AutoSecure

By using a single command-line interface (CLI), the AutoSecure feature allows a user to perform the following functions:

- Disable common IP services that can be exploited for network attacks
- Enable IP services and features that can aid in the defense of a network when under attack.

This feature also simplifies the security configuration of a router and hardens the router configuration.

Feature Specifications for the AutoSecure Feature

Feature History	
Release	**Modification**
12.3(1)	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for AutoSecure

Roll-back of the AutoSecure configuration is currently unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Information About AutoSecure

To configure the AutoSecure feature, you must understand the following concepts:

Benefits of AutoSecure

Simplified Router Security Configuration

AutoSecure is valuable to customers without special Security Operations Applications because it allows them to quickly secure their network without thorough knowledge of all the Cisco IOS features.

This feature eliminates the complexity of securing a router by creating a new CLI that automates the configuration of security features and disables certain features enabled by default that could be exploited for security holes.

Enhanced Password Security

AutoSecure provides the following mechanisms to enhance security access to the router:

- The ability to configure a required minimum password length, which can eliminate common 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.
- Syslog messages are generated after the number of unsuccessful attempts exceeds the configured threshold.

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

Secure Management Plane

Securing the management plane is one of two focus areas for the AutoSecure feature. (The other focus area is described in the following section, “Secure Forwarding Plane.”) 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 mitigate the threat of attacks. Secure access and secure logging are also configured for the router.

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

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

- Disable Global Services
- Disable Per Interface Services
- Enable Global Services
- Secure Access to the Router
- Log for Security

Disable Global Services

After enabling this feature (via the **auto secure** command), the following global services will be disabled on the router without prompting the user:

- Finger—Collects information about the system (reconnaissance) before an attack. If enabled, the information can leave your device vulnerable to attacks.
- PAD—Enables all packet assembler and disassembler (PAD) commands and connections between PAD devices and access servers. If enabled, it can leave your device vulnerable to attacks.
- 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 router, 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 switching database manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

- Identification Service—An unsecure protocol, defined in RFC 1413, that allows one 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 router, the available memory of the router can be consumed, causing the router to crash.

Caution 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 router. (If you want to turn on 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—Provided only for debugging purposes, so source routing should be disabled in all other cases. Otherwise, packets may slip away from some of the access control mechanisms that they should have gone through.

Disable Per Interface Services

After enabling this feature, the following per interface services will be disabled on the router without prompting the user:

- ICMP redirects—Disabled on all interfaces. Does not add a useful functionality to a correctly configured to network, but it could be used by attackers to exploit security holes.
- ICMP unreachables—Disabled on all interfaces. Internet Control Management Protocol (ICMP) unreachables are a known cause 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 cause for DoS attacks because the available bandwith and resources of the router can be consumed in an attempt to respond to the repeated requests that are 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.

Enable Global Services

After enabling this feature, the following global services will be enabled on the router 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.

Secure Access to the Router

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

After enabling this feature, the following options in which to secure access to the router are available to the user:

- If a text banner does not exist, users 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@xyz.com +99 876 543210 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 router. 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 AutoSecure user specifies that their device 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 router.
  - In non-interact 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 via SNMP.

- If authentication, authorization, and accounting (AAA) is not configured, configure local AAA. Autosecure will prompt users to configure a local username and password on the router.

Log for Security

After this feature is enabled, the following logging options, which allow you to identify and respond to security incidents, are available:

- Sequence numbers and time stamps for all debug and log messages. This option is useful when auditing logging messages.
- 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.

Secure Forwarding Plane

To minimize the risk of attacks on the router forward plane, AutoSecure provides the following functions:

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

Note CEF consumes more memory than a traditional cache.

- Because antispoofing is the first step in many network attacks, AutoSecure configures the following three named access lists that can be used to prevent antispoofing source addresses:
  - autosec_iana_reserved_block—Address blocks reserved by IANA.

    Note These address blocks are subject to change. To ensure that you have the latest ACLs, refer to the following URL: www.iana.org/assignments/ipv4-address-space.

