

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.

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.

Defaults

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.

Examples The following example shows that IP DNS alias lookup has been enabled:

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

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 {host-name | host-ip-address} [key string] [nat] [port [integer]]
[single-connection] [timeout [integer]]
```

```
no tacacs-server host {host-name | host-ip-address}
```

Syntax Description

<i>host-name</i>	Name of the host.
<i>host-ip-address</i>	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.
<i>string</i>	(Optional) Character string specifying authentication and encryption 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.
<i>integer</i>	(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.
<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Defaults

No TACACS+ host is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The nat keyword was added.
12.2(8)T	The nat keyword was integrated into Cisco IOS Release 12.2(8)T.

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.

Examples

The following example specifies a TACACS+ host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies 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.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
aaa accounting	Enables AAA accounting of requested services for billing or security.
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 | 7 string | string}
```

```
no tacacs-server key {0 string | 7 string | string}
```

Syntax Description

0 string	Specifies that an unencrypted key will follow. <ul style="list-style-type: none"> <i>string</i>—The unencrypted (clear text) shared key.
7 string	Specifies that a hidden key will follow. <ul style="list-style-type: none"> <i>string</i>—The hidden shared key.
<i>string</i>	The unencrypted (clear text) shared key.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.3(2)T	The 0 string and 7 string keyword and argument pairs were 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.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
tacacs-server key dare to go
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

tacacs-server packet

To modify TACACS+ packet options, use the **tacacs-server packet** command in global configuration mode. To disable the modified packet options, use the **no** form of this command.

tacacs-server packet *maxsize*

no tacacs-server packet

Syntax Description	<i>maxsize</i>	Maximum TACACS+ packet size that is acceptable. The value is from 10240 through 65536.
---------------------------	----------------	--

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

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

Command History	Release	Modification
	Prior to 12.0	This command was introduced.

Examples The following example shows that the TACACS+ packet size has been set to the minimum value of 10240:

```
tacacs-server packet 10240
```

tacacs-server timeout

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

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description	<i>seconds</i>	Timeout interval in seconds. The value is from 1 through 1000. The default is 5.
---------------------------	----------------	--

Command Default	If the command is not configured, the timeout interval is 5.
------------------------	--

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

Command History	Release	Modification
	10.0	This command was introduced.

Examples	The following example changes the interval timeout to 10 seconds:
-----------------	---

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

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}
```

```
no template {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.
<i>template-number</i>	Template interface number. The value ranges from 1 through 200.

Defaults

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

Command Modes

Identity policy configuration

Command History

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

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
<code>identity policy</code>	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

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

Defaults

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 template, use the **no** form of this command.

template config *url*

no template config *url*

Syntax Description

url One of the keywords in [Table 76](#).

Defaults

A default template will be used.

Command Modes

tti-registrar configuration

Command History

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

Usage Guidelines

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

The default template, which is used if a template is not specified, contains the following commands:

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

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

Where \$l comes from “trustpoint” configured under the petitioner, \$k comes from “rsakeypair” under the trustpoint:

```
! $l will be replaced by 'mytp.'
crypto wui tti 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.

Table 76 lists the available options for the *url* argument.

Table 76 Options for the url Argument

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.
nvr:	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.
tftp:	Retrieves from a TFTP network server.
webflash:	Retrieves from the file system.
xmodem:	Retrieves from a network machine that uses the Xmodem protocol.

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 EzSDD registrar to the EzSDD petitioner during the TTI exchange:

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

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an EzSDD 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 EzSDD operation.
crypto wui tti registrar	Configures a device to become an EzSDD registrar and enters tti-registrar configuration mode.
debug crypto wui	Displays information about an EzSDD operation.
template username	Establishes a template username and password to access the configuration template on the file system.

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

<i>name</i>	Template username.
-------------	--------------------

Defaults

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 easy secure device deployment (EzSDD) registrar to the EzSDD 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 EzSDD registrar and enters tti-registrar configuration mode.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

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, use the **test aaa group** command in privileged EXEC mode.

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

Syntax Description

<i>group-name</i>	Subset of RADIUS servers that are used as defined by the server group <i>group-name</i> .
radius	Uses RADIUS servers for authentication.
<i>username</i>	Specifies a name for the user.
<i>password</i>	Character string that specifies the password.
new-code	The code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile <i>profile-name</i>	(Optional) Identifies the user profile specified in the aaa user profile command. To associate a user profile with the RADIUS server, the user profile name must be identified.

Defaults

If this command is not enabled, DNIS or CLID attribute values will not be sent to the RADIUS server.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **test aaa group** command 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.



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
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates an AAA user profile.

text-color

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.

Defaults

Color of the text is black.

Command Modes

Web VPN configuration

Command History

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

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.

timeout

To override the global TCP idle timeout value for HTTP traffic, use the **timeout** command in appfw-policy-http configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description	<i>seconds</i>	Idle timeout value. Available range: 5 to 43200 (12 hours).
--------------------	----------------	---

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

Command Modes	appfw-policy-http configuration
---------------	---------------------------------

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

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 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	<i>seconds</i>	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.
---------------------------	----------------	--

Defaults The default login timeout value is 30 seconds.

Command Modes Line configuration

Command History	Release	Modification
	11.3	This command was introduced.

Examples The following example changes the login timeout value to 60 seconds:

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

title

To enter the HTML title string that is shown in the browser title and on the title bar for a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **title** command in Web VPN configuration mode. To remove the title, use the **no title** form of this command.

title [*title-string*]

no title [*title-string*]

Syntax Description	<i>title-string</i>	<i>(Optional) Title string to be displayed in the browser of the user. Limited to 255 characters. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. The default is “WebVPN Service.” If this argument is not configured, a title will not be displayed in the browser of the user.</i>
---------------------------	---------------------	---

Defaults If the **title** command is not configured, “WebVPN Service” is displayed in the browser of the user.

Command Modes Web VPN configuration

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

Usage Guidelines If you type the **title** command and then press the **Enter** key, a title will not be displayed on the browser. If the **no** form of this command is used, the default title string “WebVPN Service” is displayed in the browser of the user.

Examples The following example shows the title will be “Secure Corporate Access: Unauthorized users prohibited.”

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

Syntax Description	Command	Description
	webvpn	Enters Web VPN configuration mode.

title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **title-color** command in Web VPN 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 can be 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.

Defaults

Purple

Command Modes

Web VPN configuration

Command History

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

Usage Guidelines

If a new color is configured, it will override the color that was already configured.

Examples

The following examples show three ways to configure the title color.

```
title-color darkseagreen
```

```
title-color #8FBC8F
```

```
title-color 143,188,143
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

transfer-encoding type

To permit or deny HTTP traffic according to the specified transfer-encoding of the message, use the **transfer-encoding type** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

```
transfer-encoding type {chunked | compress | deflate | gzip | identity | default} action {reset |
allow} [alarm]
```

```
no transfer-encoding type {chunked | compress | deflate | gzip | identity | default} action {reset
| allow} [alarm]
```

Syntax Description

chunked	Encoding format (specified in RFC 2616, <i>Hypertext Transfer Protocol—HTTP/1</i>) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX “compress” utility.
deflate	“ZLIB” format defined in RFC 1950, <i>ZLIB Compressed Data Format Specification version 3.3</i> , combined with the “deflate” compression mechanism described in RFC 1951, <i>DEFLATE Compressed Data Format Specification version 1.3</i> .
gzip	Encoding format produced by the “gzip” (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
default	All of the transfer encoding types.
action	Encoding types outside of the specified type are subject to the specified action (reset or allow).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given type is not specified, all transfer-encoding types are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

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

Usage Guidelines

Only encoding types specified by the **transfer-encoding-type** command are allowed through the firewall.

