Integration von FDM in Defense Orchestrator

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie ein vom FirePOWER-Gerätemanager (FDM) verwaltetes Gerät mithilfe eines Registrierungsschlüssels in den Cisco Defense Orchestrator (CDO) integriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER-Gerätemanager (FDM)
- Cisco Defense Orchestrator (CDO)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER Device Manager (FDM) Azure mit Version 7.4.1

Eine umfassende Liste kompatibler Versionen und Produkte finden Sie im Secure Firewall Threat Defense Compatibility Guide für weitere Informationen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

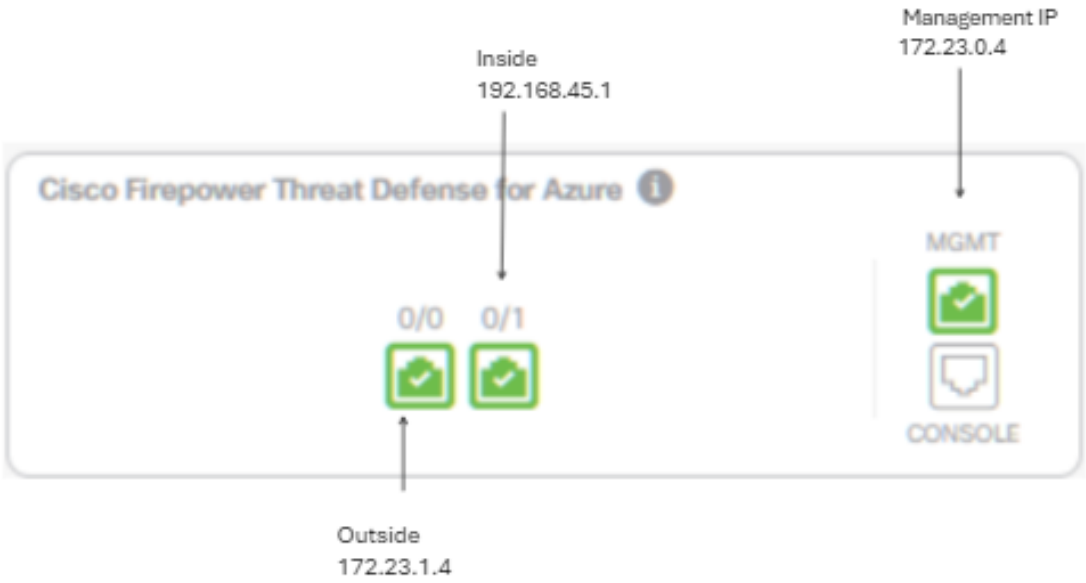
Bevor Sie ein FDM-verwaltetes Gerät mithilfe eines Registrierungsschlüssels in den Cisco Defense Orchestrator (CDO) integrieren, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

1. Kompatible Version: Ihr Gerät muss Version 6.6 oder höher ausführen.
2. Netzwerkanforderungen: Verbinden Sie Cisco Defense Orchestrator mit Ihren verwalteten Geräten
3. Managementsoftware: Das Gerät muss über den Secure Firewall Device Manager (FDM) verwaltet werden.
4. Lizenzierung: Ihr Gerät kann entweder eine 90-Tage-Testlizenz oder eine Smart-Lizenz verwenden.
5. Bestehende Registrierungen: Stellen Sie sicher, dass das Gerät nicht bereits bei Cisco Cloud Services registriert ist, um Konflikte während des Onboarding-Prozesses zu vermeiden.
6. Ausstehende Änderungen: Vergewissern Sie sich, dass auf dem Gerät keine Änderungen ausstehen.
7. DNS-Konfiguration: Die DNS-Einstellungen müssen auf dem FDM-verwalteten Gerät korrekt konfiguriert sein.
8. Zeitdienste: Zeitdienste auf dem Gerät können präzise konfiguriert werden, um die Synchronisierung mit Netzwerk-Zeitprotokollen sicherzustellen.
9. Anforderung für FDM-Support-Aktivierung. Die Unterstützung des Firewall Device Managers (FDM) und seiner Funktionen wird ausschließlich auf Anfrage gewährt. Benutzer ohne aktivierten FDM-Support auf ihrem Tenant können keine Konfigurationen auf von FDM verwalteten Geräten verwalten oder bereitstellen. Um diese Plattform zu aktivieren, müssen Benutzer eine Anfrage an das Support-Team zur Aktivierung des FDM-Supports senden.

Konfigurieren

Netzwerkdiagramm

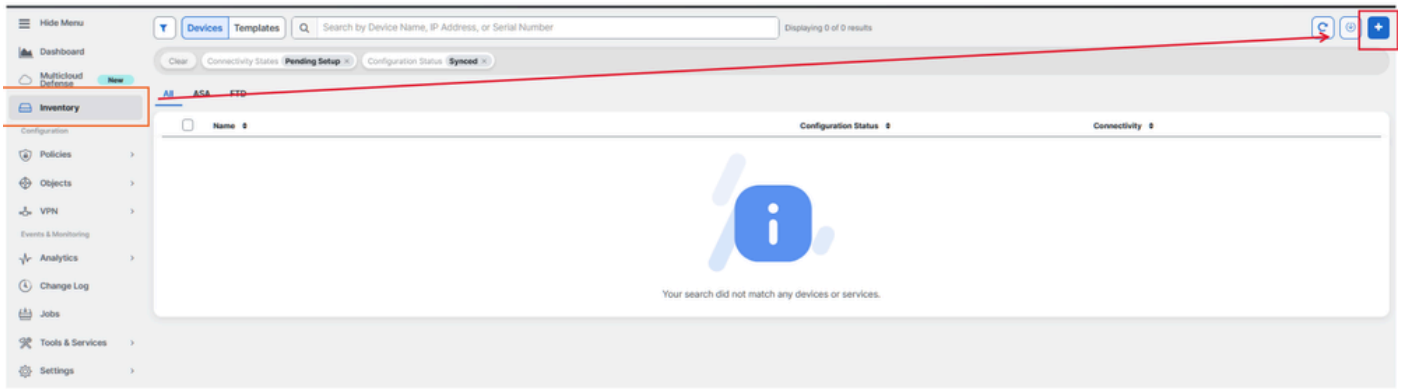
Der Schwerpunkt dieses Artikels liegt auf einem FDM-Gerät (FirePOWER Device Manager), das über seine Verwaltungsschnittstelle gesteuert wird. Diese Schnittstelle verfügt über einen Internetzugang, der für die Registrierung des Geräts bei Cisco Defense Orchestrator (CDO) erforderlich ist.



