

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server

no ip dns server

Syntax Description This command has no arguments or keywords.

Command Default The DNS server is disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines Use this command to enable the DNS server as needed.

Examples In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

ip drp access-group

To control the sources of Director Response Protocol (DRP) queries to the DRP server agent, use the **ip drp access-group** command in global configuration mode. To remove the access list, use the **no** form of this command.

ip drp access-group *access-list-number*

no ip drp access-group *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of a standard IP access list in the range from 1 to 99 or from 1300 to 1999.
---------------------------	---------------------------	---

Defaults	The DRP server agent will answer all queries.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2 F	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	This command applies an access list to the interface, thereby controlling which devices can send queries to the DRP Server Agent.
-------------------------	---

If both an authentication key chain and an access group have been specified, both security measures must permit access before a request is processed.

Examples	The following example configures access list 1, which permits only queries from the host at 10.45.12.4:
-----------------	---

```
Router(config)# access-list 1 permit 10.45.12.4
Router(config)# ip drp access-group 1
```

Related Commands	Command	Description
	ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
	show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip drp authentication key-chain

To configure authentication on the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **ip drp authentication key-chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

ip drp authentication key-chain *name-of-chain*

no ip drp authentication key-chain *name-of-chain*

Syntax Description	<i>name-of-chain</i> Name of the key chain containing one or more authentication keys.
---------------------------	--

Defaults	No authentication is configured for the DRP Server Agent.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2F	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	When a key chain and key are configured, the key is used to authenticate all DRP requests and responses. The active key on the DRP Server Agent must match the active key on the primary agent. Use the key and key-string commands to configure the key.
-------------------------	---

Examples	The following example configures a key chain named <i>ddchain</i> :
-----------------	---

```
Router(config)# ip drp authentication key-chain ddchain
```

Related Commands	Command	Description
	accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
	ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
	key	Identifies an authentication key on a key chain.
	key chain	Enables authentication for routing protocols.
	key-string (authentication)	Specifies the authentication string for a key.
	send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

Command	Description
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.
show key chain	Displays authentication key information.

ip drp domain

To add a new domain to the DistributedDirector client or to configure an existing domain, use the **ip drp domain** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip drp domain *domain-name*

no ip drp domain *domain-name*

Syntax Description

<i>domain-name</i>	The specified domain name.
--------------------	----------------------------

Command Default

No default domain is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip drp domain** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.

Enabling this command puts the client in boomerang configuration mode.

Use the **ip drp domain** command to enter a new or existing domain name. Entering a new domain name creates a new domain, and entering an existing domain name allows the user to configure the specified domain. When a domain name is configured on the boomerang client, the user can configure specific parameters, such as server address, aliases, and time to live (TTL) values, for that domain.

When a Director Response Protocol (DRP) agent receives a Domain Name System (DNS) racing message from boomerang servers such as DistributedDirector, the DRP agent extracts the specified domain name (for example, www.cisco.com) in the DNS message.

Examples

In the following example, a domain named “www.boom1.com” is added on the boomerang client:

```
Router(config)# ip drp domain www.boom1.com

Router# show running-config
.
.
.
ip drp domain www.boom1.com
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
server (boomerang)	Configures the server address for a specified boomerang domain.
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttd dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttd ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** command in global configuration mode. To disable the DRP Server Agent, use the **no** form of this command.

ip drp server

no ip drp server

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the DRP Server Agent:

```
Router(config)# ip drp server
```

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip host ns

To create a name server (NS) resource record to be returned when a Domain Name System (DNS) server is queried for the associated domain, use the **ip host ns** command in global configuration mode. To remove the NS records, use the **no** form of this command.

ip host *domain-name* **ns** *server-name*

no ip host *domain-name* **ns** *server-name*

Syntax Description	
<i>domain-name</i>	Name of the authority that is delegated to another NS, such as a second-level DistributedDirector.
<i>server-name</i>	Name of the second-level DNS server.

Command Default None.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines The **ip host ns** command allows a DistributedDirector to distribute the server selection process to multiple DistributedDirectors, providing greater scalability and better administrative control.

A DNS server can delegate responsibility for a domain to another DNS server by returning an NS record when queried. This task is especially useful to a DistributedDirector because determining the best DNS reply may be time consuming. To expedite replies, a DistributedDirector can return an NS record, delegating authority for the requested data to one or more second-level DistributedDirectors.

Examples The following example shows a top-level DistributedDirector that uses the low-cost metric random to distribute its load over second-level DistributedDirectors:

Top-Level DistributedDirector

```
Router(config)# ip host www.xyz.com ns ns.xyz.com
Router(config)# ip host ns2.xyz.com 10.0.0.1 10.0.0.2 10.0.0.3
Router(config)# ip director host ns.xyz.com priority random 1
Router(config)# ip dns primary www.xyz.com soa ns2.xyz.com
```

The following example shows second-level DistributedDirectors that use more expensive metrics such as drp-ext and drp-rtt to perform precise server selection.

Second-Level DistributedDirector

