CHAPTER 4

# Managing Auto Smartports in LMS

This chapter tells you how to configure, apply and manage Auto Smartports macros on the ASP-capable devices using LMS.

This section contains:

# What are Auto Smartports?

Macros contain multiple interface-level switch commands. You can reduce switch configuration errors and the administrative time required for performing repetitive tasks like configuring multiple interfaces with the same configuration.

Auto Smartports macros dynamically configure switch ports based on the device type detected on the port. When the switch detects a new device on a port it applies the appropriate Auto Smartports macro to the port.

For example, when you connect a Cisco IP phone to a port, Auto Smartports automatically applies the IP phone macro to the port. The IP phone macro ensures quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper handling of delay-sensitive voice traffic.

Auto Smartports uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device invokes a CDP event trigger: Cisco IP phone, Cisco wireless access point, Cisco switch, or Cisco router. Other event triggers use MAC authentication bypass (MAB) and 802.1x authentication messages.

The Auto Smartports macros embedded in the switch software are groups of CLI commands. For example, the CISCO_PHONE event detected on a port triggers the switch to apply the commands in the CISCO_PHONE_AUTO_SMARTPORT macro.

Table 4-3 explains the mapping between the System-defined events and the System-defined macros.

Device Profiling or Classifier is a new feature in LMS that provides an easy way for users to create triggers and dynamically configure the switch ports based on the device classification. You can create a specific trigger for a specific type of device.

The Device Profiling feature provides more granularity in device classification. The Device Profiling module has a rule-based device classification engine that can process attributes from various protocols.

# Auto Smartports Supported Devices and Images

Table 4-1 and Table 4-2 lists the devices and images, that support Auto Smartports.

***Table 4-1 Supported Devices and Images for Auto Smartports***

| Device Type | Minimum Software |
|---|---|
| Cisco Catalyst 2960S and 2960 Series Switches | 12.2(52)SE |
| Cisco Catalyst 3750, 3750-E, 3750v2 | 12.2(52)SE |
| Cisco Catalyst 3750-X, 3750-G | 12.2(55)SE |
| Cisco Catalyst 3560, 3560v2, 3560-E | 12.2(52)SE |
| Cisco Catalyst 3560-X | 12.2(55)SE |
| Catalyst 2975 | 12.2(52)SE |
| Catalyst 2918 | 12.2(52)SE |

**Note** Minimum supported IOS version for Device Profiling is 15.0(1)SE.

*Table 4-2 Auto Smartports Supported Switch Modules of ISRs*

| Routers | Auto Smartports Supported Switch Module | Switch Image | Minimum IOS Software |
|---|---|---|---|
| 3900 Series ISRs | SM-D-ES3G-48-P | 12.2(55)EX | 15.1(4)M |
| | SM-D-ES3-48-P | 12.2(55)EX | |
| | SM-D-ES2-48 | 12.2(55)EX | |
| | SM-ES3G-24-P | 12.2(55)EX | |
| | SM-ES3-24-P | 12.2(55)EX | |
| | SM-ES2-24-P | 12.2(55)EX | |
| | SM-ES2-24 | 12.2(55)EX | |
| | SM-ES3G-16-P | 12.2(55)EX | |
| | SM-ES3-16-P | 12.2(55)EX | |
| | SM-ES2-16-P | 12.2(55)EX | |
| | NME-16ES-1G-P | 12.2(55)EZ | |
| 2900 Series ISRs | SM-ES3G-24-P | 12.2(55)EX | 15.1(4)M |
| | SM-ES3-24-P | 12.2(55)EX | |
| | SM-ES2-24-P | 12.2(55)EX | |
| | SM-ES2-24 | 12.2(55)EX | |
| | SM-ES3G-16-P | 12.2(55)EX | |
| | SM-ES3-16-P | 12.2(55)EX | |
| | SM-ES2-16-P | 12.2(55)EX | |
| | NME-16ES-1G-P | 12.2(55)EZ | |
| 3800 Series ISRs | NME-16ES-1G-P | 12.2(55)EZ | 15.1(4)M |
| | NME-X-23ES-1G | 12.2(55)SEC | |
| | NME-X-23ES-1G-P | 12.2(55)EZ | |
| | NME-XD-24ES-1S-P | 12.2(55)EZ | |
| | NME-XD-48ES-2S-P | 12.2(55)EZ | |
| 2800 Series ISRs | NME-16ES-1G-P | 12.2(55)EZ | 15.1(4)M |
| | NME-X-23ES-1G | 12.2(55)SEC | |
| | NME-X-23ES-1G-P | 12.2(55)EZ | |

# Getting Started with Auto Smartports

The Getting Started Assistant guides you on provisioning Auto Smartports for Day 1 operations. For advanced configurations you can choose the corresponding link in the Auto Smartports TOC.

**Note** You need Adobe flash player 9 or later to display the readiness assessment pie chart. You can install the flash player from LMS. Reload the page after installing the flash player.

The Getting Started workflow for Auto Smartports is:

1. Assessing Auto Smartports Readiness of Your Network
2. Configuring Auto Smartports Using LMS
3. Configuring ASP Interfaces

## Assessing Auto Smartports Readiness of Your Network

The Auto Smartports Readiness Assessment displays Auto Smartports (ASP) based device details after assessing the network. A pie chart appears with the following types of devices.