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
!
!
! 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
!
!
```

trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the easy secure device deployment (EzSDD) petitioner and the EzSDD registrar, use the **trustpoint** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint *trustpoint-label*

no trustpoint *trustpoint-label*

Syntax Description	<i>trustpoint-label</i>	Name of trustpoint.
Defaults	If a trustpoint is not specified, a default trustpoint called “tti” is generated.	
Command Modes	tti-petitioner configuration	
Command History	Release	Modification
	12.3(8)T	This command was introduced.
Usage Guidelines	Use the trustpoint command in tti-petitioner configuration mode to associate a trustpoint with the EzSDD petitioner.	
Examples	<p>The following example shows how specify the trustpoint “mytrust”:</p> <pre>crypto wui tti petitioner trustpoint mytrust</pre> <p>After the EzSDD exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the show running-config command shows an automatically generated configuration which generates the default trustpoint “tti”:</p> <pre>crypto pki trustpoint tti enrollment url http://pkil-36a.cisco.com:80 revocation-check crl rsakeypair tti 1024 auto-enroll 70</pre>	
Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.
	crypto wui tti petitioner	Configures a device to become an EzSDD petitioner and enters tti-petitioner configuration mode.

trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint signing *trustpoint-label*

no trustpoint signing *trustpoint-label*

Syntax Description	<i>trustpoint-label</i>	Name of trustpoint.
--------------------	-------------------------	---------------------

Defaults	If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.
----------	--

Command Modes	tti-petitioner configuration
---------------	------------------------------

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

Usage Guidelines	Use the trustpoint signing command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.
------------------	--

Examples	The following example shows how to specify the trustpoint mytrust:
----------	--

```
crypto provisioning petitioner
trustpoint signing mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
enrollment url http://pki1-36a.cisco.com:80
revocation-check crl
rsakeypair tti 1024
auto-enroll 70
```

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.

Command	Description
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar.

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

```
tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip
             [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | mpls | nos | rbscp}
```

```
no tunnel mode
```

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre	Generic routing encapsulation protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. Note that this tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is ipsec and the transport is ipv4.
iptalk	Apple IPTalk encapsulation.
mpls	Multiprotocol Label Switching encapsulation.
nos	KA9Q/NOS compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Defaults

GRE tunneling

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added: <ul style="list-style-type: none"> • aurp • dvmrp • ipip
11.2	The optional decapsulate-any keyword was added.
12.2(13)T	The gre multipoint keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: <ul style="list-style-type: none"> • gre ipv6 to support GRE tunneling using IPv6 as the delivery protocol. • ipv6 to allow a Static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • rbscp to support Rate Based Satellite Control Protocol (RBSCP).
12.3(14)T	The ipsec ipv4 keyword was added.
12.2(18)SXE	The gre multipoint keyword was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The work around is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mouted router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IP Security (IPSec) profile. Combining mGRE tunnels and IPSec encryption allows a single mGRE interface to support multiple IPSec tunnels, thereby simplifying the size and complexity of the configuration.



Note

GRE tunnel keepalives configured using the **keepalive** command under GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

Examples**Cayman Tunneling**

The following example shows how to enable Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

IPSec in IPv4 Transport

The following example shows how to configure a tunnel using IPSec encapsulation with IPv4 as the transport mechanism.

```
Router(config)# crypto ipsec profile PROF
Router(config)# set transform tset
!
Router(config)# interface Tunnel0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.1.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ! Ensures longer packets are fragmented before they are encrypted; otherwise, the
 ! receiving router would have to do the reassembly.
 ip mtu 1416
 ! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
 ! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
 ! Sets IPSec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
 ! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
```

```
Router(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel protection

To associate a tunnel interface with an IP Security (IPSec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPSec profile, use the **no** form of this command.

tunnel protection ipsec profile *name* [shared]

no tunnel protection ipsec profile *name* [shared]

Syntax Description

ipsec profile	Enables generic routing encapsulation (GRE) tunnel encryption via IPSec.
<i>name</i>	Name of the IPSec profile. This value must match the <i>name</i> specified in the crypto ipsec profile command.
shared	(Optional) Allows the tunnel protection IPSec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface. Note Unlike the tunnel protection command, which specifies that IPSec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation.

