CHAPTER **12**

# Register DMPs

**Revised: May 4, 2015**
**OL-15762-05**

**We prepared this material with specific expectations of you.**

**Audience**

- **Everyone**—You understand IP addresses, subnets, and other LAN fundamentals.
- **Everyone**—Your user account permissions allow you to manage DMPs.
- **Medianet Users**—You understand Medianet fundamentals and have hands-on experience in its configuration and use. Or, because you lack this specialization, you will study technical materials on Cisco.com as needed.

# Concepts

## Overview

Before you can start to manage DMPs centrally, you must register them with DMM. You can automate this process or run it manually for one DMP at a time.

- Cisco DMS-native autoregistration finds every DMP in the subnets that you specify. Then, it configures these DMPs to recognize and trust your DMM appliance. It restarts the DMPs and then registers them in DMM for centralized management.

- Medianet autoregistration finds any DMP automatically when you attach it to a Medianet-ready switch in your Enterprise. This method optimizes the switch port for rich media delivery, and then registers the DMP in DMM for centralized management.

# Glossary

⏱

**Timesaver**    Go to terms that start with...   [ **A** | **C** | **D** | **L** | **M** ].

## A

**additional-location-information**    One of two essential Location Services values that must be configured on your Medianet-enabled switch. The "*civic-location-id*" value and the "*additional-location-information*" value are encapsulated into a CDP message that endpoints receive.

This value describes any non-default details to inject into the encapsulated CDP message. As this is a data injection, it depends wholly on the presence of a defined *civic-location-id* value. Absent **that** value, there is no way for **this** value to reach any endpoint (CSCti85043). Later, when you plug a Medianet-ready DMP into a properly configured switch, the Location Services feature of MSI populates the Location URL field automatically in DMPDM.

| Medianet Services | |
|---|---|
| MediaNet Enabled | On ▾ |
| Timeout (ms) | 30000 |
| Switch IP Address | 172.26.135.162 |
| Switch Name | me-w-austin-3.me.com |
| Switch Port | GigabitEthernet1/0/12 |
| VLAN | 282 |
| Location ID | |
| Location URL | 34=Research_Blvd&28=Broken_Spoke&27=2&25=2&24=3330&19=125&15&3=Austin&1=Texas |

**autoregistration**    *See* MSI registration service.

**Auto Smartports**[1]    A collection of interface-level switch commands bundled together as a macro that configures a switchport without human intervention. Upon detecting a connection to one of its physical interfaces (or "ports"), a Medianet-ready switch uses CDP packets or a similar mechanism[2]—in tandem with a *port-based network access control* (PNAC) standard such as 802.1x/MAB—to learn what type of device has connected to it. Device identification triggers the appropriate Auto Smartports macro to run automatically on the switch and configure its interface appropriately for the detected device type. This behavior eases the administrative burden of configuring multiple switchports manually. (Similarly, when there is a "link-down" event on the port, the switch removes the macro.) In the ITU model and framework for network management, known as *FCAPS*, Auto Smartports macros act in support of what's called *configuration management*.

See *Auto Smartports Configuration Guide, Release 12.2(58)SE* at http://cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_58_se/configuration/guide/aspcg.html.

---

1. Infrequently abbreviated as *ASP*.
2. Such as Link-Level Discovery Protocol (LLDP) packets, packets that include specific MAC addresses or Organizational Unique Identifiers (OUIs), or attribute-value pairs within a RADIUS response.

## C    ↑ *Return to Top*

**CDP**

*Cisco Discovery Protocol*. DMPs and other devices that support CDP can communicate facts about themselves, amongst themselves, over any physical network medium that supports *Subnetwork Access Protocol* (SNAP) encapsulation. CDP uses the *data link layer*, which connects physical network media to upper-layer protocols. And because CDP operates at this level, two or more CDP devices that support different network layer protocols (for example, IP and *Novell IPX*) can learn about each other.

Specifically, CDP causes devices to advertise not only their existence, but also their platform types, protocols, IP addresses, and SNMP-agent addresses to neighboring devices on their LAN switch or WAN. And when their connected switch is Medianet-ready, device identification can also trigger an Auto Smartports macro to run automatically.

Thus, CDP facilitates discovery — by network management applications — of Cisco devices that are neighbors of known devices. And this is particularly useful when such previously undiscovered neighbors use lower-layer, transparent protocols. After they possess information about such devices, network management applications can send SNMP queries to them.

In addition, CDP detects native VLAN and port duplex mismatches.

**civic-location-id**

One of two essential Location Services values that must be configured on your Medianet-enabled switch. The "*civic-location-id*" value and the "*additional-location-information*" value are encapsulated into a CDP message that endpoints receive.

This value describes the physical site — including the municipality, street address, floor designation, and so on — where a switch and its attached nodes are deployed.

## D    ↑ *Return to Top*

**DHCP**

*Dynamic Host Configuration Protocol*. A standard method for devices to request, and servers to allocate, IP addresses in a network without human intervention.

**DHCP option 125**

An optional DHCP relay class that:

- Injects "vendor-identifying, vendor-specific information" into the request (within a DHCP DISCOVER message) to receive a dynamic IP address.
- Identifies the type of client sending the DHCP DISCOVER message.

In turn, a DHCP server that is configured to support Option 125 can relay the client-generated request to some other DHCP server. This mechanism allows an organization to designate DHCP servers for clients that meet particular criteria. For example, you might want all of your DMPs to receive their IP addresses from a DHCP server that you reserve for this purpose exclusively.

# L                    ↑ *Return to Top*

**Location Services**    Mechanism by which a device can learn its actual physical ("civic") location through its connection to a Medianet-ready switch. Upon learning its location, the device can then share this information with peers, management servers, and other equipment on its network. The physical location of a DMP is almost always an important factor in which central management server it should trust, which assets it should play, which commands it should run, and which schedule it should follow.

Someone must configure two essential values on your Medianet-enabled switch: "*civic-location-id*" and "*additional-location- information*." These values are encapsulated into a CDP message that endpoints receive.

**Note**    **CDP and LLDP constrain how much location information you can store on a Medianet-enabled switch.** Make sure that this information never exceeds 255 bytes.

**Note**    **A DMP 4400G cannot receive or use Location Services information over Wi-Fi.** Its connection type to your Medianet-enabled switch must be Ethernet.

**Tip**    *Is the Location ID value blank in DMPDM?* If so, make sure that a civic-location-id value is defined correctly on your switch. (CSCti85043).

