Onboard FDM to Defense Orchestrator

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document describes how to onboard a device managed by Firepower Device Manager (FDM) to Cisco Defense Orchestrator (CDO) using registration key.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Device Manager (FDM) Azure running version 7.4.1

For a comprehensive list of compatible versions and products, consult the Secure Firewall Threat Defense Compatibility Guide for additional details.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

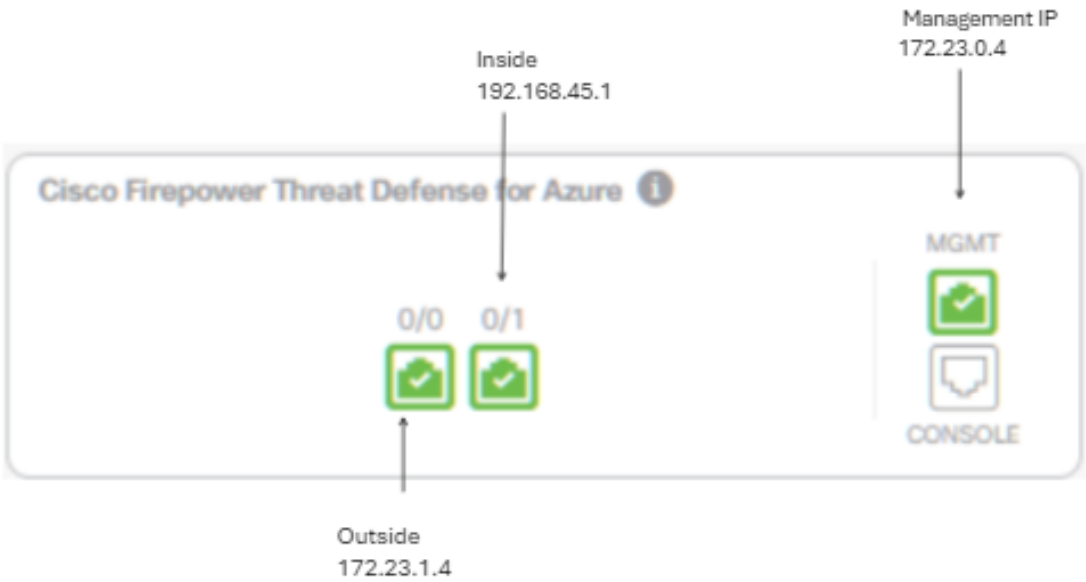
Before beginning the onboarding process of an FDM-managed device to Cisco Defense Orchestrator (CDO) using a registration key, please ensure you meet these prerequisites:

1. **Compatible Version**: Your device must be running version 6.6 or higher.
2. **Network Requirements**: Connect Cisco Defense Orchestrator to your Managed Devices
3. **Management Software**: The device must be managed via Secure Firewall Device Manager (FDM).
4. **Licensing**: Your device can use either a 90-day evaluation license or a smart license.
5. **Existing Registrations**: Ensure that the device is not already registered with Cisco Cloud Services to avoid conflicts during the onboarding process.
6. **Pending Changes**: Verify that there are no pending changes on the device.
7. **DNS Configuration**: DNS settings must be correctly configured on your FDM-managed device.
8. **Time Services**: Time services on the device can be accurately configured to ensure synchronization with network time protocols.
9. **Requirement for FDM Support Activation**. Firewall Device Manager (FDM) support and its functionality is exclusively granted upon request. Users without FDM support enabled on their tenant are unable to manage or deploy configurations to FDM-managed devices. To activate this platform, users must send a request to the support team for FDM support enablement.

Configure

Network Diagram

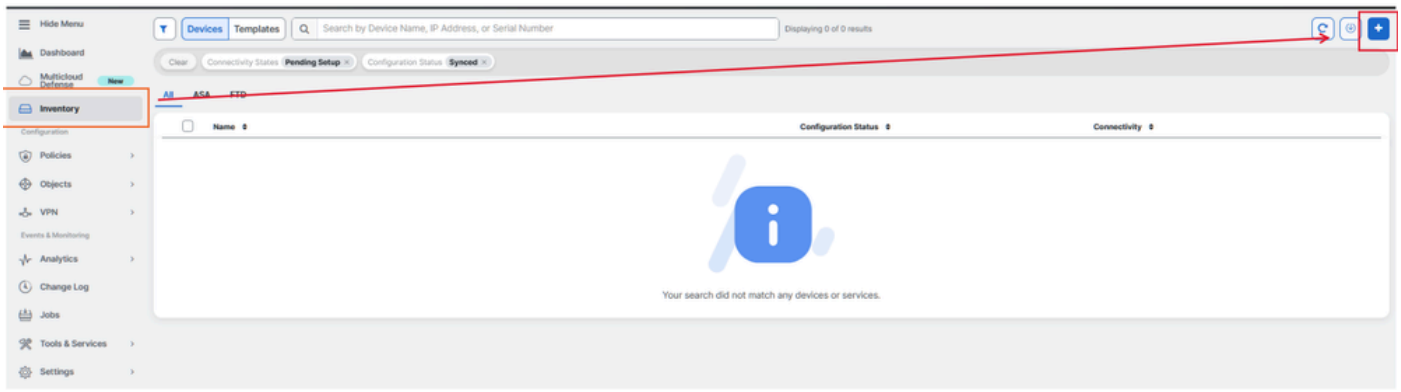
This article focuses on an FDM (Firepower Device Manager) device, which is controlled through its management interface. This interface has internet access that is essential for registering the device with Cisco Defense Orchestrator (CDO).