  - autosec_private_block—Private addresses that should not be used over internet.

Note For additional information regarding "autosec_private_block," refer to RFC 1918, *Address Allocation for Private Internets*

  - autosec_complete_bogon—Combination of the autosec_iana_reserved_block, autosec_private_block, and additional addresses that are not permitted as source addresses.

- If the TCP intercept feature is available, it can be configured on the router for connection timeout.
- If strict Unicast Reverse Path Forwarding (uRPF) is available, it can be configured on the router 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.
- If the router is being used as a firewall, it can be configured for context-based access control (CBAC) on public interfaces that are facing the Internet.

Note At the beginning of the AutoSecure dialogue, you will be prompted for a list of public interfaces

How to Configure AutoSecure

This section contains the following procedures:

- Configuring AutoSecure, page 6 (required)
- Configuring Additional Security, page 7 (required)
- Verifying AutoSecure, page 8 (optional)

Configuring AutoSecure

To configure AutoSecure, you must perform the following tasks.

The auto secure Command

The **auto secure** command takes you through a semi-interactive session (also known as the AutoSecure dialogue) to secure the management and forwarding planes. This command gives you the option to secure just the management or the forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

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

Caution Although the **auto secure** command helps to secure a router, it does not guarantee the complete security of the router.

Restrictions

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.

SUMMARY STEPS

1. **enable**
2. **auto secure** [**management** | **forwarding**] [**no-interact**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**auto secure** [**management**	**forwarding**] [**no-interact**] **Example:** `Router# auto secure`	Secures the management and forwarding planes of the router. • **management**—Only the management plane will be secured. • **forwarding**—Only the forwarding plane will be secured. • **no-interact**—The user will not be prompted for any interactive configurations.

Configuring Additional Security

To enable enhanced security access to your router, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password*}
5. **security authentication failure rate** *threshold-rate* **log**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**security passwords min-length** *length* **Example:** `Router(config)# security passwords min-length 6`	Ensures that all configured passwords are at least a specified length. • *length*—Minimum length of a configured password.
Step 4	**enable password** {*password* | [*encryption-type*] *encrypted-password*} **Example:** `Router(config)# enable password elephant`	Sets a local password to control access to various privilege levels.
Step 5	**security authentication failure rate** *threshold-rate* **log** **Example:** `Router(config)# security authentication failure rate 10 log`	Configures the number of allowable unsuccessful login attempts. • *threshold-rate*—Number of allowable unsuccessful login attempts. • **log**—Syslog authentication failures if the rate exceeds the threshold.

Verifying AutoSecure

To verify that the AutoSecure feature is working successfully, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show auto secure config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show auto secure config** **Example:** `Router# show auto secure config`	(Optional) Displays all configuration commands that have been added as part of the AutoSecure configuration.

Configuration Examples for AutoSecure

This section provides the following configuration example:

- AutoSecure Configuration Dialogue Example, page 9

AutoSecure Configuration Dialogue Example

The following example is a sample AutoSecure dialogue. After you enable the **auto secure** command, the feature will automatically prompt you with a similar dialogue unless you enable the **no-interact** keyword. (For information on which features are disabled and which features are enabled, see the sections, "Secure Management Plane" and "Secure Forwarding Plane" earlier in this document.)

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

*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                  IP-Address       OK? Method Status
Prot
ocol
FastEthernet0/1            209.165.200.225  YES NVRAM  up
down

FastEthernet1/0            209.165.201.1    YES NVRAM  up
down

FastEthernet1/1            209.165.202.129  YES NVRAM  up
up
```

```
Loopback0                  unassigned       YES NVRAM  up
up

FastEthernet0/0            209.165.200.230  YES NVRAM  up
down

Enter the interface name that is facing internet:FastEthernet0/0

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
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport

Configure SSH server? [yes]:
Enter the domain-name:cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services..