# M                    ↑ *Return to Top*

**Medianet**    End-to-end intelligent architecture for optimized delivery of rich media to a variety of endpoints throughout an enterprise. Cisco Medianet is media-aware, endpoint-aware, and network-aware.

**MSI**    *Media Services Interface*. Announces services to a DMP or any other Medianet-ready device that you connect to a Medianet-enabled switch. MSI tells devices about their neighbors and their civic location.

**MSI registration service**    Medianet feature by which:

- Devices send encrypted registration requests to management servers.
- Servers receive such requests, respond to them, and store records in a local database.

**MSI service discovery**    Mechanism that applies DHCP option 125 packets to advertise—and poll for—the availability of particular services in a network. Service discovery also notes which hosts provide these services.

# Partial Support for Cisco Medianet 2.1 Features

Some DMP endpoints support some Cisco Medianet 2.1 features.

✎
**Note**    **We do not support any Medianet features on DMP 4305G endpoints.**

🔍
**Tip**
- **To assess your network for Medianet readiness, see http://cisco.com/go/mra.**
- **To review solution reference network designs (SRNDs) for Medianet, see http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html.**

| | |
|---|---|
| **DMP 4310G** | DMP 4310G endpoints support discovery via DHCP and can learn their physical location. In addition, they know and can broadcast their product type, model, and software version.<br><br>Through their use of your Medianet, they can receive their IP address, VLAN assignment, and network configuration settings automatically. Furthermore, they receive information from Medianet through DHCP[1] that helps them to autoregister themselves with your DMM server.<br><br>Later, after a successful autoregistration, the splash screen on these DMPs includes key parameters and states explicitly that setup succeeded. |
| **DMP 4400G** | Medianet 2.1 feature support by DMP 4400G endpoints is equivalent to support by DMP 4310G endpoints, **with just one exception**.<br><br>Ordinarily, a DMP 4400G can participate in networks via Ethernet or Wi-Fi. **However:**<br><br>**A Wi-Fi connection by a DMP 4400G prevents it from obtaining or using any Location Services information that Medianet might be configured to provide.** |

1.  With DHCP option 125 (V-I Vendor-Specific Information) for service discovery, after you configure your supported DHCP server to support this option. See **RFC 3925**.

# DHCP Server Configuration Notes for MSI Service Discovery

For your MSI service discovery purposes as a DMP administrator, Medianet must know that a DMM server is available and know exactly which addressable node it is on your network. You must configure your DHCP server to facilitate this information-sharing model.

Configuration methods vary among platforms and implementations.

- dhcpd Example, page 12-6
- Windows Server Example, page 12-6

## dhcpd Example

An example here shows entries in the **dhcpd.conf** file for a Linux-based DHCP server called *dhcpd*. Entries like these advertise the IP address of your authoritative DMM appliance—converted here from decimal to hex and shown in red—to any DMPs that should trust its directives implicitly.

```
option domain-name "example.com";
option domain-name-servers 192.168.1.1;
option option-125 code 125 = string;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.200 192.168.1.210;
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
}
class "DMM" {
match if option option-125 = "\x00\x00\x00\x09\x06\x13\x04\x01\x44\x4d\x4d";
option option-125
"\x00\x00\x00\x09\x0b\x14\x09\x01\x80\x6b\xe0\xbc\x1f\x90\x00\x01";
}
```

**Tip**    **The Linux CLI can easily convert IP address octets from decimal to hexadecimal.**

**$ echo 'ibase=10;obase=16;** ⬚octet⬚ **'  |  bc** ← *(Remember to use a closing quote mark before the pipe.)*

And so, in keeping with the previous conversion example, shown in **red**:

- 128 becomes **x80**
- 107 becomes **x6b**
- 224 becomes **xe0**
- 188 becomes **xbc**

**Note**    **See the Medianet documentation on Cisco.com for detailed instructions.**

## Windows Server Example

In contrast, the DHCP offering in Windows Server 2008 (and, likewise, Windows Server 2003) cannot handle DHCP option 125 queries natively. Therefore, you must install a "callout" DLL that injects this ability into the server before you can configure it to advertise the availability of any service.

**Note**
- For **32-bit** Windows Server, the DLL filename is DHCPSDDLL**x86**.DLL.
- For **64-bit** Windows Server, the DLL filename is DHCPSDDLL**x64**.DLL.

Afterward, you must edit **\Medianet\msi\apps\dhcpsddll\src\dhcpsdconfig.reg** to include a *3-tuple* (**IP,port,transport**), converted to hexadecimal, that identifies your DMM appliance as a provider of centralized management for DMPs.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco]

