

[www.640-553.com](http://www.640-553.com) CCNA Security

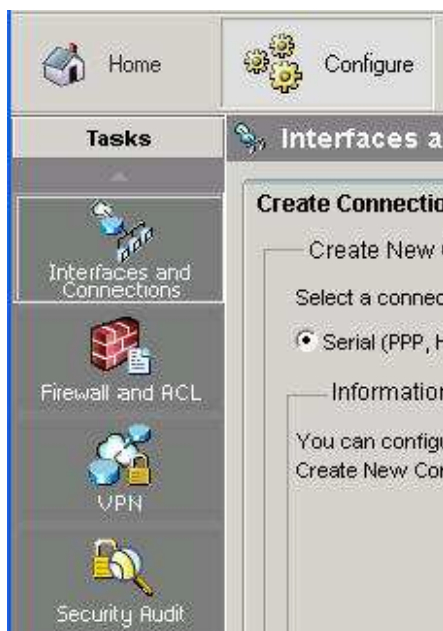
## Performing One-Step Lockdown With Security Device Manager

SDM is a Cisco GUI that can perform tasks from creating VPNs to carrying out a security audit on your router. In today's CCNA Security tutorial, we'll take a look at the process of performing a lockdown on a router.

I have no first-hand knowledge of this, but when a prison goes into lockdown, everyone and everything is locked up so there will be no trouble. When you perform a lockdown on a router, you'll enabling and disabling certain network services - so there will be no trouble!

Performing a lockdown does not guarantee the router is 100% safe, but it's going to be more secure than it was before. Later in this tutorial, we'll talk about how a lockdown can actually cause trouble - so do read this tutorial to learn how to use SDM for a lockdown, but do not rush to work tomorrow to run one!

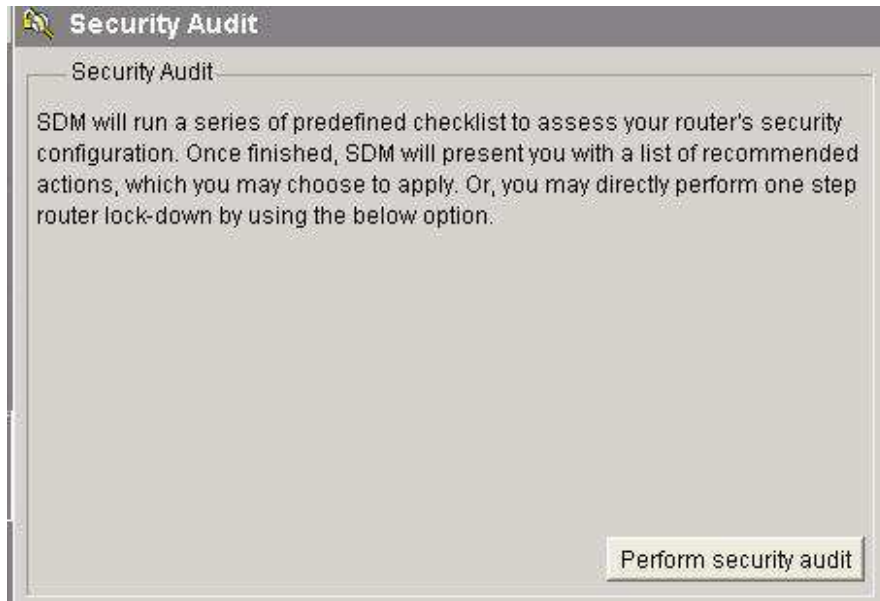
The first golden rule of SDM: If you need to carry out a task, always start by clicking the *Configure* button. After doing so, I'll click on *Security Audit*.