- ASP-enabled Devices
- ASP-capable Devices
- ASP-software-incapable Devices
- ASP-hardware-incapable Devices

Click on any of the pie chart slices to view the details of the devices.

### ASP-enabled Devices

Click the ASP-enabled devices slice of the pie chart. The details of the corresponding devices in a table. Auto Smartport feature is enabled in these devices.

Click **Filter** to filter the listed devices based on device name, IP address, device type, and version of the running image.

### ASP-capable Devices

Click the ASP-capable devices slice of the pie chart. The details of the corresponding devices in a table. These devices have Auto Smartport capable IOS images, but Auto Smartport is not yet configured on these devices. Click **Filter** to filter the listed devices based on device name, IP address, device type, and version of the running image.

Select one or more devices and click **Enable ASP** to enable ASP on the selected devices. See, Configuring ASP Interfaces for more details.

## ASP-software-incapable Devices

Click the ASP-software-incapable devices slice of the pie chart. The details of the corresponding devices in a table. The IOS image in these devices does not support Auto Smartport. You can upgrade to the IOS image version that supports Auto Smartport. See Auto Smartports Supported Devices and Images for more information.

Click **Filter** to filter the listed devices based on device name, IP address, device type, version of the running image, and recommended image version. Select one or more device and click **Upgrade Software Image** to upgrade to the Auto Smartports-capable IOS image.

## ASP-hardware-incapable Devices

Click the ASP-hardware-incapable devices slice of the pie chart. The details of the corresponding devices in a table. These devices do not support Auto Smartports technology.

Click **Filter** to filter the listed devices based on device name, IP address, device type, and location.

You can get the latest ASP-supported hardware information from Cisco.com. See Auto Smartports Supported Devices and Images for more information. See Known List of Hardware-incapable Devices for more information.

# Managing Auto Smartports Templates

LMS provides Auto Smartports templates, which allow you to group multiple Auto Smartports events and their associated macros. You can also define user-defined templates.

You can select a template and deploy it on devices using **Work Center > Auto Smartports > Configure > Auto Smartports**. Using this workflow, you can auto configure the interface to which the Medianet endpoints are connected.

You can use ASP Management (**Work Centers > Auto Smartports > Configure > Manage Auto Smartports**) to edit the configuration for CDP-based events that are fetched from the device.

LMS supports two types of system-defined templates:

- Cisco Standard Events

  This template contains all the system-defined events and their associated system-defined macro with default VLANs. Table 4-3 shows the mapping between the system-defined events and the system-defined macros, and Table 4-4 lists the Auto Smartports system-defined macros.

- Cisco Medianet Template

  This template contains only ASP events that are mapped to their corresponding system-defined macros for DMP and IPVSC.

### Device Profiling or Device Classification

Device Profiling is a new feature in LMS that provides an easy way for users to create triggers and dynamically configure the switch ports based on the device classification. You can create a specific trigger for a specific type of device.

The Device Profiling feature provides more granularity in device classification. The Device Profiling module has a rule-based device classification engine that can process attributes like device platform and OUI type from various protocols like CDP and LLDP. Device Profiles are created based on these attributes and are available on the device by default.You can select specific Device Profiles, Device Types, or OUI/MAC addresses for applying ASP macros.

To manage ASP templates:

**Step 1** Select **Work Centers > Auto Smartports > Manage Templates**. The Manage Templates page appears with the list of ASP templates.

Click **Filter** to filter the listed templates based on the template name, description, or last modified date.

**Step 2** You can:

- Select a template and click **Edit** to edit the ASP template. The Edit Auto Smartports Template page appears. See Editing Auto Smartports Templates for more details.

  You cannot edit system-defined templates, however, you can select any, click **Edit** and save it with a new name.
- Click **New** to create a new ASP template. You can add Auto Smartports events and their associated macros to an ASP template. The Add Auto Smartports Template page appears. See Creating New ASP Templates for more details.
- Select one or more templates and click **Remove** to remove the ASP templates. You cannot delete system-defined ASP templates.
- Click **Reset** to reset to the default values.

This sections contains:

- Creating New ASP Templates
- Editing Auto Smartports Templates

# Creating New ASP Templates

You can add Auto Smartports events and their associated macros to an ASP template. For endpoints which do not support CDP, you can select MAC-based events. When an endpoint connects to a switch port, LMS identifies the corresponding event using either the MAC Address or the OUI that is tracked in the switch.

To create new ASP templates:

**Step 1** Select **Work Centers > Auto Smartports > Manage Templates**. The Manage Templates page appears with the list of ASP templates.

**Step 2** Click **New.** The Add page appears.

**Step 3** Enter the name and description of the template.

You must not use any of the following special characters for Template Name:

\, /, :, *, ‘, ?, < , >, |

You can enter alphanumeric and special characters for Template Description.

