tacacs-server administration through title-color

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server**command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*

no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.

Command	Description
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection **(TACACS+)**	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout **(TACACS+)**	Configures the time to wait for a reply from the specified TACACS server.

tacacs-server administration

To enable the handling of administrative messages by the TACACS+ daemon, use the **tacacs-server administration** command in global configuration mode. To disable the handling of administrative messages by the TACACS+ daemon, use the **no** form of this command.

tacacs-server administration

no tacacs-server administration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 shows that the TACACS+ daemon is enabled to handle administrative messages:

```
tacacs-server administration
```

tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request**command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

tacacs-server directed-request [restricted] [no-truncate]

no tacacs-server directed-request

Syntax Description

restricted	(Optional) Restrict queries to directed request servers only.
no-truncate	(Optional) Do not truncate the @hostname from the username.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

Examples

The following example disables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

tacacs-server dns-alias-lookup

To enable IP Domain Name System (DNS) alias lookup for TACACS+ servers, use the command in global configuration mode. To disable IP DNS alias lookup, use the **no** form of this command.

tacacs-server dns-alias-lookup

no tacacs-server dns-alias-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IP DNS alias lookup is disabled.

Command Modes

global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 shows that IP DNS alias lookup has been enabled:

```
tacacs-server dns-alias-lookup
```

tacacs-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote TACACS+ server, use the **tacacs-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the no form of this command.

tacacs-server domain-stripping [**[right-to-left]** [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]]| **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no tacacs-server domain-stripping [**[right-to-left]** [**prefix-delimiter** *character* [*character2 ... character7*]] [**delimiter** *character* [*character2 ... character7*]]| **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name*argument specifies the name of a VRF.

Command Default Stripping is disabled. The full username is sent to the TACACS+ server.

Command Modes Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
XE 2.5	This command was integrated into Cisco IOS Release XE 2.5.

Usage Guidelines Use the **tacacs-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the TACACS+ server. If the full username is user1@cisco.com, enabling the **tacacs-server domain-stripping** command results in the username "user1" being forwarded to the TACACS+ server.

Use the **right-to-left**keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the TACACS+ server. Configuring the **right-to-left**keyword would result in the username "user@cisco.com" being forwarded to the TACACS+ server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix*to specify a particular suffix to strip from usernames. For example, configuring the **tacacs-server domain-stripping strip-suffix cisco.net**command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **tacacs-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **tacacs-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter**keyword.

Note Issuing the **no tacacs-server host** command reconfigures the TACACS server host information. You can view the contents of the current running configuration file using the **show running-config** command.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **tacacs-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]]command.
- You may configure multiple instances of the **tacacs-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **tacacs-server domain-stripping strip-suffix** *suffix*[**vrf** *per-vrf*]command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **tacacs-server domain-stripping**command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example shows how to configure the router to parse the username from right to left and set the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username "cisco/user@cisco.com" will be forwarded to the TACACS+ server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
tacacs-server domain-stripping right-to-left delimiter @\$
```

The following example shows how to configure the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
tacacs-server domain-stripping vrf abc
```

The following example shows how to enable prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example shows how to enable prefix stripping, specify the character / as the prefix delimiter, and specify the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username "user@cisco.com" will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter / delimiter #
```

The following example shows how to enable prefix stripping, configure the character / as the prefix delimiter, configure the characters $, @, and # as suffix delimiters, and configure per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the

TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username "user@cisco.com" will be forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure the router to parse the username from right to left and enable suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
tacacs-server domain-stripping right-to-left
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
tacacs-server domain-stripping strip-suffix cisco.com
!
tacacs-server domain-stripping prefix-delimiter # vrf myvrf
tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
radius-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the RADIUS server.

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host {*hostname* | *host-ip-address*} [**key** *string*] [**[nat]** [**port** [*integer*]] **[single-connection]** [**timeout** [*integer*]]]

no tacacs-server host {*hostname* | *host-ip-address*}

Syntax Description

hostname	Name of the host.
host-ip-address	IP address of the host.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command **tacacs-server key** for this server only.
string	(Optional) Character string specifying authentication and encryption key. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
port	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
integer	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Command Default No TACACS+ host is specified.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	This command was modified. The **nat** keyword was added.
12.2(8)T	This command was modified. The **nat** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key**, **single-connection**, and **nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples The following example shows how to specify a TACACS+ host named Sea_Change:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs-server host Sea_Change
```

The following example shows how to specify that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
Device> enable
Device# configure terminal
```

```
Device(config)# aaa new-model
Device(config)# tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
password encryption aes	Enables a type 6 encrypted preshared key.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key {**0** *string* | **6** *string* | **7** *string* | *string*}

no tacacs-server key {**0** *string* | **6** *string* | **7** *string* | *string*}

Syntax Description

0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an advanced encryption scheme (AES) encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (clear text) shared key.

Command Default

This authentication encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.3(2)T	This command was modified. The **0** *string* and **7** *string* keywords and argument pairs were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SX	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.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to set the authentication and encryption key to cisco123:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs-server key cisco123
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs-server host	Specifies a TACACS+ host.

tacacs-server packet

To specify the maximum size of TACACS+ packets, use the **tacacs-server packet**command in global configuration mode. To disable, use the **no** form of this command.

tacacs-server packet maxsize *size*

no tacacs-server packet maxsize

Syntax Description

maxsize *size*	Specifies maximum TACACS+ packet size. The range is from 10240 to 65536.

Command Default

The default maximum size for a TACAC+ packet is 65536.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced in a release earlier than Cisco IOS Release 12.0
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(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 shows how to set the the maximum TACACS+ packet size to 10240:

```
tacacs-server packet maxsize 10240
```

tacacs-server timeout

To set the interval for which the TACACS server waits for a server host to reply, use the **tacacs-server timeout** command in global configuration mode. To restore the default timeout interval, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description

seconds	Timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval for which the server waits for the server host to reply is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	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

Use the **tacacs-server timeout**command to set the interval for which the server waits for a server host to reply. A TCP connection between the server and the host times out during higher loads. Therefore, to delay TCP timeouts, change the timeout interval to 30 seconds. You can also configure the **tacacs-server host** command with the **single-connection** keyword to delay TCP timeouts.