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Settings]
"DebugLevel"=dword:00000000
"IgnoreProcessItFromChain"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\DhcpSd\Records\1]
"DMM"=hex:0a,c2,33,2a,1f,90,00,01
```

And finally, you must add two keys to the Windows registry, under

`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Paramters`

- **CalloutEnabled REG_DWORD 1**
- **CalloutDlls REG_MULTI_SZ** *<full_path_to_DLL>*

✎
**Note**    See the Medianet documentation on Cisco.com for detailed instructions.

# Understand Medianet Autoconfiguration for DMPs

DMP 4310G and 4400G endpoints can use CDP to announce and identify themselves on networks. And you might use Ethernet cables to connect such DMPs to switches where the autoconfiguration (Auto Smartports) features of Medianet are enabled. When you do, these switches recognize from the CDP announcements that the newly connected devices are DMPs.

After recognizing that a DMP is attached to one of its Ethernet ports, the switch can apply to this port a set of built-in configuration macros (Auto Smartports) that are optimized specifically for DMPs. By configuring so many settings automatically, Medianet can accelerate and simplify DMP mass deployments, QoS configuration, and asset tracking. In turn, these simplified deployments can lower your operating costs.

# Information That Medianet and DMPs Exchange

Medianet and a DMP can exchange these types of data.

- name of the chassis
- system name
- system object
- hardware revision
- firmware revision
- software revision
- serial number
- manufacturing name
- model name
- asset identifier
- CDP timeout
- VLAN assignment
- switch port assignment
- switch name and model
- switch IP address
- location string

If you would like to learn more about Medianet, see http://cisco.com/go/medianet.

# Medianet Activation Workflow for a DMP 4310G or 4400G

Medianet support is enabled by default on DMPs in Cisco DMS release 5.3. However, you can turn this support Off or back On again at your discretion.

✎
**Note**    **We do not support any Medianet features on DMP 4305G endpoints.**

⌕
**Tip**    **You can deactivate Medianet support on one or more DMPs.** Simply reverse step **3b** in this workflow.

1.  Issue the command to enable Medianet 2.1 on a supported network switch that runs Cisco IOS 12.2(55.0.36)SE).

    `Switch(config)#macro auto global processing`

2.  Enable the Auto Smartports feature globally on the switch.

3.  Use either DMPDM or Digital Signs to enable Medianet features on your DMP 4310G or 4400G.

    **DMPDM**
    a.  Click **Network** in the Settings area. '

    

    b.  Choose **On** from the Medianet Enabled list in the Medianet Services area.

    

    c.  Save this changed setting, and then restart your DMP.

**Digital Signs**

a. Create and save a system task that uses:

- **Set** as its request type.

- **`init.startService_msi=yes&mib.save=1&mng.reboot=1`** as its request string.

**Create New System Task**

| | |
|---|---|
| Name | |
| Description | |
| Request Type | Set |
| Request | |

**Submit**    **Cancel**

b. Schedule and deploy the system task to run on your DMP 4310G or 4400G.

The request string includes a command to restart your DMP.

# Restrictions

**Non-Medianet Autoregistration**

- DMM-native autoregistration **does not** use any Medianet technologies. It uses NMAP (CSCtk02451).

**DHCP**

- As of May 2011, these DHCP servers have passed our tests for using Medianet with DMPs.

  - Linux ISC dhcpd

  - The DHCP implementation in Windows Server 2003

  - The DHCP implementation in Windows Server 2008

  - Cisco Network Registrar

> **Note**    THIS RELEASE DOES NOT SUPPORT ANY DHCP SERVER THAT RUNS ON A CISCO ROUTER OR SWITCH.

**Login Credentials**

- All DMPs that you manage centrally in DMM must share one identical set of DMPDM login credentials.

**Medianet**

- A DMP 4310G might come to use the wrong IP address when it relies upon a Medianet switch where more than one VLAN uses DHCP. For the switch to bungle IP address assignment in this way, temporary conditions that do not sever the DMP's AC power connection must nonetheless interrupt its network connection through the switch. (Thus, this problem cannot possibly occur while the DMP uses PoE.) Specifically, the Medianet switch assigns its default VLAN to your DMP. But then—after your DMP's network connection is interrupted and restored—your Medianet switch assigns to your DMP a dynamic IP address from another VLAN on this same switch. The mismatch disrupts centralized management of your DMP.

To prevent this problem or to recover from it, you must run a shell script on your switch. See the "Prevent DHCP Address Assignments to the Wrong VLAN" section on page 12-25.

# Guidelines

## Limit Your Use of Manual Registration

⚠
**Caution**    **In addition to our support for Medianet features to autoregister your DMPs, DMM includes an efficient, timesaving feature of its own to autoregister your DMPs. Despite the presence of two robust and largely automated methods, you can register a DMP manually for testing purposes.**

We recommend that you never use the method to register a DMP manually, except in a lab for testing purposes. Manual registration is neither suitable for, nor scalable in, a production network.

Eventually, when autoregistration finds and adds a DMP that you registered manually, the device inventory database develops multiple records for the one device. We see this duplication as an IP address conflict, which interferes with normal operation and triggers an alarm in DMS-Admin.

## General Best Practices for Non-Medianet Autoregistration

### Choose Network Ranges Cautiously

When you autoregister DMPs that are new to your DMM appliance, they restart immediately even when they are known already to another DMM appliance, and even when they are running an event. Therefore, when your organization uses more than one DMM appliance, be careful to autoregister only those DMPs that you are not already managing centrally elsewhere. Otherwise, you might temporarily disrupt media playback for the signs in your network.

## Best Practices to Schedule Non-Medianet Autoregistration Events

### Stagger Deployment Schedules

DMP autoregistration operations that are native to DMM (as opposed to the superficially similar operations in a Medianet) occur in a sequence that does not tolerate disruption.

- You can schedule multiple DMP autoregistration operations to run simultaneously only when they will all search the same one subnet.
- **However**, when you define DMP autoregistration operations to search **more than one** subnet, you must not schedule them to run simultaneously, or even to overlap. When they overlap, only the first of them can run at all. Furthermore, DMM does not show any error message to explain why the similar operations all failed.

- Therefore, you should plan to stagger the start times by at least 35 minutes apiece when you schedule DMP autoregistration tasks that will search multiple subnets.

> **Note** **In a very large network that contains thousands of DMPs, the necessary interval might be longer than 35 minutes.**

- We recommend that you autoregister DMPs after normal business hours. Autoregistration of 5,000 DMPs takes approximately 4 minutes in a fast network and does not use polling.

**Set Events to Recur as Needed**

DMM runs any non-Medianet autoregistration job once each time that you schedule it to run.

DMM does not scan the specified network range continuously for DMPs that you might add in the future. Therefore, when you plan to add DMPs frequently, you should schedule a non-Medianet autoregistration event to recur accordingly.

- Your DMPs must all share identical user credentials for their respective accounts. **Otherwise, non-Medianet autoregistration cannot occur.** Nor can DMM centrally manage DMPs whose passwords differ from your universal DMP password.