**Step 4** Click **Add** in the Auto Smartports Configuration Details table to add macros to the system-defined events.

**Step 5** Select one of the following methods to identify the endpoint types:

- Device Profiles
- Device Type
- OUI/MAC Address

**Step 6** Enter the following information:

| Fields | Description |
|---|---|
| **Device Profiles** | |
| Event Name | Specify the event trigger. The switch recognizes the trigger and applies the corresponding macro to the device.<br>You can enter a maximum of 200 characters, and use all special characters other than space. |
| Profiles | Select a specific device or a class of devices to which the macro should be applied.<br>Each trigger can have many devices, but each device can be associated to only one trigger.<br>Select one or more profiles from the drop-down list and click **Add** to add the profile to the Selected Profiles list. You can use the Ctrl key to select or unselect multiple profiles.<br>If the required profile name is not available in the list, you can enter the profile name in the text box and click **Add**. You can enter multiple profile names separated by commas.<br>You can enter a maximum of 200 characters, and use all special characters other than space. |

| Fields | Description |
|---|---|
| **Device Type** | |
| Event Type | You can select one of the following:<br>• System-defined<br>Select an event to trigger the macro associated with it on the ASP-capable switch. Table 4-3 shows the mapping between the system-defined events and system-defined macros in LMS.<br>• User-defined<br>Enter the following:<br>• Event Name<br>Specify the name of the event trigger. You can enter a maximum of 200 characters, and use all special characters other than space.<br>• Device Types<br>Specify a specific device or a class of devices to which the macro should be applied. You can use the following:<br>– access-point—Autonomous access point<br>– ip-camera—Cisco IP video surveillance camera<br>– lightweight-ap—Lightweight access point<br>– media-player—Digital media player<br>– phone—Cisco IP phone<br>– router—Cisco router<br>– switch—Cisco switch<br>For example, access-point, phone, 3750-switch |
| **OUI/MAC Address** | |
| Event Name | Specify the name of the event. You can enter a maximum of 200 characters, and use all special characters other than space. |
| MAC Address | Specify the MAC Address of the endpoint. You can enter one or more MAC addresses separated by commas. For example, 0123.4567.89ab, 0129.4568.99ab |
| OUIs | Specify the OUI of the endpoint. You can enter one or more OUIs separated by commas. For example, 00-1D-E5, 00-1E-BD<br>OUI is the first three bytes of the MAC address and identifies the manufacturer of the product. You can specify the OUI to allow devices that do not support neighbor discovery protocols like Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) to be recognized. |
| **Fields Common for all Options** | |
| Macro Type | Specifies the type of macro. It can be:<br>• System-defined Macro<br>• User-defined Macro<br>• Remote Macro |

| Fields | Description |
|---|---|
| Select Macro | This field appears when you select System-defined Macro.<br>Select a macro associated with the selected event from the list. Table 4-4 lists the ASP system-defined macros in LMS. |
| Access VLAN | Devices connected to the port will be placed into this VLAN.<br>The default data VLAN is VLAN 1. |
| Voice VLAN | Devices with voice traffic will be placed into this voice VLAN.<br>The default voice VLAN is VLAN 2. |
| Native VLAN | The VLAN ID used for untagged packets on the trunk interface.<br>The default Native VLAN is VLAN 1. |
| Select Configuration Macro from file | This field appears when you select User-defined Macro.<br>Click **Browse** to open a file browser, add a user-defined macro and associate it with the event. See, Sample User-defined Macro. |
| Configuration Macro | This field appears when you select User-defined Macro.<br>The contents of the macro will appear in the Configuration Macro text box. You can also paste the user-defined macro in the Configuration Macro text box. |
| Remote Macro Location | Enter the location of the remote macro, the syntax is <transfer protocol>://<IP address or hostname>/<filename>.<br>For example, tftp://<IP address or hostname>/macro.txt.<br>For more information, see Understanding the Remote Macro Feature |

**Step 7** You can:

- Click **Save** to save your changes and return to the New Auto Smartports Template page.
- Click **Save and Add Another** to save your changes and add more events and macros to the template.

**Step 8** Click **Save** to save your changes.

**Step 9** Click **Reset** to restore the default values.

## Editing Auto Smartports Templates

You can modify the existing ASP templates by modifying existing event-to-macro associations, adding new Auto Smartports event-to-macro associations, or removing unnecessary events. The template that you create will be saved as a user-defined ASP template.

You cannot edit system-defined templates, however, you can select any, click **Edit** and save it with a new name.

To edit Auto Smartports templates:

**Step 1** Select **Work Centers > Auto Smartports > Manage Templates**. The Manage Templates page appears with the list of ASP templates.

**Step 2** Click **Edit.** The Edit Auto Smartports Template page appears.

**Step 3** Modify the description of the template, if required. You can view details of:

- User who last modified the template
- Creation date
- Modification date

**Step 4** You can:

- Select an event and click **Edit** to edit the event and the associated macro.

  You cannot change the method to identify the endpoint types.
- Click **Add** to add more Auto Smartports events and macros. The Add Auto Smartports Template page appears. See Creating New ASP Templates for more details.
- Select a template and click **Remove** to remove the event and the associated macro.
- Click **Reset** to reset to the last saved values.
- Click **Filter** to filter the listed events based on the event, macro type, macro name, and the associated VLANs.