Enabling CEF (it might have more memory requirements on some low end
platforms)
Configuring the named acls for Ingress filtering

autosec_iana_reserved_block:This block may subject to change by iana and for updated list
visit www.iana.org/assignments/ipv4-address-space.
1/8, 2/8, 5/8, 7/8, 23/8, 27/8, 31/8, 36/8, 37/8, 39/8,
41/8, 42/8, 49/8, 50/8, 58/8, 59/8, 60/8, 70/8, 71/8,
72/8, 73/8, 74/8, 75/8, 76/8, 77/8, 78/8, 79/8, 83/8,
84/8, 85/8, 86/8, 87/8, 88/8, 89/8, 90/8, 91/8, 92/8, 93/8,
94/8, 95/8, 96/8, 97/8, 98/8, 99/8, 100/8, 101/8, 102/8,
103/8, 104/8, 105/8, 106/8, 107/8, 108/8, 109/8, 110/8,
111/8, 112/8, 113/8, 114/8, 115/8, 116/8, 117/8, 118/8,
119/8, 120/8, 121/8, 122/8, 123/8, 124/8, 125/8, 126/8,
197/8, 201/8
```

```
autosec_private_block:
10/8, 172.16/12, 192.168/16
autosec_complete_block:This is union of above two and the addresses of source multicast,
class E addresses and addresses that are prohibited for use as source.
source multicast (224/4), class E(240/4), 0/8, 169.254/16,
192.0.2/24, 127/8.

Configure Ingress filtering on edge interfaces? [yes]:

[1] Apply autosec_iana_reserved_block acl on all edge interfaces
[2] Apply autosec_private_block acl on all edge interfaces
[3] Apply autosec_complete_bogon acl on all edge interfaces
Enter your selection [3]:3
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]:yes

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
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
```

```
int FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
access-list compiled
ip access-list extended autosec_iana_reserved_block
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
 deny ip 49.0.0.0 0.255.255.255 any
 deny ip 50.0.0.0 0.255.255.255 any
 deny ip 58.0.0.0 0.255.255.255 any
 deny ip 59.0.0.0 0.255.255.255 any
 deny ip 60.0.0.0 0.255.255.255 any
 deny ip 70.0.0.0 0.255.255.255 any
 deny ip 71.0.0.0 0.255.255.255 any
 deny ip 72.0.0.0 0.255.255.255 any
 deny ip 73.0.0.0 0.255.255.255 any
 deny ip 74.0.0.0 0.255.255.255 any
 deny ip 75.0.0.0 0.255.255.255 any
 deny ip 76.0.0.0 0.255.255.255 any
 deny ip 77.0.0.0 0.255.255.255 any
 deny ip 78.0.0.0 0.255.255.255 any
 deny ip 79.0.0.0 0.255.255.255 any
 deny ip 83.0.0.0 0.255.255.255 any
 deny ip 84.0.0.0 0.255.255.255 any
 deny ip 85.0.0.0 0.255.255.255 any
 deny ip 86.0.0.0 0.255.255.255 any
 deny ip 87.0.0.0 0.255.255.255 any
 deny ip 88.0.0.0 0.255.255.255 any
```

```
 deny ip 89.0.0.0 0.255.255.255 any
 deny ip 90.0.0.0 0.255.255.255 any
 deny ip 91.0.0.0 0.255.255.255 any
 deny ip 92.0.0.0 0.255.255.255 any
 deny ip 93.0.0.0 0.255.255.255 any
 deny ip 94.0.0.0 0.255.255.255 any
 deny ip 95.0.0.0 0.255.255.255 any
 deny ip 96.0.0.0 0.255.255.255 any
 deny ip 97.0.0.0 0.255.255.255 any
 deny ip 98.0.0.0 0.255.255.255 any
 deny ip 99.0.0.0 0.255.255.255 any
 deny ip 100.0.0.0 0.255.255.255 any
 deny ip 101.0.0.0 0.255.255.255 any
 deny ip 102.0.0.0 0.255.255.255 any
 deny ip 103.0.0.0 0.255.255.255 any
 deny ip 104.0.0.0 0.255.255.255 any
 deny ip 105.0.0.0 0.255.255.255 any
 deny ip 106.0.0.0 0.255.255.255 any
 deny ip 107.0.0.0 0.255.255.255 any
 deny ip 108.0.0.0 0.255.255.255 any
 deny ip 109.0.0.0 0.255.255.255 any
 deny ip 110.0.0.0 0.255.255.255 any
 deny ip 111.0.0.0 0.255.255.255 any
 deny ip 112.0.0.0 0.255.255.255 any
 deny ip 113.0.0.0 0.255.255.255 any
 deny ip 114.0.0.0 0.255.255.255 any
 deny ip 115.0.0.0 0.255.255.255 any
 deny ip 116.0.0.0 0.255.255.255 any
 deny ip 117.0.0.0 0.255.255.255 any
 deny ip 118.0.0.0 0.255.255.255 any
 deny ip 119.0.0.0 0.255.255.255 any
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date. Visit www.iana.org/assignments/ipv4-address-space
for update list
exit
ip access-list extended autosec_private_block