```
Router(config)# ip host www.xyz.com 10.0.0.4 10.0.0.5 10.0.0.6
Router(config)# ip director host www.xyz.com priority drp-ext 1
Router(config)# ip director host www.xyz.com priority drp-rtt 2
Router(config)# ip director server 10.0.0.4 drp-association 10.0.0.7
Router(config)# ip director server 10.0.0.5 drp-association 10.0.0.8
Router(config)# ip director server 10.0.0.6 drp-association 10.0.0.9
```

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

ip http access-class *access-list-number*

no ip http access-class *access-list-number*

Syntax Description	<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list global configuration command.
---------------------------	---------------------------	--

Command Default	No access list is applied to the HTTP server.
------------------------	---

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines	If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.
-------------------------	--

Examples	The following example shows how to define an access list as 20 and assign it to the HTTP server:
-----------------	--

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Router(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Router(config-std-nacl)# permit 209.165.200.225 0.255.255.255
! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit
Router(config)# ip http access-class 20
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http accounting commands

To specify a particular command accounting method for HTTP server users, use the **ip http accounting commands** command in global configuration mode. To disable a configured command accounting method, use the **no** form of this command.

ip http accounting commands *level* { **default** | *named-accounting-method-list* }

no ip http accounting commands *level*

<i>level</i>	Indicates a privilege value from 0 to 15. By default, there are the following three command privilege levels on the router: <ul style="list-style-type: none"> • 0—Includes the disable, enable, exit, help, and logout commands. • 1—Includes all user-level commands at the router prompt (>). • 15—Includes all enable-level commands at the router prompt (>).
default	Indicates the default accounting method list configured by the aaa accounting commands CLI.
<i>named-accounting-method-list</i>	Indicates the name of the predefined command accounting method list.

Command Default

Command accounting for HTTP and HTTP over Secure Socket Layer (HTTPS) is automatically enabled when authentication, authorization, and accounting (AAA) is configured on the device. It is not possible to dissable accounting for HTTP and HTTPS. HTTP and HTTPS will default to using the global AAA default method list for accounting. The CLI can be used to configure HTTP and HTTPS to use any predefined AAA method list.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **ip http accounting commands** command is used to specify a particular command accounting method for HTTP server users.

Command accounting provides information about the commands for a specified privilege level that are being executed on a device. Each command accounting record corresponds to one IOS command executed at its respective privilege level, as well as the date and time the command was executed, and the user who executed it. Command accounting will be implemented for HTTP and HTTPS. A stop accounting record will be generated for any CLI execution/configuration done by a user via HTTP and HTTPS.

If this command is not configured, HTTP and HTTPS will use the default AAA accounting list whenever AAA is turned-on using **aaa new-model** configuration CLI. If the default method-list doesn't exist, no accounting records will be generated. Whenever AAA is not turned-on, again no accounting records will be generated.

**Note**

The above behavior is essential to maintain consistency of HTTP and HTTPS accounting CLI with their counterparts available for Telnet/SSH in the IOS line configuration mode.

Examples

The following example shows how to configure HTTP and HTTPS to allow AAA accounting support:

```
Router(config)# ip http accounting commands 1 oneacct
```

Related Commands

Command	Description
aaa authentication login	Specifies the login authentication method to be used by the AAA service.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
ip http authentication aaa	Specifies a particular authentication method for HTTP server users.
ip http server	Enables the HTTP server.

ip http active-session-modules

To selectively enable HTTP applications that will service incoming HTTP requests from remote clients, use the **ip http active-session-modules** command in global configuration mode. Use the **no** form of this command to return to the default, for which all HTTP services will be enabled.

ip http active-session-modules {*listname* | **none** | **all**}

no ip http active-session-modules {*listname*}

Syntax Description

<i>listname</i>	Enables only those HTTP services configured in the list identified by the ip http session-module-list command to serve HTTP requests. All other HTTP or HTTPS applications on the router or switch will be disabled.
none	Disables all HTTP services.
all	Enables all HTTP applications to service incoming HTTP requests from remote clients.

Defaults

If no arguments or keywords are specified, all HTTP services will be enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **ip http active-session-modules** command to selectively enable HTTP applications, for servicing incoming HTTP requests from remote clients. With this command, a selected list of applications can be enabled. All the applications can be enabled or none of the applications can be enabled, in other words, all disabled. Use the **ip http session-module-list** command to define a list of HTTP or secure HTTP (HTTPS) application names to be enabled. If an HTTP request is made for a service that is disabled, a 404 error message is displayed in the remote client browser.



Note

The HTTPS server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
```

```
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
ip http session-module-list	Defines a list of HTTP or HTTPS application names.
show ip http server	Displays details about the current configuration of the HTTP server.

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** command in global configuration mode. To disable a configured authentication method, use the **no** form of this command.

ip http authentication {aaa {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**}

no ip http authentication {aaa {**command-authorization** *level listname* | **exec-authorization** *listname* | **login-authentication** *listname*} | **enable** | **local** | **tacacs**}

Syntax Description		
aaa		Indicates that the authentication method used for the authentication, authorization, and accounting (AAA) login service should be used for authentication. The AAA login authentication method is specified by the aaa authentication login default command, unless otherwise specified by the login-authentication listname keyword and argument.
command-authorization		Sets the authorization method list for commands at the specified privilege level.
<i>level</i>		Indicates a privilege value from 0 through 15. By default, there are the following three command privilege levels on the router: <ul style="list-style-type: none"> • 0—Includes the disable, enable, exit, help, and logout commands. • 1—Includes all user-level commands at the router prompt (>). • 15—Includes all enable-level commands at the router prompt (>).
<i>listname</i>		Sets the name of the method list.
exec-authorization		Sets the method list for EXEC authorization, which applies authorization for starting an EXEC session.
login-authentication		Sets the method list for login authentication, which enables AAA authentication for logins.
enable		Indicates that the “enable” password should be used for authentication. (This is the default method.)
local		Indicates that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.
tacacs		Indicates that the TACACS (or XTACACS) server should be used for authentication.

Defaults

The “enable” password is required when users (clients) connect to the HTTP server. Three command privilege levels exist on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 F	This command was introduced.
12.3(8)T	The tacacs keyword was removed. The command-authorization , exec-authorization , and login-authentication keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **ip http authentication** command specifies the authentication method to be used for login when a client connects to the HTTP server. Use of the **aaa** option is recommended. The **enable**, **local**, and **tacacs** methods should be specified using the **aaa authentication login** command.

The “enable” password method is the default HTTP server authentication method. If the enable password is used as the HTTP server login authentication method, the client connects to the HTTP server with a default privilege level of 15.

**Note**

When the “enable” password is used as the HTTP server login authentication method, any username entered will be ignored; the server will only verify the “enable” password. This may make it easier for an attacker to access the router. Because a username and password pair is more secure than using only a password for authentication, using only “enable” password for authentication is strongly discouraged. Instead, use of the **local** or **tacacs** authentication options, configured as part of a global AAA framework, is recommended.

To configure HTTP access as part of a AAA policy, use the **aaa** command option. The **local**, **tacacs**, or **enable** authentication methods should then be configured using the **aaa authentication login** command.

Examples

The following example shows how to specify that AAA should be used for authentication for HTTP server users. The AAA login method is configured as the “local” username/password authentication method. This example also shows how to specify using the local username database for login authentication and EXEC authorization of HTTP sessions:

