CHAPTER 41

# Using AutoSecure

This chapter describes how to use the AutoSecure function in Cisco IOS Software Release 12.2SX. Release 12.2(33)SXH and later releases support the AutoSecure function.

**Note** For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html

This chapter consists of these sections:


- Understanding AutoSecure, page 41-1
- Configuring AutoSecure, page 41-6
- AutoSecure Configuration Example, page 41-9


## Understanding AutoSecure

You can easily secure the switch without understanding all the security capabilities of the switch by using the AutoSecure feature. AutoSecure is a simple security configuration process that disables nonessential system services and enables a basic set of recommended security policies to ensure secure networking services.

**Caution** Although AutoSecure helps to secure a switch, it does not guarantee the complete security of the switch.

The following sections describe how AutoSecure works:


- Benefits of AutoSecure, page 41-2
- Securing the Management Plane, page 41-2
- Securing the Forwarding Plane, page 41-5
- AutoSecure Guidelines and Restrictions, page 41-6

# Benefits of AutoSecure

AutoSecure provides a variety of mechanisms to enhance security of the switch.

## Simplified Switch Security Configuration

AutoSecure automates a thorough configuration of security features of the switch. AutoSecure disables certain features that are enabled by default that could be exploited for security holes.

You can execute AutoSecure in either of two modes, depending on your individual needs:

- Interactive mode—Prompts with options to enable and disable services and other security features, suggesting a default setting for each option.
- Noninteractive mode—Automatically executes the recommended Cisco default settings.

## Enhanced Password Security

AutoSecure provides the following mechanisms to improve the security of access to the switch:

- You can specify a required minimum password length, which can eliminate weak passwords that are prevalent on most networks, such as “lab” and “cisco.”

  To configure a minimum password length, use the **security passwords min-length** command.
- You can cause a syslog message to be generated after the number of unsuccessful login attempts exceeds the configured threshold.

  To configure the number of allowable unsuccessful login attempts (the threshold rate), use the **security authentication failure rate** command.

## System Logging Message Support

System logging messages capture any subsequent changes to the AutoSecure configuration that are applied on the running configuration. As a result, a more detailed audit trail is provided when AutoSecure is executed.

# Securing the Management Plane

AutoSecure provides protection for the switch management interfaces (the management plane) and the data routing and switching functions (the forwarding plane, described in the “Securing the Forwarding Plane” section on page 41-5.) Securing the management plane is done by turning off certain global and interface services that can be potentially exploited for security attacks and turning on global services that help minimize the threat of attacks. Secure access and secure logging are also configured for the switch.

**Caution** If your device is managed by a network management (NM) application, securing the management plane could turn off some services such as the HTTP server and disrupt the NM application support.

The following sections define how AutoSecure helps to secure the management plane:

- Disables Global Services, page 41-3
- Disables Per-Interface Services, page 41-3

- Enables Global Services, page 41-4
- Secures Access to the Switch, page 41-4
- Enhances Logging for Security, page 41-5


## Disables Global Services

AutoSecure will disable the following global services on the switch without prompting the user:

- Finger—Collects information about the system (reconnaissance) before an attack.
- PAD—Enables all packet assembler and disassembler (PAD) commands and connections between PAD devices and access servers.
- Small servers—Causes TCP and User Datagram Protocol (UDP) diagnostic port attacks: a sender transmits a volume of fake requests for UDP diagnostic services on the switch, consuming all CPU resources.
- Bootp server—Bootp is an insecure protocol that can be exploited for an attack.
- HTTP server—Without secure-HTTP or authentication embedded in the HTTP server with an associated ACL, the HTTP server is insecure and can be exploited for an attack. (If you must enable the HTTP server, you will be prompted for the proper authentication or access list.)

**Note** If you are using Security Device Manager (SDM), you must manually enable the HTTP server using the **ip http server** command.

- Identification service—An unsecure protocol (defined in RFC 1413) that allows an external host to query a TCP port for identification. An attacker can access private information about the user from the ID server.
- CDP—If a large number of Cisco Discovery Protocol (CDP) packets are sent to the switch, the available memory of the switch can be consumed, which causes the switch to crash.

**Note** NM applications that use CDP to discover network topology will not be able to perform discovery.

- NTP—Without authentication or access control, Network Time Protocol (NTP) is insecure and can be used by an attacker to send NTP packets to crash or overload the switch.