Examples

The following example shows how to set the timeout interval to 20 seconds:

```
Router# configure terminal
Router(config)# tacacs-server timeout 20
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

tag cts sgt

To enable Cisco TrustSec (CTS) SGT inline tagging in a GDOI group IPsec SA, use the **tag cts sgt** command in GDOI SA IPsec configuration mode.

tag cts sgt

Syntax Description

This command has no arguments or keywords.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
15.3(2)T	This command was introduced.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

CTS maintains classification of each packet by tagging packets on ingress to the CTS network, so that they can be properly identified for applying security and other policy criteria along the data path.

You use this command on a key server (KS) or primary KS.

Because GET VPN is a technology that is based on groups, all devices in the same group (including the KS, cooperative KSs, and GMs) must support CTS SGT inline tagging before the group's KS can enable the feature. If you want to enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software by using the **show crypto gdoi feature cts-sgt** command on the KS or primary KS.

If incompatible devices exist in the group when you use this command, the following message appears:

```
WARNING for group GET-SGT: some devices cannot support SGT inline tagging. Rekey can cause
 traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
sgt'.
Are you sure you want to proceed ? [yes/no]:
```

After you use this command, you must use the **crypto gdoi ks rekey** command on the KS or primary KS to trigger a rekey.

Examples

The following example shows how to configure CTS SGT inline tagging in an IPsec SA for a KS serving a single GDOI group:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
```

```
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

Related Commands

Command	Description
crypto gdoi ks rekey	Triggers a rekey of group members in a GET VPN network.
show crypto gdoi feature cts-sgt	Displays whether each device in the GET VPN network supports CTS SGT inline tagging, and displays the version of GET VPN software running on each device.

target-value

To define the target value rating for a host, use the **target-value**command in configuration rule configuration mode. To change the target value rating or revert to the default value, use the **no** form of this command.

target-value{**mission-critical**| **high**| **medium**| **low**}**target-address** *ip-address* [*/nn*| **to***ip-address*]

notarget-value{**mission-critical**| **high**| **medium**| **low**}**target-address** *ip-address* [*/nn*| **to***ip-address*]

Syntax Description

mission-critical | **high** | **medium** | **low**	Rates how important the system is to the network.
target-address *ip-address* [*/ nn* | **to** *ip-address*	A host, which can consist of a single IP address or a range of IP addresses.

Command Default

medium

Command Modes

Configuration rule configuration (config-rul)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **target-value**command to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS Intrusion Prevention System (IPS). A host can be a single IP address or a range of IP addresses with an associated target value rating.

Note Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location**command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

tcp finwait-time

To specify how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange, use the **tcp finwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp finwait-time *seconds* [**ageout-time** *seconds*]

no tcp finwait-time

Syntax Description

seconds	Amount of time, in seconds, that a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default management time is 5 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

In a TCP connection, the client and the server terminate their end of the connection by sending a finish (FIN) message. The time the client and the server wait for their FIN message to be acknowledged by the other side before closing the sequence during a TCP connection is called the finwait-time. The timeout that you set for the finwait-time is referred to as the finwait timeout.

When the software detects a valid TCP packet that is the first in a session, it establishes state information for the new session.

Use the **tcp finwait-time** command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close. The global value specified for the timeout applies to all TCP sessions.

When you configure an inspect parameter map, you can enter the **tcp finwait-time** command only after you enter the **parameter-map type inspect** command.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example show how to change the finwait timeout to 20 seconds:

```
parameter-map type inspect eng_network_profile
 tcp finwait-time 20
```

The following example show how to change the finwait idle timeout to 40 seconds:

```
parameter-map type inspect eng_network_profile
 tcp finwait-time 20 ageout-time 40
```

Related Commands

Command	Description
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp half-close reset

To specify whether the TCP reset (RST) segment should be sent when a half-close session is cleared, use the **tcp half-close reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when a half-close session is cleared, use the **no** form of this command.

tcp half-close reset {**off**| **on**}

no tcp half-close reset {**off**| **on**}

Syntax Description

off	Disables TCP half-close RST segment transmission.
on	Enables on TCP half-close RST segment transmission.

Command Default

The TCP reset segment is sent when a half-close session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end of the connection. This TCP state is called the half-close state. A session enters the half-close state when it receives the first TCP finish (FIN) segment and starts a timer. If another segment is received before the session timeout occurs, then the timer is restarted.

You can set the timeout value for a half-close session by using the **tcp synwait-time** command. The default timeout value is 30 seconds.

When you configure an inspect type parameter map, you can enter the **tcp half-close reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp half-close reset on** command, the TCP RST segment is sent to both ends of the half-close session when half-close session is cleared. If you configure the **tcp half-close reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to configure TCP half-close RST segment transmission:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp half-close reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

tcp half-open reset

To specify whether the TCP reset (RST) segment should be sent when a half-open session is cleared, use the **tcp half-open reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when a half-open session is cleared, use the **no** form of this command.

tcp half-open reset {**off**| **on**}

no tcp half-open reset {**off**| **on**}

Syntax Description

off	Disables TCP half-open RST segment transmission.
on	Enables TCP half-open RST segment transmission.

Command Default

The TCP reset segment is sent when a half-open session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

A half-open session is an unestablished session that is initiated by a TCP synchronization (SYN) segment but has an incomplete three-way handshake. A timer is started as soon as the incomplete three-way handshake occurs.

Note You can set the timeout value for a half-open session by using the **tcp synwait-time** command. The default timeout value is 30 seconds.

When you configure an inspect type parameter map, you can enter the **tcp half-open reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp half-open reset on** command, the TCP RST segment is sent to both ends of the half-open session when the half-open session is cleared. If you configure the **tcp half-open reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to configure TCP half-open RST segment transmission:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp half-open reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

tcp idle-time

To configure the amount of time a TCP session will still be managed while there is no activity, use the **tcp idle-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp idle-time *seconds* [**ageout-time** *seconds*]

no tcp idle-time

Syntax Description

seconds	Amount of time, in seconds, during which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour). Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default time is 3600 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

When you configure an inspect parameter map, you can enter the **tcp idle-time** command after you enter the **parameter-map type inspect** command.

When the software detects a valid TCP packet that is the first in a session, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not manage state information for the session.

The value specified for this timeout applies to all TCP sessions.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to set the TCP timeout to 90 seconds:

```
parameter-map type inspect eng-network-profile
 tcp idle-time 90
```

The following example shows how to set the TCP ageout time to 70 seconds:

```
parameter-map type inspect eng-network-profile
 tcp idle-time 90 ageout-time 70
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time during which a TCP session will still be managed while there is no activity).
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp idle reset

To specify whether the TCP reset (RST) segment should be sent when an idle session is cleared, use the **tcp idle reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when an idle session is cleared, use the **no** form of this command.

tcp idle reset {**off**| **on**}

no tcp idle reset {**off**| **on**}

Syntax Description

off	Disables TCP idle session RST segment transmission.
on	Enables TCP idle session RST segment transmission.

Command Default

The TCP RST segment is sent when an idle session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

An idle session is a TCP session that is active between two devices even when no data is transmitted by either device for a prolonged period of time.

Note You can set the timeout value for an idle session by using the **tcp idle-time** command . The default timeout value for idle sessions is 3600 seconds.

When an idle TCP session is cleared, the TCP RST segment is sent and the session is reset if the TCP reset segment control is configured on the session.

When you configure an inspect type parameter map, you can enter the **tcp idle reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp idle reset on** command, the TCP RST segment is sent to both ends of the idle session when the session is cleared. If you configure the **tcp idle reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to send a TCP RST segment when an idle session is cleared:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp idle reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp idle-time	Configures the timeout for TCP sessions.

tcp max-incomplete

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the **tcp max-incomplete** command in parameter-map type inspect configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

tcp max-incomplete host *threshold* [**block-time** *minutes*]

no tcp max-incomplete

Syntax Description

host *threshold*	Number of half-open TCP sessions with the same host destination address that can simultaneously exist before the software starts deleting half-open sessions to the host. The range is from 1 to 2147483647. The default is unlimited.
block-time *minutes*	(Optional) Amount of time, in minutes, the software prevents connections to the host. The default is 0.