> **Note** **Special characters, including exclamation points (!), question marks (?), ampersands (&), at signs (@), and asterisks (*) are forbidden in DMP passwords.** (CSCsq41233; CSCsw47873; CSCub67295)

- Verify that the routers, switches, and firewalls between your DMM appliance and the NMAP address range for non-Medianet autoregistration allow TCP port 7777 to send and receive packets (CSCtk02451). Verify also that ICMP (ping) traffic is allowed to pass from your DMM appliance to your DMPs on this port. **When any of this traffic is blocked anywhere along its route, non-Medianet autoregistration cannot occur.**

> **Caution** **You can stop untrusted DMM appliances from seizing control of your DMPs.** Simply configure your network firewall to restrict which devices can send inbound traffic to your DMPs over TCP port 7777.

# Understand the Sequence of Operations for Non-Medianet Autoregistration

DMM-native (non-Medianet) autoregistration operations follow this sequence.

1. DMM scans every device in the specified address range, looking for devices where TCP port 7777 is open.
2. DMM confirms which such devices are DMPs.
3. DMPs receive information about your DMM server, and are then instructed to restart.
4. Upon restarting, DMPs transmit updated information about themselves to DMM and set their own status to "Up."
5. DMM generates new database records for all DMPs that are newly autoregistered.
6. DMM assigns newly registered DMPs to any DMP groups that match the address range that you entered.
7. DMM assigns newly registered DMPs to the "All DMPs" group.

**Related Topics**

# Procedures

## Use DMPDM to Prepare a DMP for Manual Registration

When autoregistration is not suitable, such as for testing purposes, you can perform the required steps manually to register a DMP in DMM. However, you must first prepare the DMP.

**Procedure**

**Step 1** Point your browser to the IP address of a DMP that you will manage centrally.

**Step 2** At the DMPDM login prompt, enter the username and the password that you configured for the DMP.

**Step 3** Click **DMP Management** in the Administration area, and then enter the required values.



**a.** Enter in the DMM Appliance IP Address field the full and correct IP address of your DMM appliance.

**b.** Enter in the DMM Server Timeout (in seconds) field the maximum number of seconds that your DMP should wait for a response from your DMM appliance.

**Step 4**    Click **Apply** to confirm your entries.

**Step 5**    Click **Save and Restart DMP** in the Administration area, and then click to confirm.



**Step 6**    Stop. You have completed this procedure.

**Related Topics**

# Use a System Task to Normalize DMP Passwords

*Do the management passwords on any of your DMPs differ from your norm for DMPs? Or do any DMP passwords include forbidden characters?*

If so, you must edit these values to normalize them and remove any forbidden characters. Centralized management of DMPs is possible in DMM only when your DMPs all use one identical username (**admin**) and one identical password.

✎

**Note**    **Special characters, including exclamation points (!), question marks (?), ampersands (&), at signs (@), and asterisks (*) are forbidden in DMP passwords.** (CSCsq41233; CSCsw47873; CSCub67295)

**Before You Begin**

- Log in to DMM.

**Procedure**

**Step 1**     Click **Network and Endpoints**.



**Step 2**     Choose **Digital Media Players > Advanced Tasks > System Tasks**. Then, click **Add New Application**.
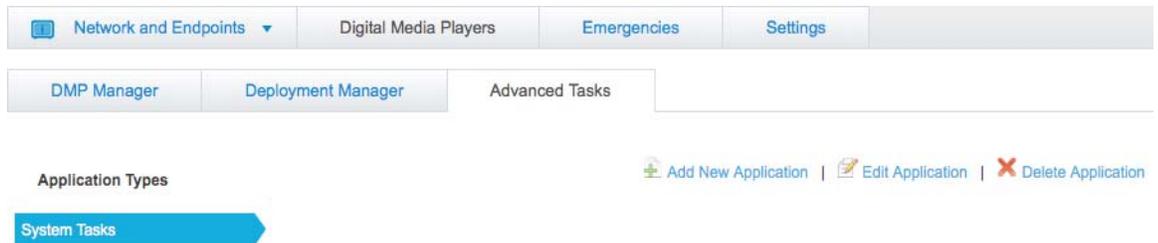


The Create New System Task form opens.



**Step 3**     Enter a name and description for your new task.

**Step 4**     Choose **Set** from the Request Type list.

**Step 5**     Enter this command string in the Request text box.

`init.WEB_password=` `new_password` `&mib.save=1&mng.reboot=1`

**Step 6**     Click **Submit** to save the task and make it available to use.

**Step 7**     Send the password-changing instruction simultaneously to multiple DMPs in your network.

   **a.**   Choose **Schedules > Play Now**.

   **b.**   Choose a group from the DMP Groups object selector.

   **c.**   Check the check box for each DMP where the DMP Web Account password should change.

    **d.** Choose from the Select an Event Type list the system task that you named in Step 2.

    **e.** Click **Submit**.

> **Note** After your targeted DMPs restart, you must update DMM user credential entries at Settings > Server Settings.

**Step 8** Stop. You have completed this procedure.

**What to Do Next**

- **MANDATORY**—Establish Trust Between Digital Signs and your Centrally Managed DMPs, page 12-17

# Establish Trust Between Digital Signs and your Centrally Managed DMPs

You must tell *Cisco Digital Signs* what user credentials to use at 5-minute intervals when it polls your DMPs and at any other time when it sends commands, queries, schedules or assets to your DMPs. Also, you must tell your DMPs which one DMM appliance to trust with this authority.

✎
**Note**    **This procedure assumes that you manage your DMPs centrally.** Furthermore, it assumes that you use *Cisco Digital Signs* and not *Cisco StadiumVision* for this purpose.

**Before You Begin**

- Verify that your DMPs all use identical credentials.
- Log in to DMM.

**Procedure**

**Step 1**    Click **Network and Endpoints**.



**Step 2**    Choose **Settings > Server Settings**.
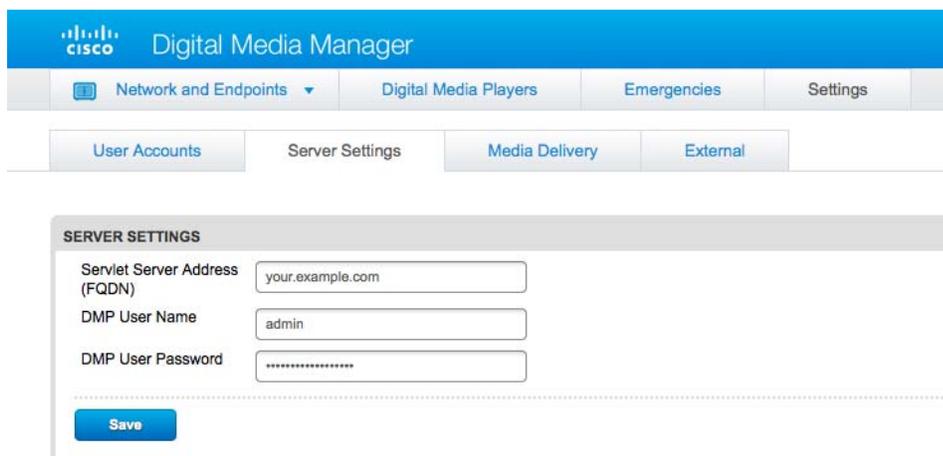
**Step 3**    Enter the required values.

- **Servlet Server Address**—If you have not already done so, enter the DNS-resolvable hostname and domain (together, these are the *FQDN*) for your DMM appliance, such as **dmm.example.com**.

  ✎

  **Note**    **YOUR ENTRY HERE MUST BE DNS-RESOLVABLE!** Otherwise your DMPs cannot load any media assets or other deployments from DMM. (**CSCtx15347**)

- **DMP User Name**—Enter **admin** or, when you have changed the DMP Web Account username from the default value, enter the new username that you assigned.

- **DMP User Password**—Enter the password that corresponds to the username.

**Step 4**    Click **Save**.

**Step 5**    Stop. You have completed this procedure.

⚠

**Caution**    **DMP credentials must match exactly in DMPDM and *Cisco Digital Signs*.** If you ever use a system task in *Cisco Digital Signs* to change DMP credentials, you must then return here and enter matching values. Otherwise, *Cisco Digital Signs* will use the wrong credentials when it tries to communicate with your DMPs. Then, after communication fails, it will consider your DMPs to be unreachable and unmanageable.

# Add or Edit Address Ranges for Non-Medianet Autoregistration

Even without access to Cisco Medianet technologies, you can autoregister all of the DMPs in any NMAP address range that you specify (**CSCtk02451**). Afterward, the registered DMPs support centralized management from DMM.

**Before You Begin**

- Log in to DMM.

**Procedure**

**Step 1**    Click **Network and Endpoints**.



**Step 2**    Choose **Digital Media Players > Advanced Tasks**.

**Step 3**    Click the **DMP Discovery** row in the Application Types list.

**Step 4**    Do one of the following.

- *Would you like to define an NMAP range?*    **When you will define a new range for autoregistration**

  **a.** Click **Add New Application**.

  **b.** The page is refreshed.

  **c.** Name and describe the deployable event that should use these settings.

- *Would you like to edit an NMAP range?*    **When you will edit a saved range for autoregistration**

  **a.** Click the Applications list row whose settings should be edited.

  **b.** Click **Edit Application**.

  **c.** The page is refreshed.

**Step 5**    Set the necessary values.

**Step 6**    Click **Submit** to save your work.

**OR**

Click **Cancel** to discard your work.

**Step 7**    Schedule a channel event to deliver or run this application.

**Step 8**    Stop. You have completed this procedure.

---

**Timesaver**    **Alternatively, you can use DMM-native (non-Medianet) autoregistration to populate a DMP group.**

1. Choose **Digital Media Players > DMP Manager.**