```
Router(config)# aaa authentication login LOCALDB local
Router(config)# aaa authorization exec LOCALDB local
Router(config)# ip http authentication aaa login-authentication LOCALDB
Router(config)# ip http authentication aaa exec-authorization LOCALDB
```

Related Commands

Command	Description
aaa authentication login	Specifies the login authentication method to be used by the AAA service.
aaa authorization	Sets parameters that restrict user access to a network.
ip http server	Enables the HTTP server.

ip http client cache

To configure the HTTP client cache, use the **ip http client cache** command in global configuration mode. To remove the specification of a value configured for the HTTP client cache, use the **no** form of this command.

```
ip http client cache { ager interval minutes | memory { file file-size-limit | pool pool-size-limit }
```

```
no ip http client cache { ager interval | memory { file | pool } }
```

Syntax Description

ager	Specifies a cache ager interval time
interval	Specifies an interval, in minutes.
<i>minutes</i>	Frequency, in minutes, at which the router removes expired cached responses from the HTTP client cache pool. The range is from 0 to 60. The default is 5. Note The explicit expiration time for a cached response can be provided by the origin server. If this information is not configured, the HTTP cache uses heuristic calculations to determine a plausible expiration time for the cached response.
memory	Specifies the maximum memory allowed for HTTP client cache.
file	Specifies the maximum file size allowed for caching.
<i>file-size-limit</i>	Maximum file size, in kilobytes, supported by the HTTP client cache. The range is from 1 to 10, and the default is 2.
pool	Specifies the maximum memory pool allowed for HTTP cache.
<i>pool-size-limit</i>	Maximum memory pool size, in kilobytes. The range is from 0 to 100. The default is 100.

Command Default

5 second ager interval for the HTTP client cache memory pool
2 KB maximum file size supported by the HTTP client cache
100 KB maximum memory pool size for the HTTP client cache

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to specify the HTTP client cache ager interval, maximum file size, or maximum memory pool size.

To display the values configured by this command, use the **show ip http client cache** command.

Examples

The following example shows how to specify an HTTP client cache ager interval of 10 minutes:

```
Router(config)# ip http client cache ager interval 10
```

The following example shows how to specify an HTTP client cache maximum file size of 7 KB:

```
Router(config)# ip http client cache memory file 7
```

The following example shows how to specify an HTTP client cache maximum memory pool size of 55 KB:

```
Router(config)# ip http client cache memory pool 55
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client connection

To configure characteristics for HTTP client connections to a remote HTTP server for all file transfers, use the **ip http client connection** command in global configuration mode. To remove the specification of a value configured for a connection characteristic, use the **no** form of this command.

```
ip http client connection {forceclose | idle timeout seconds | retry count | timeout seconds}
```

```
no ip http client connection {forceclose | idle | retry | timeout}
```

Syntax Description

forceclose	Disables a persistent connection. Enabled by default.
idle timeout	Sets the period of time allowed for an idle connection between an HTTP client and server before the connection is closed.
<i>seconds</i>	Integer in the range of 1 to 60 that specifies the number of seconds allowed for an idle connection before the connection is closed. The default is 30.
retry	Sets the connection establishment timeout. Accepted range is from 1 to 5 retries, and the default is 1.
<i>count</i>	Number of connection attempts, in the range of 1 to 5. The default is 1.
timeout	Sets the maximum time an HTTP client will wait for a connection.
<i>seconds</i>	Maximum time, in seconds, that an HTTP client will wait for a connection. Accepted range is from 1 to 60 seconds, and the default is 10.

Defaults

Persistent connection maintenance is enabled.
30-second idle timeout
1 retry attempt
10-second maximum timeout

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to change or remove the specification of a value configured as a characteristics for establishing an HTTP client connection to a remove HTTP server for all file transfers.

Examples

The following example shows how to configure the default HTTP client persistent connection for a 15-second idle connection period. The maximum time the HTTP client will wait for a connection is 10 seconds.

```
Router(config)# ip http client connection idle timeout 15
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client password

To configure the default password used for connections to remote HTTP servers, use the **ip http client password** command in global configuration mode. To remove a configured default password from the configuration, use the **no** form of this command.

ip http client password *password*

no ip http client password

Syntax Description	<i>password</i>	The password string to be used in HTTP client connection requests sent to remote HTTP servers.
---------------------------	-----------------	--

Defaults No default password exists for the HTTP connections.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines This command is used to configure a default password before a file is downloaded from a remote web server using the **copy http://** or **copy https://** command. The default password will be overridden by a password specified in the URL of the **copy** command.

The password is encrypted in the configuration files.



Note

The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

Examples In the following example, the default HTTP password is configured as Secret and the default HTTP username is configured as User2 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Secret
Router(config)# ip http client username User2
Router(config)# do show running-config | include ip http client
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client proxy-server

To configure an HTTP proxy server, use the **ip http client proxy-server** command in global configuration mode. To disable or change the proxy server, use the **no** form of this command.

ip http client proxy-server *proxy-name* **proxy-port** *port-number*]

no ip http client proxy-server

Syntax Description		
	<i>proxy-name</i>	Name of the proxy server.
	proxy-port	Specifies a proxy port for HTTP file system client connections.
	<i>port-number</i>	Integer in the range of 1 to 65535 that specifies a port number on the remote proxy server.

Defaults No default behavior or values

Command Modes Global configuration (config)

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines This command configures the HTTP client to connect to a remote proxy server for HTTP file system client connections.

Examples The following example shows how to configure the HTTP proxy server named edge2 at port 29:

```
Router(config)# ip http client proxy-server edge2 proxy-port 29
```

Related Commands	Command	Description
	copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
	debug ip http client	Enables debugging output for the HTTP client.
	ip http client cache	Configures the HTTP client cache.
	ip http client connection	Configures the HTTP client connection.

Command	Description
ip http client password	Configures a password for all HTTP client connections.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client response

To configure the number of seconds that the HTTP client waits for a response from the server for a request message, use the **ip http client response** command in global configuration mode. To remove the specified number of seconds that the HTTP client waits for a response, use the **no** form of this command.

ip http client response timeout *seconds*

no ip http client response timeout

Syntax Description	timeout	Specifies a response timeout period.
	<i>seconds</i>	The amount of time, in seconds, to wait for a response to a domain name system (DNS) query. The range is from 1 to 300.

Command Default	None
-----------------	------

Command Modes	Global configuration (config)
---------------	-------------------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines	Use this command to specify the response timeout value.
------------------	---

Examples	The following example shows how to specify a response timeout of 180 seconds:
----------	---

```
Router(config)# ip http client response timeout 180
```

Related Commands	Command	Description
	copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
	debug ip http client	Enables debugging output for the HTTP client.
	ip http client cache	Configures the HTTP client cache.
	ip http client connection	Configures the HTTP client connection.
	ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client source-interface	Configures a source interface for the HTTP client.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client secure-ciphersuite

To specify the CipherSuite that should be used for encryption over the secure HTTP connection from the client to a remote server, use the **ip http client secure-ciphersuite** command in global configuration mode. To remove a previously configured CipherSuite specification for the client, use the **no** form of this command.

ip http client secure-ciphersuite [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]

no ip http client secure-ciphersuite

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5—RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The client and server negotiate the best CipherSuite that they both support from the list of available CipherSuites.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command allows you to restrict the list of CipherSuites (encryption algorithms) that the client offers when connecting to a secure HTTP server. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default). The **no** form of this command returns the list of available CipherSuites to the default (that is, all CipherSuites supported on your device are available for negotiation).

Examples

The following example shows how to configure the HTTPS client to use only the SSL_RSA_WITH_3DES_EDE_CBC_SHA CipherSuite:

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

Related Commands

Command	Description
show ip http client secure status	Displays the configuration status of the secure HTTP client.

ip http client secure-trustpoint

To specify the remote certificate authority (CA) trustpoint that should be used if certification is needed for the secure HTTP client, use the **ip http client secure-trustpoint** command in global configuration mode. To remove a client trustpoint from the configuration, use the **no** form of this command.

ip http client secure-trustpoint *trustpoint-name*

no ip http client secure-trustpoint *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated crypto ca trustpoint command.
------------------------	--

Command Default

If the remote HTTPS server requests client certification, the secure HTTP client will use the trustpoint configured using the **primary** command in the CA trustpoint configuration. If a trustpoint is not configured, client certification will fail.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used by the HTTPS client for cases when the remote HTTPS server requires client authorization.

Use this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode commands. If the remote HTTPS server requires client authorization and a trustpoint is not configured for the client, the remote HTTPS server will reject the connection.

If this command is not used, the client attempts to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** command.

Examples

In the following example, the CA trustpoint is configured and referenced in the secure HTTP server configuration:

!The following commands specify a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.

```
Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
```

!The following command is used to actually obtain the security certificate.
!A trustpoint NAME is used because there could be multiple trust points
!configured for the router.

```
Router(config)# crypto ca enrollment TP1
```

!The following command specifies that the secure HTTP client
!should use the certificate associated with the TP1 trustpoint for HTTPS connections.
Router(config)# **ip http client secure-trustpoint tp1**

Related Commands

Command	Description
crypto ca trustpoint	Specifies a name for a certificate authority trustpoint and enters CA trustpoint configuration mode.
primary	Indicates that the CA trustpoint being configured should be used as the primary (default) trustpoint.

ip http client source-interface

To configure a source interface for the HTTP client, use the **ip http client source-interface** command in global configuration mode. To change or disable the source interface, use the **no** form of this command.

ip http client source-interface *type number*

no ip http client source-interface

Syntax Description

<i>type</i>	Name of the source interface.
<i>number</i>	Number of the source interface.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use this command to specify a source interface to use for HTTP connections.

Examples

The following example shows how to configure the source interface as Ethernet 0/1:

```
Router(config)# ip http client source-interface Ethernet 0/1
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.

Command	Description
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client username	Configures a login name for all HTTP client connections.
show ip http client	Displays a report about the HTTP client.

ip http client username

To configure the default username used for connections to remote HTTP servers, use the **ip http client username** command in global configuration mode. To remove a configured default HTTP username from the configuration, use the **no** form of this command.

ip http client username *username*

no ip http client username

Syntax Description

<i>username</i>	String that is the username (login name) to be used in HTTP client connection requests sent to remote HTTP servers.
-----------------	---

Defaults

No default username exists for the HTTP connections.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to configure a default username before a file is copied to or from a remote web server using the **copy http://** or **copy https://** command. The default username will be overridden by a username specified in the URL of the **copy** command.



Note

The secure HTTP (HTTPS) client is not supported in Cisco IOS Release 12.2(31)SB.

Examples

In the following example, the default HTTP password is configured as Secret and the default HTTP username is configured as User1 for connections to remote HTTP or HTTPS servers:

```
Router(config)# ip http client password Secret
Router(config)# ip http client username User1
```

Related Commands

Command	Description
copy	Copies a file from any supported remote location to a local file system, or from a local file system to a remote location, or from a local file system to a local file system.
debug ip http client	Enables debugging output for the HTTP client.