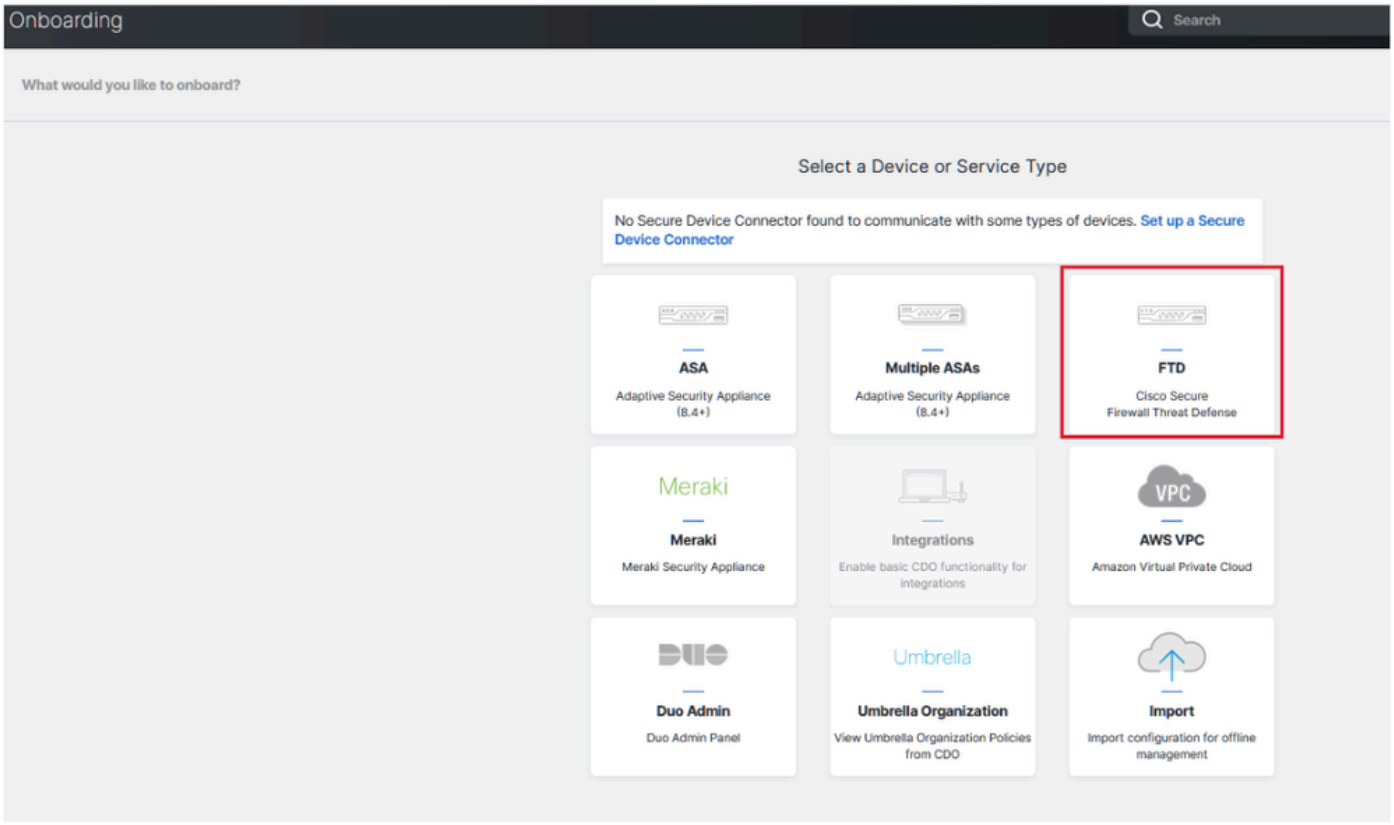
Konfigurationen

Schritt 1: Melden Sie sich bei Cisco Defense Orchestrator (CDO) an.

Schritt 2: Navigieren Sie zum Inventarbereich, und wählen Sie die blaue Plustaste aus, um ein Gerät zu integrieren.



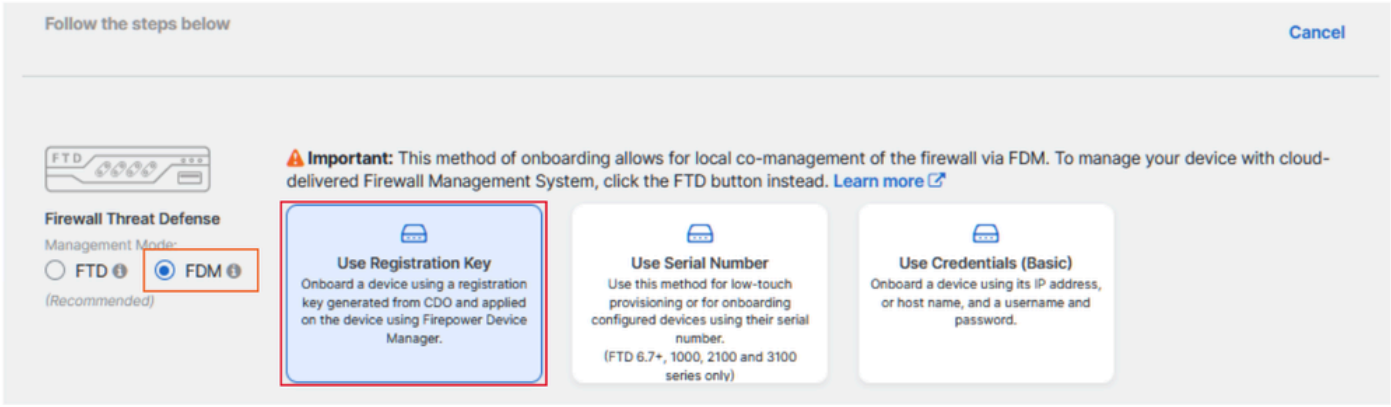
Schritt 3: Wählen Sie die FTD-Option aus.



