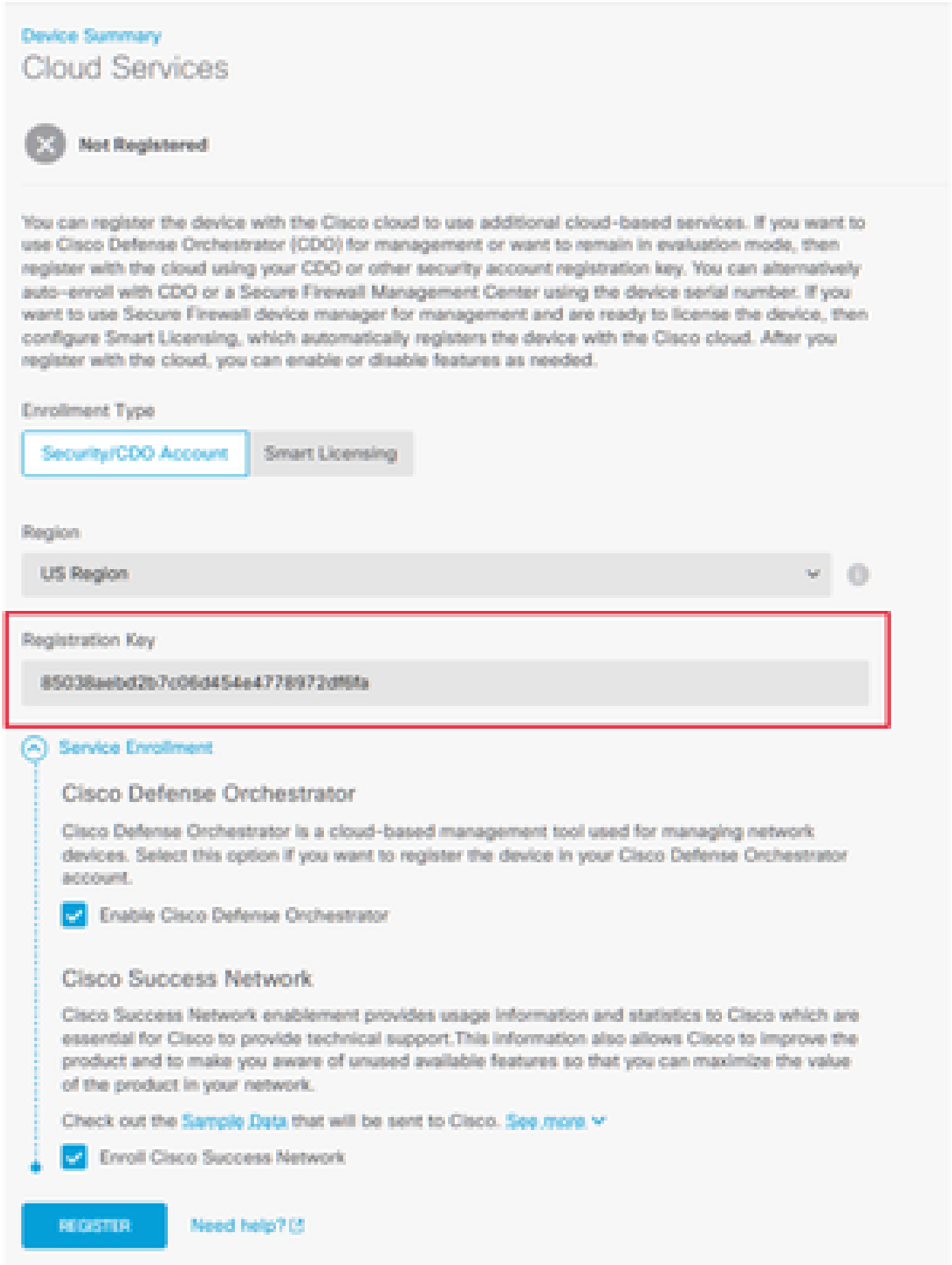
- Per defenseorchestrator.com, selezionare US (USA).
- Per defenseorchestrator.eu, selezionare EU.
- Per apj.cdo.cisco.com, selezionare APJ.