Defaults

Tunnel interfaces are not associated with IPSec profiles.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(5)T	The shared keyword was added through DDTS CSCec28392.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines

Use the **tunnel protection** command to specify that IPSec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPSec peer address. With mGRE tunnels, multiple IPSec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPSec peer addresses.

The shared Keyword

If you wish to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPSec tunnels on the same router with the same local endpoint (tunnel source) configuration, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

**Note**

GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

Examples

The following example shows how to associate the IPsec profile “vpnprof” with an mGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPsec destination peer address will be 172.16.2.1. The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**. Other NHRP mappings (static or dynamic) will automatically create additional IPsec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPsec proxy for these NHRP mappings will be as follows: **permit gre host ethernet0-ip-address host NHRP-mapping-NBMA-address**.

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
  ! receiving router would have to do the reassembly.
  ip mtu 1416
  ip nhrp authentication donttell
  ip nhrp map multicast dynamic
  ip nhrp network-id 99
  ip nhrp holdtime 300
  ! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
  ! advertise routes that are learned via the mGRE interface back out that interface.
  no ip split-horizon eigrp 1
  no ip next-hop-self eigrp 1
  delay 1000
  ! Sets the IPsec peer address to the Ethernet interface's public address.
  tunnel source Ethernet0
  tunnel mode gre multipoint
  ! The following line must match on all nodes that want to use this mGRE tunnel.
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

The following example shows how to associate the IPsec profile “vpnprof” with a p-pGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. The IPsec destination peer address will be 172.16.1.10 (per the **tunnel destination address** command). The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**.

```
interface Tunnel1
  ip address 10.0.1.1 255.255.255.252
  ! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
  ! receiving router would have to do the reassembly.
  ip mtu 1420
  tunnel source Ethernet0
  tunnel destination 172.16.1.10
  tunnel protection ipsec profile vpnprof
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
interface	Configures an interface type and enters interface configuration mode.
keepalive (tunnel interfaces)	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface.
permit	Sets conditions for a named IP access list.

url-list

To configure the list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSLVPN) and to enter URL configuration mode, use the **url-list** command in Web VPN configuration mode. To remove a URL, use the **no** form of this command.

url-list *list-name*

no url-list *list-name*

Syntax Description

<i>list-name</i>	URL list name.
------------------	----------------

Defaults

A URL is not shown on the portal page.

Command Modes

Web VPN configuration

Command History

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

Examples

The following example shows that the URL list name is Mylist:

```
url-list Mylist
```

Related Commands

Command	Description
heading	Sets the heading that is displayed above all URLs on the portal page of a SSLVPN.
url-text	Sets the text of the link to be displayed on the portal page and the URL that is under the link.
webvpn	Enters Web VPN configuration mode.

url-text

To set the text of the link that is to be displayed on the portal page and the URL that is under the link, use the **url-text** command in Web VPN URL configuration mode. To remove the text and URL or the text or URL, use the **no** form of this command.

url-text *text* **url-value** *URL*

no url-text *text* **url-value** *URL*

Syntax Description

<i>text</i>	Text of the link.
url-value <i>URL</i>	URL of the link.

Command Modes

Web VPN URL configuration

Command History

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

Usage Guidelines

There is no checking performed on the URL text or URL value before it is added to the URL list. It is up to the administrator to verify the effect of this command on the portal page.

Examples

The following example shows that the text for the link to be displayed on the portal page is “ENG” and that the URL is “Mycompany.com”:

```
Router (config)# webvpn
Router (config-webvpn)# url-list englist
Router (config-webvpn-url)# heading Engineering
Router (config-webvpn-url)# url-text ENG url-value http://www.Mycompany.com
```

Related Commands

Command	Description
heading	Sets the heading that is displayed above all URLs on the portal page of a SSLVPN.
url-list	Configures the list of URLs to which a user has access on the portal page of a SSLVPN and enters URL configuration mode.
webvpn	Enters Web VPN configuration mode.

user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user** command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

