



**One-Step Lockdown with Cisco SDM**



## Router Hardening...Automagically

The process of turning off unnecessary services is called “hardening” a router to prevent attacks or exploits. The basic steps of router hardening are:

- 1) Administratively shut down any unused router interfaces
- 2) Disable any unused services.

Two methods of “automagically” hardening your router:

- 1) AutoSecure - The AutoSecure IOS feature is invoked by issuing the “auto secure” command from the CLI. This allows an administrator to lock down the device with a single CLI command.
- 2) Cisco SDM One-Step Lockdown - The Cisco SDM One-Step Lockdown method for securing a router uses a wizard in the Cisco SDM graphical interface.



## One-Step Router Lockdown

*Simplifies firewall and Cisco IOS Software configuration without requiring expertise about security or Cisco IOS Software.*

### One-step lockdown

One-step lockdown configures the router with set of defined security features with recommended settings. Clicking the below button will deliver the configurations to the router.

One-step lockdown



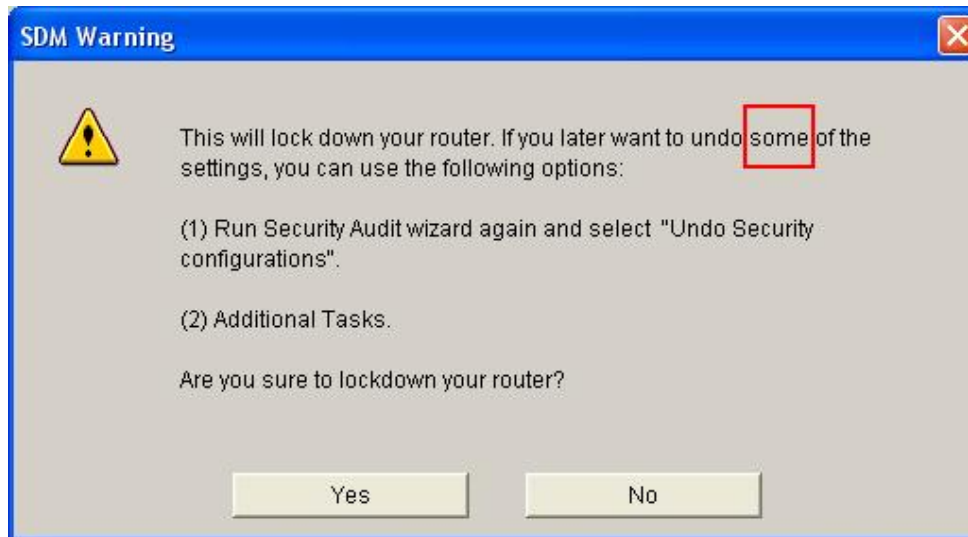
## One-Step Router Lockdown

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The title bar reads "Cisco Router and Security Device Manager (SDM): 10.1.1.1". The menu bar includes "File", "Edit", "View", "Tools", and "Help". The main toolbar contains icons for "Home", "Configure" (highlighted with a red box), "Monitor", "Refresh", "Save", "Search", and "Help". The Cisco logo is in the top right corner. On the left, a "Tasks" sidebar lists various configuration options, with "Security Audit" highlighted by a red box. The main content area is titled "Security Audit" and contains two sections: "Security Audit" and "One-step lockdown", both highlighted with red boxes. The "Security Audit" section includes a description of the audit process and a "Perform security audit" button. The "One-step lockdown" section includes a description of the lockdown process and a "One-step lockdown" button. A "Use Case Scenario" diagram is also visible on the right side of the interface. The status bar at the bottom shows "Security Audit" and the timestamp "20:42:33 UTC Mon Jan 04 2010".



## One-Step Router Lockdown

This is an all or nothing solution. If you choose to institute One-Step Lockdown, SDM will configure your router with a set of best-practice security commands. You can supposedly roll the changes back:



But this process is not quite as complete as Cisco would have you believe(Security Audit) nor easy(Additional Tasks).




## One-Step Router Lockdown

As you can see, there are a lot of configuration items that One-Step Lockdown will send to your router:

**One-step lockdown**

Please wait while One-step lockdown is configuring the router with recommended security settings.




No	Item Name	Status
16	Authentication Failure Rate will be set for 3 retries	✓
17	TCP Synwait time will be set to 10 sec	✓
18	Banner will be set	✓
19	Logging will be enabled	✓
20	SNMP will be disabled	✓
21	Scheduler Allocate will be set	✓
22	NetFlow switching will be enabled	✓
23	IP Redirects will be disabled	✓
24	IP Proxy Arp will be disabled	✓
25	IP Directed Broadcast will be disabled	✓
26	MOP service will be disabled	✓
27	IP Unreachables will be disabled	✓
28	IP Mask Reply will be disabled	✓
29	IP Unreachables will be disabled on NULL interface	✓
30	SSH will be enabled for access to the router	✓
31	AAA will be enabled	✓

Deliver

**Commands Delivery Status**

Command Delivery Status:

Preparing commands for delivery...  
Submitting 54 commands, please wait...