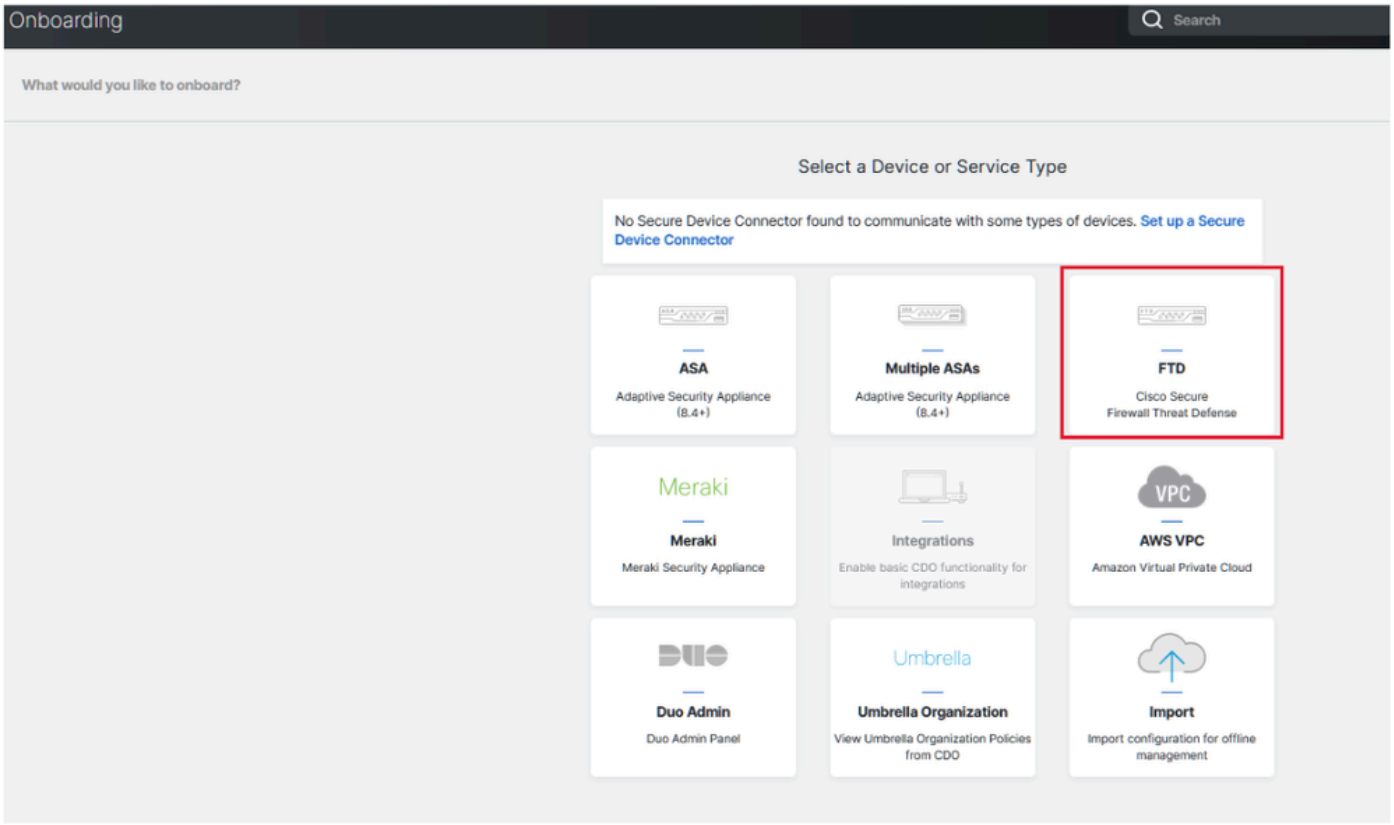
Configurations

Step 1. Log in to Cisco Defense Orchestrator (CDO).

Step 2. Navigate to the Inventory pane and select the blue plus button to onboard a device.



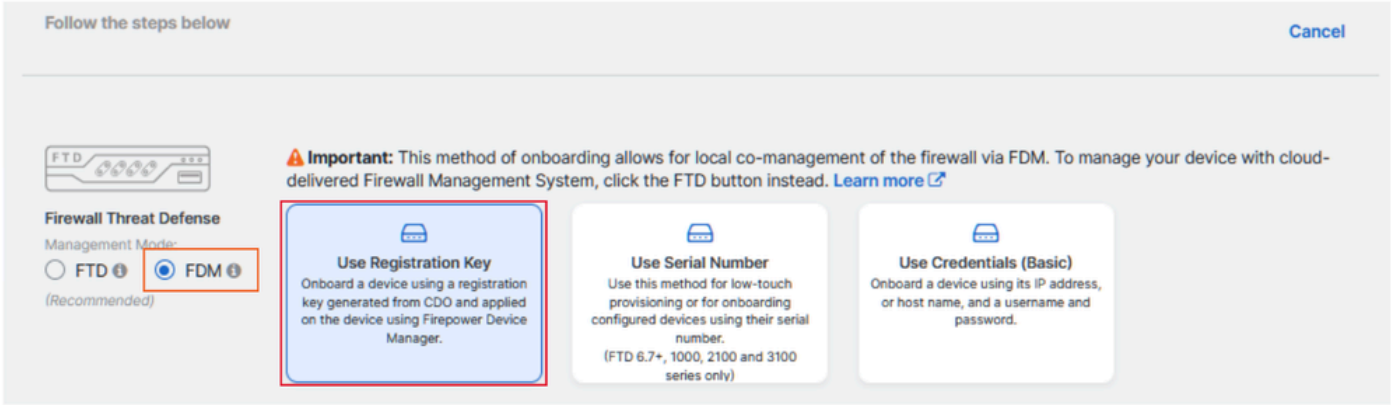
Step 3. Choose the FTD option.



