

Troubleshoot Smartports on your CBS250 or CBS350 Series Switch

Objective:

The objective of this document is to show how to identify, troubleshoot, and disable the Smartport feature if it is causing problems with your switch.

Applicable Devices | Software Version

- CBS250 Series | 3.1 [Download Latest](#)
- CBS350 Series | 3.1 [Download Latest](#)
- Sx550X Series | 3.1 [Download Latest](#)

Introduction

Did you know that your CBS250 or CBS350 switch includes a Smartport feature?

This Smartport feature applies a preconfigured setup to that switch port based on the type of device that is trying to connect. Auto Smartport lets the switch apply these configurations to interfaces automatically when it detects the device.

Smartports have preset configurations for the following:

- Printer
- Desktop
- Guest
- Server
- Host
- IP Camera
- IP Phone
- IP Phone + Desktop
- Switch
- Router
- Wireless Access Points

Smartports can be a huge time-saver for you, but there may be circumstances where you need to change settings. In some instances, it might be easier to just [disable the Smartport feature](#) and move on! Not sure? Check this article out for more details.

This article will answer these questions:

- [Do I have the Smartport feature enabled?](#)
- [What if I have the Smartport feature enabled, but it doesn't seem to be working?](#)

- [How do I disable the Smartport feature?](#)

First things first, let's figure out if you have the Smartport feature enabled.

Do I have the Smartport feature enabled?

The short answer, it depends!

If you have a 3.0.0.69 (or earlier) firmware version and you upgrade to the latest (March 2021 release) 3.1 version (or later when available), the default setting will remain with the Smartport feature enabled.

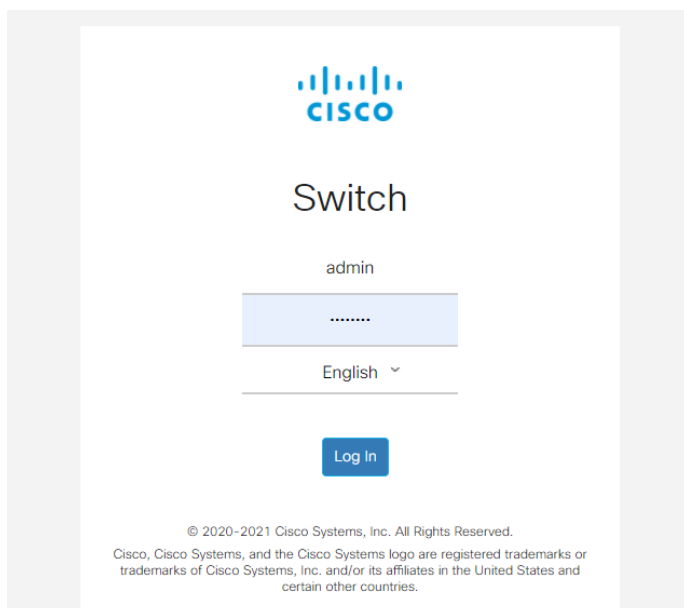
If you purchase a switch that has the 3.1 firmware version (or later), the firmware will have the Smartport feature **disabled** by default. This change was made because some customers didn't necessarily want to use the Smartport feature or it was causing an issue with connectivity and customers didn't realize it was enabled.

If you aren't sure if you have the feature enabled, you can check. Navigate to **Smartport > Properties**. At this location, you can view the Smartport settings or simply [disable the feature](#) if you choose.

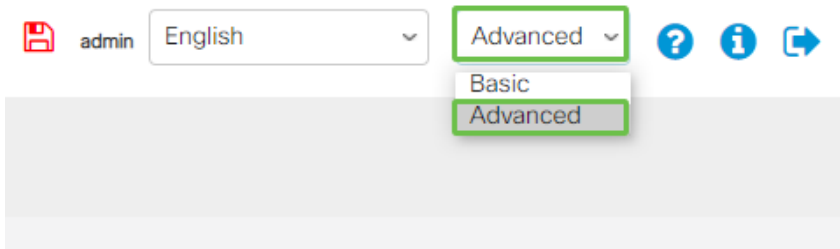
If you would like detailed steps for upgrading firmware, check out the article [Upgrade Firmware on a Switch](#).

What if I have the Smartport feature enabled, but it doesn't seem to be working?

To check these possible issues, log into the Web User Interface (UI) the Switch.



Once in the Web UI, change Display Mode from Basic to Advanced. This is located in the top-right corner of your screen.



Check the discovery protocol settings

The switch requires Cisco Discovery Protocol (CDP) and/or Layer Link Discovery Protocol (LLDP) to be enabled. These protocols share identification information between connecting devices or network equipment, which enables a device to advertise the type of device, operating system version, IP address, configuration, and capabilities to the switch. CDP is specific to Cisco and probably won't discover non-Cisco equipment. Both CDP and LLDP are enabled by default, so unless you manually changed it, you can move on to the [next section](#).