 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 permit ip any any
exit
ip access-list extended autosec_complete_bogon
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
```

```
deny ip 49.0.0.0 0.255.255.255 any
deny ip 50.0.0.0 0.255.255.255 any
deny ip 58.0.0.0 0.255.255.255 any
deny ip 59.0.0.0 0.255.255.255 any
deny ip 60.0.0.0 0.255.255.255 any
deny ip 70.0.0.0 0.255.255.255 any
deny ip 71.0.0.0 0.255.255.255 any
deny ip 72.0.0.0 0.255.255.255 any
deny ip 73.0.0.0 0.255.255.255 any
deny ip 74.0.0.0 0.255.255.255 any
deny ip 75.0.0.0 0.255.255.255 any
deny ip 76.0.0.0 0.255.255.255 any
deny ip 77.0.0.0 0.255.255.255 any
deny ip 78.0.0.0 0.255.255.255 any
deny ip 79.0.0.0 0.255.255.255 any
deny ip 83.0.0.0 0.255.255.255 any
deny ip 84.0.0.0 0.255.255.255 any
deny ip 85.0.0.0 0.255.255.255 any
deny ip 86.0.0.0 0.255.255.255 any
deny ip 87.0.0.0 0.255.255.255 any
deny ip 88.0.0.0 0.255.255.255 any
deny ip 89.0.0.0 0.255.255.255 any
deny ip 90.0.0.0 0.255.255.255 any
deny ip 91.0.0.0 0.255.255.255 any
deny ip 92.0.0.0 0.255.255.255 any
deny ip 93.0.0.0 0.255.255.255 any
deny ip 94.0.0.0 0.255.255.255 any
deny ip 95.0.0.0 0.255.255.255 any
deny ip 96.0.0.0 0.255.255.255 any
deny ip 97.0.0.0 0.255.255.255 any
deny ip 98.0.0.0 0.255.255.255 any
deny ip 99.0.0.0 0.255.255.255 any
deny ip 100.0.0.0 0.255.255.255 any
deny ip 101.0.0.0 0.255.255.255 any
deny ip 102.0.0.0 0.255.255.255 any
deny ip 103.0.0.0 0.255.255.255 any
deny ip 104.0.0.0 0.255.255.255 any
deny ip 105.0.0.0 0.255.255.255 any
deny ip 106.0.0.0 0.255.255.255 any
deny ip 107.0.0.0 0.255.255.255 any
deny ip 108.0.0.0 0.255.255.255 any
deny ip 109.0.0.0 0.255.255.255 any
deny ip 110.0.0.0 0.255.255.255 any
deny ip 111.0.0.0 0.255.255.255 any
deny ip 112.0.0.0 0.255.255.255 any
deny ip 113.0.0.0 0.255.255.255 any
deny ip 114.0.0.0 0.255.255.255 any
deny ip 115.0.0.0 0.255.255.255 any
deny ip 116.0.0.0 0.255.255.255 any
deny ip 117.0.0.0 0.255.255.255 any
deny ip 118.0.0.0 0.255.255.255 any
deny ip 119.0.0.0 0.255.255.255 any
deny ip 120.0.0.0 0.255.255.255 any
deny ip 121.0.0.0 0.255.255.255 any
deny ip 122.0.0.0 0.255.255.255 any
deny ip 123.0.0.0 0.255.255.255 any
deny ip 124.0.0.0 0.255.255.255 any
deny ip 125.0.0.0 0.255.255.255 any
deny ip 126.0.0.0 0.255.255.255 any
deny ip 197.0.0.0 0.255.255.255 any
deny ip 201.0.0.0 0.255.255.255 any
```