2. Click a DMP group to highlight it.
3. Choose **More Actions > Edit Group.**
4. Proceed as you would with any other non-Medianet autoregistration.

**Related Topics**

- Understand the Sequence of Operations for Non-Medianet Autoregistration, page 12-12

- Elements to Autoregister DMPs, page 12-23

- Elements to Configure Non-Medianet Autoregistration, page 12-25

# Delete Address Ranges for Non-Medianet Autoregistration

You can delete network range definitions you saved for DMP autoregistration events.

**Before You Begin**

- Log in to DMM.
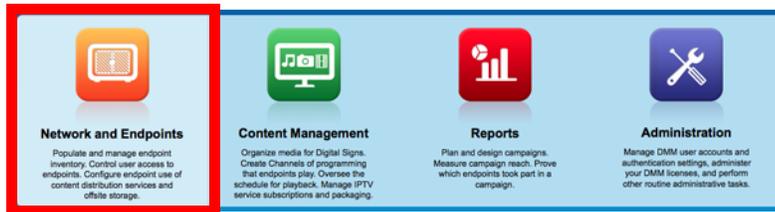
**Procedure**

**Step 1**    Click **Network and Endpoints**.



**Step 2**    Choose **Digital Media Players > Advanced Tasks**.

**Step 3**    Click the **DMP Discovery** row in the Application Types list.

**Step 4**    Click the Applications list row whose settings should be deleted.

**Step 5**    Click **Delete Application**.

**Step 6**    Click **Submit** to save your work.

**OR**

Click **Cancel** to discard your work.

**Step 7**    Schedule a calendar event to deliver or run this application.

**Step 8**    Stop. You have completed this procedure.

**Related Topics**

- [Elements to Configure Non-Medianet Autoregistration, page 12-25](#)

# Add or Edit One DMP Manually

**Before You Begin**

- Log in to DMM.

**Procedure**

**Step 1**    Click **Network and Endpoints**.
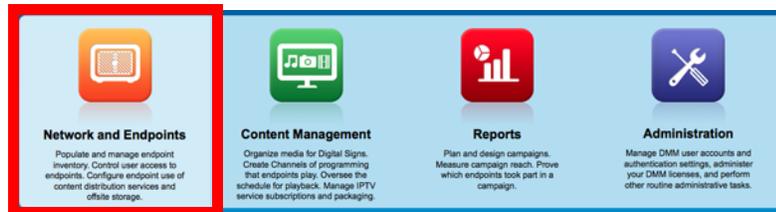


**Step 2**    Choose **Digital Media Players > DMP Manager**.

**Step 3**    *Do either of the following.*

- Click **Add DMP** above the DMP List table.

    **OR**

- Click the name of a DMP group to choose it in the object selector, and then click **Edit DMP** above the DMP List table.

🔎

**Tip**    **Is the Add DMP button missing from your DMP Manager page?** If so, something has blocked port 843 on your switch or router. Open port 843 and try again.

**Step 4**    Choose options and enter required values for the DMP.

After you register a DMP manually, its Description value in DMP Manager might be blank, even though your other DMPs show "registered" as their Description value. This happens only when you have not entered anything in the Description field. (**CSCtr51123**)

**Step 5**    Click **Submit** to save your work.

    **OR**

Click **Clear** to discard your work.

**Step 6**    (**Optional**) Add the DMP to a DMP group.

**Step 7**    Schedule a calendar event to deliver or run this application.

**Step 8**    Stop. You have completed this procedure.

**Related Topics**

- Elements to Add or Edit One DMP Manually, page 12-24
- Add or Edit Address Ranges for Non-Medianet Autoregistration, page 12-18

# Delete DMPs Manually from Your Device Inventory

**Before You Begin**

- Log in to DMM.

**Procedure**

**Step 1**    Click **Network and Endpoints**.



**Step 2**    Choose **Digital Media Players > DMP Manager**.

**Step 3**    *Do either of the following.*

- Browse the DMP Groups tree until you find the parent group whose member DMP should be deleted. Then, click the name of this DMP group.

    **OR**

- Choose an option from the Filter list to restrict which DMPs the DMP List table describes.

**Step 4**    Click to highlight the DMP to be deleted.

**Step 5**    Choose **More Actions > Delete from System**.

DMM shows a warning message and asks that you either confirm or cancel your request.

**Step 6**    Click **OK** to save your work.

    **OR**

Click **Cancel** to discard your work.

**Step 7**    Schedule a calendar event to deliver or run this application.

**Step 8**    Stop. You have completed this procedure.

**Related Topics**

- Elements to Delete One DMP Manually, page 12-24

# Reference

## Software UI and Field Reference Tables

### Elements to Autoregister DMPs

**Navigation Path**

*Either of these.*

- Network and Endpoints > Digital Media Players > DMP Manager > Create Group
- Network and Endpoints > Digital Media Players > DMP Manager > More Actions > Edit Group

*Table 12-1        Elements to Add and Edit DMP Groups*

| Element | Description |
|---|---|
| Name | A unique and human-readable name for the group. |
| Description | A brief description of the group and its purpose. |
| Add Range | IP address subnet ranges in which to find and autoregister DMPs.<br>• Add the IP address subnet range you have inserted in the Range (CIDR) field. |
| Delete a Range | Deletes the range that you highlighted. |
| Range (CIDR) | The field where you add/edit one IP address subnet range that should be automatically added to the group.<br>• Only CIDR format (IP address/netmask) is valid/acceptable. |
| Automatic Grouping Range | Shows a list of all the defined CIDR address ranges. Click a range to edit it. |

**Related Topics**

- Add or Edit Address Ranges for Non-Medianet Autoregistration, page 12-18
- Understand the Sequence of Operations for Non-Medianet Autoregistration, page 12-12

## Elements to Add or Edit One DMP Manually

**Navigation Path**

*Either of these.*

- Network and Endpoints > Digital Media Players > DMP Manager > Add DMP
- Network and Endpoints > Digital Media Players > DMP Manager > Edit DMP

**Tip**     **Is the Add DMP button missing from your DMP Manager page?** If so, something has blocked port 843 on your switch or router. Open port 843 and try again.

***Table 12-2     Elements to Add and Edit One DMP***

| Element | Description |
|---|---|
| Name | A unique and human-readable name for the DMP. Do not use any name that includes the '&' character. |
| IP Address | The public IP address that receives instructions and data from DMM. |
| MAC Address | The MAC address that the DMP NIC uses. |
| Description | **Note**     **After you register a DMP manually, its Description value in DMP Manager might be blank, even though your other DMPs show "registered" as their Description value.** This happens only when you have not entered anything in the Description field. (CSCtr51123)<br><br>Optional, brief description of the DMP, its deployment site, or other details that are relevant or meaningful to you. |
| WLAN | The WLAN address of a DMP 4400G.<br><br>**Note**     **We do not provide this value for other DMP models.** |
| Serial No. | The serial number of a DMP 4310G.<br><br>**Note**     **We do not provide this value for other DMP models.** |

## Elements to Delete One DMP Manually

**Navigation Path**

- Network and Endpoints > Digital Media Players > DMP Manager > Delete DMPs

***Table 12-3     Elements to Delete One DMP***

| Element | Description |
|---|---|
| Delete DMP | Deletes from your inventory database all records of the DMP that you highlighted. |

**Related Topics**

- Delete DMPs Manually from Your Device Inventory, page 12-22

## Elements to Configure Non-Medianet Autoregistration

**Navigation Path**

- Network and Endpoints > Digital Media Players > Advanced Tasks > DMP Discovery

*Table 12-4        Elements to Configure Autoregistration*

| Element | Description |
|---|---|
| Name | A unique and human-readable name for this autoregistration IP address range task. You must enter a name. The name is unique in the sense that you have not used it previously as the name for anything that can be scheduled. |
| Description | A brief description. The description is optional. |
| Discovery IP Range | The NMAP syntax to describe one or multiple ranges of IP addresses. |
| WLAN | The WLAN address of a DMP 4400G.<br>**Note**    **We do not provide this value for other DMP models.** |
| Serial No. | The serial number of a DMP 4310G.<br>**Note**    **We do not provide this value for other DMP models.** |

# Prevent DHCP Address Assignments to the Wrong VLAN

**Note** **You can run the following shell script** ("mandatory.cdp.sh") **on a Cisco Catalyst 3750 Series switch. This shell script can prevent a type of DHCP-VLAN misalignment problem that we describe under the "Medianet" heading in the "Restrictions" section on page 12-10.**

**Tip** **To learn about shell script execution on your switch, see the documentation for your switch on Cisco.com.**

\