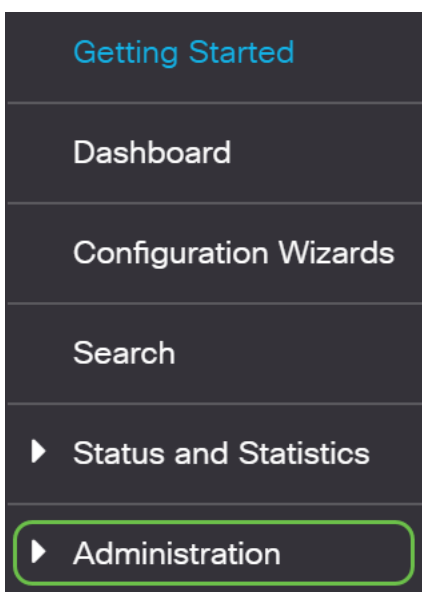
If you need to manually change CDP and LLDP back to enabled, you should restart your equipment to see if the Smartport feature is now working. You can check these under the **Administration** tab. If that fixes your issue, congratulations!

If a device is not clearly identified by either CDP or LLDP, you might want to disable the Smartport feature to clear away issues. Click to jump to the [disable Smartports](#) section of this article.

Check Port Configurations

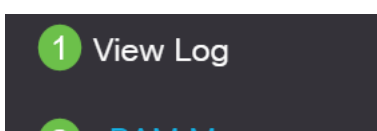
Step 1

Go to **Administration**.



Step 2

Scroll down and select **Logs > RAM Memory**.



Step 3

Check the device logs. Look for port locking placed to classic lock or any entries that did not result from a configuration that you set. Also, look for any entries that may place ports as *Disabled* or *Down*.

RAM Memory

Alert Icon Blinking: Enabled [Disable Alert Icon Blinking](#)

Pop-Up Syslog Notifications: Enabled [Disable Pop-Up Syslog Notifications](#)

Current Logging Threshold: Informational [Edit](#)

RAM Memory Log Table

[Clear Logs](#)

Log Index	Log Time	Severity
2147478549	2021-Feb-03 12:53:39	Informational
2147478550	2021-Feb-03 12:52:22	Informational
2147478551	2021-Feb-03 12:51:42	Informational
2147478552	2021-Feb-03 12:50:54	Informational
2147478553	2021-Feb-03 12:50:38	Informational
2147478554	2021-Feb-03 12:49:33	Informational
2147478555	2021-Feb-03 12:49:24	Informational
2147478556	2021-Feb-03 12:48:52	Informational
2147478557	2021-Feb-03 12:48:28	Informational
2147478558	2021-Feb-03 12:46:56	Informational
2147478559	2021-Feb-03 12:46:55	Informational
2147478560	2021-Feb-03 12:46:45	Informational
2147478561	2021-Feb-03 12:46:17	Informational
2147478562	2021-Feb-03 12:44:26	Informational
2147478563	2021-Feb-03 12:43:42	Informational
2147478564	2021-Feb-03 12:43:38	Informational
2147478565	2021-Feb-03 12:43:34	Informational

Step 4

Navigate to **Administration**.

- Getting Started
- Dashboard
- Configuration Wizards
- Search
- ▶ Status and Statistics
- ▶ Administration

Step 5

Scroll down and select **Discovery – CDP > CDP Neighbor Information**.

- 1 Discovery - CDP
- Properties
- Interface Settings

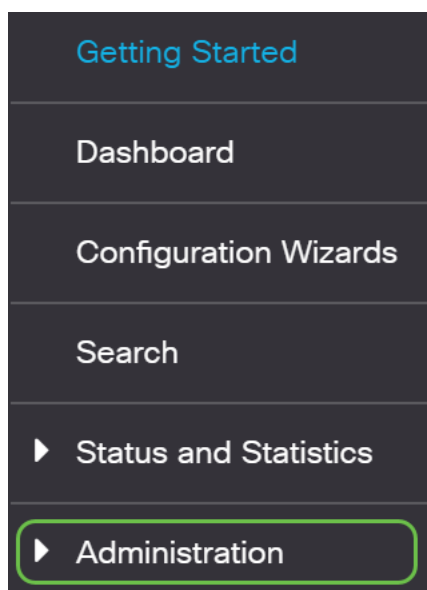
Step 6

Check devices that may or may not be Cisco devices connected to your switch. Verify they are the correct devices and that the IP addresses are correct.

