Consent Feature for Cisco IOS Routers

First Published: July 19, 2007
Last Updated: July 19, 2007

The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. This webpage lists the terms and conditions in which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent webpage.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Authentication Proxy with Consent Support" section on page 30.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

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

Prerequisites for Consent Feature for Cisco IOS Routers

To enable a consent webpage, you must be running an Advanced Enterprise image.

Information About Consent Feature for Cisco IOS Routers

Before enabling the consent feature for Cisco IOS routers, you should understand the following concepts:

Authentication Proxy Overview

Authentication proxy is an ingress authentication feature that grants access to an end user (out an interface) only if the user submits valid username and password credentials for an ingress traffic that is destined for HTTP, Telnet, or FTP protocols. After the submitted authentication credentials have been checked against the credentials that are configured on an Authentication, Authorization, Accounting (AAA) server, access is granted to the requester (source IP address).

When an end user posts an HTTP(S), FTP, or Telnet request on a router's authentication-proxy-enabled ingress interface, the Network Authenticating Device (NAD) verifies whether or not the same host has already been authenticated. If a session is already present, the ingress request is not authenticated again, and it is subjected to the dynamic (Auth-Proxy) ACEs and the ingress interface ACEs. If an entry is not present, the authentication proxy responds to the ingress connection request by prompting the user for a valid username and password. When authenticated, the Network Access Profiles (NAPs) that are to be applied are either downloaded from the AAA server or taken from the locally configured profiles.

An Integrated Consent–Authentication Proxy Webpage

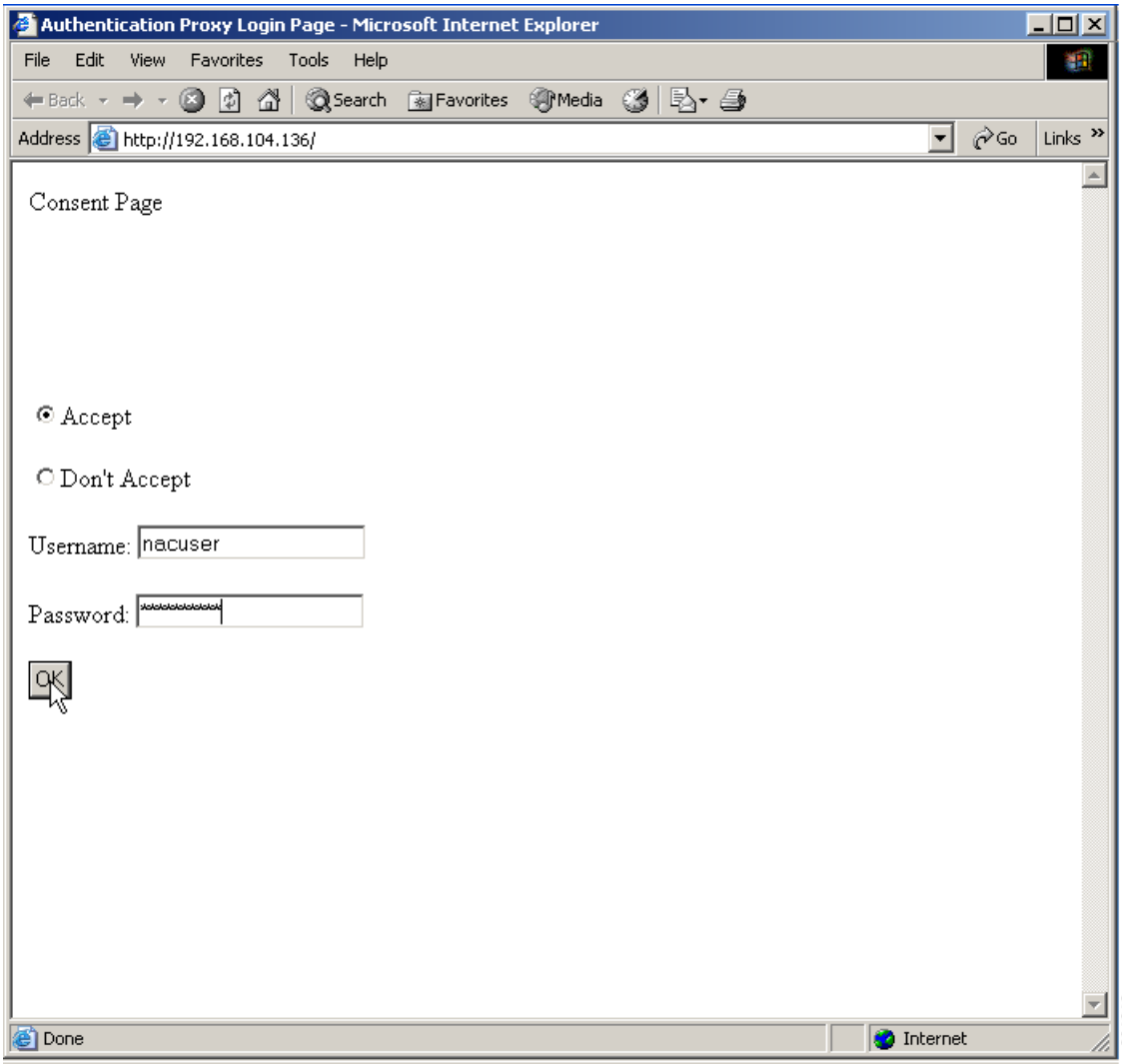
The HTTP authentication proxy webpage has been extended to support radio buttons—"Accept" and "Don't Accept"—for the consent webpage feature. The consent webpage radio buttons are followed by the authentication proxy input fields for a username and a password. (See Figure 1.)