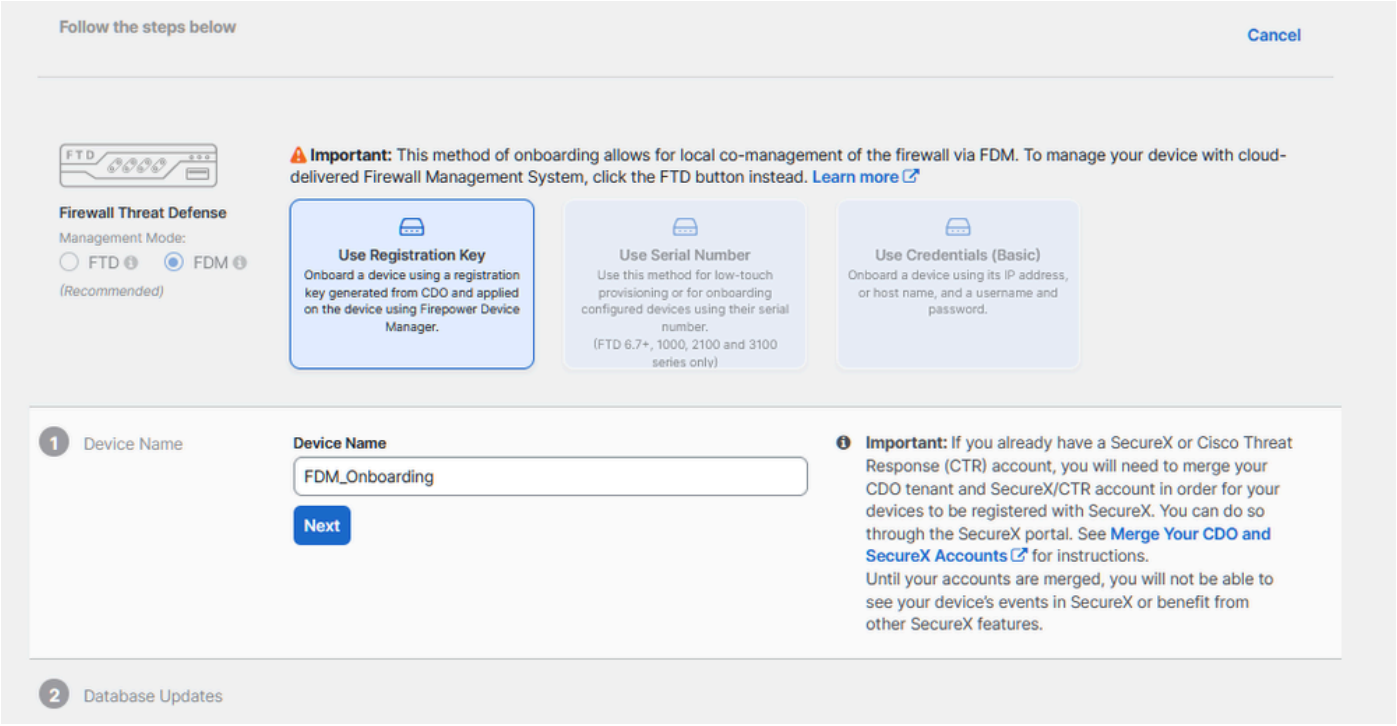
Step 4 Proceed to the Onboard FTD Device' section to commence the registration process. It is important to note the available methods for onboarding a Threat Defense Device:

- By Serial Number: This method applies to physical devices such as the Firepower 1000, Firepower 2100, or Secure Firewall 3100 series with supported software versions. It necessitates the chassis or PCA serial number and a network connection to the internet.
- By Registration Key: This is the preferred method for onboarding, particularly advantageous for devices that receive IP addresses via DHCP, as it helps maintain connectivity with CDO even if there is a change in the device IP address.
- Using Credentials: This alternative involves entering the device credentials and the IP address of its outside, inside, or management interface, tailored to the device configuration within the network.

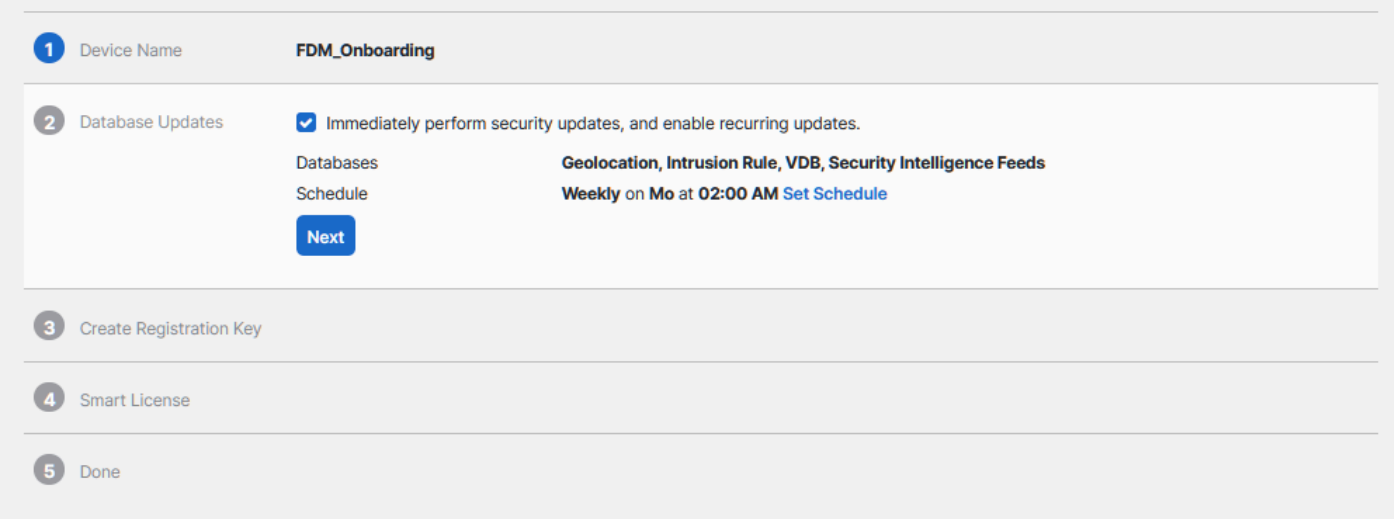
For this process, select the FDM option and then the **Use Registration Key** option to ensure consistent connectivity to CDO, irrespective of potential changes in the device IP address.