**Step 5** You can:

- Click **Save** to save your changes and edit the templates.
- Click **Save As** to save the template with a different name.

# Configuring Auto Smartports Using LMS

LMS provides you with Auto Smartports templates that contains events and associated macros to be deployed on the selected devices. You can select a template and customize it, if required.

To deploy Auto Smartports templates on ASP-capable and ASP-enabled devices, select **Work Centers > Auto Smartports> Configure > Auto Smartports**. You can view both categories of devices for Day 1 or Day N operations.

Device Profiling is a new feature introduced for ASP in LMS 4.1. For more details, see Device Profiling or Device Classification.

The workflow for deploying ASP templates on the ASP-capable and ASP-enabled devices is:

1. Select devices

   Select the devices on which you want to deploy ASP macros from the list of devices from the Select Device pane.

   Click **Filter** to filter the listed devices based on device name, IP address, ASP status, device type and version of the running image.

2. Configure Auto Smartports

   You can select templates from the list and deploy them on the selected devices. See Configuring Auto Smartports, for more details.

3. Schedule deployment

   You must schedule a job to deploy the ASP configurations to the ASP-enabled devices. See Scheduling Auto Smartports Configuration Jobs, for more details.

**Note** A port should not be a member of an EtherChannel when applying Auto Smartports macros, LMS automatically excludes all ether-channel ports in the ASP-capable switches and ASP-enabled devices.

# Configuring Auto Smartports

You can easily configure switches to automatically apply Auto Smartports macros using the Auto Smartports templates. The Auto Smartports templates contain groups of multiple Auto Smartports events and their associated macros, system-defined or user-defined. These macros will be deployed on all ports, when a device connects to the port.

You can deploy Auto Smartports templates on ASP-capable and ASP-enabled devices. You can view both categories of devices for Day 1 or Day N operations.

To deploy Auto Smartports templates on devices:

**Step 1** Select **Work Center > Auto Smartports > Configure > Auto Smartports**. The Configure Auto Smartports single-page wizard appears.

**Step 2** From the Select Devices pane, select the devices on which you want to deploy ASP templates from the list of ASP-capable and ASP-enabled devices.

**Step 3** Click **Next**. The Configure Auto Smartports page appears with a list of Auto Smartports templates.

By default, LMS provides two templates:

- Cisco Standard Events

  Contains all the seven system-defined events and the system-defined macros. Table 4-3 shows the mapping between the system-defined events and system-defined macros in LMS . Table 4-4 lists the Auto Smartports System-defined Macros in LMS .

- Cisco Medianet Template

  Contains all the system-defined events and the system-defined macros for the Medianet endpoints.

When you select a template, the list of events and the associated macros appears with the following details:

| Fields | Description |
|---|---|
| Event | Select an event to trigger the macro associated with it on the ASP-capable switch. Table 4-3 shows the mapping between the system-defined events and system-defined macros in LMS . |
| Macro Type | Specifies the type of macro. It can be:<br>• System-defined macro<br>• User-defined macro<br>• Remote macro |
| Select Macro | Select a macro associated with the selected event. Table 4-4 lists the ASP system-defined macros in LMS. You can view the commands of the macro in the text box. |
| Access VLAN | Devices connected to the port will be placed into this VLAN.<br>The default data VLAN is VLAN 1. |
| Voice VLAN | Devices with voice traffic will be placed into this voice VLAN.<br>The default voice VLAN is VLAN 2. |
| Native VLAN | The VLAN ID used for untagged packets on the trunk interface.<br>The default Native VLAN is VLAN 1. |

**Step 4** You can do one of the following:

- You can select an event and click **Edit** to edit the macro associated with it.

  You can map a user-defined macro, or add a remote macro. See Adding and Editing Macros Associated With Events, for more details.

- You can click **Add** to configure Device Profiling and add a new system-defined, user-defined macro, or a remote macro. The fields in the Add page are the same as the Create new template page. For more details, see Creating New ASP Templates.

  Device Profiling is a new feature introduced for ASP in LMS 4.1. For more details, see Device Profiling or Device Classification.

- You can select an event and click **Remove** to delete any macro associated with it.
- You can click **Reset** to restore the default values.
- You can click **Filter** to filter the listed events and macros based on event, macro type, macro name, and VLANs.

**Step 5** After you add or edit an Auto Smartports template, you can choose to:

- Click **Save as ASP Template** to save the changes and create a new template.
- Click **Save Template** to save the changes in the selected template.

**Step 6** Click **Next**. The Other Configuration pane appears.

You can enable CDP Fallback and enable Macro Sticky here. You can:

- Enable CDP Fallback—Select this check box to enable the ASP-enabled device to use Cisco Discovery Protocol (CDP) when 802.1x and the RADIUS server does not send an event trigger.

- Enable Macro Sticky—Select this check box to enable the ASP macros to remain active on the ASP-enabled device after a link-down event.

  Macro Sticky keeps down the number of syslog events. In most cases, the same device reconnects to the switch in the same port. In those cases where the device changes, a syslog will be generated, and the appropriate device configuration will be configured on the interface.