Device ID	System Name	Local Interface	Advertisement Version	Time to Live (sec)	Capabilities	Platform	Neighbor Interface
SEP5006AB802AF1		GE1/5	2	151	Host, Phone, Two Port Rel...	Cisco IP Phone 8865	Port 1
SEP00C1B1E51F6E		GE1/7	2	176	Host, Phone, Two Port Rel...	Cisco IP Phone 7832	Port 1
10f9201286ce	switch1286ce	GE1/22	2	154	Router, Switch, IGMP	Cisco CBS250-8FP-E-2G...	gi7
3c57316dcd67	switch6dcd67	XG1/1	2	160	Router, Switch, IGMP	Cisco CBS250-48P-4G (...)	gi52
a0f8495c3941	SG350x-24	XG1/2	2	123	Router, Switch, IGMP	Cisco SG350X-24PD (PID...	te1/0/4

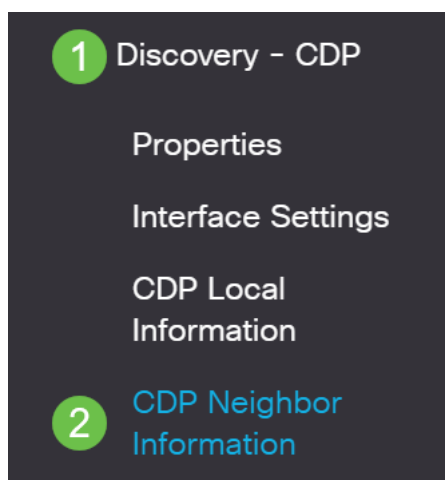
Step 7

Click **Administration**.



Step 8

Select **Discovery - CDP > CDP Neighbor Information**.



Step 9

Check any available CDP information. If you are still having connectivity issues, follow the steps in the next section to disable the Smartport feature.

CDP Neighbor Information

CDP Neighbor Information Table

Clear Table Details...

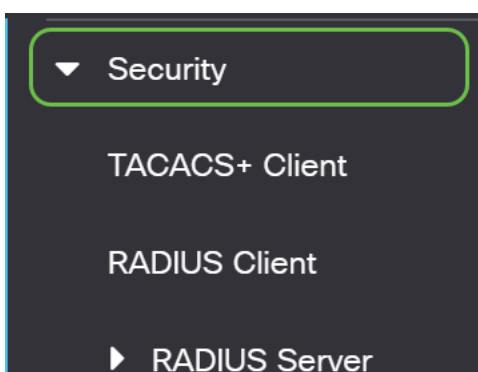
Filter: Local interface equals to GE1/5 Go Clear Filter

Device ID	System Name	Local Interface	Advertisement Version	Time to Live (sec)	Capabilities	Platform	Neighbor Interface
<input type="radio"/> SEP5006AB802AF1		GE1/5					Port 1
<input type="radio"/> SEP00C1B1E51F6E		GE1/7					Port 1
<input type="radio"/> 10f9201286ce	switch1286ce	GE1/22					gi7
<input type="radio"/> a0f8495c3941	SG350x-24	GE1/23					gi1/0/10
<input type="radio"/> 3c57316dcd67	switch6dcd67	GE1/24					gi48

Check Port Security

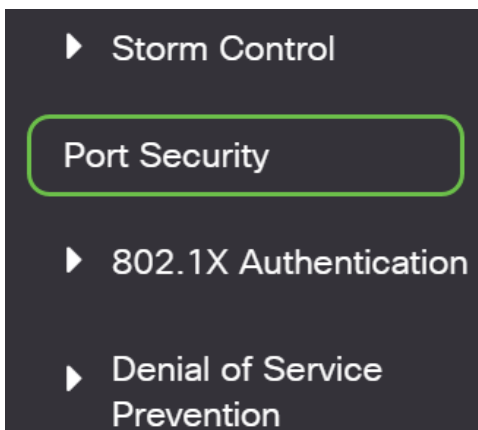
Step 1

Navigate to **Security**.



Step 2

Scroll down and select **Port Security**.



Step 3

On the *Port Security* page, check for any ports that are not on *Classic Lock*. Classic Lock is the default for each port. Any port that is not on classic lock, has a limit on the number of devices on that port, which can cause disconnections. If you did not configure this setting, you can follow the steps to disable Smartports to fix this issue.