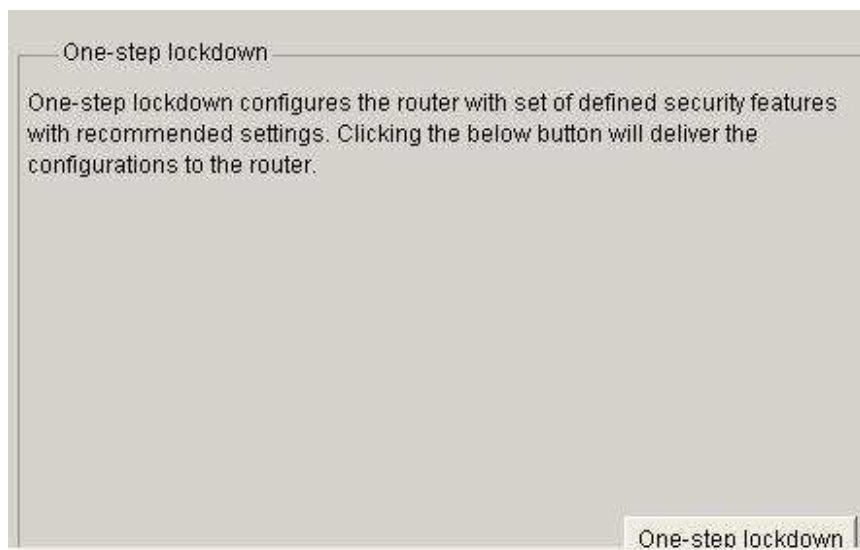
SDM does give excellent descriptions of the task you're about to carry out, and the Security Audit section is no exception. We'll be shown two options on the Security Audit screen, with the first being the Security Audit option itself.

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)



The option below that is to run a one-step lockdown.

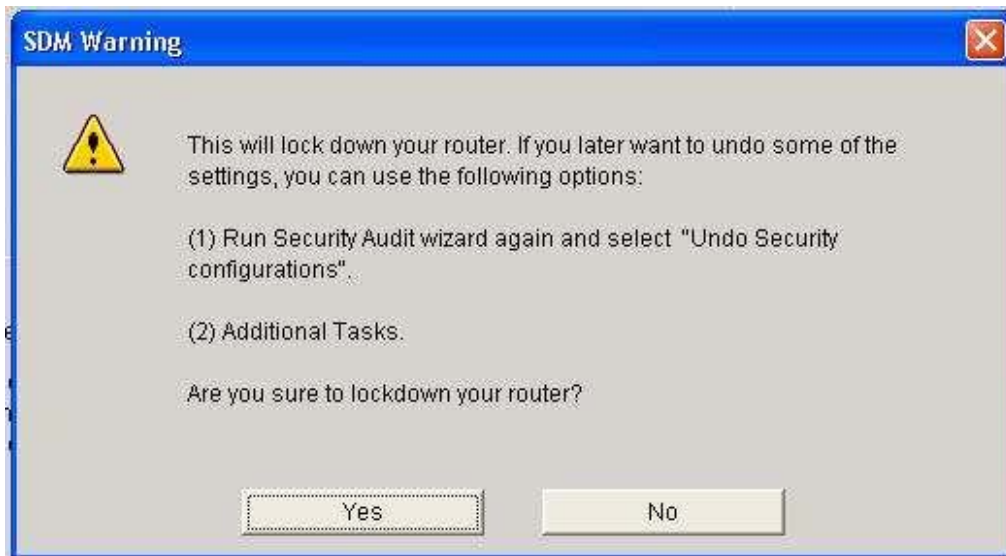


So our options at present are to run a *security audit*, after which we'll be given the opportunity to implement the audit's suggestions, and a *one-step lockdown*, which places our router in lockdown with no input or further permission needed from us.

I'll choose the one-step lockdown, and here's the next screen:

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)



As I always say, when a Cisco router or program asks you "Are you sure?", don't just click it - think about it!

And when you see a window like this that not only asks you if you're sure you want to perform this task, but also tells you how to roll the changes back if you don't like them, you better *really* consider what you're about to do!