```
user username { password | nthash } password [group group-name]
```

```
no user username { password | nthash } password [group group-name]
```

Syntax Description

<i>username</i>	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
<i>password</i>	User password.
group <i>group-name</i>	(Optional) Name of group to which the user will be added.

Defaults

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

Examples

The following example shows that user “user1” has been allowed to authenticate using the local authentication server (using the password “userisok”). The user will be added to the group “team1”:

```
user user1 password userisok group team1
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	Specifies a VLAN to be used by members of a user group.

username

To establish a username-based authentication system, use the **username** command in global configuration mode. Use the **no** form of this command to remove an established username-based authentication.

username *name* { **nopassword** | **password** *password* | **password** *encryption-type* *encrypted-password* }

username *name* **password** *secret*

username *name* [**access-class** *number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]

username *name* **dnis**

username *name* [**nocallback-verify**]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* **user-maxlinks** *number*

username [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*

no username *name*

Syntax Description

<i>name</i>	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
nopassword	No password is required for this user to log in. This is usually most useful in combination with the autocommand keyword.
password	Specifies a possibly encrypted password for this username.
<i>password</i>	Password a user enters.
<i>encryption-type</i>	Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
<i>encrypted-password</i>	Encrypted password a user enters.
password	Password to access the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.

<i>secret</i>	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
access-class	(Optional) Specifies an outgoing access list that overrides the access list specified in the access-class line configuration command. It is used for the duration of the user's session.
<i>number</i>	(Optional) Access list number.
autocommand	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
<i>command</i>	(Optional) The command string. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
callback-dialstring	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
<i>telephone-number</i>	(Optional) For asynchronous callback only: telephone number to pass to the DCE device.
callback-rotary	(Optional) For asynchronous callback only: permits you to specify a rotary group number. The next available line in the rotary group is selected.
<i>rotary-group-number</i>	(Optional) For asynchronous callback only: integer between 1 and 100 that identifies the group of lines on which you want to enable a specific username for callback.
callback-line	(Optional) For asynchronous callback only: specific line on which you enable a specific username for callback.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
<i>line-number</i>	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you want to enable a specific username for callback. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as tty), then <i>line-number</i> and <i>ending-line-number</i> are absolute rather than relative line numbers.
dnis	Do not require password when obtained via DNIS.
nocallback-verify	(Optional) Authentication not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the autocommand keyword) has completed. Instead, the user gets another EXEC prompt.
privilege	(Optional) Sets the privilege level for the user.
<i>level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.

user-maxlinks	Limit the user's number of inbound links.
<i>number</i>	User-maxlinks limit for inbound links.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
<i>name</i>	Host name, server name, user ID, or command name. The name argument can be only one word. Blank spaces and quotation marks are not allowed.
privilege	(Optional) Sets the privilege level for the user.
<i>privilege-level</i>	(Optional) Number between 0 and 15 that specifies the privilege level for the user.
view	(Optional) For command-line interface (CLI) view only: associates a CLI view name with the local authentication, authorization, and accounting (AAA) database.
<i>view-name</i>	(Optional) For CLI view only: view name, which was specified via the parser view command, that is to be associated with the AAA local database.
password <i>password</i>	Password to access the CLI view.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords and arguments were added: <ul style="list-style-type: none"> username <i>name</i> [callback-dialstring <i>telephone-number</i>] username <i>name</i> [callback-rotary <i>rotary-group-number</i>] username <i>name</i> [callback-line [tty] <i>line-number</i> [<i>ending-line-number</i>]] username <i>name</i> [nocallback-verify]
12.3(7)T	The following keywords and arguments were added: <ul style="list-style-type: none"> lawful-intercept view <i>view-name</i>

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for the Challenge Handshake Authentication Protocol (CHAP). Add a username entry for each remote system from which the local router requires authentication.

**Note**

To enable the local router to respond to remote CHAP challenges, one **username name** entry must be the same as the **hostname** entry that has already been assigned to the other router.

**Note**

To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).