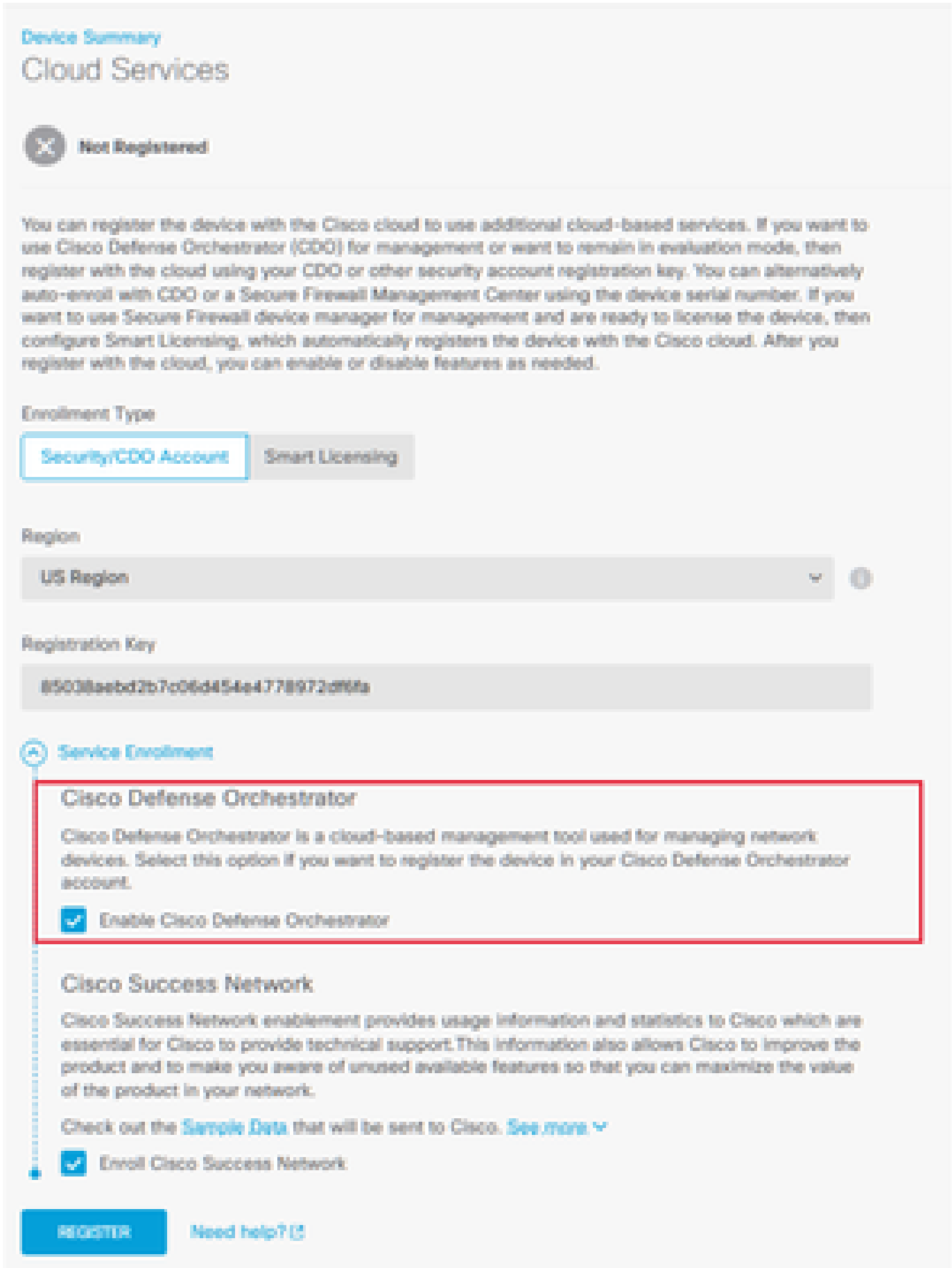
Passaggio 12. Nella sezione Tipo di registrazione selezionare l'opzione Account di protezione.