```
##::cisco::eem::event_register_neighbor_discovery interface .* cdp update
#---------------------------------------------------------------
#
# February 2009, Cisco EEM team
#
# Copyright (c) 2009-2010 by Cisco Systems, Inc.
# All rights reserved.
#---------------------------------------------------------------
fetch IS_MASTER /oper/platform/stack/manager/all/role
if [[ $IS_MASTER -eq NO ]]; then
    return 0
fi

INTERFACE=$_nd_local_intf_name
fetch IS_ASP_ENABLED /config/interface{$INTERFACE}/macro/auto/processing/enabled
if [[ $IS_ASP_ENABLED -eq NO ]]; then
    return 0
fi

fetch IS_AUTH_ENABLED /config/interface{$INTERFACE}/macro/auto/processing/auth-enabled
if [[ $IS_AUTH_ENABLED -eq YES ]]; then
```

```
      fetch CDP_CHECK_ENABLED
/config/interface{$INTERFACE}/macro/auto/processing/cdp-fallback
      if [[ $CDP_CHECK_ENABLED -eq NO ]]; then
            return 0
      fi
fi

DETECTION_CDP="cdp"
ROUTER="CISCO_ROUTER_EVENT"
SWITCH="CISCO_SWITCH_EVENT"
LWAP="CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT"
AP="CISCO_WIRELESS_AP_EVENT"
PHONE="CISCO_PHONE_EVENT"
IPVSC="CISCO_IPVSC_EVENT"
LAST_RESORT="last-resort"
DMP="CISCO_DMP_EVENT"

fetch IS_CDP_DETECTION_ENABLED
/config/interface{$INTERFACE}/detection_method{$DETECTION_CDP}/macro_auto_detection_cntrl
if [[ $IS_CDP_DETECTION_ENABLED -eq NO ]]; then
      return 0
fi

fetch CURRENT_TRIGGER /config/interface{$INTERFACE}/macro/description
fetch CURRENT_AP125X /config/interface{$INTERFACE}/macro/device_descr