OK



## One-Step Router Lockdown

### A LOT of configuration:

```
r1#show archive config differences flash:archived_config-1 system:running-config
Contextual Config Diffs:
+no service pad
+service tcp-keepalives-in
+service tcp-keepalives-out
+service timestamps debug datetime msec localtime show-timezone
+service timestamps log datetime msec localtime show-timezone
+service password-encryption
+service sequence-numbers
+security authentication failure rate 3 log
+security passwords min-length 6
+logging buffered 51200
+logging console critical
+aaa new-model
+aaa authentication login local_authen local
+aaa authorization exec local_author local
+aaa session-id common
+no ip source-route
+no ip bootp server
+username packetlab privilege 15 password 7 12090414190E18082B29
<-- output truncated -->
```



## AutoSecure vs. One-Step Lockdown

One-Step Lockdown does not allow you to specify which portions of the router you want to lockdown, while AutoSecure gives you some control over this (management plane, forwarding plane, etc.)

One-Step Lockdown is exactly what it says it is: one step. There is no input/feedback provided like the AutoSecure Dialogue.

One-Step Lockdown requires Cisco SDM to implement. This entails configuring HTTP or HTTPS (preferred) access to the router.

You can “rollback” both AutoSecure and One-Step Lockdown by reverting to the startup configuration, provided you do not write the configuration after either is applied.

Rollback – short of reloading into startup/saved configuration – is easier with One-Step Lockdown, though not quite as complete as Cisco would have you believe.





## AutoSecure Features Not Implemented in Cisco SDM

The following AutoSecure features are not implemented in this version of Cisco SDM:

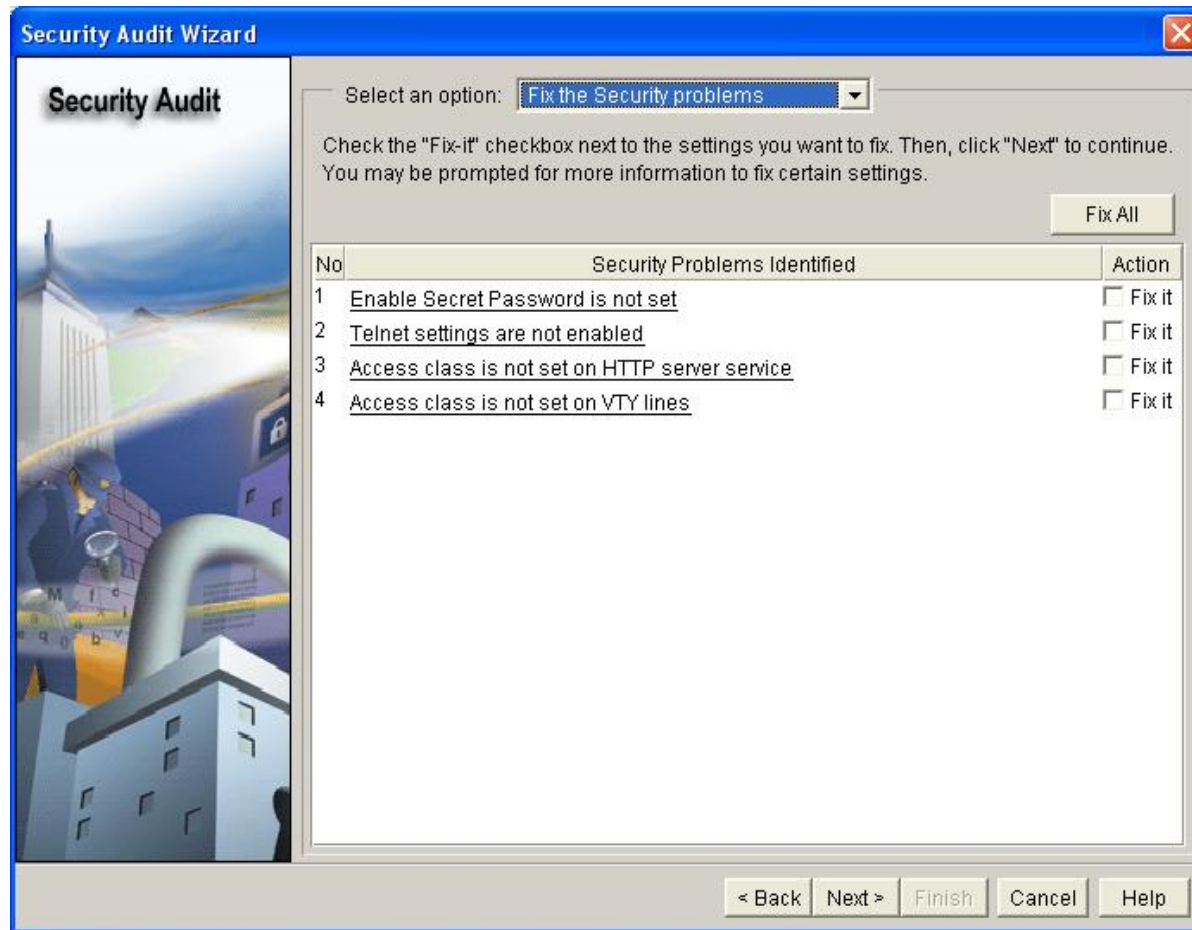
- Disabling NTP—Based on input, AutoSecure will disable the Network Time Protocol (NTP) if it is not necessary. Otherwise, NTP will be configured with MD5 authentication. Cisco SDM does not support disabling NTP.
- Configuring AAA—If the Authentication, Authorization, and Accounting (AAA) service is not configured, AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. Cisco SDM does not support AAA configuration. **<-Not true**
- Setting SPD Values—Cisco SDM does not set Selective Packet Discard (SPD) values.
- Enabling TCP Intercepts—Cisco SDM does not enable TCP intercepts.
- Configuring anti-spoofing ACLs on outside interfaces—AutoSecure creates three named access lists used to prevent anti-spoofing source addresses. Cisco SDM does not configure these ACLs.