Passaggio 13. Incollare la chiave di registrazione nel campo Chiave di registrazione.

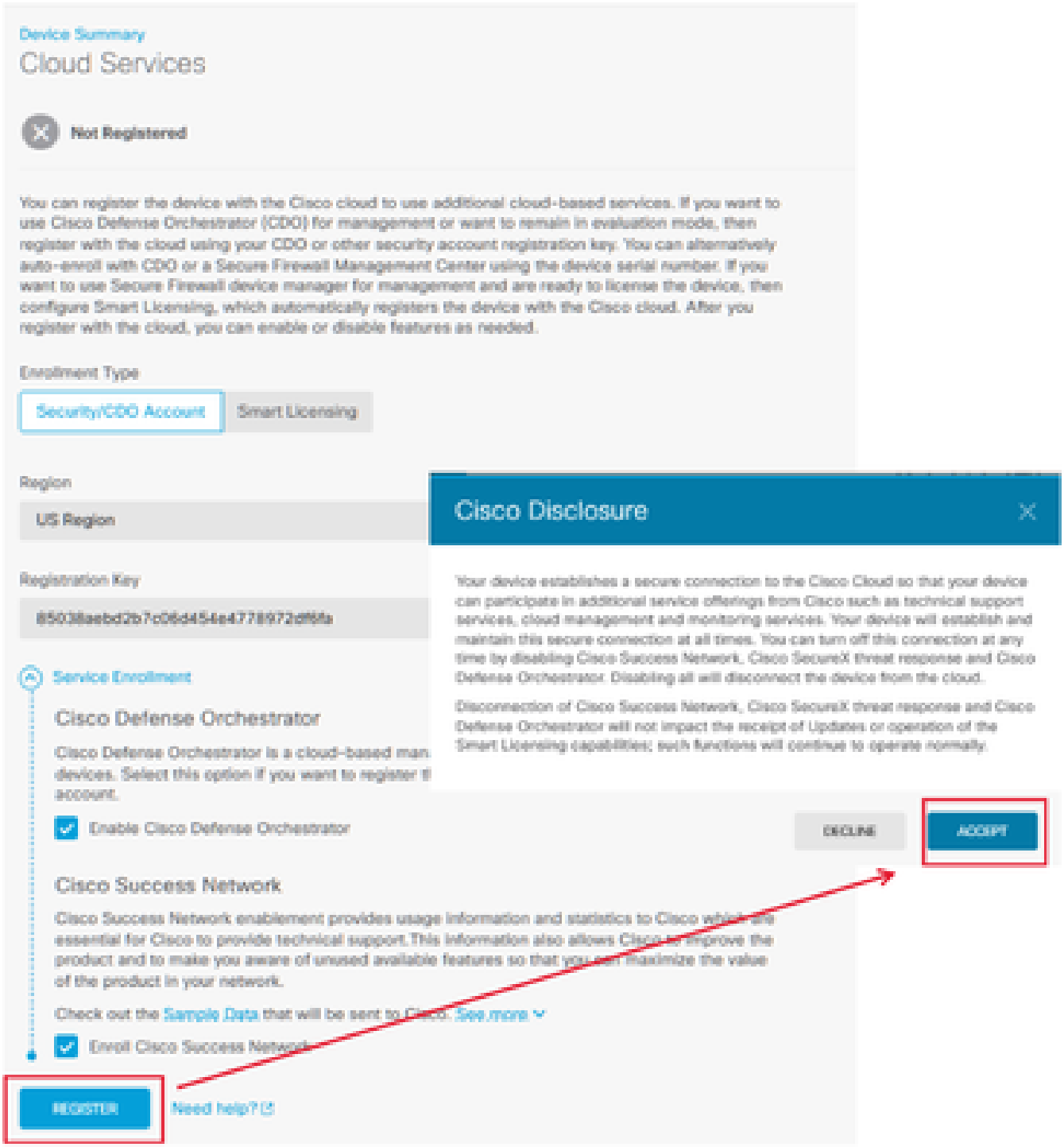


Passaggio 14. Per i dispositivi della versione 6.7 o successive, verificare che Cisco Defense Orchestrator sia abilitato nella sezione Service Enrollment.



Passaggio 15. (Facoltativo) Verificare i dettagli di Cisco Success Network Enrollment. Se non si desidera partecipare, deselezionare la casella di controllo Registra Cisco riuscito in rete.

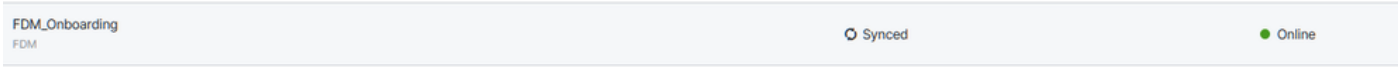