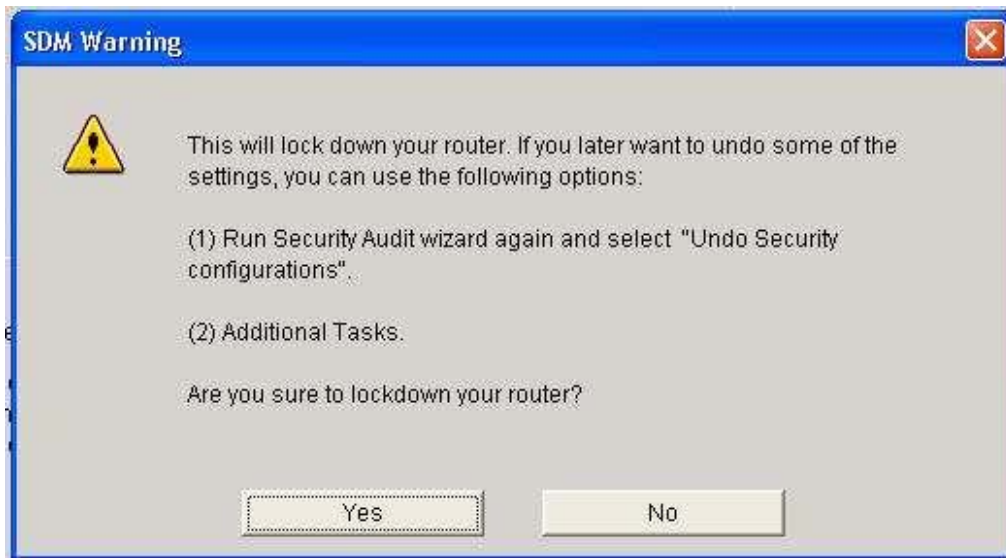
Having said that, we'll pick up the next part of this CCNA Security tutorial by saying "Yes" to the above question and then seeing what happens!

In the first part of this [CCNA Security Exam tutorial](#), we were in the process of using