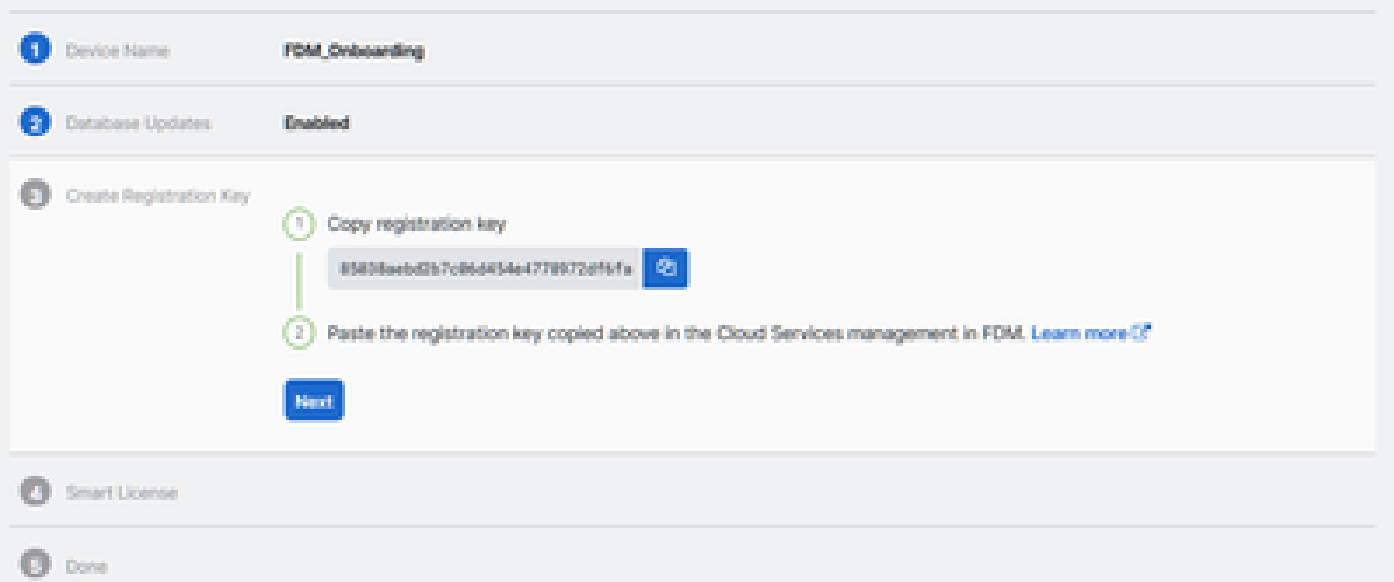
Step 5. Input the desired device name in the Device Name field and specify the Policy Assignment. Also, choose the Subscription License that must be associated with the device.



Step 6. The Database Updates section is configured by default to execute security updates immediately and set up recurring updates. Changing this setting does not alter any existing update schedules established through the Secure Firewall device manager.



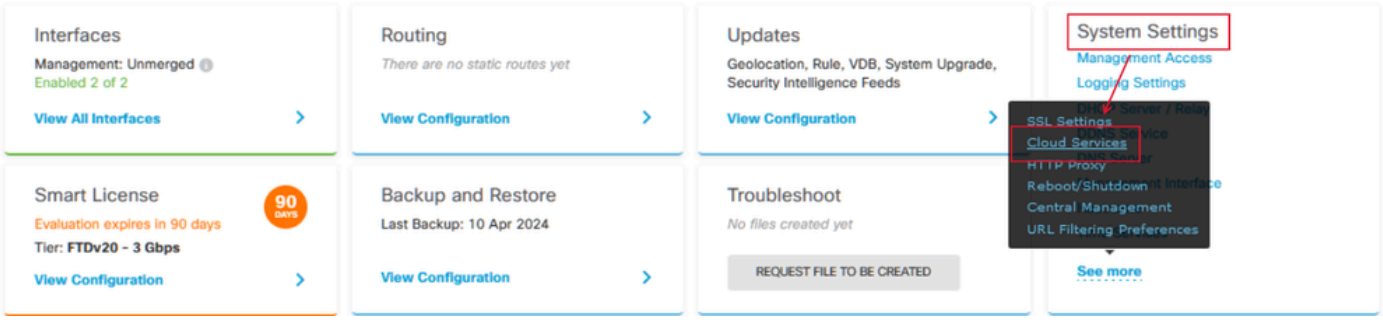
Step 7. In the CLI Registration Key section, CDO auto-generates a registration key. Exiting the onboarding interface before completion results in the creation of a placeholder for the device within the Inventory. The registration key can be retrieved from this location at a later time if necessary.



Step 8. Utilize the Copy icon to copy the generated registration key.