  If you require NTP, you must configure NTP authentication using Message Digest 5 (MD5) and the **ntp access-group** command. If NTP is enabled globally, disable it on all interfaces on which it is not needed.
- Source routing—Source routing is provided only for debugging purposes, and should be disabled in all other cases. Otherwise, packets may avoid some of the access control mechanisms of the switch.

## Disables Per-Interface Services

AutoSecure will disable the following per-interface services on the switch without prompting the user:

- ICMP redirects—Disabled on all interfaces. Does not add a useful functionality to a correctly configured network, but could be used by attackers to exploit security holes.
- ICMP unreachables—Disabled on all interfaces. Internet Control Management Protocol (ICMP) unreachables are a known method for some ICMP-based denial of service (DoS) attacks.

- ICMP mask reply messages—Disabled on all interfaces. ICMP mask reply messages can give an attacker the subnet mask for a particular subnetwork in the internetwork.
- Proxy-arp—Disabled on all interfaces. Proxy-arp requests are a known method for DoS attacks because the available bandwidth and resources of the switch can be consumed in an attempt to respond to the repeated requests sent by an attacker.
- Directed broadcast—Disabled on all interfaces. Potential cause of SMURF attacks for DoS.
- Maintenance Operations Protocol (MOP) service—Disabled on all interfaces.

## Enables Global Services

AutoSecure will enable the following global services on the switch without prompting the user:

- The **service password-encryption** command—Prevents passwords from being visible in the configuration.
- The **service tcp-keepalives-in** and **service tcp-keepalives-out** commands—Ensures that abnormally terminated TCP sessions are removed.

## Secures Access to the Switch

**Caution** If your device is managed by an NM application, securing access to the switch could turn off vital services and may disrupt the NM application support.

AutoSecure will make the following options available for securing access to the switch:

- If a text banner does not exist, you will be prompted to add a banner. This feature provides the following sample banner:

```
Authorized access only
    This system is the property of ABC Enterprise
    Disconnect IMMEDIATELY if you are not an authorized user!
    Contact abc@example.com +1 408 5551212 for help.
```

- The login and password (preferably a secret password, if supported) are configured on the console, AUX, vty, and tty lines. The **transport input** and **transport output** commands are also configured on all of these lines. (Telnet and secure shell (SSH) are the only valid transport methods.) The **exec-timeout** command is configured on the console and AUX as 10.
- When the image on the device is a crypto image, AutoSecure enables SSH and secure copy (SCP) for access and file transfer to and from the switch. The **timeout** *seconds* and **authentication-retries** *integer* options for the **ip ssh** command are configured to a minimum number. (Telnet and FTP are not affected by this operation and remain operational.)
- If the user specifies that the switch does not use Simple Network Management Protocol (SNMP), one of the following functionalities will occur:
  - In interactive mode, the user is asked whether to disable SNMP regardless of the values of the community strings, which act like passwords to regulate access to the agent on the switch.
  - In noninteractive mode, SNMP will be disabled if the community string is public or private.

**Note** After AutoSecure has been enabled, tools that use SNMP to monitor or configure a device will be unable to communicate with the device using SNMP.

- If authentication, authorization, and accounting (AAA) is not configured, AutoSecure configures local AAA. AutoSecure will prompt the user to configure a local username and password on the switch.

### Enhances Logging for Security

AutoSecure provides the following logging options, which allow you to identify and respond to security incidents:

- Sequence numbers and time stamps for all debug and log messages. This option is useful when auditing logging messages.
- Logging messages for login-related events. For example, the message "Blocking Period when Login Attack Detected" will be displayed when a login attack is detected and the switch enters quiet mode. (Quiet mode means that the switch will not allow any login attempts using Telnet, HTTP, or SSH.)
- The **logging console critical** command, which sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
- The **logging buffered** command, which copies logging messages to an internal buffer and limits messages logged to the buffer based on severity.
- The **logging trap debugging** command, which allows all commands with a severity higher than debugging to be sent to the logging server.

## Securing the Forwarding Plane

To minimize the risk of attacks on the switch forwarding plane, AutoSecure provides the following functions:

- Cisco Express Forwarding (CEF)—AutoSecure enables CEF or distributed CEF (dCEF) on the switch whenever possible. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF operates more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Switches configured for CEF perform better under SYN attacks than switches using the traditional cache.