the Security Device Manager to put a router into lockdown - "one-step lockdown", that is!

Here's the last screen we saw in Part One:

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)

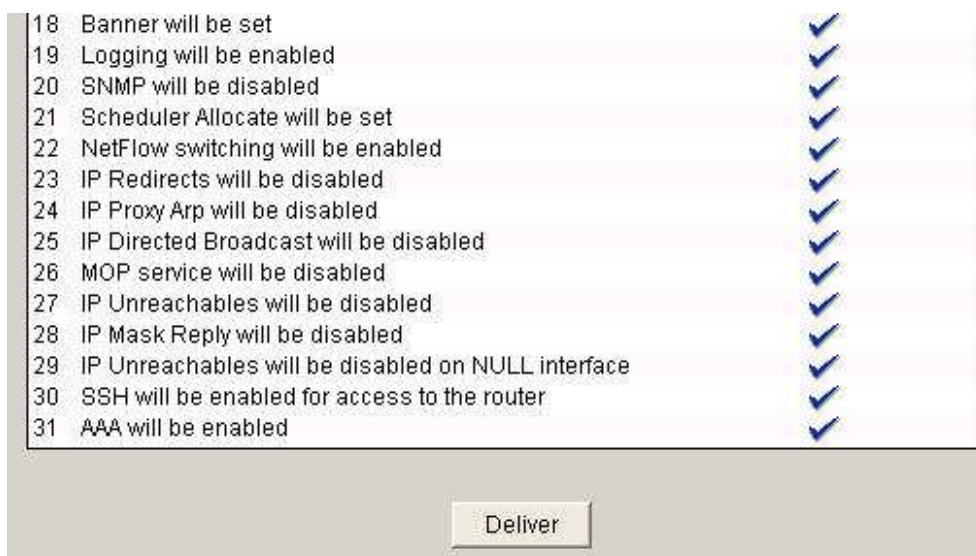
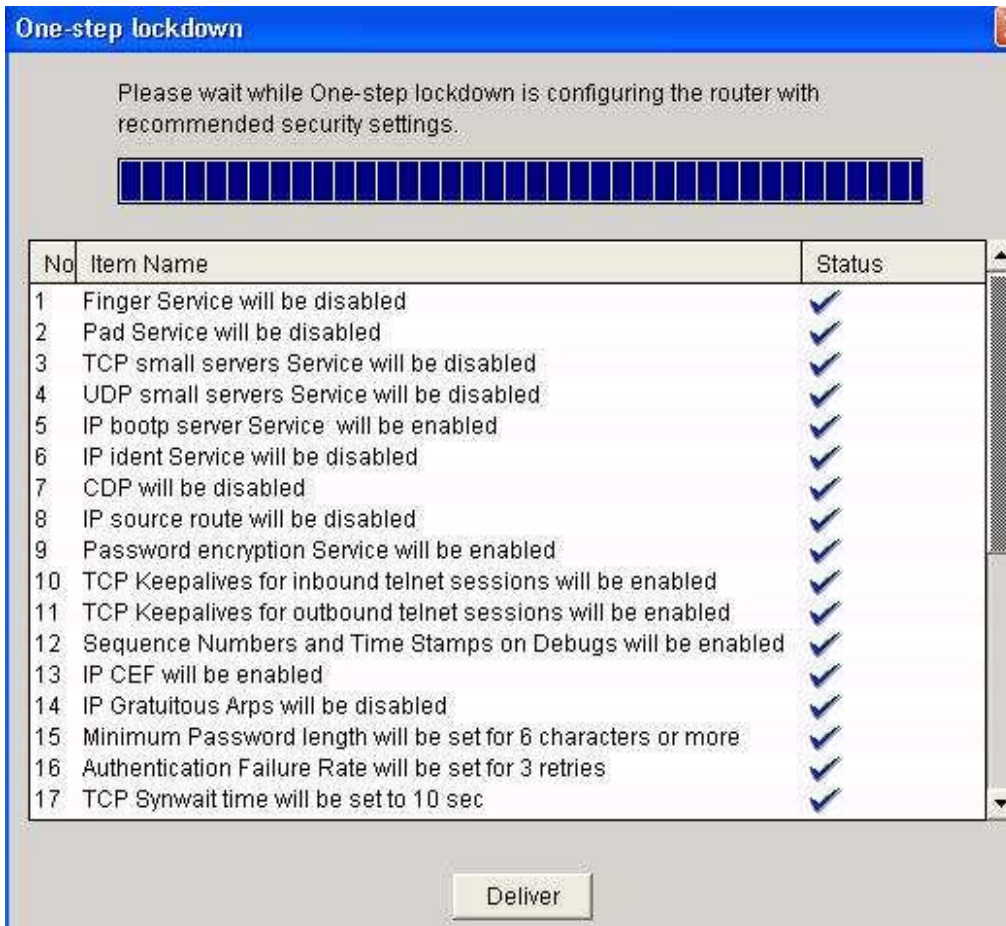