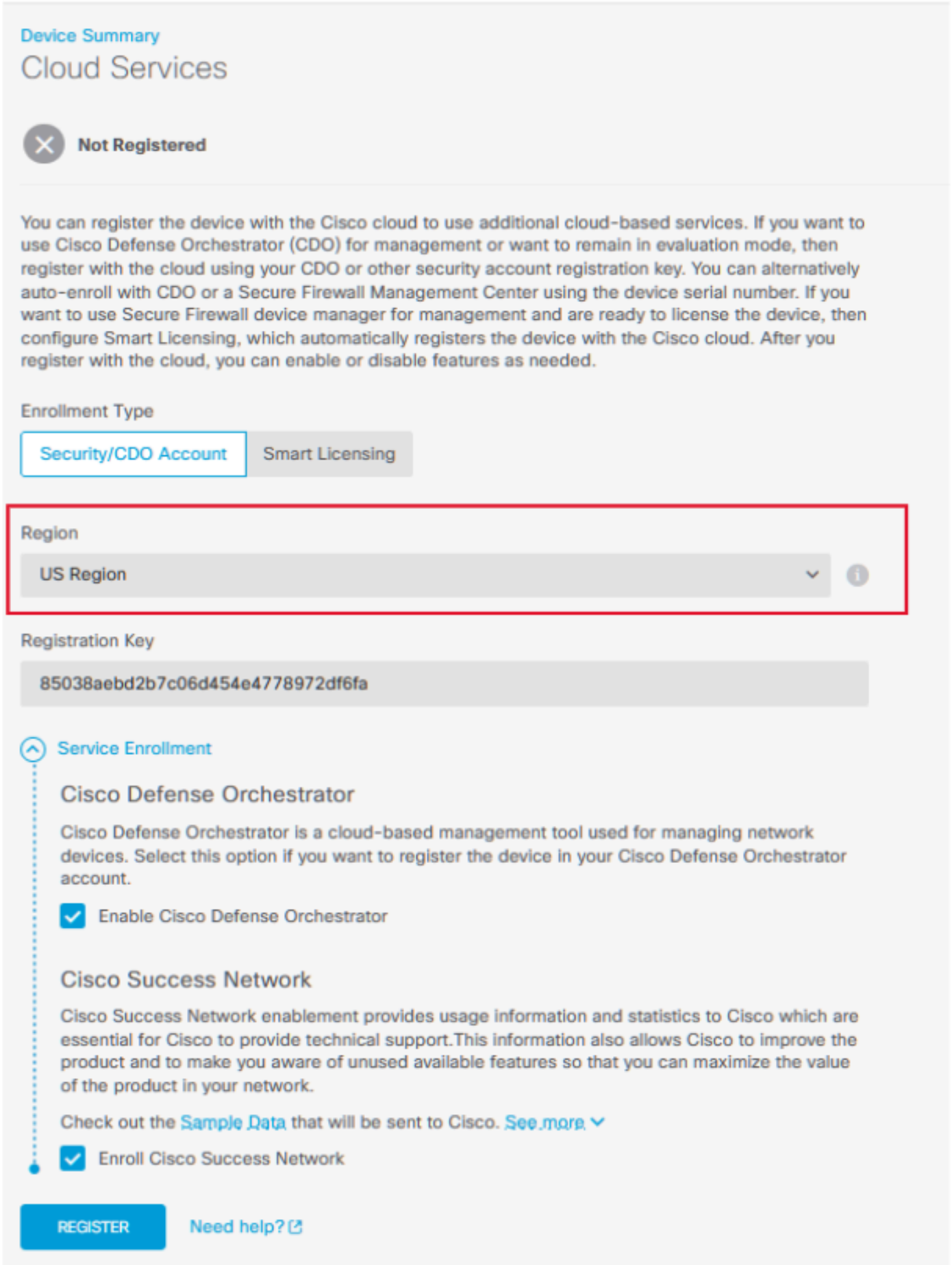
Step 9. Access the Secure Firewall Device Manager device intended for onboarding to CDO.

Step 10. Select Cloud Services from within the System Settings menu.

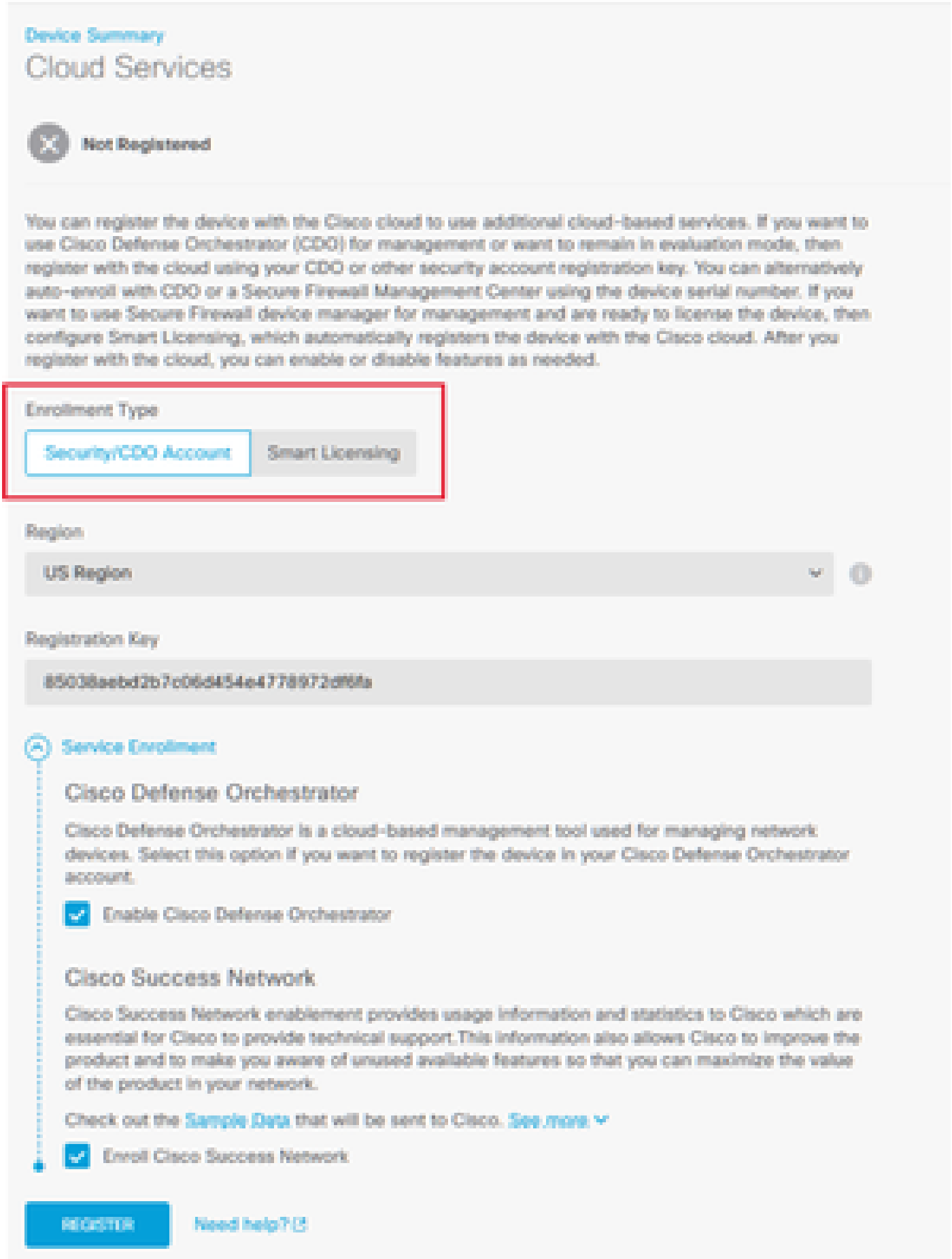


Step 11. Designate the correct Cisco cloud region in the Region dropdown, aligning with the tenant geographic location:

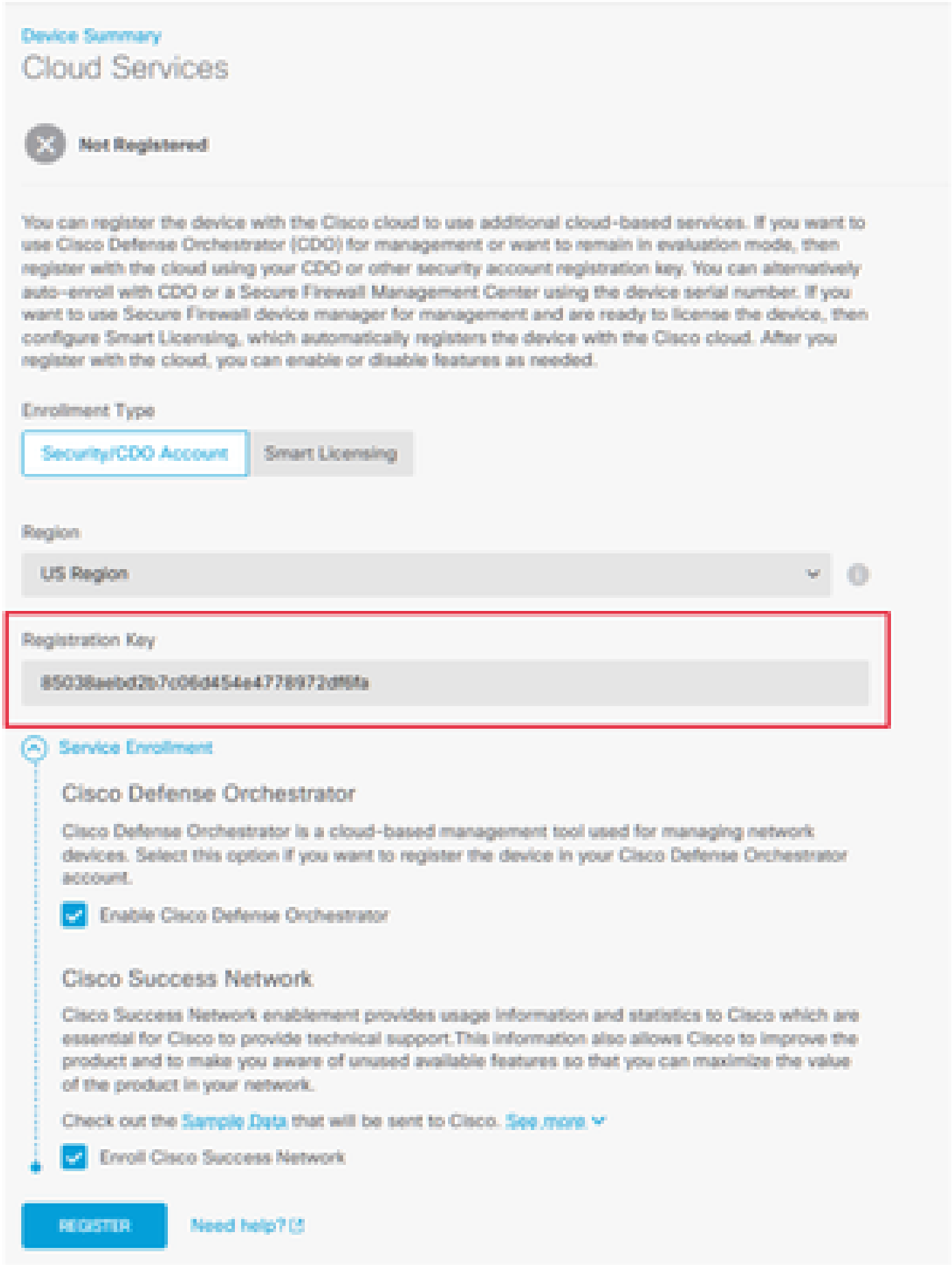
- For defenseorchestrator.com, select US.
- For defenseorchestrator.eu, select EU.
- For apj.cdo.cisco.com, select APJ.