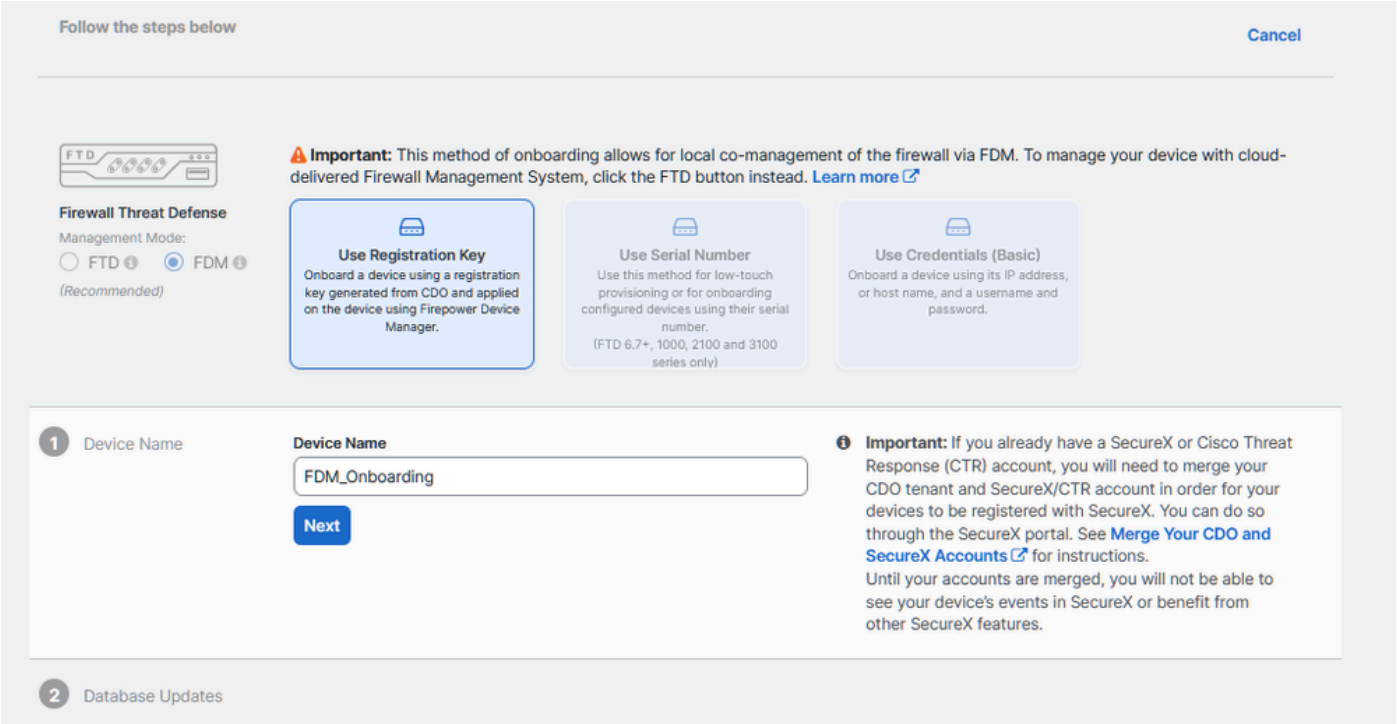
Schritt 4 Fahren Sie mit dem Abschnitt zum Onboard-FTD-Gerät fort, um den Registrierungsprozess zu beginnen. Beachten Sie die verfügbaren Methoden zum Integrieren eines Threat Defence-Geräts:

- Nach Seriennummer: Diese Methode gilt für physische Geräte wie die Firepower 1000-, Firepower 2100- oder Secure Firewall 3100-Serie mit unterstützten Softwareversionen. Hierfür sind die Seriennummer des Gehäuses oder des PCA-Geräts und eine Netzwerkverbindung mit dem Internet erforderlich.
- By Registration Key (Nach Registrierungsschlüssel): Dies ist die bevorzugte Methode für das Onboarding und besonders vorteilhaft für Geräte, die IP-Adressen über DHCP empfangen, da sie dazu beiträgt, die Verbindung mit CDO aufrechtzuerhalten, selbst wenn sich die IP-Adresse des Geräts ändert.
- Verwendung von Anmeldedaten: Bei dieser Alternative müssen die Geräteanmeldedaten und die IP-Adresse der externen, internen oder Managementschnittstelle eingegeben werden, die auf die Gerätekonfiguration im Netzwerk zugeschnitten ist.

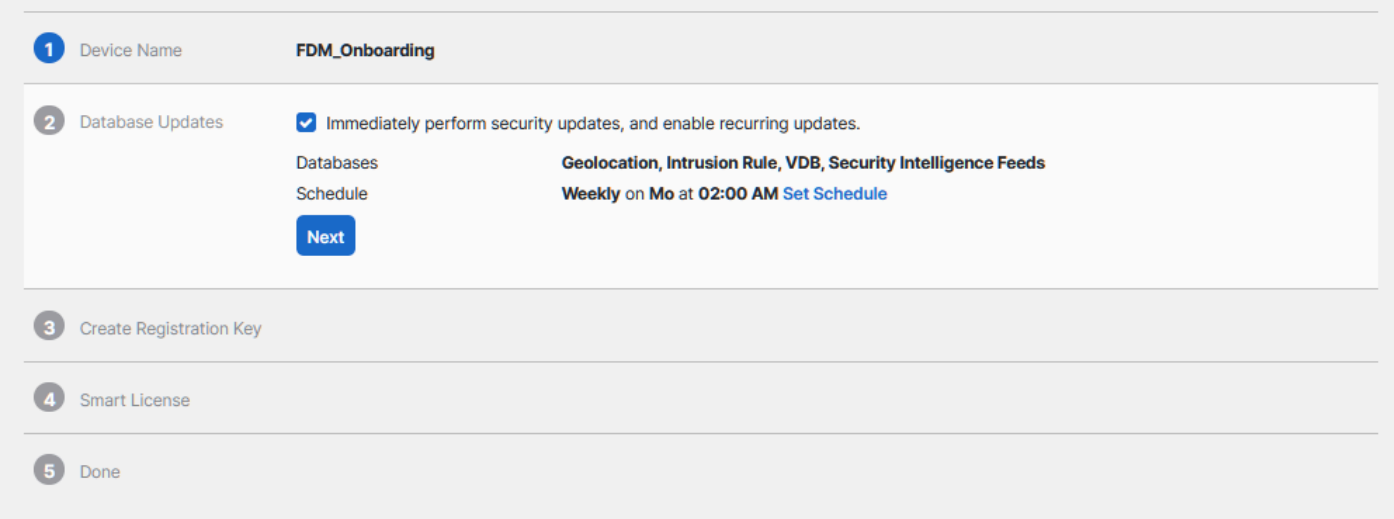
Wählen Sie für diesen Prozess die FDM-Option und anschließend die Option Registrierungsschlüssel verwenden, um eine konsistente Verbindung mit CDO sicherzustellen, unabhängig von möglichen Änderungen an der Geräte-IP-Adresse.