**Note**

Per-user privilege levels override virtual terminal (VTY) privilege levels.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If there is no *secret* specified and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example implements a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example implements an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example implements an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example enables CHAP on interface serial 0 of “server_1.” It also defines a password for a remote server named “server_r.”

```
hostname server_1
username server_r password theirsystem
interface serial 0
  encapsulation ppp
  ppp authentication chap
```

When you look at your configuration file, the passwords will be encrypted, and the display will look similar to the following:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
  encapsulation ppp
  ppp authentication chap
```

In both of the following configuration examples, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco

username user 2 privilege 2 password 0 cisco
```

The following example removes the username-based authentication for user 2:

```
no username user 2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username secret

To encrypt a user password with Message Digest 5 (MD5) encryption, use the **username secret** command in global configuration mode.

```
username name secret {[0] password | 5 encrypted-secret}
```

Syntax Description

<i>name</i>	Username.
0	(Optional) Clear text password, which will be MD5 encrypted.
<i>password</i>	Clear text password.
5 encrypted-secret	MD5-encrypted text string, which will be stored as the encrypted user password.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. The optional **0** keyword enables MD5 encryption on a clear text password; the **5** keyword enters an MD5 encryption string and saves it as the user MD5-encrypted secret. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using nonreversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Examples

The following example shows how to configure username “abc” and enable MD5 encryption on the clear text password “xyz”:

```
username abc secret xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

■ **username secret**

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

```
view view-name
```

```
no view view-name
```

Syntax Description

<i>view-name</i>	CLI view that is to be added to the given superview.
------------------	--

Defaults

A superview will not contain any CLI views until this command is enabled.

Command Modes

View configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **password 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
password5 <encoded password>
view view_one
view view_two
!
parser view su_view2 superview
password5 <encoded password>
view view_three
view view_four
!
```

Related Commands!

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
password 5	Associates a CLI view or a superview with a password.

vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

```
vlan vlan
```

```
no vlan vlan
```

Syntax Description

<i>vlan</i>	VLAN ID.
-------------	----------

Defaults

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

Examples

The following example shows that VLAN “225” *is* to be used by members of the user group:

```
vlan 225
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.

Command	Description
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

```
vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port {vpdn-nas | physical-channel-id}}
```

```
no vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port}
```

Syntax Description	
nas-ip-address vpdn-nas	Enable reporting of the VPDN NAS IP address to the AAA server.
nas-port vpdn-nas	Enable reporting of the VPDN NAS port to the AAA server.
nas-port physical-channel-id	Enable reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default AAA attributes are not reported to the AAA server.

Command Modes Global configuration

Command History	Release	Modification
	11.3 NA	This command was introduced.
	11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
	12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
	12.2(13)T	Support was added for the physical-channel-id keyword.

Usage Guidelines This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```

vpdn enable
vpdn-group 1
  accept-dialin
  protocol any
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id

```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```

vpdn enable
vpdn-group L2TP-tunnel
  accept-dialin
  protocol l2tp
  virtual-template 1
!
  terminate-from hostname nas1
  local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 171.79.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas

```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vrf (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf** command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

```
vrf ivrf
```

```
no vrf ivrf
```

Syntax Description

<i>ivrf</i>	VRF to which the IPSec tunnel will be mapped.
-------------	---

Defaults

The VRF will be the same as the front door VRF (FVRF).

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
  vrf vpn1
  keyring vpn1
  match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
  vrf vpn2
  keyring vpn2
  match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set vpn1
```

```
set isakmp-profile vpn1
match address 101
crypto map crypmap 3 ipsec-isakmp
set peer 10.1.1.1
set transform-set vpn2
set isakmp-profile vpn2
match address 102
!
!
interface Ethernet1/2
ip address 172.26.1.1 255.255.255.0
duplex half
no keepalive
no cdp enable
crypto map crypmap
```

webvpn

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

Web VPN configuration mode is not entered.

Command Modes

Global configuration

Command History

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

Examples

The following example shows that Web VPN configuration mode has been entered:

```
Router (config)# webvpn  
Router (config-webvpn)#
```

Related Commands

Command	Description
webvpn enable	Enables WebVPN in the system.

webvpn enable

To enable WebVPN in the system, use the **webvpn enable** command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

webvpn enable [*gateway-addr ip-address*]

no webvpn enable [*gateway-addr ip-address*]

Syntax Description	gateway-addr <i>ip-address</i>	(Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses.
---------------------------	--	--

Defaults WebVPN is disabled in the system.

Command Modes Web VPN configuration

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

Usage Guidelines This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

Examples The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

Related Commands	Command	Description
	webvpn	Enters Web VPN configuration mode.

wins

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

wins *primary-server secondary-server*

no wins *primary-server secondary-server*

Syntax Description

<i>primary-server</i>	Name of the primary WINS server.
<i>secondary-server</i>	Name of the secondary WINS server.

Defaults

No default behavior or values.

Command Modes

ISAKMP group configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **wins** command.

Examples

The following example shows how to define a primary and secondary WINS server for the group “cisco”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server client {any | eap | leap | mac} *list*

no wlccp authentication-server client {any | eap | leap | mac} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
<i>list</i>	List of client devices.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.

Command	Description
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no** form of this command.

wlccp authentication-server infrastructure *list*

no wlccp authentication-server infrastructure *list*

Syntax Description	<i>list</i>	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.
---------------------------	-------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

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

Command History	Release	Modification
	12.2(11)JA	This command was introduced on Cisco Aironet access points.
	12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:

```
Router (config)# wlccp authentication-server infrastructure wlan-list1
```

Related Commands	Command	Description
	debug wlccp packet	Displays packet traffic to and from the WDS router.
	debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
	show wlccp wds	Shows information about access points and client devices on the WDS router.
	wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
	wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide WDS, use the **wlccp wds priority interface** command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of the command .

wlccp wds priority *priority interface interface*

no wlccp wds priority *priority interface interface*

Syntax Description

<i>priority</i>	Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
<i>interface</i>	Interface on which the router sends out WDS advertisements. Supported interface types are as follows: <ul style="list-style-type: none"> • For access points—bvi • For wireless-aware routers—bvi, svi, Fast Ethernet, and Gigabit Ethernet.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.

Command	Description
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

xauth userid mode

To specify how the Easy VPN client handles extended authentication (Xauth) requests, use the **xauth userid mode** command in Cisco IOS Easy VPN remote configuration mode. To remove the setting, use the **no** form of this command.

```
xauth userid mode {http-intercept | interactive | local}
```

```
no xauth userid mode {http-intercept | interactive | local}
```

Syntax Description	http-intercept	HTTP connections are intercepted from the user through the inside interface and the prompt.
	interactive	To authenticate, the user must use the command-line interface (CLI) prompts on the console. Interactive is the default behavior.
	local	The saved username or password is used in the configuration.

Defaults If the command is not configured, the default behavior is interactive.

Command Modes Cisco IOS Easy VPN remote configuration

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

Usage Guidelines If you want to be prompted by the console, use the **interactive** keyword. If you want to use a saved username or password, use the **local** keyword. If a local username or password is defined, the mode changes to that username or password.

Examples The following example shows that HTTP connections will be intercepted from the user and that the user can authenticate using web-based activation:

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.0.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
  crypto ipsec client ezvpn tunnel22 inside !
interface Ethernet1
  ip address 192.0.0.13 255.255.255.128
  duplex auto
  crypto ipsec client ezvpn catch22
```

!

Related Commands	Command	Description
	crypto ipsec client ezvpn	Creates a Cisco Easy VPN remote configuration.
	debug crypto ipsec client ezvpn	Displays information about voice control messages that have been captured by the Voice DSP Control Message Logger.
	debug ip auth-proxy ezvpn	Displays information related to proxy authentication behavior for web-based activation.
	show crypto ipsec client ezvpn	Displays the Cisco Easy VPN Remote configuration.
	show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