**AutoSecure Features Implemented Differently in Cisco SDM:**

- Disable SNMP—Cisco SDM will disable SNMP, but unlike AutoSecure, it does not provide an option for configuring SNMP version 3.
- Enable SSH for Access to the Router—Cisco SDM will enable and configure SSH on crypto Cisco IOS images, but unlike AutoSecure, it will not enable Service Control Point (SCP) or disable other access and file transfer services, such as FTP.



## Security Audit – One-Step Lockdown





## Security Audit – AutoSecure(no-interact)

Security Audit Wizard

**Security Audit**

Select an option:

Check the "Fix-it" checkbox next to the settings you want to fix. Then, click "Next" to continue. You may be prompted for more information to fix certain settings.

No	Security Problems Identified	Action
1	<u>TCP Synwait time is not set</u>	<input type="checkbox"/> Fix it
2	<u>Banner is not set</u>	<input type="checkbox"/> Fix it
3	<u>Enable Secret Password is not set</u>	<input type="checkbox"/> Fix it
4	<u>Scheduler Allocate is not set</u>	<input type="checkbox"/> Fix it
5	<u>Telnet settings are not enabled</u>	<input type="checkbox"/> Fix it
6	<u>NetFlow Monitoring is not enabled</u>	<input type="checkbox"/> Fix it
7	<u>IP Unreachables is enabled on NULL interface</u>	<input type="checkbox"/> Fix it
8	<u>Access class is not set on HTTP server service</u>	<input type="checkbox"/> Fix it
9	<u>Access class is not set on VTY lines</u>	<input type="checkbox"/> Fix it
10	<u>SSH is disabled for access to the router</u>	<input type="checkbox"/> Fix it
11	<u>AAA is not enabled</u>	<input type="checkbox"/> Fix it

< Back   Next >   Finish   Cancel   Help



## Security Audit – AutoSecure(All features enabled)

Security Audit Wizard

Security Audit

Select an option: **Fix the Security problems**

Check the "Fix-it" checkbox next to the settings you want to fix. Then, click "Next" to continue. You may be prompted for more information to fix certain settings.

Fix All

No	Security Problems Identified	Action
1	<u>TCP Synwait time is not set</u>	<input type="checkbox"/> Fix it
2	<u>Banner is not set</u>	<input type="checkbox"/> Fix it
3	<u>Scheduler Allocate is not set</u>	<input type="checkbox"/> Fix it
4	<u>Telnet settings are not enabled</u>	<input type="checkbox"/> Fix it
5	<u>NetFlow Monitoring is not enabled</u>	<input type="checkbox"/> Fix it
6	<u>IP Unreachables is enabled on NULL interface</u>	<input type="checkbox"/> Fix it
7	<u>Unicast RPF is not enabled in all the outside interfaces</u>	<input type="checkbox"/> Fix it
8	<u>Access class is not set on HTTP server service</u>	<input type="checkbox"/> Fix it
9	<u>Access class is not set on VTY lines</u>	<input type="checkbox"/> Fix it

**NOTE: AutoSecure configures the MOTD banner. Security Audit checks for the LOGIN banner.**

< Back Next > Finish Cancel Help



## One-Step Lockdown – Use It?

Much like my advice for AutoSecure, the biggest advantage of using One-Step Lockdown is that you can harden a router with a single mouse click. This is a blessing and a curse. The command is intended to assist those who don't know much about routers and want to make sure their device is secure. The problem with this is that if you don't know much about routers then you're going to have a hell of a time troubleshooting any issues brought on by One-Step Lockdown .

While AutoSecure asks you for some input(unless you specify 'no-interact'), One-Step Lockdown does not. This makes it slightly easier to configure, but does require that you have already configured the router to be accessed by SDM.

My suggestion is if you want to use this feature, go ahead and use it. After you use it, run the Security Audit feature and then disable any changes that One-Step Lockdown has made that you will need to use on your network.

Definitely give the Cisco Router and Security Device Manager 2.5 User Guide section for Security Audit a read as it includes information on One-Step Lockdown. More importantly, it has a great breakdown of each of the features that One-Step Lockdown(and AutoSecure) disables.