Passaggio 16. Selezionare Register e accettare Cisco Disclosure (Registra). Gestione periferiche firewall protette invia la registrazione al CDO.



Passaggio 17. Tornare a CDO, nell'area di creazione della chiave di registrazione, scegliere Avanti.

Passaggio 18. (Facoltativo) Identificare e selezionare le licenze destinate al dispositivo, quindi continuare selezionando Avanti.

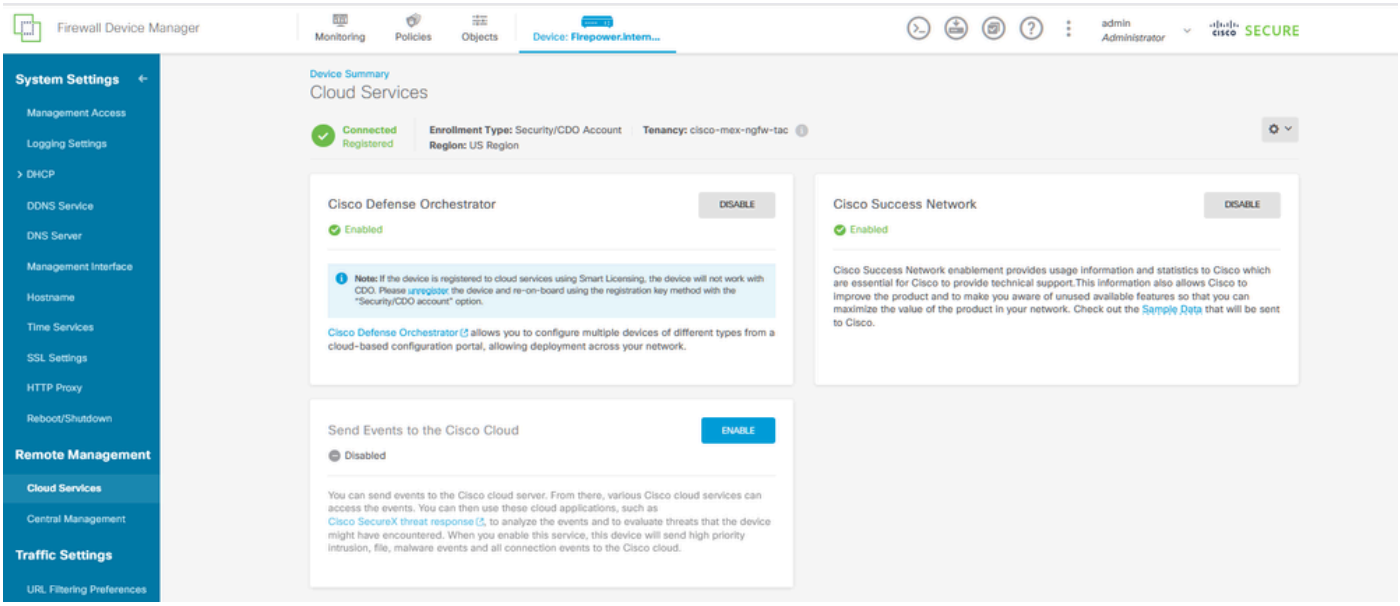
Passaggio 19. Osservare lo stato del dispositivo nella transizione dall'inventario CDO Unprovisioned all'individuazione, quindi alla sincronizzazione e infine alla sincronizzazione.