# Predefine the trigger in case no capabilities match
DEVICE_TYPE="Default device"
NEW_TRIGGER=CISCO_CDPDEVICE_EVENT
if [[ $_nd_cdp_capabilities_bit_4 -eq YES ]]; then
      DEVICE_TYPE="Host"
      NEW_TRIGGER=CISCO_HOST_EVENT
      if [[ $_nd_cdp_platform =~ ^(CIVS-IPC-2[45]|CIVS-IPC-4[35]) ]]; then
            DEVICE_TYPE="Camera"
            NEW_TRIGGER=CISCO_IPVSC_EVENT
            fetch IS_IPVSC_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$IPVSC}/macro_auto_device_cntrl
            if [[ $IS_IPVSC_DETECTION_ENABLED -eq NO ]]; then
                  return 0
            fi
      fi
      if [[ $_nd_cdp_platform =~ ^(CTS[13]000) ]]; then
            DEVICE_TYPE="CTS"
            NEW_TRIGGER=CISCO_CTS_EVENT
      fi
      if [[ $_nd_cdp_platform =~ "((Cisco DMP 4305G)|(Cisco DMP 4400G)|(Cisco DMP 4310G))"
]]; then
                  NEW_TRIGGER=CISCO_DMP_EVENT
                  DEVICE_TYPE="DMP"
                  fetch IS_DMP_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$DMP}/macro_auto_device_cntrl
                  if [[ $IS_DMP_DETECTION_ENABLED -eq NO ]]; then
                        return 0
                  fi
      fi
      if [[ $_nd_cdp_platform =~ "^((Cisco IP Phone)|(Cisco IP Confe))" ]]; then
            DEVICE_TYPE="Phone"
            NEW_TRIGGER=CISCO_PHONE_EVENT
            fetch IS_PHONE_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$PHONE}/macro_auto_device_cntrl
            if [[ $IS_PHONE_DETECTION_ENABLED -eq NO ]]; then
                  return 0
            fi
      fi
```

```
fi
if [[ $_nd_cdp_capabilities_bit_7 -eq YES ]]; then
    DEVICE_TYPE="Phone"
    NEW_TRIGGER=CISCO_PHONE_EVENT
    fetch IS_PHONE_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$PHONE}/macro_auto_device_cntrl
    if [[ $IS_PHONE_DETECTION_ENABLED -eq NO ]]; then
      return 0;
    fi
fi
if [[ $_nd_cdp_qos_tlv_bandwidth -eq "" ]]; then
    BANDWIDTH_LIMIT=0
else
    BANDWIDTH_LIMIT=$_nd_cdp_qos_tlv_bandwidth
fi
IS_AP125X=""
LIMIT=0

if [[ $_nd_cdp_platform =~ "^(cisco AIR-LAP)" ]]; then
    if [[ $_nd_cdp_platform =~ "^(cisco AIR-LAP125)" ]]; then
       IS_AP125X=AP125X
    else
       IS_AP125X=""
    fi
    DEVICE_TYPE="LightWeight Access Point"
    NEW_TRIGGER=CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
    LIMIT=$BANDWIDTH_LIMIT
    fetch IS_LWAP_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$LWAP}/macro_auto_device_cntrl
    if [[ $IS_LWAP_DETECTION_ENABLED -eq NO ]]; then
       return 0
    fi
fi
if [[ $_nd_cdp_platform =~ "^(cisco AIR-AP)" ]]; then
    if [[ $_nd_cdp_platform =~ "^(cisco AIR-AP125)" ]]; then
       IS_AP125X=AP125X
    else
       IS_AP125X=""
    fi
    DEVICE_TYPE="Autonomous Access Point"
    NEW_TRIGGER=CISCO_WIRELESS_AP_EVENT
    LIMIT=$BANDWIDTH_LIMIT
    fetch IS_AP_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$AP}/macro_auto_device_cntrl
    if [[ $IS_AP_DETECTION_ENABLED -eq NO ]]; then
       return 0
    fi
fi
if [[ $_nd_cdp_platform =~ "^(cisco AIR-SAP)" ]]; then
    DEVICE_TYPE="Autonomous Access Point"
    NEW_TRIGGER=CISCO_WIRELESS_AP_EVENT
    LIMIT=$BANDWIDTH_LIMIT
    fetch IS_AP_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$AP}/macro_auto_device_cntrl
    if [[ $IS_AP_DETECTION_ENABLED -eq NO ]]; then
       return 0
    fi
fi
if [[ $_nd_cdp_capabilities_bit_0 -eq YES ]]; then
    DEVICE_TYPE="Router"
    NEW_TRIGGER=CISCO_ROUTER_EVENT
    fetch IS_ROUTER_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$ROUTER}/macro_auto_device_cntrl
    if [[ $IS_ROUTER_DETECTION_ENABLED -eq NO ]]; then
```

```
            return 0
        fi
fi
if [[ $_nd_cdp_capabilities_bit_3 -eq YES ]]; then
       DEVICE_TYPE="Switch"
       NEW_TRIGGER=CISCO_SWITCH_EVENT
       fetch IS_SWITCH_DETECTION_ENABLED
/config/interface{$INTERFACE}/device_trigger{$SWITCH}/macro_auto_device_cntrl
       if [[ $IS_SWITCH_DETECTION_ENABLED -eq NO ]]; then
          return 0
       fi
fi
if [[ $DEVICE_TYPE =~ "^((Default device)|Host)$"  ]]; then
     NEW_TRIGGER=CISCO_LAST_RESORT_EVENT
     fetch IS_LASTRESORT_TRIGGER_ENABLED
/config/interface{$INTERFACE}/trigger_type{$LAST_RESORT}/macro_auto_trigger_cntrl
     if [[ $IS_LASTRESORT_TRIGGER_ENABLED -eq NO ]]; then
        return 0
     fi
fi

# With config persistency the macro applied interface commands
# are not removed on linkdown. But when interface comes up and a
# new device has been detected the config should change.
# Checks for current_trigger, new_trigger and triggers being null
# are required so that the new trigger event is generated
# and configs applied without having changing configs when
# multiple devices are connected to the same interface.
# Configs for only the first device that is detected will be applied.

fetch SW_POE /oper/interface{$INTERFACE}/switch_poe_support
if [[ $NEW_TRIGGER -eq $CURRENT_TRIGGER ]]; then
   if [[ $SW_POE -eq YES ]];then
       if [[ $CURRENT_AP125X -eq $IS_AP125X ]]; then
          set_oper /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state NO
          return 0;
       else
          set_oper /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state YES
       fi
   else
       set_oper /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state NO
       return 0;
   fi
fi