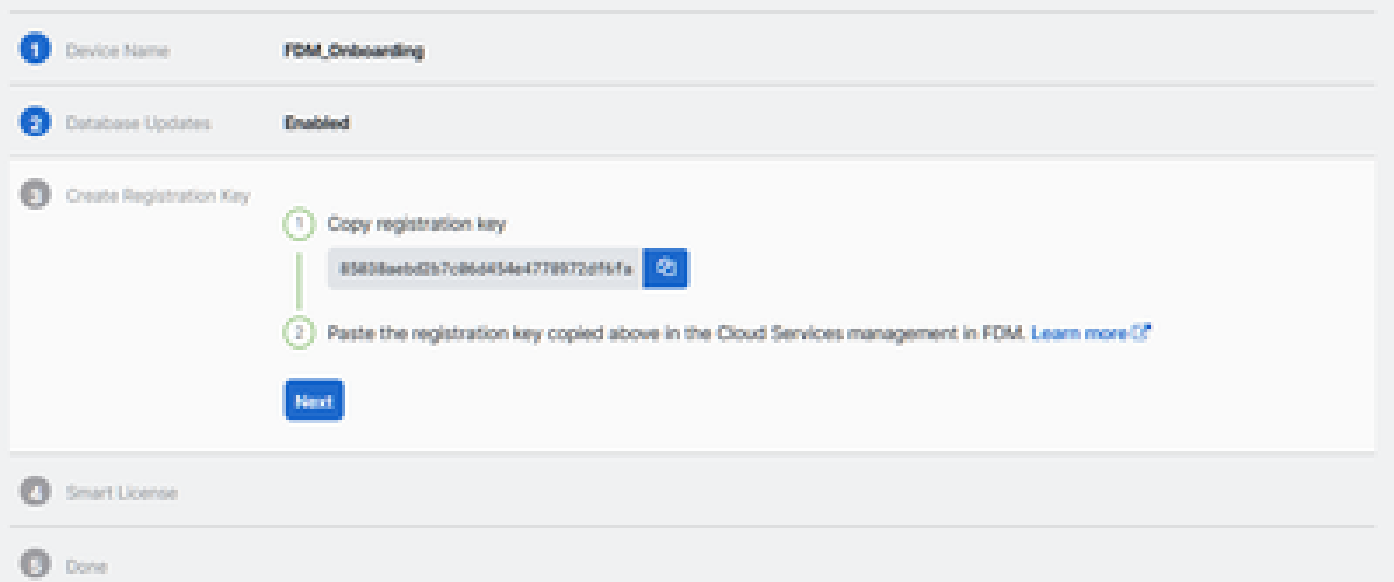
Schritt 5: Geben Sie den gewünschten Gerätenamen in das Feld Gerätename ein, und geben Sie die Richtlinienzuweisung an. Wählen Sie außerdem die Abonnementlizenz aus, die mit dem Gerät verknüpft werden muss.



Schritt 6: Der Abschnitt "Datenbankaktualisierungen" ist standardmäßig so konfiguriert, dass Sicherheitsaktualisierungen sofort ausgeführt und regelmäßige Updates eingerichtet werden. Durch Ändern dieser Einstellung werden keine bestehenden Aktualisierungspläne geändert, die über den Secure Firewall-Gerätemanager erstellt wurden.



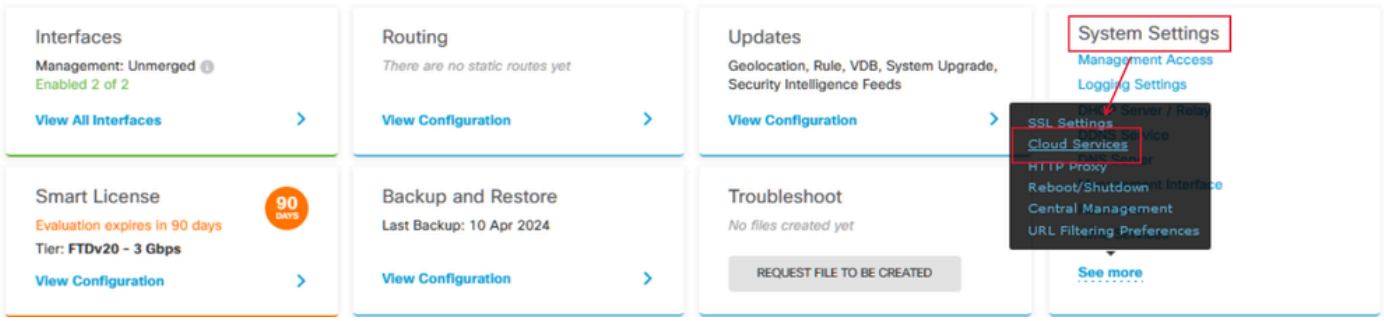
Schritt 7. Im Abschnitt "CLI Registration Key" (CLI-Registrierungsschlüssel) generiert CDO automatisch einen Registrierungsschlüssel. Wenn Sie die Onboarding-Schnittstelle vor Abschluss verlassen, wird ein Platzhalter für das Gerät im Inventar erstellt. Der Registrierungsschlüssel kann bei Bedarf zu einem späteren Zeitpunkt von diesem Ort abgerufen werden.



Schritt 8: Verwenden Sie das Symbol "Kopieren", um den generierten Registrierungsschlüssel zu kopieren.