  When you disable the Macro Sticky option, a config change syslog is generated whenever there is a link flap. LMS will trigger a config fetch for every link up and link down event.

**Step 7** Click **Next**. The Schedule Deployment pane appears. See Scheduling Auto Smartports Configuration Jobs, for more details.

**Step 8** You can preview the commands that will be applied to the switch by selecting **Preview CLI** button, and click **Finish**. A new job is created.

---

Table 4-3 shows the mapping between the System-defined events and the System-defined macros.

*Table 4-3 System-defined events and the associated System-defined macros*

| System Defined Events | System Defined Macros |
|---|---|
| CISCO_PHONE_EVENT | CISCO_PHONE_AUTO_SMARTPORT |
| CISCO_ROUTER_EVENT | CISCO_ROUTER_AUTO_SMARTPORT |
| CISCO_SWITCH_EVENT | CISCO_SWITCH_AUTO_SMARTPORT |
| CISCO_AP_EVENT | CISCO_AP_AUTO_SMARTPORT |
| CISCO_DMP_EVENT | CISCO_DMP_AUTO_SMARTPORT |
| CISCO_LWAP_EVENT | CISCO_LWAP_AUTO_SMARTPORT |
| CISCO_IPVSC_EVENT | CISCO_IP_CAMERA_AUTO_SMARTPORT |

Table 4-4 lists the Auto Smartports System-defined Macros in LMS .

*Table 4-4 Auto Smartports System-Defined Macros in LMS*

| Macro Name | Description |
|---|---|
| CISCO_PHONE_AUTO_SMARTPORT | Use this macro to apply the IP phone macro for Cisco IP phones. It enables Quality of Service (QoS), port security, DHCP snooping, storm control and spanning-tree protection on the port. |
| CISCO_ROUTER_AUTO_SMARTPORT | Use this macro to apply the router macro for Cisco routers. It enables QoS, trunking, and spanning-tree protection on the port. |
| CISCO_SWITCH_AUTO_SMARTPORT | Use this macro to apply the switch macro for Cisco switches. It enables trunking on the port. |
| CISCO_AP_AUTO_SMARTPORT | Use this macro to apply the wireless access point (AP) macro for Cisco APs. It enables support for an autonomous wireless access point and QoS on the port. |
| CISCO_LWAP_AUTO_SMARTPORT | Use this macro to apply the light-weight wireless access point macro for Cisco light-weight wireless APs. It enables QoS, port security, DHCP snooping, storm control, and spanning-tree protection on the port. |

*Table 4-4 Auto Smartports System-Defined Macros in LMS*

| Macro Name | Description |
|---|---|
| CISCO_DMP_AUTO_SMARTPORT | Use this macro to apply the digital media player macro for Cisco digital media players. It enables QoS trust, port security, and spanning-tree protection. It configures the access VLAN for the interface and provides network protection from unknown unicast packets. |
| CISCO_IP_CAMERA_AUTO_SMARTPORT | Use this macro to apply the IP camera macro for Cisco video surveillance IP camera. It enables QoS trust and port security. |

## Adding and Editing Macros Associated With Events

LMS allows you to add or edit macros, system-defined, user-defined, or remote macro, associated to an event. To do this:

**Step 1** Select **Work Center > Auto Smartports > Configure > Auto Smartports**. The Configure Auto Smartports single-page wizard appears.

**Step 2** From the Select Devices pane, select the devices on which you want to deploy ASP templates, from the list of ASP-capable devices.

**Step 3** Click **Next**. The Configure Auto Smartports page appears

**Step 4** You can select an event and click:

- **Add** to add a macro and associate it with the event. The Add page appears for the selected event.
- **Edit** to edit the macro associated with it. The Edit page appears for the selected event.

**Step 5** For an event you can choose to add or edit a:

- System-defined Macro

  You can view the macro in the text box.

  Enter the Native, Access, or Voice VLAN, as applicable to the macro, into which the device is placed after authentication. The default data VLAN is VLAN 1 and the default voice VLAN is VLAN 2.

- User-defined Macro

  Click **Browse** to open a file browser, add a user-defined macro and associate it with the event. The contents of the macro will appear in the Configuration Macro text box. See, Sample User-defined Macro.

- Remote Macro

  Enter the location of the remote macro, the syntax is
  <transfer protocol>://<IP address or hostname>/<filename>.
  For example, tftp://<IP address or hostname>/macro.txt.
  For more information, see Understanding the Remote Macro Feature

**Step 6** After you update the template:

- For the Add page: Click **Save, Save and Add another** or **Cancel**.
- For the Edit page: Click **Save, Save and Edit next** or **Cancel**.

The details get updated in the Event and macro association table.

## Understanding the Remote Macro Feature

The remote macro feature enables you to store Auto Smartports macros in a central location. This allows you to maintain and update the Auto Smartports macro files so that multiple switches can use them. There are no specific file extension requirements for saved macro files.

## Sample User-defined Macro

```
Switch(config)# macro auto execute MP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
interface $INTERFACE
macro description $TRIGGER
switchport access vlan 1
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
exit
fi
}
```

# Scheduling Auto Smartports Configuration Jobs

Every configuration is deployed as a job. In many workflows the Schedule Deployment pane appears at the end. It displays details of the schedule and job options.