Command Default

The thresholds is unlimited, and the blocking time value is 0.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **tcp max-incomplete** command after you enter the **parameter-map type inspect** command.

After the specified threshold is exceeded, the router drops packets.

Half-open means that the session has not reached the established state.An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.

When the number of half-open sessions with the same destination host address rises above a threshold (the host threshold number), the software deletes half-open sessions according to one of the following methods.

- If the **block-time** *minutes* timeout is 0 (the default):

The software deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host never exceeds the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software deletes all existing half-open sessions for the host and then blocks all new connection requests to the host. The software continues to block all new connection requests until the block-time expires.

The software also sends syslog messages whenever the specified threshold is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections that Cisco IOS stateful packet inspection inspects.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specifiy a maximum of 100 half-open sessions and a block time of 10 minutes. If a single host receives 400 half-open sessions, subsequent connections after 100 will be dropped. If a host receives 50 connections and another host receives 50 connections, no packets are dropped.

```
parameter-map type inspect eng-network-profile
 tcp max-incomplete host 100 block-time 10
```

Related Commands

Command	Description
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
max-incomplete aggressive-aging	Configures aggressive aging of half-open firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp reassembly

To change the default parameters for Out-of-Order (OoO) queue processing of TCP sessions, use the **tcp reassembly** command in parameter-map type configuration mode. To revert to the default parameters, use the **no** form of this command.

tcp reassembly {**alarm** {**on | off**} | **queue length** *queue-length* | **timeout** *seconds*}

no tcp reassembly {**alarm** {**on | off**} | **queue length** *queue-length* | **timeout** *seconds*}

Syntax Description

alarm {**on** | **off**}	Enables or disables the alert message configuration for OoO packets. The default is off.
queue length *queue-length*	Specifies the length of OoO queues. The range is from 0 to 1024. The default is 16.
timeout *seconds*	Specifies the timeout for OoO queues in seconds. The range is from 1 to 3600. The default is 5.

Command Default

Alert messages are disabled, the default OoO queue length is 16, and the default timeout for OoO queues is 5 seconds.

Command Modes

Parameter-map type configuration mode (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If the TCP queue length is set to 0, the TCP OoO packet buffering and reassembly is disabled.

If the TCP alarm is enabled, a syslog message is generated when an OoO packet is dropped.

Examples

The following example shows how to configure parameters for OoO queue processing of TCP sessions:

```
Device# configure terminal
Device(config)# parameter-map type ooo global
Device(config-profile)# tcp reassembly alarm on
Device(config-profile)# tcp reassembly queue length 89
```

Related Commands

parameter-map type ooo global	Configures an OoO global parameter map for all firewall policies.

show parameter-map type ooo global	Displays OoO global parameter-map information.
tcp reassembly memory limit	Specifies the limit of the OoO queue size for TCP sessions.

tcp reassembly memory limit

To specify the limit of the out-of-order (OOO) queue size for TCP sessions, use the **tcp reassembly memory limit** command in parameter map type OOO global configuration mode. To disable the configuration, use the **no** form of this command.

tcp reassembly memory limit *queue-size*

no tcp reassembly memory limit

Syntax Description

queue-size	Queue size, in kilobytes (KB). The range is from 1 to 4194303.

Command Default

The default OOO queue size is 1024 KB.

Command Modes

Parameter map type OOO global configuration (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)T	This command was modified. The maximum limit value for the *queue-size*argument was changed from 4294967295 to 4194303.

Usage Guidelines

You must use the **tcp reassembly memory limit** command to specify the limit of the OOO queue size for TCP sessions when the deep packet inspection feature is configured on the router.

Examples

The following example shows how to specify 200 KB as the OOO queue size for TCP sessions:

```
Router(config)# parameter-map type ooo global
Router(config-profile)# tcp reassembly memory limit
 200
```

Related Commands

Command	Description
tcp reassembly queue length	Specifies the length of the OOO queue parameters.
tcp reassembly timeout	Specifies the timeout for the OOO TCP queues.

Command	Description
tcp reassembly alarm	Specifies the alert message configuration for the TCP sessions.

tcp syn-flood limit

To configure a limit to the number of TCP half-open sessions before triggering synchronization (SYN) cookie processing for new SYN packets, use the **tcp syn-flood limit**command in profile configuration mode. To disable the configuration, use the **no** form of this command.

tcp syn-flood limit *maximum-session-limit*

no tcp syn-flood limit *maximum-session-limit*

Syntax Description

maximum-session-limit	Maximum number of sessions. Valid values are from 1 to 4294967295.

Command Default

No limit to the number of TCP half-open sessions are set.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

A TCP half-open session is a session that has not reached the established state.

In a VRF-aware firewall, you can configure a limit to the number of TCP half-open sessions for each VRF. At both the global level and at the VPN Routing and Forwarding (VRF) level, when the configured TCP SYN flood limit is reached, the TCP SYN cookie verifies the source of the half-open sessions before creating more sessions.

You must configure the **parameter-map type inspect-vrf** or the **parameter-map type inspect global**command before you can configure the **tcp syn-flood limit** command.

Examples

The following example shows how to limit the number of TCP half-open sessions to 500 at an inspect-VRF parameter map level:

```
Router(config)# parameter-map type inspect-vrf
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

The following example shows how to limit the number of TCP half-open sessions to 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood limit 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.
parameter-map type inspect-vrf	Configures a parameter map of type inspect VRF and enters profile configuration mode.

tcp syn-flood rate per-destination

To configure a TCP synchronization (SYN) flood rate limit for each destination address, use the **tcp syn-flood rate per-destination** command in profile configuration mode. To disable TCP SYN flood packets, use the **no** form of this command.

tcp syn-flood rate per-destination *maximum-packet-rate*

no tcp syn-flood rate per-destination *maximum-packet-rate*

Syntax Description

maximum-packet-rate	Maximum rate of TCP SYN packets. Valid values are from 1 to 1000000000.

Command Default

No TCP SYN-flood packets are configured.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.

You must configure the **parameter-map type inspect-zone** or the **parameter-map type global**command before you can configure the **tcp syn-flood rate per-destination** command.

Examples

The following example shows how to configure the TCP SYN-flood packet rate of 500 at an inspect-zone parameter map level:

```
Router(config)# parameter-map type inspect-zone
Router(config-profile)# tcp syn-flood rate per-destination 500
Router(config-profile)# end
```

The following example shows how to configure the TCP SYN-flood packet rate of 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood rate per-destination 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.
parameter-map type inspect-zone	Configures a parameter map of type inspect zone and enters profile configuration mode.

tcp synwait-time

To specify how long the software will wait for a TCP session to reach the established state before dropping the session, use the **tcp synwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp synwait-time *seconds* [**ageout-time** *seconds*]

no tcp synwait-time

Syntax Description

seconds	Time, in seconds, that the system will wait for a TCP session to reach the established state before dropping the session. The default is 30. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default TCP synchronization (SYN) wait time is 30 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

You must configure the **parameter-map type inspect** command before you can configure the **tcp synwait-time** command.

Examples

The following example shows how to specify that the TCP session will be dropped if the TCP session does not reach the established state in 3 seconds:

```
parameter-map type inspect eng-network-profile
 tcp synwait-time 3
```

The following example shows how to specify the aging out time after which the TCP session will be dropped:

```
parameter-map type inspect eng-network-profile
 tcp synwait-time 3 ageout-time 20
```

Related Commands

Command	Description
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp window-scale-enforcement loose

To disable the checking of the TCP window-scale option in a Zone-Based Policy Firewall, use the **tcp window-scale-enforcement loose** command in parameter-map type inspect configuration mode. To return to the command default, use the **no** form of this command.

tcp window-scale-enforcement loose

no tcp window-scale-enforcement loose

Syntax Description

This command has no arguments or keywords.

Command Default

A strict window-scale option check is enabled on the firewall.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S

Usage Guidelines

The window-scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header. The firewall enforces the strict checking of the TCP window scale option. See RFC 1323 for more information on this function.

Sometimes server uses a non-RFC compliant TCP/IP protocol stack. In this case, the intiator does not offer the window-scale option, but the responder has the option enabled with a window-scale factor that is not zero.

Network administrators who experience issues with a noncompliant server may not have control over the server to which they need to connect. Disabling the firewall to connect to a noncompliant server is not desirable and may fail if each endpoint cannot agree on the window-scaling factor to use for its respective receive window.

Use the **tcp window-scale-enforcement loose** command in parameter-map type inspect configuration mode to allow noncompliant window scale negotiation and to ensure the window-scale option works without the firewall being disabled to access the noncompliant servers. This command is used by the firewall, which provides a unidirectional firewall policy between groups of interfaces known as zones.

Examples

The following example shows how to disable the window scale option check in the Zone-Based Firewall parameter map for a TCP packet that has an invalid window scale option:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
```

```
Device(config-profile)# tcp window-scale-enforcement loose
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

host	A hostname or an IP address.
port	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
keyword	(Optional) One of the keywords listed in the table below.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	The **/ipv4** and **/ipv6** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The table below lists the optional **telnet** command keywords.

Table 1: telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: *path*	Specifies loose source routing. The *path* argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.

Option	Description
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
port-number	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.

Option	Description
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname--as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. The table below lists the special Telnet escape sequences.

Table 2: Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

1 The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt: **Ctrl-^ ?**

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router>

telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1* :

```
router>
telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router>
host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router>

telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

template (identity policy)

To specify a virtual template from which commands may be cloned, use the **template** command in identity policy configuration mode. To disable the virtual template, use the **no** form of this command.

template {**virtual-template** *template-number*}

notemplate {**virtual-template** *template-number*}

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
template-number	Template interface number. The value ranges from 1 through 200.

Command Default

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity policy**command must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that an identity policy and a template have been specified:

```
Router (config)# identity policy mypolicy
Router (config-identity-policy)# template virtual-template 1
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

template (identity profile)

To specify a virtual template from which commands may be cloned, use the **template** command in identity profile configuration mode. To disable the virtual template, use the **no** form of this command.

template *virtual-template*

no template *virtual-template*

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.

Command Default

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **identity profile command and default**keyword must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that a default identity profile and a template have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# template virtualtemplate1
```

Related Commands

Command	Description
description	Enters an identity profile description.
device	Statically authorizes or rejects individual devices.
identity profile	Creates an identity profile.

template config

To specify a remote URL for a Cisco IOS command-line interface (CLI) configuration template, use the **template config** command in tti-registrar configuration mode. To remove the template from the configuration and use the default configuration template, use the **no** form of this command.

template config *url* **[post]**

no template config *url*

Syntax Description

url	One of the keywords in the table below.
post	(Optional) Specifies that the registrar will issue an HTTP POST to the external management system. The HTTP POST will include information about the device such as the device name, the current Cisco IOS version, and the current configuration in order for the external management system to return a Cisco IOS configuration more specific to the device. **Note** Common Gateway Interface (CGI) scripts must be issued with the **post** keyword.

Command Default

A default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **post** keyword was added.

Usage Guidelines

Use the **template config** command to specify a URL in which to retrieve the template that will be sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

If neither a configuration template nor the **post** keyword is specified, the default configuration template is used. The default configuration template contains the following commands:

```
!
$t
!
$c
!
```

```
! end
END_CONFIG
;
```

The variable "$t" will be expanded to include a Cisco IOS public key infrastructure (PKI) trustpoint that is configured for autoenrollment with the certificate server of the registrar. The variable "$c" will be expanded into the correct certificate chain for the certificate server of the registrar.

If an external template is specified, it must include the "$t" and "$c" variables to enable the petitioner device to obtain a certificate. The **end** command must be specified. If you want to specify details about the trustpoint, you can specify a template as follows:

```
!
crypto ca trustpoint $t
 enrollment url http://<registrar fqdn>
 rsakeypair $k $s
 auto-enroll 70
!
$c
end
```

Where $t comes from "trustpoint" configured under the petitioner, $k comes from "rsakeypair" under the trustpoint:

```
! $l will be replaced by 'mytp.'
crypto provisioning petitioner
  trustpoint mytp
! $k will be replaced by 'mykey.'
crypto ca trustpoint mytp
rsakeypair mykey
!
```

Note The template configuration location may include a variable "$n", which is expanded to the name of the introducer.

The table below lists the available options for the *url* argument.

Table 3: URL Keywords for the CLI Template

Keyword	Description
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server (also called a web server).
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.

Keyword	Description
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tftp:	Retrieves from a TFTP network server.
webflash:	Retrieves from the file system.
xmodem:	Retrieves from a network machine that uses the Xmodem protocol.

Expanded SDP CGI Template Support

Expanded SDP CGI template support allows you to specify a bootstrap configuration based on the client type, model, Cisco IOS version, and current configuration. Specifying a boot strap configuration is accomplished by the TTI registrar forwarding the device information to the external management system when requesting a bootstrap configuration.

The **template config** command with the **post** keyword supports expanded SDP CGI templates by allowing the SDP registrar to send the additional information about the device configuration to an external management system by issuing an HTTP POST or an HTTPS POST. Without the use of the **post** keyword, the SDP registrar requests information only from the management system based on the device name.

Note In order to use the expanded SDP CGI support, the registrar must be running Cisco IOS Release 12.4(6)T or a later release, the **template config** command must be issued with the **post** keyword, and the *url* argument must include either the HTTP or HTTPS protocol. No other protocol (for example, FTP) is supported for the expanded CGI template functionality.

The additional information sent to the external management system with the issuance of an HTTP POST from the SDP registrar to the external management system is shown in the table below.