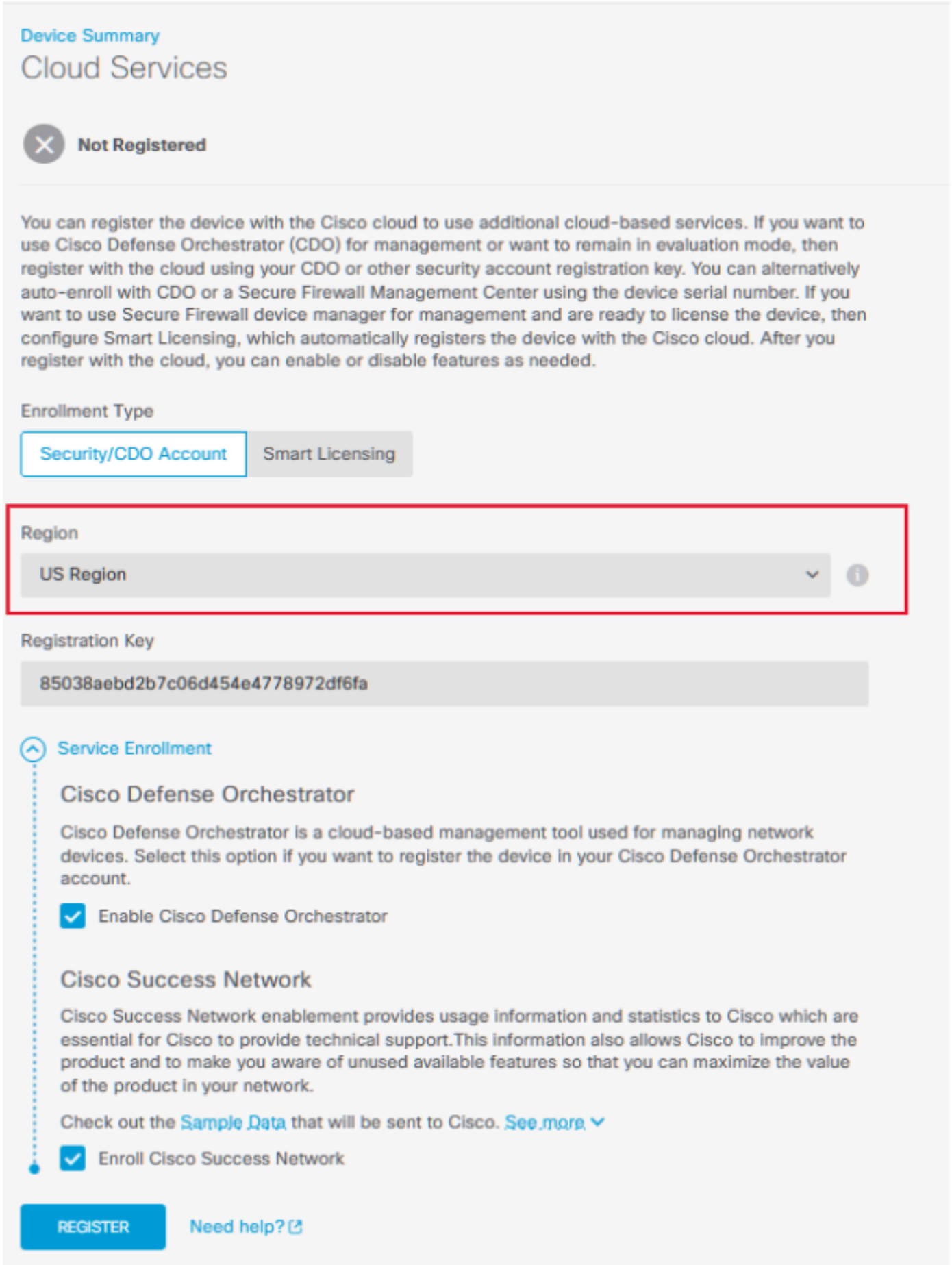
Schritt 9. Greifen Sie auf den Secure Firewall Device Manager zu, der für das Onboarding in CDO vorgesehen ist.

Schritt 10. Wählen Sie im Menü "Systemeinstellungen" die Option "Cloud-Services" aus.

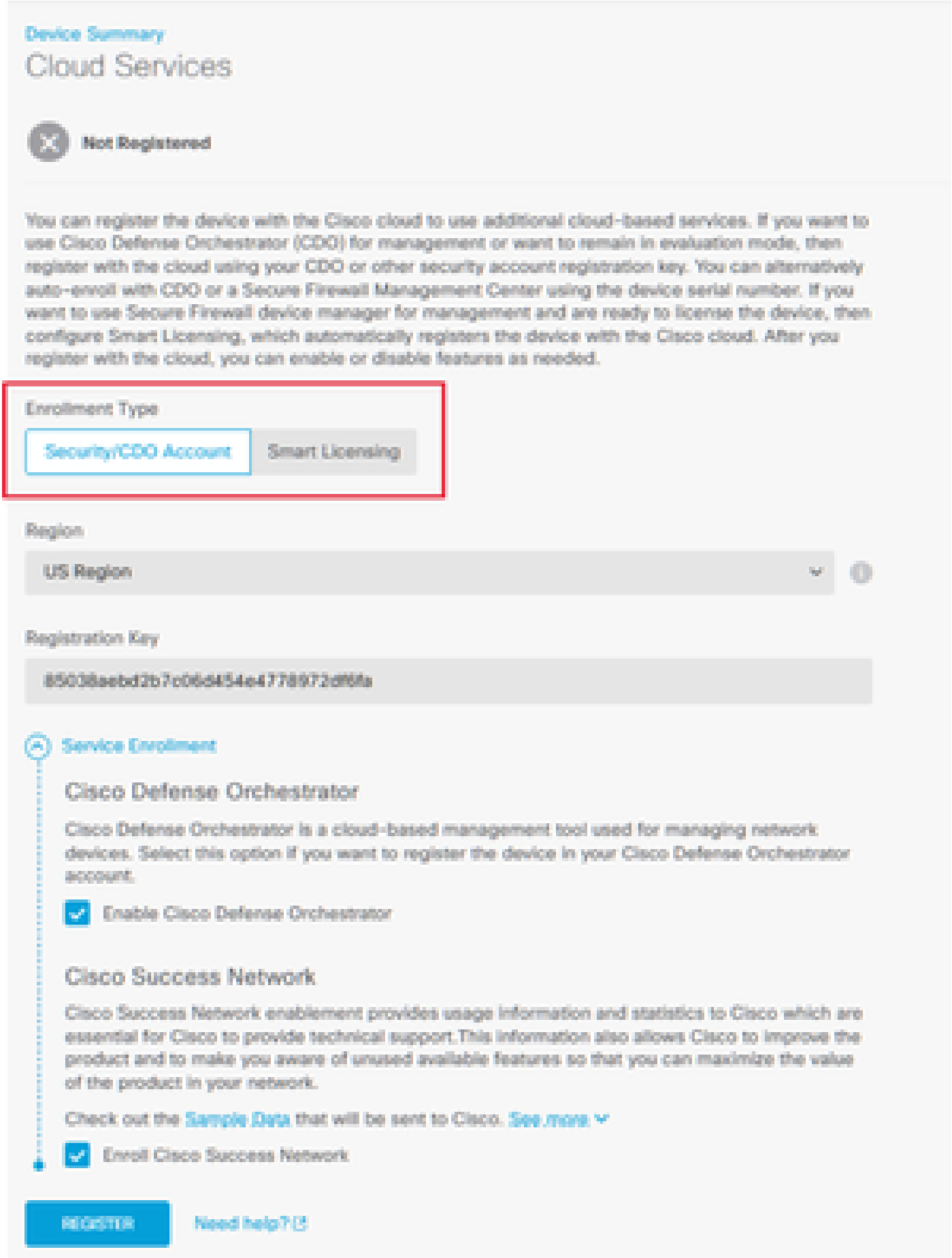


Schritt 11. Legen Sie in der Dropdown-Liste "Region" die richtige Cisco Cloud-Region fest, und richten Sie diese auf den geografischen Standort des Tenants aus:

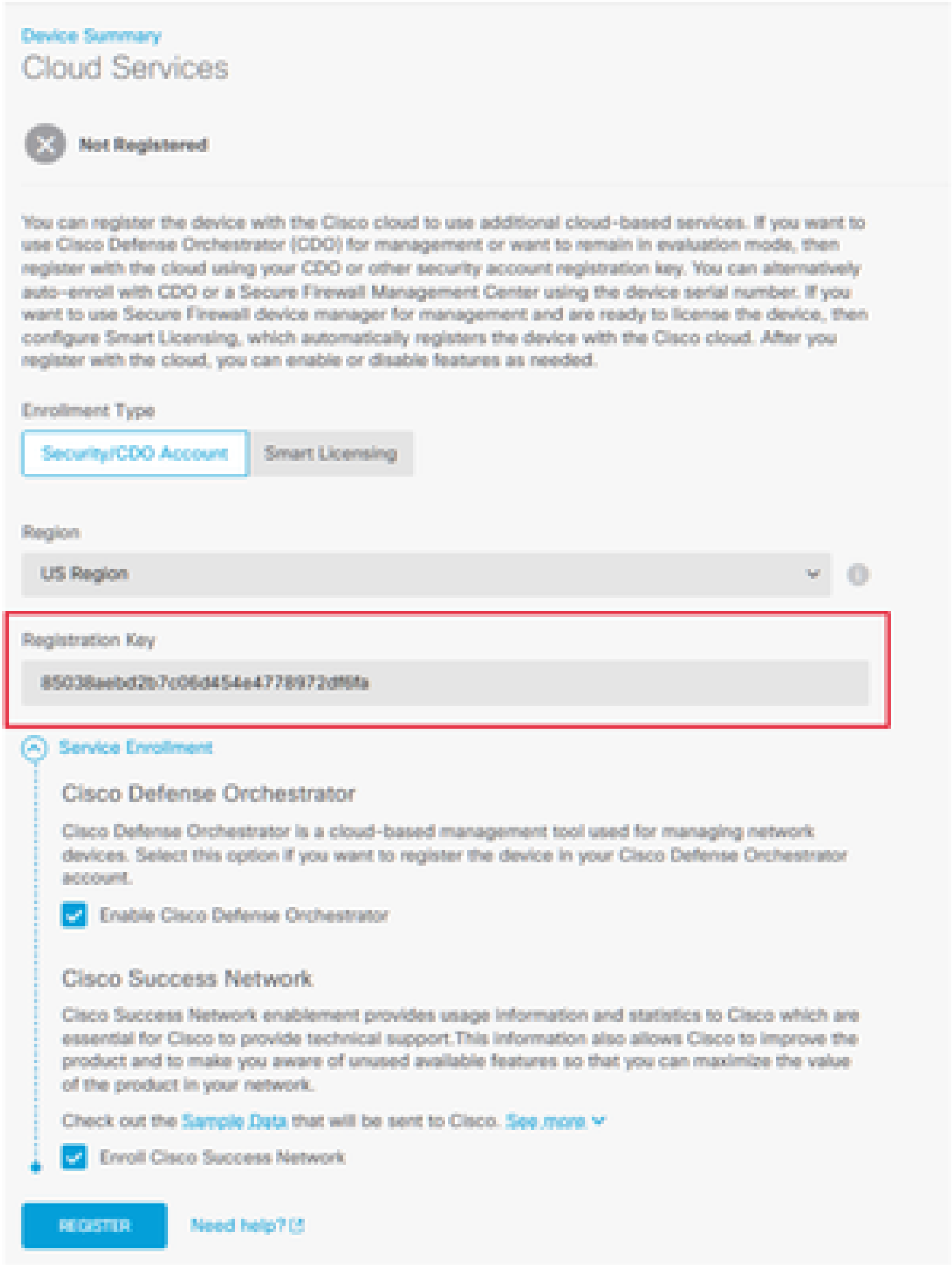
- Wählen Sie für defenseorchestrator.com die Option US aus.
- Wählen Sie für defenseorchestrator.eu die Option EU aus.
- Wählen Sie für apj.cdo.cisco.com APJ aus.



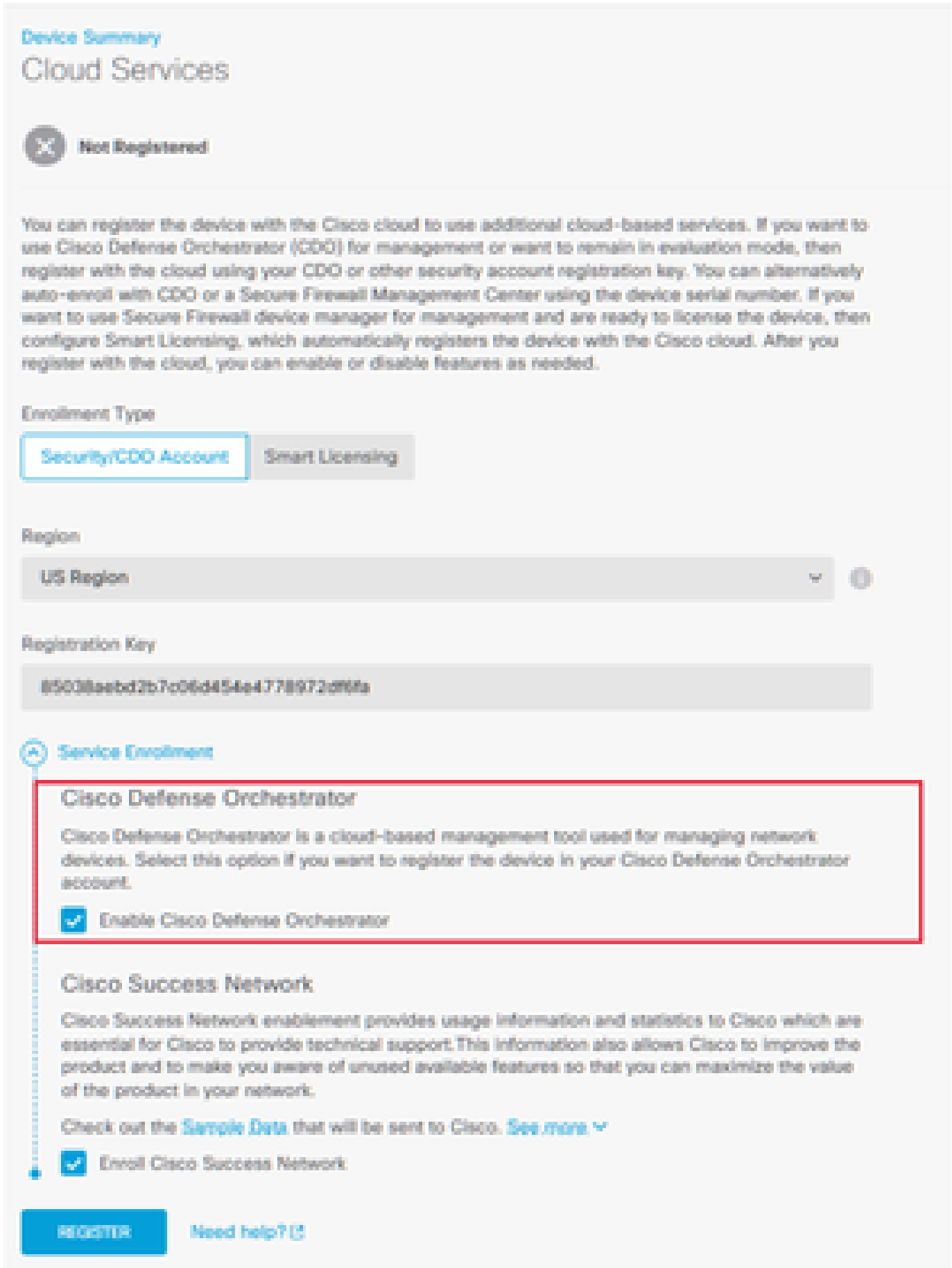
Schritt 12: Wählen Sie im Abschnitt "Anmeldungstyp" das Sicherheitskonto aus.



