Device Configuration Prerequisites

Required Platform Configurations

You need to make the following configuration changes on these platforms for Discovery to work properly.

Table 1: Required Platform Configurations

Feature	Platform	Required Configuration
Discovery (device inventory collection)	Cisco ASR 9000 router or any other Cisco device that requires NETCONF support for their device pack.	Configure NETCONF on these platforms. For information, see NETCONF Configuration, on page 2.
Discovery (host inventory collection)	Devices connected to hosts using SNMP.	Configure SNMP traps on these devices. For information, see SNMP Trap Configuration, on page 2.
	Devices connected to hosts using IPDT.	Enable IPDT for these devices. For information, see IP Device Tracking Configuration, on page 3.
	• Cisco Series 2504 WLC • Cisco Series 5508/5520 WLC • Cisco Series 8510/8540 WLC	Configure SNMP traps and object identifiers on these wireless LAN controllers. For information, see Wireless LAN Controller Configuration, on page 3.

NETCONF Configuration

You must enable the NETCONF protocol for the Cisco ASR 9000 router or for any other Cisco device that requires NETCONF support for their device pack. If NETCONF is not enabled, then the controller's inventory collection process will be incomplete for that device.

Note Though NETCONF typically runs over SSH or on its own port, with the Cisco APIC-EM and for the Cisco ASR 9000 router NETCONF is run over a CLI session.

For specific information about enabling NETCONF for your own Cisco device, refer to that device's documentation. As an example, a typical configuration sequence on a terminal to enable NETCONF on a Cisco device is as follows:

```
#ssh server v2
#netconf agent tty
#!
#xml agent tty
#!
#commit
#end
#crypto key generate rsa
```

Note The rsa key needs to be generated to succeed with SSH. For this reason, the crypto key generate rsa command needs to be executed in exec mode at the end of the configuration sequence if it has not already been done.

SNMP Trap Configuration

To ensure that Cisco APIC-EM captures data about the hosts connected to your network devices, you must set up SNMP traps or notifications. Enter the following SNMP commands to set up SNMP traps on the devices that connect to hosts within your network:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **version 2c public**

Note For Cisco Nexus devices, enter the following SNMP commands instead of the commands listed above:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **use-vrf default**

After configuring SNMP traps on the network devices, the following data is captured and made available in the controller's GUI:

- Host data including the MAC address, IP address, and type
- Device interface status

IP Device Tracking Configuration

The Cisco APIC-EM discovery function uses several protocols and methods to retrieve network information, such as hosts IP addresses, MAC addresses, and network attachment points. To use IP Device Tracking (IPDT) for discovery, you must manually enable IPDT on the devices and interfaces for this protocol to be used to collect host information. To enable IPDT on your devices, refer to your specific device documentation. For general information about IPDT, see IP Device Tracking (IPDT) Overview.

Wireless LAN Controller Configuration

The Cisco APIC-EM accepts SNMP traps from several Cisco Wireless LAN Controllers (WLCs). The SNMP traps are used to update the host inventory database. You need to configure the WLCs so that the Cisco APIC-EM is the trap receiver, and the WLCs send the enhanced traps to the Cisco APIC-EM.

The following WLCs require SNMP traps to be enabled:

- Cisco Series 2504 Wireless LAN Controller
- Cisco Series 5508/5520 Wireless LAN Controller
- Cisco Series 8510/8540 Wireless LAN Controller

The following table specifies the SNMP traps and object identifiers that must be set on the WLCs.

Trap Name	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9
ciscoLwappDot11ClientDeAuthenticatedTrap	1.3.6.1.4.1.9.9.599.0.10
ciscoLwappDot11ClientMovedToRunStateNewTrap	1.3.6.1.4.1.9.9.599.0.11
ciscoLwappDot11ClientMobilityTrap	1.3.6.1.4.1.9.9.599.0.12

The following configurations must be set to enable the above SNMP traps:

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

Note When setting the SNMP traps on the WLCs, ensure you configure the IP address of the Cisco APIC-EM as the SNMP trap destination IP address. You set the Cisco APIC-EM IP address using the configuration wizard during the deployment process. For information about this process and the controller IP address, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information.