Table 4: AV Pairs Sent During HTTP Post to External Management System

AV Pair	Description
TTIFixSubjectName	AAA_AT_TTI_SUBJECTNAME (sent only if the realm authentication user is not the root user on the registrar)
TTIIosRunningConfig	Output of **show running-config brief**
TTIKeyHash	Digest calculated over the device public key

AV Pair	Description
TTIPrivilege	AAA_AT_TTI_PRIVILEGE--"admin" is sent if the user is an administrator; "user" is sent if the user is not an administrator (sent only if the realm authentication user is an administrator and the information is available from the authentication, authorization, and accounting [AAA] server)
TTISignature	Digest calculated over all attribute-value (AV) pairs except UserDeviceName and TTISignCert
TTISignCert	Device current certificate (sent only if the device currently has a certificate)
TTITemplateVar	AAA_AT_TTI_IOSCONFIG(1-9) (sent only if the realm authentication user is not the root user on the registrar)
TTIUserName	Device name as entered by the administrative introducer (sent only if the realm authentication user is an administrator)
TTIVersion	TTI version of the registrar

Examples

The following example shows how to specify the HTTP URL "http://pki1-36a.cisco.com:80" for the Cisco IOS CLI configuration template, which is sent from the SDP registrar to the external management system during the TTI exchange:

```
crypto provisioning registrar
 pki-server cs1
 template config
http://pki1-36a.cisco.com:80
```

The following example shows how to specify that the SDP registrar will send additional device information to the external management system to retrieve a more specific bootstrap configuration file:

```
crypto provisioning registrar
 pki-server cs1
 template config http://myserver/cgi-bin/mycgi post
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an SDP operation.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation.

Command	Description
template username	Establishes a template username and password to access the configuration template on the file system.

template file

To specify the source template file location on the registrar and the destination template file location on the petitioner, use the **template file** command in tti-registrar configuration mode.

template file *sourceURL destinationURL*

Syntax Description

sourceURL	Specifies the source URL on the registrar for the template file using one of the keywords in .
destinationURL	Specifies the destination URL on the petitioner for template file using one of the keywords in .

Command Default

None

Command Modes

tti-registrar configuration (tti-registrar)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **template file** command to specify the location where a template file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine template files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:.

The file content is expanded on the registrar. The destination URL and file content are expanded on the petitioner.

Table 5: Source and Destination URL Keywords

Keyword	Description
archive:	Retrieves from the archive location.
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
disk0:	Retrieves from disk0.

Keyword	Description
disk1:	Retrieves from disk1.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server.
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tar:	Retrieves from a compressed file in tar format.
tftp:	Retrieves from a TFTP network server.
tmpsys:	Retrieves from a temporary system location.
unix:	Retrieves from the UNIX system location.
usbtoken:	Retrieves from the USB token.

Examples

The following example shows how to specify where the source template file is located and where the template file will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  template file http://myserver/file1 usbtoken0://file1
  template file http://myserver/file2 flash://file2
```

Related Commands

Command	Description
binary file	Specifies the binary file location on the registrar and the destination binary file location on the petitioner.

Command	Description
crypto provisioning registrar	Configures a device to become an SDP registrar and enter tti-registrar configuration mode.

template http admin-introduction

To use a custom administrator introduction template rather than the default template, issue the **template http admin-introduction** command in tti-registrar configuration mode.

template http admin-introduction *URL*

Syntax Description

URL	Location of the custom administrator introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

You may want to use a custom administrator introduction template rather than a default template because the device name can be prefilled on the web page for the user. Without this command, the welcome page must be the first page requested by the user.

Examples

The following example shows how to direct the registrar to use the administrator introduction page template located at tftp://walnut.cisco.com/admin-introducer.html:

```
template http admin-introduction tftp://walnut.cisco.com/admin-introducer.html
```

Related Commands

Command	Description
template http completion	Uses a custom completion template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.

Command	Description
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http completion

To use a custom completion template rather than the default template, issue the **template http completion** command in tti-registrar configuration mode.

template http completion *URL*

Syntax Description

URL	Location of the custom completion template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the completion page template located at specified location:

```
template http completion tftp://walnut.cisco.com/completion.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.

Command	Description
template http welcome	Uses a custom welcome template rather than the default template.

template http error

To use a custom error template rather than the default template, issue the **template http error** command in tti-registrar configuration mode.

template http error *URL*

Syntax Description

URL	Location of the custom error template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the error page template located at specified location:

```
template http error tftp://walnut.cisco.com/error.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.

Command	Description
template http welcome	Uses a custom welcome template rather than the default template.

template http introduction

To use a custom introduction template rather than the default template, issue the **template http introduction** command in tti-registrar configuration mode.

template http introduction *URL*

Syntax Description

URL	Location of the custom introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom introduction page, the completion URL of the petitioner may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the customer introduction template located at specified location:

```
template http introduction tftp://walnut.cisco.com/introduction.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http start

To direct the Trusted Transitive Introduction (TTI) registrar to use the custom start page template, issue the **template http start** command in tti-registrar configuration mode.

template http start *URL*

Syntax Description

URL	Location of the start page template.

Command Default

If this command is not issued, the welcome page will be the initial communication between the introducer and the petitioner.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **template http start**command to display the start page on the registrar and make that page the starting point of the TTI transaction. From the start page, the registrar can direct the user to the welcome page on the petitioner.

Examples

The following example shows how to direct the registrar to use the start page template located at the specified location:

```
template http start tftp://walnut.cisco.com/start.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.

Command	Description
template http welcome	Uses a custom welcome template rather than the default template.

template http welcome

To use a custom welcome template rather than the default template, issue the **template http welcome** command in tti-registrar configuration mode.