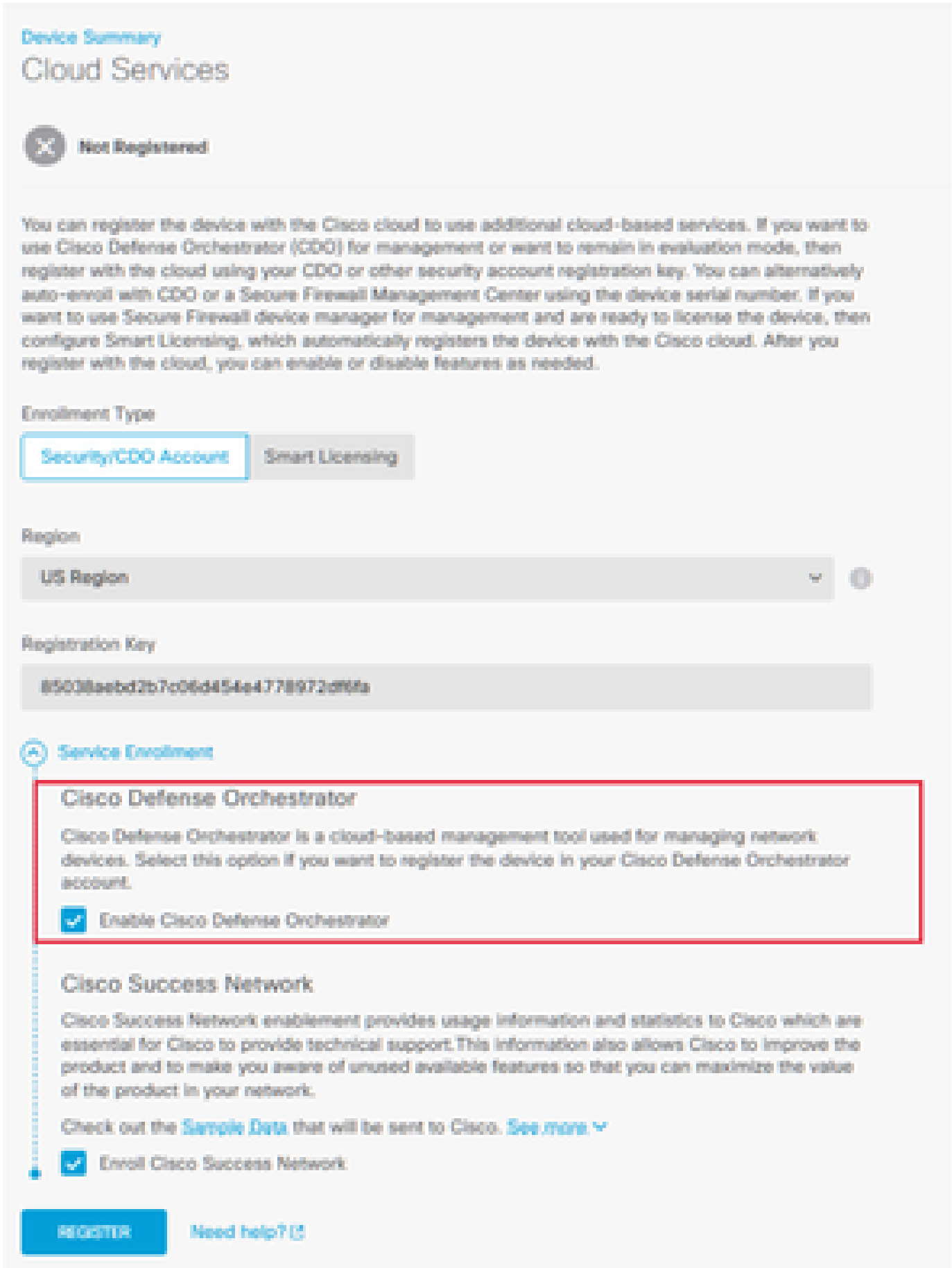
Step 12. In the Enrollment Type section, opt for the Security Account.



Step 13. Paste the registration key into the Registration Key field.

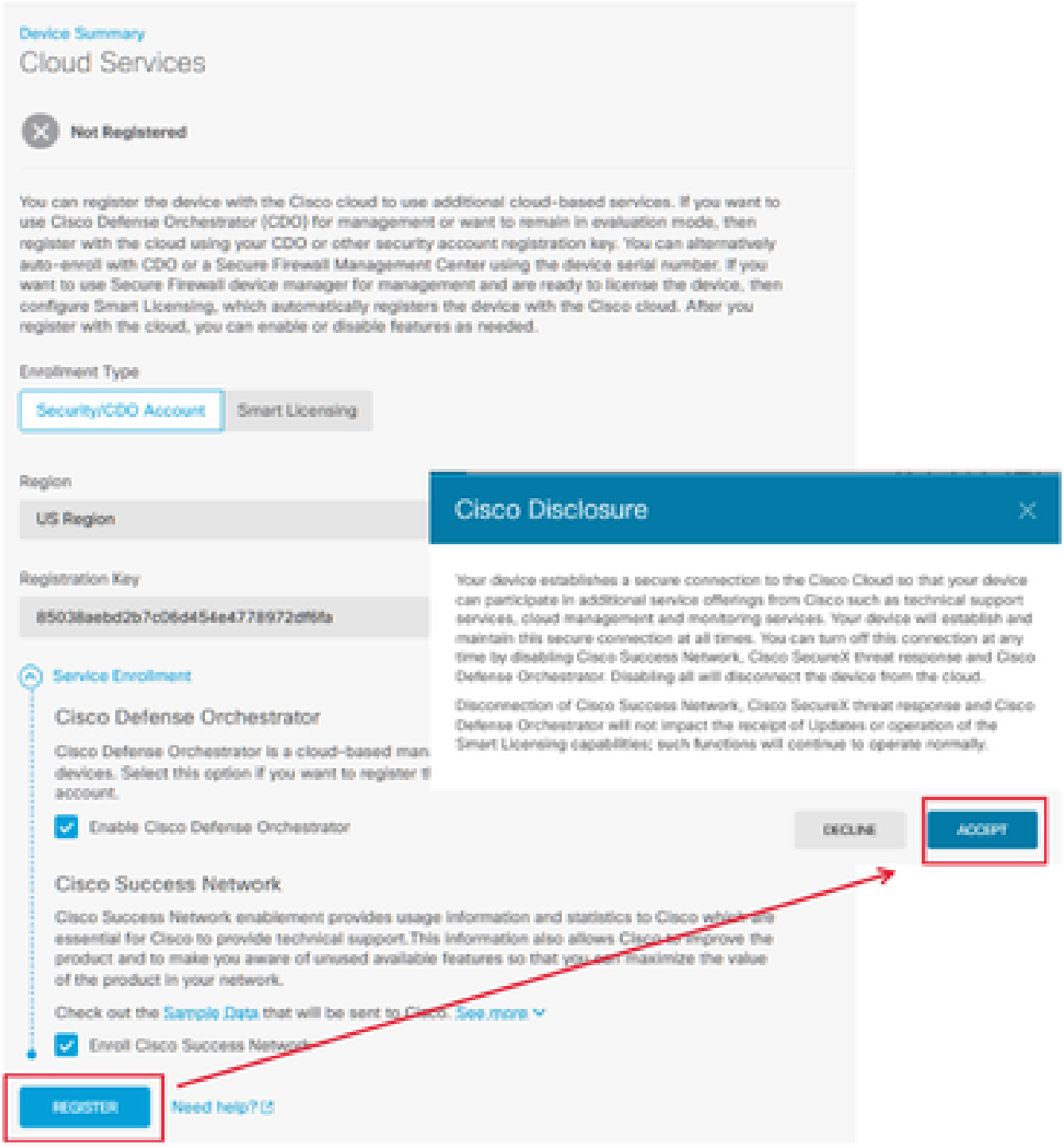


Step 14. For devices on version 6.7 or later, verify that Cisco Defense Orchestrator is enabled in the Service Enrollment section.