Schritt 13: Fügen Sie den Registrierungsschlüssel in das Feld für den Registrierungsschlüssel ein.



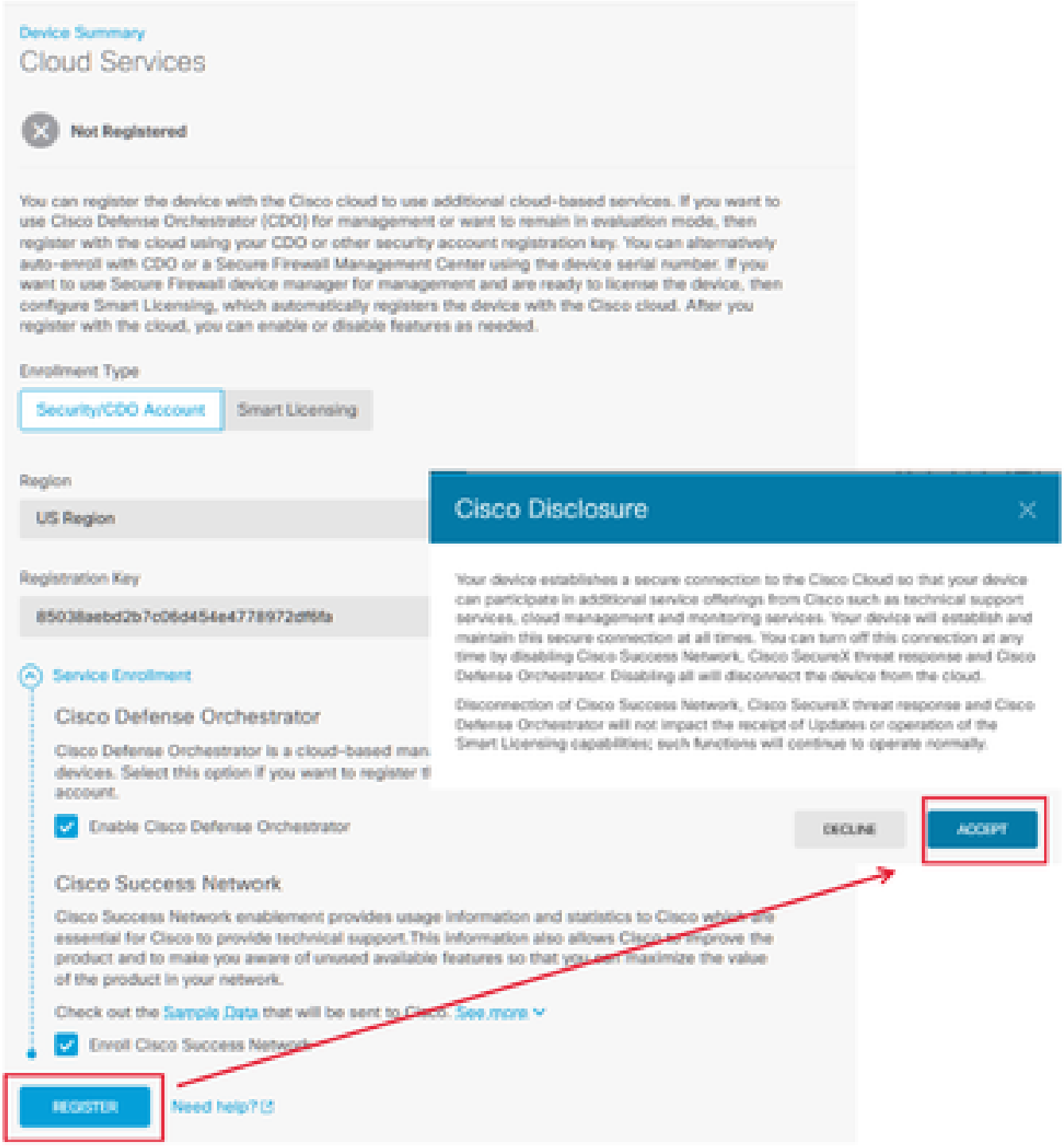
Schritt 14: Überprüfen Sie für Geräte ab Version 6.7 im Abschnitt "Service Enrollment" (Dienstregistrierung), ob Cisco Defense Orchestrator aktiviert ist.



Schritt 15: (Optional) Überprüfen Sie die Registrierungsdetails für das Cisco Success Network. Wenn Sie nicht teilnehmen möchten, deaktivieren Sie das Kontrollkästchen Cisco Success

Network anmelden.

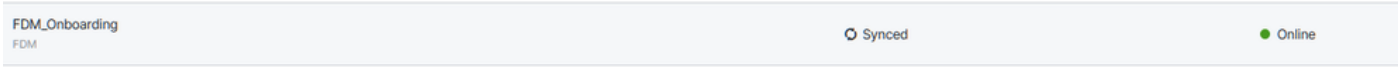
Schritt 16: Wählen Sie Registrieren aus, und akzeptieren Sie die Offenlegung von Cisco. Der Secure Firewall Device Manager sendet die Registrierung an CDO.



Schritt 17: Wählen Sie in CDO im Bereich zur Erstellung des Registrierungsschlüssels Weiter aus.

Schritt 18. (Optional) Identifizieren und wählen Sie die für das Gerät vorgesehenen Lizenzen, und klicken Sie dann auf Weiter.