**Note** Auto Smartports in LMS uses NetConfig protocol order to communicate with the device. See Defining the NetConfig Protocol Order, for more information.

Table 4-5 describes the fields and options in the Schedule Deployment page.

***Table 4-5 Fields in the Schedule Deployment Page***

| Field | Description |
|---|---|
| Scheduler | Specifies when you want to run the job. Select one of the following:<br>• Immediate—Runs the job immediately.<br>• Once—Runs the job once at the specified date and time.<br>• Daily—Runs daily at the specified date and time.<br>• Weekly—Runs weekly at the specified days of the week and at the specified time.<br>• Monthly—Runs monthly at the specified day of the month and at the specified time. |
| Job Description | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters. |

*Table 4-5 Fields in the Schedule Deployment Page*

| Field | Description |
|---|---|
| E-mail | Enter e-mail addresses to which the job sends messages. You can enter multiple e-mail addresses separated by commas. |
| **Job Options** | |
| Fail on Mismatch of Config Versions | Select this check box to cause the job to be considered a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job. |
| Sync Archive before Job Execution | Select this check box to cause the job to archive running configuration before making configuration changes. |
| Copy Running Config to Startup | Select this check box to cause the job to write the running configuration to the startup configuration on each device after configuration changes are made successfully. |
| **Enable Job Password** | |
| Login Username | Enter the login username to access the device. This option is available to you if you have set the appropriate job password policy in **Admin > Network > Configuration Job Settings > Config Job Policies**.<br>This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module. |
| Login Password | Enter the login password to access the device. This option is available to you if you have set the appropriate job password policy in **Admin > Network > Configuration Job Settings > Config Job Policies**.<br>This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module. |

*Table 4-5 Fields in the Schedule Deployment Page*

| Field | Description |
|---|---|
| Enable Password | Enter the Enable password to access the device. This option is available to you if you have set the appropriate job password policy in **Admin > Network > Configuration Job Settings > Config Job Policies**.<br>This overrides the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module. |
| Failure Policy | Select one of these options to specify what the job should do if it fails to run on a device.<br>• Stop on failure—If the job fails to execute on a device, the job is stopped. The database is updated only for the devices on which the job was executed successfully.<br>• Ignore failure and continue—If the job fails on a device, the job skips the device and continues with the remaining devices.<br>The database is updated only for the devices on which the job was executed successfully.<br>• Rollback device and stop—Rolls back the changes on the failed device and stops the job.<br>• Rollback device and continue—Rolls back the changes on the failed device and continues the job.<br>• Rollback job on failure—Rolls back the changes on all devices and stops the job. |

- Click **Preview CLI** to see the CLI commands that will be applied to the ASP-enabled devices. You can select a device from the Preview CLI pop-up and see the CLI commands.

  You can modify an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.
- Click **Finish** after you review the CLI commands.

  A notification message appears along with the Job ID. The newly created job appears in the Auto Smartports Job Browser (**Work Center > Auto Smartports > Jobs**). See Managing Auto Smartports Jobs for more details.

# Defining the NetConfig Protocol Order

To define or modify the NetConfig protocol order:

**Step 1** Select **Admin > Collection Settings > Config > Config Transport Settings**. The Transport Settings page appears.

**Step 2** Select NetConfig from the Application drop-down list.

**Step 3** Select a protocol from the Available Protocols pane and click **Add**.

If you want to remove a protocol or change the protocol order, you must remove the protocol using the **Remove** button and add the protocol, again.

The list of protocols that you have selected appears in the Selected Protocol Order pane.

**Step 4** Click **Apply**.

A message appears, `New settings saved successfully`.

**Step 5** Click **OK**.

# Auto Smartports Readiness Assessment

The Auto Smartports Readiness Assessment (**Work Centers > Auto Smartports > Readiness Assessment**) displays Auto Smartports (ASP) based device details after assessing the network. A pie chart appears with the following types of devices.

- ASP-enabled Devices
- ASP-capable Devices
- ASP-software-incapable Devices
- ASP-hardware-incapable Devices

Click on any of the pie chart slices to view the details of the devices.

## ASP-enabled Devices

Click the ASP-enabled devices slice of the pie chart. The details of the corresponding devices in a table. Auto Smartport feature is enabled in these devices. If you configure the Auto Smartport macro on these devices then the macro will be applied to the ports to which devices will be connected.

You can select an ASP-enabled device click **Filter** to filter the listed devices based on device name, IP address, device type, and version of the running image.

## ASP-capable Devices

Click the ASP-capable devices slice of the pie chart. The details of the corresponding devices in a table. These devices are running with Auto Smartport capable IOS images, but Auto Smartport is not yet configured on these devices.

Click **Filter** to filter the listed devices based on device name, IP address, device type, and version of the running image.

Select one or more devices and click **Enable ASP** to enable ASP on the selected devices. See, Configuring ASP Interfaces for more details.