template http welcome *URL*

Syntax Description

URL	Location of the custom welcome template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom welcome page, the introduction URL of the registrar may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the welcome page template located at specified location:

```
template http welcome tftp://walnut.cisco.com/welcome.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.

template location

To specify the location of the template that the SDP Registrar should use while responding to a request received through the URL profile, use the **template location**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template location *location*

no template location *location*

Syntax Description

location	Specifies the template location for the SDP Registrar.

Command Default

No template *location* is associated with the SDP Registrar.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template location**command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.

Command	Description
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

template username

To establish a template username in which to access the file system, use the **template username** command in tti-registrar configuration mode.

template username *name*

Syntax Description

name	Template username.

Command Default

A template username is not established.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **template username**command to create a username-based authentication system that allows you to access the configuration template, which is sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

Examples

The following example shows how to create the username "mycs" to access the configuration template for the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
 template username mycs
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

template variable p

To specify the value that goes into the Organizational Unit (OU) field of the subject name in the trustpoint certificate to be issued by the SDP Registrar, use the **template variable**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template variable p *value*

no template variable p *value*

Syntax Description

value	Specifies the OU field value.

Command Default

No OU field value is associated with the trustpoint certificate.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template variable p**command can be specified optionally in the SDP registrar configuration.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.

Command	Description
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the **test aaa group** command in privileged EXEC mode.

DNIS and CLID User Profile

test aaa group {*group-name*| **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {**yes**| **no**}]

Syntax Description

group-name	Subset of RADIUS servers that are used, as defined by the server group group-name.
radius	Uses RADIUS servers for authentication.
username	Name for the test user. **Caution** If you use this command to manually test RADIUS load-balancing server state, it is recommended that a test user, one that is not defined on the RADIUS server, be used to protect against security issues that may arise if the test user is not correctly configured.
password	Password.
new-code	Code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile *profile-name*	(Optional) Identifies the user profile specified in the aaa user profile command. To associate a user profile with the RADIUS server, you must identify the user profile name.
server *ip-address*	(Optional) For RADIUS server load balancing, specifies to which server in the server group the test packets will be sent.
auth-port	(Optional) User Datagram Protocol (UDP) destination port for authentication requests.

port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1646.
acct-port	(Optional) UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
count *requests*	(Optional) Number of authentication and accounting requests that are to be sent to the server for each port. Range: 1 to 50000. Default: 1.
rate *requests-per-second*	(Optional) Number of requests per second that are to be sent to the server. Range: 1 to 1000. Default: 10.
blocked {**yes** | **no**}	(Optional) Specifies whether the request is sent in blocking or nonblocking mode. If the **blocked** keyword is not used and one request is sent, the default is **yes**; if more than one request is sent, the default is **no**.

Command Default

DNIS or CLID attribute values are not sent to the RADIUS server.

RADIUS Server Load Balancing Manual Testing

RADIUS server load-balancing server status manual testing does not occur.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS load balancing manual testing functionality: **server** *ip-address*, **auth-port** *port-number*, **acct-port** *port-number*, **count** *request*, **rate** *requests-per-second*, **blocked**.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)ZV1	This command was enhanced to show user attributes returned from RADIUS authentication when authentication is successful.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **test aaa group** command can be used to

- Associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.
- Verify RADIUS load-balancing server status.

Note The **test aaa group**command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named prfl1 and associate it with a **test aaa group**command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

The following example shows the response from a load-balanced RADIUS server that is alive when the username "test" does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Examples

The following example shows the user attribute list that the RADIUS server returns when you issue the test aaa command and authentication is successful:

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Authen Requests to Send    : 1
AAA/SG/TEST:      Authen Requests Processed  : 1
AAA/SG/TEST:      Authen Requests Sent       : 1
AAA/SG/TEST:      Authen Requests Replied    : 1
AAA/SG/TEST:      Authen Requests Successful : 1
AAA/SG/TEST:      Authen Requests Failed     : 0
AAA/SG/TEST:      Authen Requests Error      : 0
AAA/SG/TEST:      Authen Response Received   : 1
AAA/SG/TEST:      Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Account Requests to Send    : 0
AAA/SG/TEST:      Account Requests Processed  : 0
AAA/SG/TEST:      Account Requests Sent       : 0
AAA/SG/TEST:      Account Requests Replied    : 0
AAA/SG/TEST:      Account Requests Successful : 0
AAA/SG/TEST:      Account Requests Failed     : 0
AAA/SG/TEST:      Account Requests Error      : 0
AAA/SG/TEST:      Account Response Received   : 0
AAA/SG/TEST:      Account No Response Received: 0
USER ATTRIBUTES
username              "Username:viral"
nas-ip-address        3.1.1.1
interface             "210"
service-type          1 [Login]
Framed-Protocol       3 [ARAP]
ssg-account-info      "S20.5.0.2"
ssg-command-code      0B 4C 32 54 50 53 55 52 46
Router
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates a AAA user profile.
load-balance	Enables RADIUS server load-balancing for RADIUS-named server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load-balancing for the global RADIUS server group.

test content-scan

To test the content-scan configuration, use the **test content-scan** command in privileged EXEC mode.

test content-scan {**off-tower-check | on-tower-check | telemetry now**}

Syntax Description

off-tower-check	Disables Cloud Web Security tower validation.
on-tower-check	Enables Cloud Web Security tower validation.
telemetry now	Immediately sends telemetry and exceptions data to the Cloud Web Security tower.

Command Default

Telemetry and exceptions data are sent at configured intervals.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Note This command is used by the Technical Assistance Center to troubleshoot issues.

Telemetry is an automated communications process in which measurements are made and data that is collected at remote sites is transmitted to receiving equipment for monitoring.

The device on which the Cloud Web Security is configured is monitored, and data is generated periodically. Because most of these devices do not have a lot memory or secondary storage, the generated data is exported and stored in the Cloud Web Security tower. The device connects to a URL hosted by the Cloud Web Security tower by using the HTTP POST method to periodically send telemetry data.

Because the Cloud Web Security tower does not have information about all web traffic, a connector (a persistent, out-of-band secure channel between the device and the Cloud Web Security tower) periodically sends all exception rules to the tower. The connector makes a POST request and pushes all exception rules to a URL. This URL is separate from the telemetry URL.

Examples

The following example shows how to immediately send telemetry and exceptions data to the Cloud Web Security tower:

```
Device# test content-scan telemetry now
```

Related Commands

Command	Description
out-of-band telemetry	Enables out-of-band telemetry and content-scan exception rules.
parameter-map type content-scan	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

test crypto self-test

To test the crypto configuration to see if it passes or fails, use the **test crypto self-test**command in privileged or user EXEC mode.

test crypto self-test

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

User EXEC (>)

Command History

Release	Modification
12.2XN	This command was introduced.

Usage Guidelines

As a result of the test, a new SELF_TEST_RESULT system log is generated. If the crypto test fails, a SELF_TEST_FAILURE system log is generated.

Examples

The following example displays the output of the **test crypto self-test**command:

```
Router# test crypto self-test
*Apr 23 01:48:49.678: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test ac)
*Apr 23 01:48:49.822: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DH self test)
*Apr 23 01:48:49.954: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software Cry)
*Apr 23 01:48:50.054: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software che)
*Apr 23 01:48:50.154: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encrypti)
Router#
*Apr 23 01:48:50.254: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encrypt)
*Apr 23 01:48:50.354: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing )
*Apr 23 01:48:50.454: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Random KAT t)
*Apr 23 01:48:50.674: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encrypti)
*Apr 23 01:48:50.774: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (HMAC-SHA    )
Router#
*Apr 23 01:48:50.874: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA256 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA512 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (ALL TESTS PA)
```

test urlf cache snapshot

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

test urlf cache snapshot *file-name*

Syntax Description

file-name	The name of the Cisco IOS file in which the contents of the URL filtering cache are saved. Use the Cisco IOS file system naming conventions.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

Examples

The following example shows how to save the contents of the URL filtering cache to a flash memory file system in the file trend-cache-snapshot:

```
Router# test urlf cache snapshot flash:trend-cache-snapshot
```

text-color

Note Effective with Cisco IOS Release 12.4(6)T, the **text-color**command is not available in Cisco IOS software.

To set the color of the text on the title bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

text-color [**black**| **white**]

no text-color [**black**| **white**]

Syntax Description

black	(Optional) Color of the text is black. This is the default value
white	(Optional) Color of the text is white.

Command Default

Color of the text is black.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

This command is limited to only two values to limit the number of icons that are on the toolbar.

Examples

The following example shows that the text color will be white:

```
text-color white
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

threat-detection basic-threat

To configure basic threat detection for a zone, use the **threat-detection basic-threat** command in parameter-map type inspect configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection basic-threat

no threat-detection basic-threat

Syntax Description

This command has no arguments or keywords.

Command Default

Threat detection is not enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure threat detection.