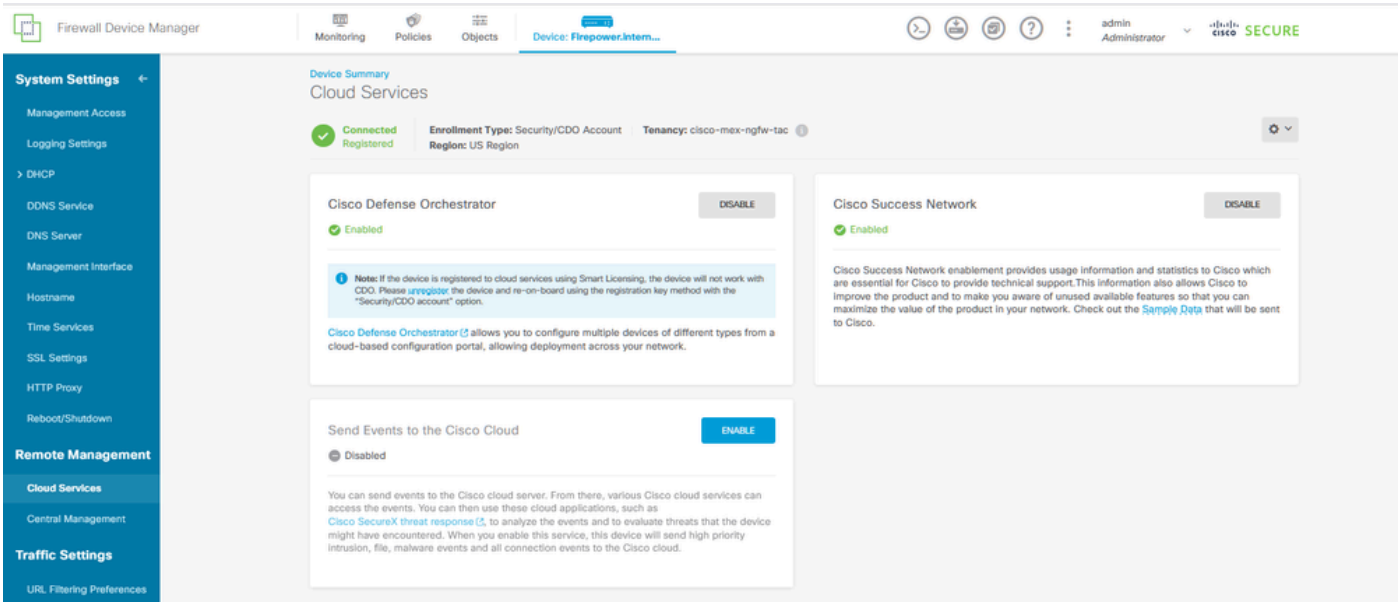
Schritt 19: Beobachten Sie den Gerätestatus beim CDO-Bestandsübergang von Nicht bereitgestellt zu Lokalisierung, dann zu Synchronisierung und schließlich zu Synchronisierung.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Navigieren Sie zum CDO-Portal, und überprüfen Sie den Gerätestatus, der auf Online und Synchronisiert verweist. Die Statusüberprüfung kann darüber hinaus über die FDM-GUI durchgeführt werden. Navigieren Sie zu System > Cloud Services, um den Verbindungsstatus für Cisco Defense Orchestrator und Cisco Success Network zu beobachten. Die Schnittstelle zeigt den Status "Verbunden" an und bestätigt die erfolgreiche Integration mit den Services.



Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

- Behebung des FQDN-Ausfalls des Cloud-Services

Wenn die Geräteregistrierung fehlschlägt, weil der Cloud-Service-FQDN nicht aufgelöst werden kann, überprüfen Sie die Netzwerkverbindung oder die DNS-Konfiguration, und versuchen Sie erneut, das Gerät einzubinden.

- Ungültiger Registrierungsschlüssel.

Wenn die Geräteregistrierung aufgrund der Eingabe eines ungültigen Registrierungsschlüssels im Firewall-Geräte-Manager nicht abgeschlossen wird, kopieren Sie den korrekten Registrierungsschlüssel vom Cisco Defense Orchestrator, und wiederholen Sie den Registrierungsprozess. Wenn das Gerät bereits über eine Smart-Lizenz verfügt, entfernen Sie die Smart-Lizenz, bevor Sie den Registrierungsschlüssel in den Firewall Geräte-Manager eingeben.

- Unzureichendes Lizenzproblem

Wenn der Verbindungsstatus des Geräts "Unzureichende Lizenz" anzeigt, fahren Sie wie folgt fort:

1. Warten Sie etwas, bis das Gerät die Lizenz erhält, da der Cisco Smart Software Manager unter Umständen einen Zeitraum benötigt, um eine neue Lizenz auf das Gerät anzuwenden.

2. Wenn der Gerätestatus unverändert bleibt, aktualisieren Sie das CDO-Portal, indem Sie sich abmelden und anschließend erneut anmelden, um potenzielle Probleme bei der Netzwerkkommunikation zwischen dem Lizenzserver und dem Gerät zu beheben.

3. Wenn der Gerätestatus durch die Portalaktualisierung nicht aktualisiert wird, gehen Sie wie folgt vor:

    - Erstellen Sie einen neuen Registrierungsschlüssel vom Cisco Smart Software Manager, und kopieren Sie ihn. Weitere Informationen finden Sie im Video Generate Smart Licensing.
    - Wählen Sie in der CDO-Navigationsleiste die Seite "Inventory" (Bestand) aus.
    - Wählen Sie das aufgeführte Gerät mit dem Status Unzureichende Lizenz aus.
    - Klicken Sie im Bereich "Device Details" (Gerätedetails) auf Manage Licenses (Lizenzen verwalten) unter der Warnmeldung Inenough Licenses (Nicht ausreichende Lizenzen). Daraufhin wird das Fenster Lizenzen verwalten angezeigt.
    - Fügen Sie im Feld Activate (Aktivieren) den neuen Registrierungsschlüssel ein, und wählen Sie Register Device (Gerät registrieren) aus.

Nachdem der neue Registrierungsschlüssel erfolgreich angewendet wurde, muss der Geräteverbindungsstatus in "Online" geändert werden.

Eine umfassende Anleitung zur Registrierung des Firepower Device Manager (FDM) mithilfe alternativer Methoden zum Registrierungsschlüssel finden Sie in der detaillierten Dokumentation unter dem Link "Troubleshoot FDM-Managed Devices".

Diese Ressource bietet Schritt-für-Schritt-Anleitungen und Tipps zur Fehlerbehebung für verschiedene Registrierungsverfahren, mit denen FDM erfolgreich in Cisco Defense Orchestrator (CDO) integriert werden kann.

Zugehörige Informationen

- Fehlerbehebung bei FDM-verwalteten Geräten
- Management von FDM-Geräten mit Cisco Defense Orchestrator
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.