Command	Description
ip http client cache	Configures the HTTP client cache.
ip http client connection	Configures the HTTP client connection.
ip http client password	Configures a password for all HTTP client connections.
ip http client proxy-server	Configures an HTTP proxy server.
ip http client response	Configures HTTP client characteristics for managing HTTP server responses to request messages.
ip http client source-interface	Configures a source interface for the HTTP client.
show ip http client	Displays a report about the HTTP client.

ip http digest algorithm

To configure the digest algorithm parameter, use the **ip http digest algorithm** command in global configuration mode.

ip http digest algorithm [*digest-algorithm*]

Syntax Description

<i>digest-algorithm</i>	(Optional) The digest algorithm method. The choices for the digest algorithm parameter are MD5 and MD5-sess. MD5 is the default.
-------------------------	--

Command Default

The digest algorithm parameter is set to MD5.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to change the digest algorithm parameter from MD5 to MD5-sess:

```
Device(config)# ip http digest algorithm md5-sess
```

ip http help-path

To configure the help root used to locate help files for use by the user's current GUI screen, use the **ip http help-path** command in global configuration mode.

ip http help-path *url*

Syntax Description	<i>url</i>	Uniform Resource Locator (URL) specifying the root for the location of help files used by the user's GUI screens. The currently configured complete path of the location of specific help files can be obtained from the output of the show ip http help-path user EXEC command.
---------------------------	------------	---

Command Default	No URL is specified.
------------------------	----------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.4(2)T	This command was introduced.

Usage Guidelines	The URL specified in this command must be populated with 'help' files with read access that are appropriate for the application that will be using the URL.
-------------------------	---

Examples	In the following example, the HTML files are located in the specified location on the system:
-----------------	---

```
Router(config)# ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
```

Related Commands	Command	Description
	ip http server	Enables the HTTP server, including the Cisco web browser user interface.
	show ip http-help path	Displays the IP HTTP help-path URL.

ip http max-connections

To configure the maximum number of concurrent connections allowed for the HTTP server, use the **ip http max-connections** command in global configuration mode. To return the maximum connection value to the default, use the **no** form of this command.

ip http max-connections *value*

no ip http max-connections

Syntax Description	<i>value</i>	An integer in the range from 1 to 16 that specifies the maximum number of concurrent HTTP connections. The default is 5.
---------------------------	--------------	--

Command Default	Five concurrent HTTP connections is the default.
------------------------	--

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.	
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.	
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.	

Usage Guidelines	<p>Platform-specific implementations can supersede the upper range limit of 16.</p> <p>If a new value is configured that is less than the previously configured value while the current number of connections exceeds the new maximum value, the HTTP server will not abort any of the current connections. However, the server will not accept new connections until the current number of connections falls below the new configured value.</p>
-------------------------	---

Examples	The following example shows how to configure the HTTP server to allow up to 10 simultaneous connections:
-----------------	--

```
Router(config)# ip http server
Router(config)# ip http max-connections 10
```

Related Commands	Command	Description
	ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http path

To specify the base path used to locate files for use by the HTTP server, use the **ip http path** command in global configuration mode. To remove the base path specification, use the **no** form of this command.

ip http path *url*

no ip http path

Syntax Description	<i>url</i>	Cisco IOS File System (IFS) URL specifying the location of the HTML files used by the HTTP server.
---------------------------	------------	--

Command Default The HTTP server is disabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines After enabling the HTTP server, you should set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

Examples In the following example, the HTML files are located in the default flash location on the system:

```
Router(config)# ip http path flash:
```

In the following example, the HTML files are located in the directory named web on the flash memory card inserted in slot 0:

```
Router(config)# ip http path slot0:web
```

Related Commands	Command	Description
	ip http server	Enables the HTTP server, including the Cisco web browser user interface.

ip http port

To specify the port number to be used by the HTTP server, use the **ip http port** command in global configuration mode. To return the port number to the default, use the **no** form of this command.

ip http port *port-number*

no ip http port

Syntax Description	<i>port-number</i>	The integer 80 or any integer in the range from 1025 to 65535 that specifies the port number to be used for the HTTP server. The default is 80.
---------------------------	--------------------	---

Command Default The HTTP server uses port 80.

Command Modes Global configuration (config)

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	This command was modified to restrict port numbers. The port number 443 is now reserved for secure HTTP (HTTPS) connections.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines HTTP port 80 is the standard port used by web servers.



Note

The secure HTTP (HTTPS) server is not supported in Cisco IOS Release 12.2(31)SB.

Examples The following example shows how to change the HTTP server port to port 8080:

```
Router(config)# ip http server
Router(config)# ip http port 8080
```

Related Commands

Command	Description
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip http secure-active-session-modules

To selectively activate HTTP Secure (HTTPS) services to process incoming HTTPS requests from remote clients, use the **ip http secure-active-session-modules** command in global configuration mode. To return to the default in which all HTTPS services are activated, use the **no** form of this command.

ip http secure-active-session-modules {*listname* | **all** | **none**}

no ip http secure-active-session-modules

Syntax Description

<i>listname</i>	List of specifically configured HTTPS services to activate.
all	Activates all HTTPS services.
none	Deactivates all HTTPS services.

Command Default

All HTTPS services are activated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **ip http secure-active-session-modules** command to activate or deactivate HTTPS services to process incoming HTTPS requests from remote clients. Use the **ip http session-module-list** command to define a list of HTTP or HTTPS services to be enabled.

If an HTTPS request is made for a service that is disabled, an error message is displayed in the remote client browser.