```
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any

 deny ip 224.0.0.0 15.255.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 deny ip 0.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date. Visit www.iana.org/assignments/ipv4-address-space
for update list
exit
interface FastEthernet0/0
 ip access-group autosec_complete_bogon in
exit
interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
!
end


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

Applying the config generated to running-config
The name for the keys will be:ios210.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]

Router#
```

Additional References

For additional information related to the AutoSecure feature, refer to the following references:

Related Documents

Related Topic	Document Title
Additional information regarding router configuration	*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.3
Additional router configuration commands	*Cisco IOS Configuration Fundamentals Command Reference*, Release 12.3

Standards

Standards[1]	Title
None	—

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs[1]	Title
RFC 1918	*Address Allocation for Private Internets*
RFC 2267	*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

- **auto secure**
- **security authentication failure rate**
- **security passwords min-length**
- **show auto secure config**

auto secure

To secure the management and forwarding planes of the router, use the **auto secure** command in privileged EXEC mode.

auto secure [**management** | **forwarding**] [**no-interact**]

Syntax Description

management	(Optional) Only the management plane will be secured.
forwarding	(Optional) Only the forwarding plane will be secured.
no-interact	(Optional) The user will not be prompted for any interactive configurations. If this keyword is not enabled, the command will show the user the noninteractive configuration and the interactive configurations thereafter.

Defaults

Autosecure is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **auto secure** command allows a user to disable common IP services that can be exploited for network attacks by using a single CLI. This command eliminates the complexity of securing a router both by automating the configuration of security features and by disabling certain features that are enabled by default and that could be exploited for security holes.

Caution If you are using switching database manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

This command takes you through a semi-interactive session (also known as the AutoSecure dialogue) in which to secure the management and forwarding planes. This command gives you the option to secure just the management or forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

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

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

Note Roll-back of the AutoSecure configuration is currently unavailable; thus, you should always save the running configuration before configuring AutoSecure.

Examples

The following example shows how to enable AutoSecure to secure only the management plane:

```
auto secure management
```

Related Commands

Command	Description
show auto secure config	Displays AutoSecure configurations.

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure-rate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure-rate *threshold-rate* **log**

no security authentication failure-rate *threshold-rate* **log**

Syntax Description

threshold-rate	Number of allowable unsuccessful login attempts. The default is 10.
log	Syslog authentication failures if the rate exceeds the threshold.

Defaults

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **security authentication failure-rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

Command	Description
security passwords min-length	Ensures that all configured passwords are at least a specified length.

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*

no security passwords min-length *length*

Syntax Description

length	Minimum length of a configured password. The default is six characters.

Defaults

Six characters

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **security passwords min-length** command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

Examples

The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length:

```
security password min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
security authentication failure rate	Configures the number of allowable unsuccessful login attempts.

show auto secure config

To display AutoSecure configurations, use the **show auto secure** command in privileged EXEC mode.