DEF_TRIGGER=CISCO_CUSTOM_EVENT

# trigger $DEF_TRIGGER TRIGGER=$DEF_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
AUTH_ENABLED=$IS_AUTH_ENABLED

# Apply the new trigger as there is none already applied on interface


if [[ $CURRENT_TRIGGER -eq "" ]]; then
    set_oper /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state NO
    fetch ACCESS_VLAN /config/trigger{$NEW_TRIGGER}/vlan_access
    fetch VOICE_VLAN /config/trigger{$NEW_TRIGGER}/vlan_voice
    fetch NATIVE_VLAN /config/trigger{$NEW_TRIGGER}/vlan_native
    if [[ $NEW_TRIGGER -eq CISCO_WIRELESS_AP_EVENT ]]; then
       trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
LIMIT=$LIMIT SW_POE=$SW_POE AP125X=$IS_AP125X NATIVE_VLAN=$NATIVE_VLAN
       send log facility AUTOSMARTPORT severity 5 mnemonics INSERT Device $DEVICE_TYPE
detected on interface $INTERFACE, executed $NEW_TRIGGER
       return 0;
```

```
     fi
     if [[ $NEW_TRIGGER -eq CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT ]]; then
          trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
LIMIT=$LIMIT SW_POE=$SW_POE AP125X=$IS_AP125X ACCESS_VLAN=$ACCESS_VLAN
     else
          trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
AUTH_ENABLED=$IS_AUTH_ENABLED LIMIT=$LIMIT ACCESS_VLAN=$ACCESS_VLAN VOICE_VLAN=$VOICE_VLAN
NATIVE_VLAN=$NATIVE_VLAN
     fi
     send log facility AUTOSMARTPORT severity 5 mnemonics INSERT Device $DEVICE_TYPE
detected on interface $INTERFACE, executed $NEW_TRIGGER
     trigger $DEF_TRIGGER TRIGGER=$DEF_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
AUTH_ENABLED=$IS_AUTH_ENABLED
     return 0;
fi

# Check the reset pending state and only then trigger the new event
# to apply new device configurations.

fetch IS_CFG_RESET_PENDING_STATE /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state
fetch IS_INT_MACRO_CFG_STICKY /config/interface{$INTERFACE}/auto/sticky
STICKY=$IS_INT_MACRO_CFG_STICKY

if [[ $IS_CFG_RESET_PENDING_STATE -eq YES ]]; then
     set_oper /oper/interface{$INTERFACE}/macro_cfg_reset_pending_state NO
     fetch ACCESS_VLAN /config/trigger{$NEW_TRIGGER}/vlan_access
     fetch VOICE_VLAN /config/trigger{$NEW_TRIGGER}/vlan_voice
     fetch NATIVE_VLAN /config/trigger{$NEW_TRIGGER}/vlan_native
     trigger $CURRENT_TRIGGER TRIGGER=$CURRENT_TRIGGER INTERFACE=$INTERFACE LINKUP=NO
AUTH_ENABLED=$IS_AUTH_ENABLED LIMIT=$LIMIT SW_POE=$SW_POE AP125X=$CURRENT_AP125X
STICKY=$STICKY
     send log facility AUTOSMARTPORT severity 5 mnemonics REMOVE Device on interface
$INTERFACE executed $CURRENT_TRIGGER to remove the configuration
     if [[ $NEW_TRIGGER -eq CISCO_WIRELESS_AP_EVENT ]]; then
        trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
LIMIT=$LIMIT SW_POE=$SW_POE AP125X=$IS_AP125X NATIVE_VLAN=$NATIVE_VLAN
        send log facility AUTOSMARTPORT severity 5 mnemonics INSERT Device $DEVICE_TYPE
detected on interface $INTERFACE, executed $NEW_TRIGGER
        return 0;
     fi
     if  [[ $NEW_TRIGGER -eq CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT ]]; then
          trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
LIMIT=$LIMIT SW_POE=$SW_POE AP125X=$IS_AP125X ACCESS_VLAN=$ACCESS_VLAN
     else
          trigger $NEW_TRIGGER TRIGGER=$NEW_TRIGGER INTERFACE=$INTERFACE LINKUP=YES
AUTH_ENABLED=$IS_AUTH_ENABLED ACCESS_VLAN=$ACCESS_VLAN VOICE_VLAN=$VOICE_VLAN
NATIVE_VLAN=$NATIVE_VLAN
     fi
     send log facility AUTOSMARTPORT severity 5 mnemonics INSERT Device $DEVICE_TYPE
detected on interface $INTERFACE, executed $NEW_TRIGGER
fi
```

# FAQs and Troubleshooting

## FAQs

**Q.**  **Why does DMM report that a DMP is down within 5 minutes of my registering the DMP successfully in DMM?**

**A.** Make sure that the "Servlet Server Address" value is correct in DMM. See the "Establish Trust Between Digital Signs and your Centrally Managed DMPs" section on page 12-17.

**Q.** Can I take advantage of DMM autoregistration without any Medianet-ready switch?

**A.** Yes. You can use the DMM-native autoregistration that we have always supported or you can configure your DHCP server to support option 125, and thereby advertise to your DMPs the IP address of their trusted DMM appliance.

**Q.** Can I use a Cisco switch or router as my DHCP server?

**A.** No. Cisco switches and routers do not support DHCP configurations that include option 125.

**Q.** Can a DMP that uses a static IP address autoregister itself to DMM?

**A.** It depends. Although a DMP with a static IP address does not communicate with any DHCP server—and, thus, is blind to information that it might otherwise receive via DHCP option 125—it should still be possible to use DMM native-autoregistration, as described elsewhere in this chapter.

**Q.** Can I obtain the serial number of a DMP?

**A.** Yes, you can—*but only for a* **DMP 4310G** *whose installed firmware version is at least* **5.2.3**. There are two methods.

- **Use DMM**

  1. Define an advanced task in DMM.
  2. Choose **Get** as its request type.
  3. Enter exactly this request string.

     `init.serial`

  4. Name and save your advanced task.
  5. Send your advanced task to one or more DMP 4310G endpoints.

- **Use HTTP**

  Follow exactly this syntax.

  `https://admin:` password `@` DMP_IP_address `:7777/get_param?p=init.serial`