Examples

The following example shows how to configure different sets of services to be available for HTTP and HTTPS requests. In this example, all HTTP services are activated, but only the HTTPS services defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are activated.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http session-module-list	Defines a list of HTTP or HTTPS services.

ip http secure-ciphersuite

To specify the CipherSuites that should be used by the secure HTTP server when negotiating a connection with a remote client, use the **ip http secure-ciphersuite** command in global configuration mode. To return the configuration to the default set of CipherSuites, use the **no** form of this command.

```
ip http secure-ciphersuite [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]
```

```
no ip http secure-ciphersuite
```

Syntax Description

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA—Rivest, Shamir, and Adleman (RSA) key exchange with 3DES and DES-EDE3-CBC for message encryption and Secure Hash Algorithm (SHA) for message digest.
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and SHA for message digest.
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5 —RSA key exchange (RSA Public Key Cryptography) with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA—RSA key exchange with DES-CBC for message encryption and SHA for message digest.

Command Default

The HTTPS server negotiates the best CipherSuite using the list received from the connecting client.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to restrict the list of CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection. For example, you may want to allow only the most secure CipherSuites to be used.

Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

The supported CipherSuites vary by Cisco IOS software image. For example, “IP Sec56” (“k8”) images support only the SSL_RSA_WITH_DES_CBC_SHA CipherSuite in Cisco IOS Release 12.2(15)T.

In terms of router processing load (speed), the following list ranks the CipherSuites from fastest to slowest (slightly more processing time is required for the more secure and more complex CipherSuites):

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

Additional information about these CipherSuites can be found online from sources that document the Secure Sockets Layer (SSL) 3.0 protocol.

Examples

The following example shows how to restrict the CipherSuites offered to a connecting secure web client:

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

Related Commands

Command	Description
ip http secure-server	Enables the HTTPS server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-client-auth

To configure the secure HTTP server to authenticate connecting clients, use the **ip http secure-client-auth** command in global configuration mode. To remove the requirement for client authorization, use the **no** form of this command.

ip http secure-client-auth

no ip http secure-client-auth

Syntax Description

This command has no arguments or keywords.

Command Default

Client authentication is not required for connections to the secure HTTP server.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.

In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all web clients may be configured for certificate authority (CA) authentication.

Examples

In the following example the secure web server is enabled and the server is configured to accept connections only from clients with a signed security certificate:

```
Router(config)# no ip http server
Router(config)# ip http secure-server
Router(config)# ip http secure-client-auth
```

Related Commands

Command	Description
ip http secure-server	Enables the HTTPS server.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http secure-port

To set the secure HTTP (HTTPS) server port number for listening, use the **ip http secure-port** command in global configuration mode. To return the HTTPS server port number to the default, use the **no** form of this command.

ip http secure-port *port-number*

no ip http secure-port

Syntax Description

<i>port-number</i>	Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.
--------------------	--

Command Default

The HTTPS server port number is not set for listening.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

An HTTP server and an HTTPS server cannot use the same port. If you try to configure both on the same port, the following message is displayed:

```
% Port port_number in use by HTTP.
```

where *port_number* is the port number that is already assigned to the HTTP server.

If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format:

```
https://device:port_number
```

where *port_number* is the HTTPS port number.

Examples

The following example shows how to assign port 1025 for HTTPS server connections:

```
Router(config)# ip http secure-port 1025
```

Related Commands

Command	Description
ip http secure-server	Enables an HTTPS server.

ip http secure-server

To enable a secure HTTP (HTTPS) server, use the **ip http secure-server** command in global configuration mode. To disable an HTTPS server, use the **no** form of this command.

ip http secure-server

no ip http secure-server

Syntax Description This command has no arguments or keywords.

Command Default The HTTPS server is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.



Note

When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# ip http secure-server
Router(config)# ip http secure-trustpoint CA-trust-local
Router(config)# end
```

```
Router# show ip http server secure status
```

```
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip http secure-trustpoint

To specify the certificate authority (CA) trustpoint that should be used for obtaining signed certificates for a secure HTTP (HTTPS) server, use the **ip http secure-trustpoint** command in global configuration mode. To remove a previously specified CA trustpoint, use the **no** form of this command.

ip http secure-trustpoint *trustpoint-name*

no ip http secure-trustpoint *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	Name of a configured trustpoint. Use the same trustpoint name that was used in the associated crypto ca trustpoint command.
------------------------	--

Command Default

The HTTPS server uses the trustpoint configured when you use the **primary** command. If a trustpoint is not configured, the HTTPS server uses a self-signed certificate.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command specifies that the HTTPS server should use the X.509v3 certificate associated with the trustpoint indicated by the *trustpoint-name* argument. Use the same trustpoint name that you used in the associated **crypto ca trustpoint** command.

The specified X.509v3 security certificate will be used to authenticate the server to connecting clients, and, if remote client authentication is enabled, to authenticate the connecting clients.

Use this command only if you have already declared a CA trustpoint using the **crypto ca trustpoint** command and associated submode commands. If a trustpoint is not configured, the HTTPS server will use a self-signed certificate.

If this command is not used, the server will attempt to use the certificate associated with the primary trustpoint. The primary trustpoint is configured using the **primary** command.

Examples

In the following example, the CA trustpoint is configured, a certificate is obtained, and the certificate is referenced in the HTTPS server configuration:

```
!The following commands specifies a CA trustpoint that can be used
!to obtain a X.509v3 security certificate.
!A trustpoint NAME is used because there could be multiple trustpoints
!configured for the router.
```

```

Router(config)# crypto ca trustpoint tp1
Router(config-ca)# enrollment url http://host1:80
Router(config-ca)# exit
Router(config)# crypto ca authenticate tp1

```

!The following command is used to actually obtain the security certificate.

```

Router(config)# crypto ca enrollment tp1
Router(config)# ip http secure-server

```

!The following command specifies that the secure HTTP server should use a certificate associated with the TP1 trustpoint for HTTPS connections.

```

Router(config)# ip http secure-trustpoint tp1

```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your routing device should use.
ip http secure-server	Enables the HTTPS server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
show ip http server secure status	Displays the configuration status of the secure HTTP server.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled on the Cisco Catalyst 4000 series switch. The HTTP server is enabled for clustering on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

The HTTP server uses the standard port 80 by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	IPv6 support was added.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

With IPv6 support added in Cisco IOS Release 12.2(2)T, the **ip http server** command simultaneously enables and disables both IP and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command will only be applied to IPv4 traffic. IPv6 traffic filtering is not supported.