Port Security

Port Security Table

Filter: Interface Type equals to Port of Unit 1

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Addresses Allowed	Action on Violation	Trap	Trap Frequency (sec)
<input type="radio"/>	1	GE1	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	2	GE2	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	3	GE3	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	4	GE4	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	5	GE5	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	6	GE6	Unlocked	Limited Dynamic Lock 10			Disabled
<input type="radio"/>	7	GE7	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	8	GE8	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	9	GE9	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	10	GE10	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	11	GE11	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	12	GE12	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	13	GE13	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	14	GE14	Unlocked	Limited Dynamic Lock 10			Disabled
<input type="radio"/>	15	GE15	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	16	GE16	Unlocked	Limited Dynamic Lock 10			Disabled
<input type="radio"/>	17	GE17	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	18	GE18	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	19	GE19	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	20	GE20	Unlocked	Classic Lock	1		Disabled

Step 4

Navigate back to *Port Security* and verify all ports are back to *Classic Lock* and verify connectivity with devices in your network.

If you experienced any disconnections or Internet problems, verify connectivity has returned. If this did not fix your port issues, you may want to disable the Smartport feature as detailed in the next section of this article.

Port Security Table

Filter: Interface Type equals to Port of Unit 1

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Addresses Allowed	Action on Violation	Trap	Trap Frequency (sec)
<input type="radio"/>	1	GE1	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	2	GE2	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	3	GE3	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	4	GE4	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	5	GE5	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	6	GE6	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	7	GE7	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	8	GE8	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	9	GE9	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	10	GE10	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	11	GE11	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	12	GE12	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	13	GE13	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	14	GE14	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	15	GE15	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	16	GE16	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	17	GE17	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	18	GE18	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	19	GE19	Unlocked	Classic Lock	1		Disabled
<input type="radio"/>	20	GE20	Unlocked	Classic Lock	1		Disabled

How do I disable the Smartport feature?

Step 1

Choose **Smartport > Properties**.

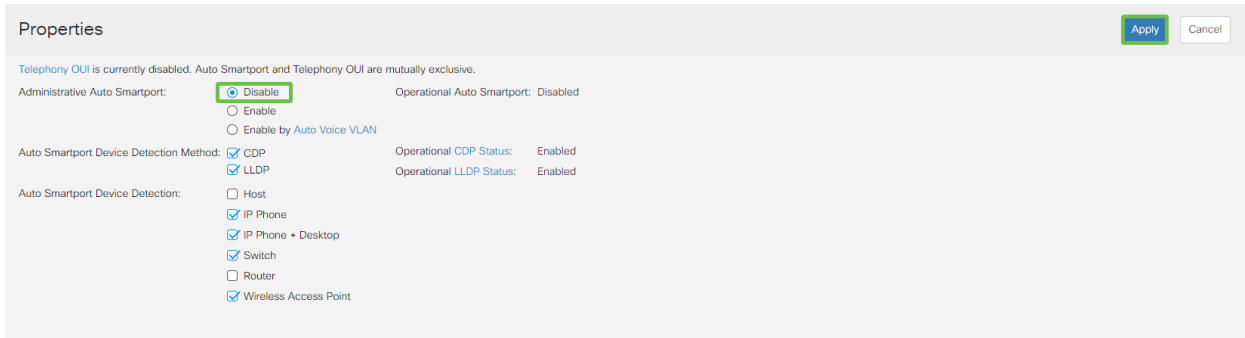
1 Smartport

2 Properties

Step 2

Select *Disable* next to *Administrative Auto Smartport*, to disable the Smartport globally on the switch. Click the **Apply** button.

This will disable the Smartport on all interfaces but will not affect manual VLAN configurations.



The screenshot shows the 'Properties' configuration page for a switch. At the top right, there are 'Apply' and 'Cancel' buttons. A blue note states: 'Telephony OUI is currently disabled. Auto Smartport and Telephony OUI are mutually exclusive.' The 'Administrative Auto Smartport' section has three radio buttons: 'Disable' (selected and highlighted with a green box), 'Enable', and 'Enable by Auto Voice VLAN'. The 'Operational Auto Smartport' status is 'Disabled'. The 'Auto Smartport Device Detection Method' section has two checked checkboxes: 'CDP' and 'LLDP'. The 'Operational CDP Status' and 'Operational LLDP Status' are both 'Enabled'. The 'Auto Smartport Device Detection' section has several checked checkboxes: 'IP Phone', 'IP Phone + Desktop', 'Switch', and 'Wireless Access Point'. The 'Host' and 'Router' options are unchecked.

Conclusion:

In this document, you learned how to troubleshoot and disable the Smartport feature when connectivity issues arise in your network.

Looking for more articles on your CBS250 or CBS350 switch? Check out any of the links below for more information!

[SNMP Settings](#) [SNMP Views](#) [SNMP Groups](#) [DHCP Image Upgrade](#) [Password Strength](#) [TCP and UDP Settings](#) [Port Security](#) [Time Settings](#) [Upgrade Firmware](#) [Smartport Best Practices](#) [Reset Switch](#) [Troubleshoot: No IP Address](#) [Troubleshoot Link Flapping](#) [Create VLANs](#)