**Note** CEF consumes more memory than a traditional cache.

- If strict Unicast Reverse Path Forwarding (uRPF) is available, it can be configured on the switch to help mitigate problems that are caused by the introduction of forged (spoofed) IP source addresses. uRPF discards IP packets that lack a verifiable IP source address.
- Hardware rate limiting—AutoSecure will enable hardware rate-limiting of the following types of traffic without prompting the user:
  - IP errors
  - RPF failures
  - ICMP no-route messages
  - ICMP acl-drop messages
  - IPv4 multicast FIB miss messages
  - IPv4 multicast partially switch flow messages

  AutoSecure will provide the option for hardware rate-limiting of the following types of traffic:

- ICMP redirects
- TTL failures
- MTU failures
- IP unicast options
- IP multicast options
- Ingress and egress ACL bridged packets

**Note** Rate-limiting of ingress and egress ACL bridged packets can interfere with ACL logging and can increase session setup rates for hardware accelerated features such as NAT, Layer 3 WCCP, and TCP intercept.

## AutoSecure Guidelines and Restrictions

When configuring AutoSecure, follow these guidelines and restrictions:

- Because there is no command to undo configuration changes made by AutoSecure, always save your running configuration before configuring AutoSecure.
- The AutoSecure configuration can be configured at run time or setup time. If any related configuration is modified after AutoSecure has been enabled, the AutoSecure configuration may not be fully effective.
- After AutoSecure has been enabled, tools that use SNMP to monitor or configure a device will be unable to communicate with the device using SNMP.
- If your device is managed by a network management (NM) application, securing the management plane could turn off some services such as HTTP server and disrupt the NM application support.
- If you are using Security Device Manager (SDM), you must manually enable the HTTP server using the **ip http server** command.
- NM applications that use CDP to discover network topology will not be able to perform discovery.

# Configuring AutoSecure

These sections describe how to configure AutoSecure:

- Using the AutoSecure Command, page 41-6
- Configuring Additional Security, page 41-8
- Verifying AutoSecure, page 41-8

## Using the AutoSecure Command

The **auto secure** command guides you through a semi-interactive session (also known as the AutoSecure session) to secure the management and forwarding planes. You can use this command to secure just the management plane or the forwarding plane; if neither option is selected in the command line, you can choose to configure one or both planes during the session.

This command also allows you to go through all noninteractive configuration portions of the session before the interactive portions. The noninteractive portions of the session can be enabled by selecting the optional **no-interact** keyword.

The AutoSecure session will request the following information from you:

- Is the device going to be connected to the Internet?
- How many interfaces are connected to the Internet?
- What are the names of the interfaces connected to the Internet?
- What will be your local username and password?
- What will be the switch hostname and domain name?

At any prompt you may enter a question mark (**?**) for help or Ctrl-C to abort the session.

In interactive mode, you will be asked at the end of the session whether to commit the generated configuration to the running configuration of the switch. In noninteractive mode, the changes will be automatically applied to the running configuration.

**Note** There is no undo command for configuration changes made by AutoSecure. You should always save the running configuration before executing the **auto secure** command.

To execute the AutoSecure configuration process, beginning in privileged EXEC mode, perform this task:

| Command | Purpose |
|---|---|
| `Router# auto secure [management \| forwarding] [no-interact \| full]` | Executes the AutoSecure session for configuring one or both planes of the switch.<br>• **management**—Only the management plane will be secured.<br>• **forwarding**—Only the forwarding plane will be secured.<br>• **no-interact**—The user will not be prompted for any interactive configurations.<br>• **full**—The user will be prompted for all interactive questions. This is the default. |

For an example of the AutoSecure session, see the "AutoSecure Configuration Example" section on page 41-9.