## ASP-software-incapable Devices

Click the ASP-software-incapable devices slice of the pie chart. The details of the corresponding devices in a table. The IOS image in these devices does not support Auto Smartport. You can upgrade to the IOS image version that supports Auto Smartport. See Auto Smartports Supported Devices and Images for more information.

Click **Filter** to filter the listed devices based on device name, IP address, device type, version of the running image, and recommended image version.

Select one or more device and click **Upgrade Software Image** to upgrade to the Auto Smartports-capable IOS image.

**Note** You can perform a software upgrade only if you have the privileges of a Network Operator, Network Administrator, or a Super Admin.

## ASP-hardware-incapable Devices

Click the ASP-hardware-incapable devices slice of the pie chart. The details of the corresponding devices in a table. These devices do not support Auto Smartports technology.

Click **Filter** to filter the listed devices based on device name, IP address, device type, and location.

You can get the latest ASP-supported hardware from Cisco.com. See Auto Smartports Supported Devices and Images for more information. See Known List of Hardware-incapable Devices for more information.

# Configuring ASP Interfaces

You can enable or disable ASP on selected interfaces of the selected devices.

When ASP is enabled, it is automatically applied to all ports unless explicitly disabled on a port. We recommend you to disable ASP on interfaces that you do not wish to have changed should a link down/up transition occur (for example, switch to switch trunk interfaces), or any interface for which the macro configuration for a specific port is not desired.

To configure ASP interfaces:

**Step 1** Select **Work Centers > Auto Smartports > Configure > Auto Smartports Interfaces**.

**Step 2** Select devices from the list of ASP-enabled devices.

Click **Filter** to filter the listed devices based on display name, IP address, and device type.

**Step 3** Select ports groups from the Port Group Selector.

**Step 4** Click **Next**. The Review Port Groups page appears with a list of selected devices and the ports associated with each device. Unselect the ports that you want to exclude from ASP configuration.

**Step 5** Click **Next**. The Configure Interface for Auto Smartports page appears.

**Step 6** Select the Enable or Disable radio button to enable or disable ASP on the selected interface.

**Step 7** Click **Next** to proceed to the Schedule Deployment page. See Scheduling Auto Smartports Configuration Jobs for more information.

# Managing Auto Smartports

You can edit or disable Auto Smartports configuration on ASP-enabled devices.

To manage ASP:

**Step 1** Select **Work Centers > Auto Smartports > Configure > Manage Auto Smartports**. The ASP-enabled devices appear.

Click **Filter** to filter the listed devices based on the device name, IP address, device type, and running image version.

**Step 2** Select devices to edit or disable Auto Smartports configuration.

**Step 3** You can either:

- Click **Edit ASP Configuration** to edit the ASP configurations of the selected ASP-enabled devices. The Edit Auto Smartports Configurations page appears.

  You can import macros and their associated events from a client, and export the same to a client.

  LMS uses the **`sh macro auto device`** command to display the macro details of the device, and uses telnet credentials to execute this command on the device. The macro details will appear only if the telnet credentials of the device is configured in DCR.
- Click **Disable ASP** to disable the ASP configurations from the selected ASP-enabled devices. The Schedule Deployment page appears.

# Viewing Auto Smartport Reports

Select **Work Centers > Auto Smartports > Reports**.

Or

Select **Reports > Fault and Event > Syslog > Auto Smartports**.

The Syslog Custom Report page appears. To generate this report:

**Step 1** Select the required devices using the Device Selector or Group Selector.

**Step 2** Enter the information required to generate the required report.

**Step 3** After you enter the required information, click **Finish**.

The columns in the Auto Smartports Syslog Report are:

| Column | Description |
|---|---|
| Device Name | Name of the Auto Smartports device. |
| Interface | Name or IP address of the interface in that device generating the Syslog message. |

| Column | Description |
|---|---|
| Timestamp | Time when the Syslog message was generated.<br>The format used by timestamp is:<br>*mmm dd yyyy hh:mm:ss*<br>where:<br>*mmm* represents month<br>*dd* represents date<br>*yyyy* represents year<br>*hh* represents hour<br>*mm* represents minute<br>*ss* represents second<br>Example:<br>`Nov 18 2010 12:24:36` |
| Facility | Facility is AUTOSMARTPORT. |
| Sub-Facility | Sub-Facility is the sub facility, if any, in the device that generated the Syslog message. In most cases, this is blank. An example of an entry in this field is CCM_CDR_INSERT-GENERIC-0-OutOfMemory. |
| Severity | The severity level for the messages. The following are the severity codes:<br>0—Emergencies<br>1—Alerts<br>2—Critical<br>3—Errors<br>4—Warnings<br>5—Notifications<br>6—Informational |
| Mnemonic | Code that uniquely identifies the error message. For example, UPLOAD, RELOAD,CONFIG. |
| Description | Description of the Syslog message. |

# Managing Auto Smartports Jobs

You can browse the Auto Smartports jobs that are deployed on the ASP-enabled devices. Using the Auto Smartports Job Browser you can manage Auto Smartports jobs; you can stop, or delete jobs using this job browser.

To invoke the Auto Smartports job browser:

Select **Work Center > Auto Smartports > Jobs**.