Note that if this lockdown doesn't give us the results we're looking for, we can run the Security Audit wizard and undo the configuration.

I clicked "Yes", and after a few seconds, we're presented with a list of 31 lockdown settings that will be enforced if we click *Deliver*. It's a good idea to be familiar with these settings for both the CCNA Security exam and real-world networks, so here are two screen shots showing all 31 settings.

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)



Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)

I have the *Preview Commands* option enabled in Preferences, the actual commands are shown in a separate window after clicking *Deliver*. We do need to click *Deliver* again to actually deliver the commands. I'll select *Save To File* and then *Deliver*.

The *Delivery Status* window shows that this lockdown takes 79 commands to enforce.



Clicking OK takes us back to the original *Security Audit / One-Step Lockdown* window. Let's take a look at that configuration file. Note the login banner SDM wrote.

Configuration commands for the router: 172.31.1.1

```
-----  
-----  
aaa authentication login local_authen local  
aaa authorization exec local_author local  
ip cef  
line vty 0 4  
  login authentication local_authen  
  authorization exec local_author  
  no privilege level  
  transport input ssh  
  exit  
line con 0  
  login authentication local_authen  
  exit
```

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)

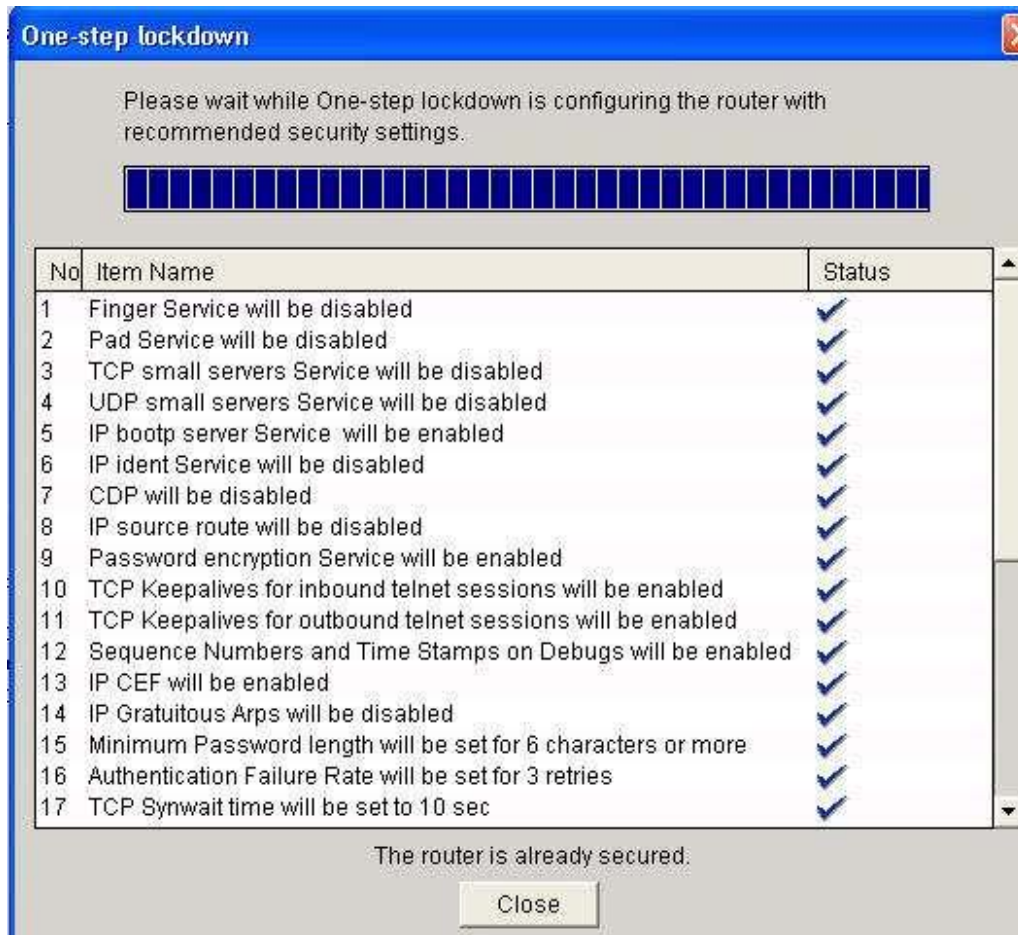
```
line aux 0
 login authentication local_authen
 exit
no service pad
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no ip bootp server
no ip source-route
service sequence-numbers
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
scheduler allocate 20000 1000
ip tcp synwait-time 10
no cdp run
security authentication failure rate 3 log
security passwords min-length 6
ip ssh time-out 60
ip ssh authentication-retries 2
banner login ~Authorized access only!
 Disconnect IMMEDIATELY if you are not an authorized
user!
~
logging console critical
logging trap debugging
logging buffered 51200 debugging
interface Loopback0
 no ip proxy-arp
 no ip redirects
 no ip unreachableables
 ip route-cache flow
 exit
interface Serial0/0/0
 no ip proxy-arp
 no ip redirects
 no ip unreachableables
 ip route-cache flow
 exit
interface Null0
 exit
default interface Null0
interface Null0
 no ip unreachableables
```

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)

```
exit
interface Serial0/1/1
  no ip proxy-arp
  no ip redirects
  no ip unreachable
  ip route-cache flow
  exit
interface FastEthernet0/1
  no ip proxy-arp
  no ip redirects
  no ip unreachable
  ip route-cache flow
  no mop enabled
  exit
interface Serial0/1/0
  no ip proxy-arp
  no ip redirects
  no ip unreachable
  ip route-cache flow
  exit
! IP address / user account command
interface FastEthernet0/0
  no ip proxy-arp
  no ip redirects
  no ip unreachable
  ip route-cache flow
  no mop enabled
  exit
```

If you run One-Step Lockdown after the router's already been locked down, you'll see a series of check marks next to each configured feature and a message at the bottom of the screen that the router is already in lockdown.



At this point, the router's been secured!

However, you may need to go back and change one or more of these settings for your particular network's needs. We'll take a look at how to change some or all of these lockdown settings in the next installment of this [CCNA Security Exam tutorial](#) series!

Source:

[www.thebryantadvantage.com/](http://www.thebryantadvantage.com/)