Step 15. (Optional) Review the Cisco Success Network Enrollment details. If not wishing to partake, deselect the Enroll Cisco Success Network check box.

Step 16. Select Register and accept the Cisco Disclosure. The Secure Firewall Device Manager submits the registration to CDO.



Step 17. Back in CDO, in the registration key creation area, choose Next.

Step 18. (Optional) Identify and select the licenses intended for the device, then proceed by selecting Next.

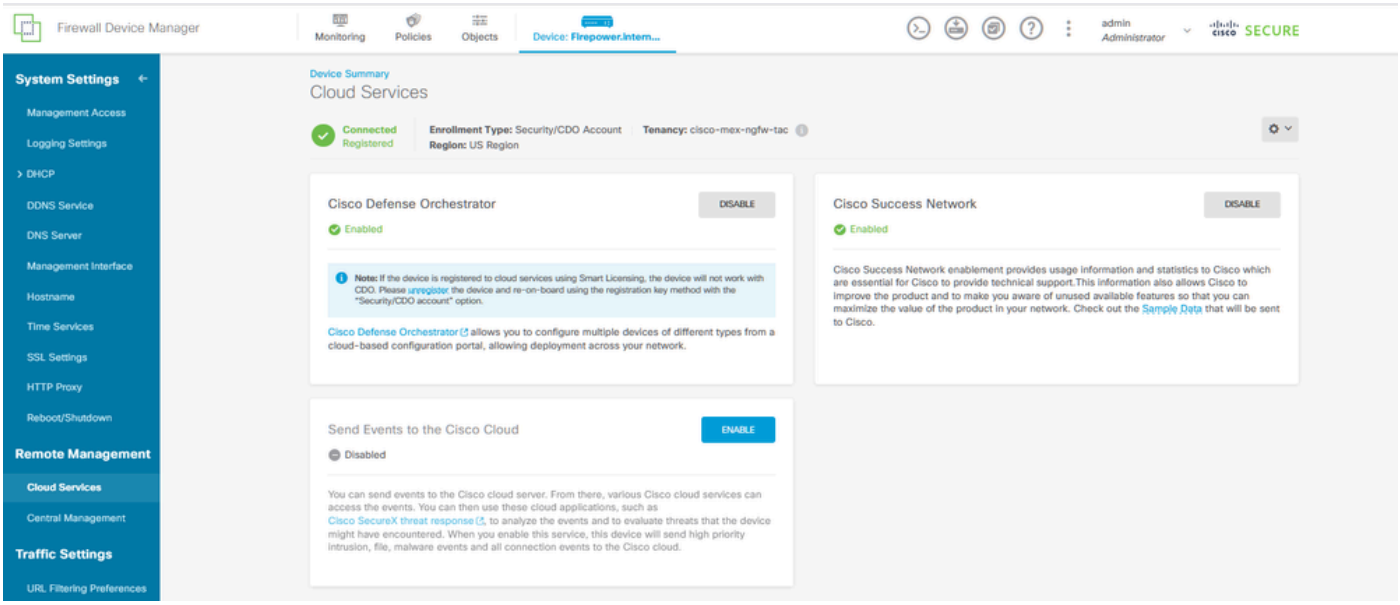
Step 19. Observe the device status in the CDO Inventory transition from **Unprovisioned** to **Locating**, then to **Syncing**, and finally, to **Synced**.



Verify

Use this section in order to confirm that your configuration works properly.

Navigate to the CDO portal and check the device status, which indicates **Online** and **Synced**. Additionally, verification of the status can be conducted via the FDM GUI. Navigate to **System > Cloud Services** to observe the connection status for Cisco Defense Orchestrator and Cisco Success Network. The interface displays a **Connected** status, confirming successful integration with the services.



Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

- Resolution of Cloud Service FQDN Failure

If device registration fails due to an inability to resolve the cloud service FQDN, check the network connectivity or DNS configuration and attempt device onboarding again.

- Invalid Registration Key Error

When device registration does not complete due to the entry of an invalid registration key in the Firewall Device Manager, proceed to copy the correct registration key from Cisco Defense Orchestrator and retry the registration process. If the device is already smart licensed, remove the smart license before entering the registration key in the Firewall Device Manager.

- Insufficient License Issue

In instances where the device connectivity status indicates "Insufficient License", proceed to:

1. Allow some time for the device to obtain the license, as Cisco Smart Software Manager can require a period to apply a new license to the device.

2. If the device status remains unchanged, refresh the CDO portal by signing out and then signing back in to resolve potential network communication issues between the license server and the device.

3. If the portal refresh does not update the device status, take these actions:

- Generate a new registration key from Cisco Smart Software Manager and copy it. Refer to the Generate Smart Licensing video for guidance.
- In the CDO navigation bar, select the Inventory page.
- Choose the device listed with the **Insufficient License** state.
- In the Device Details pane, click on **Manage Licenses** under the **Insufficient Licenses** alert. The Manage Licenses window prompts.
- In the Activate field, paste the new registration key and select **Register Device**.

After the new registration key is successfully applied, the device connectivity state must change to 'Online'.

For comprehensive guidance on registering Firepower Device Manager (FDM) using alternative methods to the Registration Key, please refer to the detailed documentation provided in the link: Troubleshoot FDM-Managed Devices.

This resource offers step-by-step instructions and troubleshooting tips for different registration techniques that can be employed to successfully onboard FDM to Cisco Defense Orchestrator (CDO).

Related Information

- Troubleshoot FDM-Managed Devices
- Managing FDM Devices with Cisco Defense Orchestrator
- Cisco Technical Support & Downloads