The Auto Smartports job browser appears with a detailed list of all scheduled Auto Smartports jobs. The browser has the following information:

| Column | Description |
|---|---|
| Job ID | Unique number assigned to job when it is created.<br>For periodic jobs such as Daily, and Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the job ID 1001.<br>Click on the hyperlink to view the Job details (see Viewing Job Details). |
| Status | Status of the job:<br>• Successful—When the job is successful.<br>• Failed—When the job has failed.<br>The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed.<br>• Stopped—When the job has been stopped.<br>• Running—When the job is in progress. |
| Description | Description of the job, entered at the time of job creation. |
| Owner | Username of the job creator. |
| Scheduled at | Date and time at which the job was scheduled. |
| Completed at | Date and time at which the job was completed. |
| Schedule Type | Type of job schedule—Immediate, Once, Daily, Weekly, Monthly.<br>For periodic jobs, the subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.<br>For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3. |

You can filter the jobs displayed in the Auto Smartports Job Browser using any of the following criteria and clicking **Filter**. When you click **Filter**, you can select any of the following criteria from the Filter by drop-down list, enter the details in the textbox, and click **Go**.

| Filter Criteria | Description |
|---|---|
| All | Select All to display all jobs in the job browser |
| Job ID | Select Job ID and enter the Job IDs that you want to display. For a non-periodic job, the specified Job ID appears in the browser. For periodic jobs, all the instances of the selected Job ID will also be displayed in the browser. |

| Filter Criteria | Description |
|---|---|
| Status | Select Status and then enter any one of these:<br>• Successful<br>• Failed<br>• Stopped<br>• Running<br>• Scheduled |
| Description | Select Description and enter the complete description. |
| Owner | Select Owner and enter the full name. |
| Scheduled at | Select Scheduled at and enter the date and time at which the job was scheduled. |
| Completed at | Select Completed at and enter the date and time at which the job was completed. |
| Schedule Type | Select the schedule type and enter any one of these:<br>• Immediate<br>• Once<br>• Daily<br>• Weekly<br>• Monthly |

You can click Refresh icon to refresh the Auto Smartports job browser, and Refresh Job icon to refresh the selected Auto Smartports job.

Records for all jobs need to be purged periodically. You can schedule a default purge job for this purpose (**Admin > Purge Settings > Config Job Purge Settings**).

You can perform the following operations using the Auto Smartports job browser. (See Table 4-6):

*Table 4-6 Operations Using the Auto Smartports Job Browser*

| Button | Description |
|---|---|
| Stop | Stops or cancels a running job.<br>You can stop or cancel a running job. You will be asked to confirm the cancellation of the job.<br>However, the job will be stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state.<br>If the job that you want to stop is a periodic job, you will also be asked whether you want to cancel all the instances of the job.<br>Click **OK** to cancel all instances.<br>If you click **Cancel**, only the selected instance of the job is cancelled. The next instance of the job will appear in the Job browser with the status `Scheduled`.<br>Unless you own the job, your login determines whether you can use this option. You cannot re-start the stopped job. |
| Delete | Deletes the selected job from the job browser. You can select more than one job to delete.<br>You will be asked to confirm the deletion. If the job that you have selected for deletion is a periodic job, this message appears:<br>`If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue?`<br>Click **OK** to confirm the deletion. The job, and its instances will be deleted.<br>You can delete a job that has been successful, failed, or stopped, but you cannot delete a running job.<br>Unless you own the job, your login determines whether you can use this option. You must stop a running job before you can delete it. |

You can click Refresh icon to refresh the Auto Smartports job browser, and Refresh Job icon to refresh the selected Auto Smartports job.

# Viewing Job Details

From the Job Browser dialog box, you can learn more about any job by viewing its details.

The Job Details appears below the list of Auto Smartports jobs. The details are grouped into three parts:

- Work Order
- Device Details
- Job Summary

| Page/Folder | Description |
|---|---|
| Work Order | Displays general information about the job:<br>• Job policies<br>• Job approval details (if you have enabled job approval)<br>• Device details<br>• Task<br>• CLI commands that will be executed on the selected devices as part of this job |
| Device Details | Contains detailed job results for each device in a table:<br>• Device—List of devices on which the job ran.<br>• Status—Status of job (success, failure, etc.)<br>• Message—A message about the status of a job.<br>– If the job failed on the device, the reason for failure is displayed.<br>– If the job was a success on that device, the message `Deploy Successful is` displayed.<br>You can filter the devices by selecting a status and clicking **Filter**.<br>This page displays the number of rows you have set for display in the Rows per Page field. You can increase the rows up to 500 in each page.<br>You can navigate among the pages of the report using the navigation icons at the right bottom of this table.<br>Click on a device to view the details such as protocol, status and reason when applicable, task used, and the CLI output for that device. These details appear in a pop-up window.<br>Double-click to display status folders that correspond to possible device status. |
| Job Summary | Click to display summary of completed job:<br>• Job Summary:<br>– Status<br>– Start Time<br>– End Time<br>• Job Messages:<br>– Pre-job Execution<br>– Post-job Execution<br>• Device Update:<br>– Successful<br>– Failed<br>– Not attempted<br>– Pending |