Caution

The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Examples

The following example shows how to enable the HTTP server on both IP and IPv6 systems:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.

ip http session-module-list

To define a list of HTTP or secure HTTP (HTTPS) application names, use the **ip http session-module-list** command in global configuration mode. To remove the defined list, use the **no** form of this command.

ip http session-module-list *listname prefix1 [prefix2,...,prefixn]*

no ip http session-module-list *listname prefix1 [prefix2,...,prefixn]*

Syntax Description

<i>listname</i>	Name of the list.
<i>prefix1</i>	Associated HTTP or HTTPS application names. Prefix strings represent the names of applications, for example, SCEP, WEB_EXEC or HOME_PAGE.
<i>prefix2,...,prefixn</i>	(Optional) Additional associated HTTP or HTTPS application names. Each application is separated by a comma.

Defaults

No list of HTTP or HTTPS application names is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use this command to define a list of HTTP or HTTPS application names. The defined list can then be used by the **ip http active-session-modules** or **ip http secure-active-session-modules** commands to selectively enable HTTP or HTTPS applications, respectively, for servicing incoming HTTP and HTTPS requests from remote clients.

When defining a list of HTTP or HTTPS application names, use the following guidelines:

- A maximum of four lists can be defined on a router or switch. Attempts to define more than four lists will fail and an error message will be displayed stating the limit restrictions.
- An existing list can be removed using the **no ip http session-module-list** command.
- You cannot reconfigure an existing list. Instead of reconfiguring an existing list, remove the existing list and create a new list with the same name.
- There is no limit to how many application names can be in the list. However, the maximum number of sessions that can be registered with the Cisco IOS HTTP or HTTPS server is 32.



Note

The HTTPS server is not supported in Cisco IOS Release 12.2(31)SB.

Examples

The following example shows how to configure a different set of services to be available for HTTP and HTTPS requests. In this example, all HTTP applications are enabled for providing services to remote clients, but for HTTPS services, only the HTTPS applications defined in list1 (Simple Certificate Enrollment Protocol [SCEP] and HOME_PAGE) are enabled.

```
ip http session-module-list list1 SCEP,HOME_PAGE
ip http active-session-modules all
ip http server
ip http secure-server
ip http secure-active-session-modules list1
```

Related Commands

Command	Description
ip http active-session-modules	Selectively enables HTTP applications that will service incoming HTTP requests from remote clients.
ip http secure-active-session-modules	Selectively enables HTTPS applications that will service incoming HTTPS requests from remote clients.
show ip http server	Displays details about the current configuration of the HTTP server.

ip http timeout-policy

To configure the parameters for closing connections to the local HTTP server, use the **ip http timeout-policy** command in global configuration mode. To return the parameters to their defaults, use the **no** form of this command.

ip http timeout-policy idle *seconds* **life** *seconds* **requests** *value*

no ip http timeout-policy

Syntax Description

idle	Specifies the maximum number of seconds that a connection will be kept open if no data is received or response data cannot be sent out.
life	Specifies the maximum number of seconds that a connection will be kept open from the time the connection is established.
<i>seconds</i>	When used with the idle keyword, an integer in the range of 1 to 600 that specifies the number of seconds (10 minutes maximum). The default is 180 (3 minutes). When used with the life keyword, an integer in the range of 1 to 86400 that specifies the number of seconds (24 hours maximum). The default is 180 (3 minutes).
requests	Specifies that a maximum limit is set on the number of requests processed on a persistent connection before it is closed.
<i>value</i>	Integer in the range from 1 to 86400. The default is 1.

Defaults

HTTP server connection idle time: 180 seconds (3 minutes)

HTTP server connection life time: 180 seconds (3 minutes)

HTTP server connection maximum requests: 1

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command sets the characteristics that determine how long a connection to the HTTP server should remain open.

This command may not take effect immediately on any HTTP connections that are open at the time you use this command. In other words, new values for idle time, life time, and maximum requests will apply only to connections made to the HTTP server after this command is issued.

A connection may be closed sooner than the configured idle time if the server is too busy or the limit on the life time or the number of requests is reached.

Also, since the server will not close a connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes.

A connection may be closed before the maximum number of requests are processed if the server is too busy or the limit on the idle time or life time is reached.

The **ip http timeout-policy** command allows you to specify a general access policy to the HTTP server by adjusting the connection timeout values. For example, if you want to maximize throughput for HTTP connections, you should configure a policy that minimizes connection overhead. You can do this by specifying large values for the **life** and **requests** options so that each connection stays open longer and more requests are processed for each connection.

Another example would be to configure a policy that minimizes the response time for new connections. You can do this by specifying small values for the **life** and **requests** options so that the connections are quickly released to serve new clients.

A throughput policy would be better for HTTP sessions with dedicated management applications, as it would allow the application to send more requests before the connection is closed, while a response time policy would be better for interactive HTTP sessions, as it would allow more people to connect to the server at the same time without having to wait for connections to become available.

In general, you should configure these options as appropriate for your environment. The value for the **idle** option should be balanced so that it is large enough not to cause an unwanted request or response timeout on the connection, but small enough that it does not hold a connection open longer than necessary.