Threat detection refers to the ability of a security device to detect and take action against possible threats, anomalies, or attacks. Basic threat detection monitors the rate of predefined events per zone. Once the rate of a certain type of event exceeds the event rate monitoring limit, an alert is sent if the **alert on** command is configured.

Note You cannot associate a default zone to a zone parameter map. As a result, the Event Rate Monitoring feature is not configured as part of the default zone.

After you enable logging for a zone, a log message is logged for each threat detected.

Examples

The following example shows how to configure basic threat detection:

```
Router(config)# parameter-map type inspect-zone pmap-zone
Router(config-profile)# threat-detection basic-threat
Router(config-profile)# end
```

Related Commands

Command	Description
alert on	Turns on or off console display of Cisco IOS stateful packet inspection alert messages.
parameter-map type inspect-zone	Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode.
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.
threat-detection rate	Configures the threat detection rate for a zone.

threat-detection rate

To configure the threat detection rate for an event type, use the **threat-detection rate** command in parameter-map type inspect configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection rate {**fw-drop | inspect-drop| syn-attack**} **average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*

no threat-detection rate {**fw-drop | inspect-drop| syn-attack**}

Syntax Description

fw-drop	Configures the threat detection rate for firewall drop events.
inspect-drop	Configures the threat detection rate for firewall inspection-based drop events.
syn-attack	Configures the threat detection rate for SYN attack events.
average-time-frame *seconds*	Configures the average time frame for threat detection, in seconds. Valid values are from 600 to 3600.
average-threshold *packet-per-second*	Configures the average threat detection threshold, in packets per second. Valid values are from 1 to 4294967295.
burst-threshold *packets-per-second*	Configures the burst threshold for threat detection, in packets per second. Valid values are from 1 to 1000000000.

Command Default

Threat detection rate is enabled by default.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure the threat detection rate.

You must configure the **threat-detection basic-threat** command before you can configure the **threat-detection rate** command that configures the event rate monitoring rate limit.

Threat detection refers to the ability of a security device to detect possible threats, anomalies, or attacks and to take action against them.

Note Because you cannot associate a default zone to a zone parameter map, the Event Rate Monitoring feature is not configured as part of the default zone.

When you enable logging for a zone, a log message is logged for each threat detected.

Examples

The following example shows how to configure the threat detection rate for inspection-based drop events for a zone:

```
Router(config)# parameter-map type inspect-zone pmap-zone
Router(config-profile)# threat-detection rate inspect-drop average-time-frame 200
average-threshold 30 burst-threshold 40
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect-zone	Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode.
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.
threat-detection basic-threat	Configures basic threat detection for a zone.

throttle

To configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **throttle**command in server group configuration mode. To disable server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]

no throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]

Syntax Description

accounting *threshold*	Configures the specified server group threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access *threshold*	Configures the specified server group threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout *number-of-timeouts*	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request from the specified server group is dropped. The range is 1 through 10. The default value is 3.

Command Default

Throttling is disabled.

Command Modes

Server-group configuration (config-sg-radius)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. Server group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.

Examples

The following examples shows how to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server throttle	Configures global throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

timeout (application firewall application-configuration)

To specify the elapsed length of time before an inactive connection is torn down, use the **timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	Idle timeout value. Available range: 5 to 43200 (12 hours).

Command Default

If this command is not issued, the default value specified via the **ip inspect tcp idle-time**command will be used.

Command Modes

cfg-appfw-policy-http configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **timeout** command overrides the global TCP idle timeout value for HTTP traffic or for traffic of a specified instant messenger application (AOL, Yahoo, or MSN).

Before you can issue the **timeout** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
```

```
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
  timeout 60
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will be managed while there is no activity).

timeout (config-radius-server)

To specify the time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting, use the **timeout** command in RADIUS server configuration mode. To restore the default value, use the **no** form of this command.

timeout *seconds*

no timeout

Syntax Description

seconds	Specifies the timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval is 5 seconds.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the number of seconds a router waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the router, it is recommended that you configure the RADIUS server timeout to 15 seconds.

Examples

The following example shows how to set the interval timer to 10 seconds:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# timeout 10
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

timeout (GTP)

To configure timeout values for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **timeout** command in parameter-map type inspect configuration mode. To remove the configured timeout values, use the **no** form of this command.

timeout {**pdp-context**| **request-queue**}*time*

no timeout {**pdp-context**| **request-queue**}

Syntax Description

pdp-context *time*	Configures the timeout, in minutes, for inactive Packet Data Protocol (PDP) contexts. Valid values are from 1 to 35791. The default is 30.
request-queue *time*	Configures the timeout, in seconds, for inactive request queues. Valid values are from 0 to 2147483. The default is 60.

Command Default

Timeout values are not configured for GTP.

Command Modes

Parameter-map type inspect configuration mode (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

When you configure the **timeout pdp-context** command, inactive PDP request queues are dropped based on the timeout value. Similarly, when you configure **timeout request-queue** command, GTP requests that are queued to wait for a response are dropped based on the timeout value.

Examples

The following example shows how to configure a timeout of 3000 minutes for inactive PDP contexts:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# timeout pdp-context 3000
Device(config-profile)#
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

timeout (parameter-map)

To configure the time interval for content scanning, use the **timeout** command in parameter-map type inspect configuration. To disable the time interval for content scanning, use the **no** form of this command.

timeout {**server** *seconds* | **session-inactivity** *seconds*}

no timeout {**server** *seconds* | **session-inactivity** *seconds*}

Syntax Description

server	Specifies the server keepalive time in seconds.
seconds	Timeout in seconds. Valid values are from 5 to 43200. The default is 300.
session-inactivity	Specifies the session inactivity time in seconds.
seconds	Timeout in seconds. Valid values are from 5 to 43200. The default is 3600.

Command Default

The time interval for content scanning is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The **timeout** command configures the timeout to check the availability of the ScanSafe servers and to determine the active tower. The primary tower is tried first and if it fails, the secondary tower is chosen as the active. The secondary tower falls back to the primary tower, if the primary is detected to be active for three consecutive timeouts. The session inactivity timer is used to remove the sessions that are inactive for the configured duration.

Examples

The following example shows how to configure the server timeout:

```
Router(config)# parameter-map type content-scan global
Router(config-profile)# timeout server 3450
```

Related Commands

Command	Description
parameter-map type content-scan global	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

timeout (policy group)

To configure the length of time that an end user session can remain idle or the total length of time that the session can remain connected, use the **timeout** command in webvpn group policy configuration mode. To configure timeout timers to default values, use the **no** form of this command.

timeout {**idle** *seconds*| **session** *seconds*}

no timeout {**idle**| **session**}

Syntax Description

idle *seconds*	Configures the length time that an end user connection can remain idle.
session *seconds*	Configures the total length of time that an end user can maintain a single connection.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

idle 2100 **session** 43200

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to configure the idle or session timer value. The idle timer sets the length of time that a session will remain connected when the end user generates no activity. The session timer sets the total length of time that a session will remain connected, with or without activity. Upon expiration of either timer, the end user connection is closed. The user must login or reauthenticate to access the Secure Sockets Layer Virtual Private Network (SSL VPN).

Note The idle timer is not the same as the dead peer timer. The dead peer timer is reset when any packet type is received over the Cisco AnyConnect VPN Client tunnel. The idle timer is reset only when the end user generates activity.

Examples

The following example sets the idle timer to 30 minutes and session timer to 10 hours:

```
Router(config)# webvpn context context1
```

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# timeout idle 1800
Router(config-webvpn-group)# timeout session 36000
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout**command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.

Command Default

Time to wait is 5 seconds.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

timeout file download

To specify how often the consent webpage should be downloaded from the file server, use the **timeout file download** command in parameter-map-type consent configuration mode. To remove the configured download time, use the **no** form of this command with the configured time.

timeout file download *minutes*

no timeout file download *minutes*

Syntax Description

minutes	The time, in minutes, that specifies how often the consent webpage should be downloaded from the file server. Available range: 1 to 525600.

Command Default

The consent webpage is not downloaded from the file server.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Using the **timeout file download**command ensures that the consent file has the most current parameter map defintions.

Examples

In the following example, the file "consent_page.html" will be downloaded from the file server every 35791 minutes:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response**command in line configuration mode. To set the timeout value to 30 seconds (which is the default timeout value), use the **no**form of this command.

timeout login response *seconds*

no timeout login response *seconds*

Syntax Description

seconds	Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds. The default value is 30 seconds.

Command Default

The default login timeout value is 30 seconds.

Command Modes

Line configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(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 changes the login timeout value to 60 seconds:

```
line 10
 timeout login response 60
```

timeout retransmit

To set an interval for a router to wait for a reply from the Lightweight Directory Access Protocol (LDAP) server before it times out, use the **timeout retransmit**command in LDAP server configuration. To restore the default, use the **no** form of this command.

timeout retransmit *seconds*

no timeout retransmit *seconds*

Syntax Description

seconds	The timeout interval, in seconds. The range is from 1 to 65535. The default is 30.

Command Default

The default timeout interval value is 30 seconds.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The recommended value to configure the LDAP server to timeout is 30 seconds.

Examples

The following example shows how to set an interval timer of 20 seconds for the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# timeout retransmit 20
```

Related Commands

Command	Description
ipv4(ldap)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

timer (Diameter peer)

To configure the Diameter Credit Control Application (DCCA) for peer-to-peer communication, use the **timer** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

timer {**connection**| **transaction**| **watchdog**} **value**

no timer {**connection**| **transaction**| **watchdog**} **value**

Syntax Description

connection	Maximum interval, in seconds, for the Gateway General Packet RadioService (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after after being disconnected because of a transport failure. The range is from 1 to 1000. The default is 30. A value of 0 configures the GGSN not to attempt reconnection.
transaction	Maximum interval, in seconds, the GGSN waits for a Diameter peer to respond before trying another peer. The range is from 1 to 1000. The default is 30.
watchdog	Maximum interval, in seconds, the GGSN waits for a Diameter peer response to a watchdog packet. The range is from 1 to 1000. The default is 30. **Note** When the watchdog timer expires, a device watchdog request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a device watchdog answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.
value	The valid range, in seconds, from 1 to 1000. The default is 30.

Command Default

The default for each timer is 30 seconds.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

When configuring timers, the value for the transaction timer should be larger than the transmission-timeout value, and, on the Serving GPRS Support Node (SGSN), the values configured for the number of GPRS Tunneling Protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter Credit Control Application (DCCA), and Cisco Content Services Gateway (CSG)). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

- The factor *2* is for both authentication and accounting.
- *The value N* is for the number of Diameter servers configured in the server group.

Examples

The following example shows how to configure the Diameter base protocol timers for a Diameter peer:

```
Router (config-dia-peer)# timer connection
 20
Router (config-dia-peer)# timer watchdog
 25
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration sub-mode.
diameter peer timer	Configures the Diameter base protocol timers globally.

timer reauthentication (config-if-cts-dot1x)

To set the reauthentication timer period to be used if the authentication server does not specify a period, use the **timer reauthentication** command in CTS dot1x interface configuration mode. Use the **no** form of the command to disable the timer.

timer reauthentication *seconds*

no timer reauthentication *seconds*

Syntax Description

seconds	Specifies the reauthentication timer period in seconds.

Command Default

86400 seconds.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When the reauthentication timer expires, the device reauthenticates to the CTS network (NDAC).

Examples

The following example sets the reauthentication timer to 44 seconds:

```
Router(config-if-cts-dot1x)# timer reauthentication 44
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
propagate sgt (config-if-cts-dot1x)	Enables Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface.
sap mode-list (config-if-cts-dot1x)	Configures CTS Security Association Protocol (SAP) authentication.
show cts interface	Displays CTS interface status and configurations.

Command	Description
show dot1x interface	Displays IEEE 802.1x configurations and statistics.

timers delay

To configure the time that a redundancy group takes to delay role negotiations that start after a fault occurs or the system is reloaded, use the **timers delay**command in redundancy application group configuration mode. To disable the timer, use the **no** form of this command.

timers delay *seconds* [**reload** *seconds*]

no timers delay *seconds* [**reload** *seconds*]

Syntax Description

seconds	Delay value. The range is from 0 to 10000. The default is 10.
reload	(Optional) Specifies the redundancy group reload timer.
seconds	(Optional) Reload timer value in seconds. The range is from 0 to 10000. The default is 120.

Command Default

The default is 10 seconds for timer delay and 120 seconds for reload delay.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to set the timer delay value and reload value for a redundancy group named group 1:

```
Router# configure terminal
Router(config)# redundancy

Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# timers delay 100 reload 400
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime**command in redundancy application protocol configuration mode. To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [msec] *seconds* **holdtime [msec]** *seconds*

no timers hellotime [msec] *seconds* **holdtime [msec]** *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages.
seconds	Interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application protocol configuration (config-red-app-prtc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

title

To configure the HTML title string that is shown in the browser title and on the title bar of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title** command in webvpn context configuration mode. To revert to the default text string, use the **no** form of this command.

title [*title-string*]

no title [*title-string*]

Syntax Description

title-string	(Optional) Title string, up to 255 characters in length, that is displayed in the browser of the user. The string value may contain 7-bit ASCII characters, HTML tags, and escape sequences.

Command Default

If this command is not configured or if the **no** form is entered, the following text is displayed:

"WebVPN Service"

Command Modes

Webvpn context configuration

Command History

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

Usage Guidelines

The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string "WebVPN Service" is displayed.

Examples

The following example configures "Secure Access: Unauthorized users prohibited" as the title string:

```
Router(config)#
webvpn context context1
Router(config-webvpn-context)# title "Secure Access: Unauthorized users prohibited"
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title-color** command in webvpn context configuration mode. To remove the color, use the **no** form of this command.

title-color *color*

no title-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default is purple.

Command Default

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	Support for the SSL VPN enhancements feature was added.

Usage Guidelines

Configuring a new color overrides the color the preexisting color.

Examples

The following examples show the three command forms that can be used to configure the title color:

```
Router(config-webvpn-context)# title-color darkseagreen
Router(config-webvpn-context)# title-color #8FBC8F
Router(config-webvpn-context)# title-color 143,188,143
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.