show auto secure

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example is sample output from the **show auto secure config** command:

```
Router# show auto secure config

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
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
ip domain-name cisco.com
```

```
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
ip cef
access-list compiled
ip access-list extended autosec_iana_reserved_block
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
 deny ip 49.0.0.0 0.255.255.255 any
 deny ip 50.0.0.0 0.255.255.255 any
 deny ip 58.0.0.0 0.255.255.255 any
 deny ip 59.0.0.0 0.255.255.255 any
 deny ip 60.0.0.0 0.255.255.255 any
```

```
 deny ip 70.0.0.0 0.255.255.255 any
 deny ip 71.0.0.0 0.255.255.255 any
 deny ip 72.0.0.0 0.255.255.255 any
 deny ip 73.0.0.0 0.255.255.255 any
 deny ip 74.0.0.0 0.255.255.255 any
 deny ip 75.0.0.0 0.255.255.255 any
 deny ip 76.0.0.0 0.255.255.255 any
 deny ip 77.0.0.0 0.255.255.255 any
 deny ip 78.0.0.0 0.255.255.255 any
 deny ip 79.0.0.0 0.255.255.255 any
 deny ip 83.0.0.0 0.255.255.255 any
 deny ip 84.0.0.0 0.255.255.255 any
 deny ip 85.0.0.0 0.255.255.255 any
 deny ip 86.0.0.0 0.255.255.255 any
 deny ip 87.0.0.0 0.255.255.255 any
 deny ip 88.0.0.0 0.255.255.255 any
 deny ip 89.0.0.0 0.255.255.255 any
 deny ip 90.0.0.0 0.255.255.255 any
 deny ip 91.0.0.0 0.255.255.255 any
 deny ip 92.0.0.0 0.255.255.255 any
 deny ip 93.0.0.0 0.255.255.255 any
 deny ip 94.0.0.0 0.255.255.255 any
 deny ip 95.0.0.0 0.255.255.255 any
 deny ip 96.0.0.0 0.255.255.255 any
 deny ip 97.0.0.0 0.255.255.255 any
 deny ip 98.0.0.0 0.255.255.255 any
 deny ip 99.0.0.0 0.255.255.255 any
 deny ip 100.0.0.0 0.255.255.255 any
 deny ip 101.0.0.0 0.255.255.255 any
 deny ip 102.0.0.0 0.255.255.255 any
 deny ip 103.0.0.0 0.255.255.255 any
 deny ip 104.0.0.0 0.255.255.255 any
 deny ip 105.0.0.0 0.255.255.255 any
 deny ip 106.0.0.0 0.255.255.255 any
 deny ip 107.0.0.0 0.255.255.255 any
 deny ip 108.0.0.0 0.255.255.255 any
 deny ip 109.0.0.0 0.255.255.255 any
 deny ip 110.0.0.0 0.255.255.255 any
 deny ip 111.0.0.0 0.255.255.255 any
 deny ip 112.0.0.0 0.255.255.255 any
 deny ip 113.0.0.0 0.255.255.255 any
 deny ip 114.0.0.0 0.255.255.255 any
 deny ip 115.0.0.0 0.255.255.255 any
 deny ip 116.0.0.0 0.255.255.255 any
 deny ip 117.0.0.0 0.255.255.255 any
 deny ip 118.0.0.0 0.255.255.255 any
 deny ip 119.0.0.0 0.255.255.255 any
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date.
Visit www.iana.org/assignments/ipv4-add ress-space for update list
ip access-list extended autosec_private_block
```

```
 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any
 permit ip any any
ip access-list extended autosec_complete_bogon
 deny ip 1.0.0.0 0.255.255.255 any
 deny ip 2.0.0.0 0.255.255.255 any
 deny ip 5.0.0.0 0.255.255.255 any
 deny ip 7.0.0.0 0.255.255.255 any
 deny ip 23.0.0.0 0.255.255.255 any
 deny ip 27.0.0.0 0.255.255.255 any
 deny ip 31.0.0.0 0.255.255.255 any