Examples

In the following example, a Throughput timeout policy is applied. This configuration would allow each connection to be idle for a maximum of 30 seconds (approximately). Each connection will remain open (be “alive”) until either the HTTP server has been busy processing requests for approximately 2 minutes (120 seconds) or until approximately 100 requests have been processed.

```
Router(config)# ip http timeout-policy idle 30 life 120 requests 100
```

In the following example, a Response Time timeout policy is applied. This configuration would allow each connection to be idle for a maximum of 30 seconds (approximately). Each connection will be closed as soon as the first request has been processed.

```
Router(config)# ip http timeout-policy idle 30 life 30 requests 1
```

Related Commands

Command	Description
ip http server	Enables the HTTP server, including the Cisco web browser user interface.

kron occurrence

To specify schedule parameters for a Command Scheduler occurrence and enter kron-occurrence configuration mode, use the **kron occurrence** command in global configuration mode. To delete a Command Scheduler occurrence, use the **no** form of this command.

kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays:*] *numhours:*] *nummin* | **at** *hours:min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring** | **system-startup**}

no kron occurrence *occurrence-name* [**user** *username*] {**in** [[*numdays:*] *numhours:*] *nummin* | **at** *hours:min* [[*month*] *day-of-month*] [*day-of-week*]} {**oneshot** | **recurring** | **system-startup**}

Syntax Description

<i>occurrence-name</i>	Name of the occurrence. The length of <i>occurrence-name</i> is from 1 to 31 characters. If the <i>occurrence-name</i> is new, an occurrence structure will be created. If the <i>occurrence-name</i> is not new, the existing occurrence will be edited.
user	(Optional) Identifies a particular user.
<i>username</i>	(Optional) Name of the user.
in	Indicates that the occurrence is to run after a specified time interval. The timer starts when the occurrence is configured.
<i>numdays:</i>	(Optional) Number of days. If used, add a colon after the number.
<i>numhours:</i>	(Optional) Number of hours. If used, add a colon after the number.
<i>nummin</i>	Number of minutes.
at	Indicates that the occurrence is to run at a specified calendar date and time.
<i>hours:</i>	Hour as a number using the twenty-four hour clock. Add a colon after the number.
<i>min</i>	Minute as a number.
<i>month</i>	(Optional) Month name. If used, you must also specify <i>day-of-month</i> .
<i>day-of-month</i>	(Optional) Day of month as a number.
<i>day-of-week</i>	(Optional) Day of week name.
oneshot	Indicates that the occurrence is to run only one time. After the occurrence has run, the configuration is removed.
recurring	Indicates that the occurrence is to run on a recurring basis.
system-startup	Indicates that the occurrence is to run on system startup, in addition to the recurring or oneshot occurrences.

Command Default

No schedule parameters are specified.

Command Modes

Global configuration (config)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(15)T	The system-startup keyword was added. The user keyword and <i>username</i> argument were removed from this command in Cisco IOS Release 12.4(15)T.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Prior to Cisco IOS Release 12.4, when you configured a kron occurrence for a calendar time when the system clock was not set, you received a printf message stating that the clock was not set and the occurrence would not be scheduled until it was set.

Beginning in Cisco IOS Release 12.4, when you configure a kron occurrence for a calendar time when the system clock is not set, the occurrence is scheduled but a printf message appears stating that the clock is not set and that it currently reads <current clock time>.

If you set the clock, the schedule of the occurrence is affected in one of the following ways:

- A new clock time set for less than 3 hours after the occurrence is scheduled to happen causes the occurrence to happen immediately.
- A new clock time set for less than 3 hours before the occurrence is scheduled to happen causes the occurrence to happen as scheduled.
- A new clock time set for more than 3 hours after the occurrence is scheduled to happen causes the occurrence to be rescheduled for the next regular calendar time.
- A new clock time set for more than 3 hours before the occurrence is scheduled to happen causes the occurrence to be rescheduled for the previous regular calendar time.

Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time.

Use the **show kron schedule** command to display the name of each configured occurrence and when it will next run.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a Command Scheduler occurrence named info-three and schedule it to run every three days, 10 hours, and 50 minutes. The EXEC CLI in the policy named three-day-list is configured to run as part of occurrence info-three.

```
Router(config)# kron occurrence info-three user IT2 in 3:10:50 recurring
Router(config-kron-occurrence)# policy-list three-day-list
```

The following example shows how to create a Command Scheduler occurrence named auto-mkt and schedule it to run once on June 4 at 5:30 a.m. The EXEC CLI in the policies named mkt-list and mkt-list2 are configured to run as part of occurrence auto-mkt.

```
Router(config)# kron occurrence auto-mkt user marketing at 5:30 jun 4 oneshot  
Router(config-kron-occurrence)# policy-list mkt-list  
Router(config-kron-occurrence)# policy-list mkt-list2
```

Related Commands

Command	Description
cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.
show kron schedule	Displays the status and schedule information for Command Scheduler occurrences.

kron policy-list

To specify a name for a Command Scheduler policy and enter kron-policy configuration mode, use the **kron policy-list** command in global configuration mode. To delete the policy list, use the **no** form of this command.

kron policy-list *list-name*

no kron policy-list *list-name*

Syntax Description

<i>list-name</i>	String from 1 to 31 characters that specifies the name of the policy.
------------------	---

Command Default

If the specified list name does not exist, a new policy list is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy containing EXEC command-line interface (CLI) commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

When the *list-name* is new, a policy list structure is created. When the *list-name* is not new, the existing policy list is edited.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to create a policy named sales-may and configure EXEC CLI commands to run the CNS command that retrieves an image from a server:

```
Router(config)# kron policy-list sales-may
Router(config-kron-policy)# cli cns image retrieve server https://10.21.2.3/imgsvr/ status
https://10.21.2.5/status/
```

Related Commands	Command	Description
	cli	Specifies EXEC CLI commands within a Command Scheduler policy list.
	kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.
	policy-list	Specifies the policy list associated with a Command Scheduler occurrence.