# Configuring Additional Security

After completing the AutoSecure configuration, you can further enhance the security of management access to your switch by performing this task:

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | `Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | `Router(config)# security passwords min-length` *length* | Ensures that all configured passwords are at least a specified length.<br>• *length*—Minimum length of a configured password. The range is 0 to 16 characters. |
| **Step 3** | `Router(config)# enable password` {*password* \| [*encryption-type*] *password*} | Sets a local password to control access to various privilege levels.<br>• *encryption-type*—A value of 0 indicates that an unencrypted password follows. A value of 7 indicates that a hidden password follows.<br>**Note** You usually will not enter an encryption type unless you enter a password that has already been encrypted by a Cisco router or switch. |
| **Step 4** | `Router(config)# security authentication failure rate` *threshold-rate* `log` | Configures the number of allowable unsuccessful login attempts.<br>• *threshold-rate*—Number of allowable unsuccessful login attempts. The range is 1 to 1024.<br>• **log**—Syslog authentication failures if the number of failures in one minute exceeds the threshold. |

The following example shows how to configure the switch for a minimum password length of 10 characters and a threshold of 3 password failures in one minute. The example also shows how to set a hidden local password.

```
Router# configure terminal
Router(config)# security passwords min-length 10
Router(config)# security authentication failure rate 3
Router(config)# enable password 7 elephant123
```

# Verifying AutoSecure

To verify that the AutoSecure feature has executed successfully, perform this task:

| Command or Action | Purpose |
|---|---|
| `Router# show auto secure config` | Displays all configuration commands that have been added as part of the AutoSecure configuration. The output is the same as the configuration generated output |

# AutoSecure Configuration Example

The following example is a sample AutoSecure session. After you execute the **auto secure** command, the feature will automatically prompt you with a similar response unless you enable the **no-interact** keyword. (For information on which features are disabled and which features are enabled, see the "Securing the Management Plane" section on page 41-2 and the "Securing the Forwarding Plane" section on page 41-5.)

```
Router# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

 AutoSecure will modify the configuration of your device.

All the configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: y

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan77                 77.1.1.4        YES NVRAM  down                  down
GigabitEthernet6/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet6/2     21.30.30.1      YES NVRAM  up                    up
Loopback0              3.3.3.3         YES NVRAM  up                    up
Tunnel1                unassigned      YES NVRAM  up                    up
Enter the interface name that is facing the internet: Vlan77

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
```

```
  This system is the property of <Name of Enterprise>.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k
banner
k
Enter the new enable secret:
Confirm the enable secret :
Enable password is not configured or its length
is less than minimum no. of charactersconfigured
Enter the new enable password:
Confirm the enable password:

Configuration of local user database
Enter the username: cisco
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected (in seconds): 5

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts (in seconds): ?
% A decimal number between 1 and 32767.

Maximum time period for crossing the failed login attempts (in seconds): 5

Configure SSH server? [yes]: no

Configuring interface specific AutoSecure services
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

The following rate-limiters are enabled by default:
  mls rate-limit unicast ip errors 100 10
  mls rate-limit unicast ip rpf-failure 100 10
  mls rate-limit unicast ip icmp unreachable no-route 100 10
  mls rate-limit unicast ip icmp unreachable acl-drop 100 10
  mls rate-limit multicast ipv4 fib-miss 100000 100
  mls rate-limit multicast ipv4 partial 100000 100

Would you like to enable the following rate-limiters also?
mls rate-limit unicast ip icmp redirect 100 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
mls rate-limit unicast ip options 100 10
mls rate-limit multicast ipv4 ip-options 100 10

Enable the above rate-limiters also? [yes/no]: yes
```

```
Would you like to enable the rate-limiters for Ingress/EgressACL bridged packets also?
NOTE: Enabling the ACL in/out rate-limiters can affect ACL logging
      and session setup rate for hardware accelerated features such
      as NAT, Layer 3 WCCP and TCP Intercept
mls rate-limit unicast acl input 100 10
mls rate-limit unicast acl output 100 10

Enable the ACL in/out rate-limiters also? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner k
banner
k
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$30kP$f.KDndYPz/Hv/.yTlJStN/
enable password 7 08204E4D0D48574446
username cisco password 7 08204E4D0D48574446
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 15
 login authentication local_auth
 transport input telnet
login block-for 5 attempts 3 within 5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int Vlan77
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
```

```
 no mop enabled
int GigabitEthernet6/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Vlan77
 ip verify unicast source reachable-via rx
mls rate-limit unicast ip icmp redirect 100 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
mls rate-limit unicast ip options 100 10
mls rate-limit multicast ipv4 ip-options 100 10
!
end


Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

Router#
```