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passare al portale CDO e controllare lo stato del dispositivo, che indica In linea e Sincronizzato. Inoltre, la verifica dello stato può essere eseguita tramite la GUI di FDM. Selezionare Sistema > Servizi cloud per osservare lo stato della connessione di Cisco Defense Orchestrator e Cisco Success Network. L'interfaccia visualizza lo stato Connesso, a conferma della corretta integrazione con i servizi.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Risoluzione errore FQDN servizio cloud

Se la registrazione del dispositivo non riesce a causa di un'impossibilità di risolvere il nome di dominio completo del servizio cloud, controllare la connettività di rete o la configurazione DNS e tentare di nuovo l'onboarding del dispositivo.

- Errore chiave di registrazione non valida

Se la registrazione del dispositivo non viene completata a causa dell'immissione di una chiave di registrazione non valida in Gestione dispositivi firewall, procedere con la copia della chiave di registrazione corretta da Cisco Defense Orchestrator e riprovare il processo di registrazione. Se il dispositivo dispone già di una licenza intelligente, rimuoverla prima di immettere la chiave di registrazione in Gestione periferiche firewall.

- Problema di licenza insufficiente

Se lo stato di connettività del dispositivo indica "Licenza insufficiente", procedere come segue:

1. Concedere al dispositivo un po' di tempo per ottenere la licenza, in quanto Cisco Smart Software Manager può richiedere un periodo per applicare una nuova licenza al dispositivo.

2. Se lo stato del dispositivo rimane invariato, aggiornare il portale CDO disconnettendosi e quindi eseguendo nuovamente l'accesso per risolvere i potenziali problemi di comunicazione di rete tra il server licenze e il dispositivo.

3. Se l'aggiornamento del portale non aggiorna lo stato del dispositivo, eseguire le azioni seguenti:

    - Generare una nuova chiave di registrazione da Cisco Smart Software Manager e copiarla. Per ulteriori informazioni, vedere il video Generate Smart Licensing.
    - Nella barra di navigazione CDO, selezionare la pagina Inventario.
    - Scegliere il dispositivo elencato con lo stato Licenza insufficiente.
    - Nel riquadro Dettagli dispositivo, fare clic su Gestisci licenze sotto l'avviso Licenze insufficienti. Viene visualizzata la finestra Gestisci licenze.
    - Nel campo Activate (Attiva), incollate la nuova chiave di registrazione e selezionate Register Device (Registra dispositivo).

Dopo aver applicato la nuova chiave di registrazione, lo stato di connettività del dispositivo deve passare a 'In linea'.

Per istruzioni complete sulla registrazione di Firepower Device Manager (FDM) con metodi alternativi alla chiave di registrazione, fare riferimento alla documentazione dettagliata disponibile nel collegamento Risoluzione dei problemi relativi ai dispositivi gestiti da FDM.

Questa risorsa offre istruzioni dettagliate e suggerimenti per la risoluzione dei problemi per le diverse tecniche di registrazione che possono essere utilizzate per integrare con successo FDM in Cisco Defense Orchestrator (CDO).

Informazioni correlate

- Risoluzione dei problemi relativi ai dispositivi gestiti da FDM
- Gestione dei dispositivi FDM con Cisco Defense Orchestrator
- Supporto tecnico Cisco e download

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).