 deny ip 36.0.0.0 0.255.255.255 any
 deny ip 37.0.0.0 0.255.255.255 any
 deny ip 39.0.0.0 0.255.255.255 any
 deny ip 41.0.0.0 0.255.255.255 any
 deny ip 42.0.0.0 0.255.255.255 any
 deny ip 49.0.0.0 0.255.255.255 any
 deny ip 50.0.0.0 0.255.255.255 any
 deny ip 58.0.0.0 0.255.255.255 any
 deny ip 59.0.0.0 0.255.255.255 any
 deny ip 60.0.0.0 0.255.255.255 any
 deny ip 70.0.0.0 0.255.255.255 any
 deny ip 71.0.0.0 0.255.255.255 any
 deny ip 72.0.0.0 0.255.255.255 any
 deny ip 73.0.0.0 0.255.255.255 any
 deny ip 74.0.0.0 0.255.255.255 any
 deny ip 75.0.0.0 0.255.255.255 any
 deny ip 76.0.0.0 0.255.255.255 any
 deny ip 77.0.0.0 0.255.255.255 any
 deny ip 78.0.0.0 0.255.255.255 any
 deny ip 79.0.0.0 0.255.255.255 any
 deny ip 83.0.0.0 0.255.255.255 any
 deny ip 84.0.0.0 0.255.255.255 any
 deny ip 85.0.0.0 0.255.255.255 any
 deny ip 86.0.0.0 0.255.255.255 any
 deny ip 87.0.0.0 0.255.255.255 any
 deny ip 88.0.0.0 0.255.255.255 any
 deny ip 89.0.0.0 0.255.255.255 any
 deny ip 90.0.0.0 0.255.255.255 any
 deny ip 91.0.0.0 0.255.255.255 any
 deny ip 92.0.0.0 0.255.255.255 any
 deny ip 93.0.0.0 0.255.255.255 any
 deny ip 94.0.0.0 0.255.255.255 any
 deny ip 95.0.0.0 0.255.255.255 any
 deny ip 96.0.0.0 0.255.255.255 any
 deny ip 97.0.0.0 0.255.255.255 any
 deny ip 98.0.0.0 0.255.255.255 any
 deny ip 99.0.0.0 0.255.255.255 any
 deny ip 100.0.0.0 0.255.255.255 any
 deny ip 101.0.0.0 0.255.255.255 any
 deny ip 102.0.0.0 0.255.255.255 any
 deny ip 103.0.0.0 0.255.255.255 any
 deny ip 104.0.0.0 0.255.255.255 any
 deny ip 105.0.0.0 0.255.255.255 any
 deny ip 106.0.0.0 0.255.255.255 any
 deny ip 107.0.0.0 0.255.255.255 any
 deny ip 108.0.0.0 0.255.255.255 any
 deny ip 109.0.0.0 0.255.255.255 any
 deny ip 110.0.0.0 0.255.255.255 any
 deny ip 111.0.0.0 0.255.255.255 any
 deny ip 112.0.0.0 0.255.255.255 any
 deny ip 113.0.0.0 0.255.255.255 any
 deny ip 114.0.0.0 0.255.255.255 any
```

```
 deny ip 115.0.0.0 0.255.255.255 any
 deny ip 116.0.0.0 0.255.255.255 any
 deny ip 117.0.0.0 0.255.255.255 any
 deny ip 118.0.0.0 0.255.255.255 any
 deny ip 119.0.0.0 0.255.255.255 any
 deny ip 120.0.0.0 0.255.255.255 any
 deny ip 121.0.0.0 0.255.255.255 any
 deny ip 122.0.0.0 0.255.255.255 any
 deny ip 123.0.0.0 0.255.255.255 any
 deny ip 124.0.0.0 0.255.255.255 any
 deny ip 125.0.0.0 0.255.255.255 any
 deny ip 126.0.0.0 0.255.255.255 any
 deny ip 197.0.0.0 0.255.255.255 any
 deny ip 201.0.0.0 0.255.255.255 any

 deny ip 10.0.0.0 0.255.255.255 any
 deny ip 172.16.0.0 0.15.255.255 any
 deny ip 192.168.0.0 0.0.255.255 any

 deny ip 224.0.0.0 15.255.255.255 any
 deny ip 240.0.0.0 15.255.255.255 any
 deny ip 0.0.0.0 0.255.255.255 any
 deny ip 169.254.0.0 0.0.255.255 any
 deny ip 192.0.2.0 0.0.0.255 any
 deny ip 127.0.0.0 0.255.255.255 any
 permit ip any any
remark This acl might not be up to date.
Visit www.iana.org/assignments/ipv4-address-space for update list
interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
Router#
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.