The following consent scenarios are possible:

- If consent is declined (that is, the "Don't Accept" radio button is selected), the authentication proxy radio buttons are disabled. The ingress client session's access will be governed by the default ingress interface ACL.
- If consent is accepted (that is, the "Accept" radio button is selected), the authentication proxy radio buttons are enabled. If the wrong username and password credentials are entered, HTTP-Auth-Proxy authentication will fail. The ingress client session's access will again be governed only by the default ingress interface ACL.
- If consent is accepted (that is, the "Accept" radio button is selected) and valid username and password credentials are entered, HTTP-Auth-Proxy authentication is successful. Thus, one of the following possibilities can occur:
  - If the ingress client session's access request is HTTP_GET, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

– If the ingress client session's access request is HTTPS_GET, a "Security Dialogue Box" will be displayed on the client's browser. If the user selects YES on the Security Dialogue Box window, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs. If the user selects NO on the Security Dialogue Box window, the destination page will not open and the user will see the message "Page cannot be displayed." However the ingress client session's access will still be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

Figure 1 Consent WebPage: Example



How to Configure Authentication Proxy Consent

Use the following tasks to configure a consent webpage and enable a consent webpage that is to be displayed to end users:

- Configuring an IP Admission Rule for Authentication Proxy Consent, page 4
- Defining a Parameter Map for Authentication Proxy Consent, page 5

Configuring an IP Admission Rule for Authentication Proxy Consent

Use this task to define the IP admission rule for authentication proxy consent and to associate the rule with an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]
4. **ip admission consent banner** [**file** *file-name* | **text** *banner-text*]
5. **interface** *type number*
6. **ip admission** *admission-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]] **Example:** `Router(config)# ip admission name consent_rule consent absolute-timer 304 list 103 inactivity-time 204 parameter-map consent_parameter_map`	Defines the IP admission rule for authentication proxy consent.
Step 4	**ip admission consent banner** [**file** *file-name* | **text** *banner-text*] **Example:** `Router(config)# ip admission consent banner file flash:consent_page.html`	(Optional) Displays a banner in the authentication proxy consent webpage.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Specifies the interface in which the consent IP admission rule will be applied and enters interface configuration mode.
Step 6	**ip admission** *admission-name* **Example:** `Router(config-if)# ip admission consent_rule`	Applies the IP admission rule created in Step 3 to an interface.

Troubleshooting Tips

To display authentication proxy consent page information on the router, you can use the **debug ip admission consent** command.

```
Router# debug ip admission consent errors
IP Admission Consent Errors debugging is on

Router# debug ip admission consent events
IP Admission Consent Events debugging is on

Router# debug ip admission consent messages
IP Admission Consent Messages debugging is on
Router#
Router# show debugging

IP Admission Consent:
IP Admission Consent Errors debugging is on
IP Admission Consent Events debugging is on
IP Admission Consent Messages debugging is on
```

Defining a Parameter Map for Authentication Proxy Consent

Use this task to define a parameter map that is to be used for authentication proxy consent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type consent** *parameter-map-name*
4. **copy** *src-file-name dst-file-name*
5. **file** *file-name*
6. **authorize accept identity** *identity-policy-name*
7. **timeout file download** *minutes*
8. **logging enabled**
9. **exit**
10. **show parameter-map type consent** [*parameter-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type consent** *parameter-map-name* **Example:** `Router(config)# parameter-map type consent consent_parameter_map`	Defines an authentication proxy consent-specific parameter map and enters parameter-map type consent configuration mode. To use a default policy-map, enter **default** for the parameter-map-name.
Step 4	**copy** *src-file-name dst-file-name* **Example:** `Router(config-profile)# copy tftp://192.168.104.136/consent_page.html flash:consent_page.html`	Transfers a file (consent webpage) from an external server to a local file system on your device.
Step 5	**file** *file-name* **Example:** `Router(config-profile)# file flash:consent_page.html`	(Optional) Specifies a local filename that is to be used as the consent webpage.
Step 6	**authorize accept identity** *identity-policy-name* **Example:** `Router(config-profile)# authorize accept identity consent_identity_policy`	(Optional) Configures an accept policy. **Note** Currently, only an accept policy can be configured.
Step 7	**timeout file download** *minutes* **Example:** `Router(config-profile)# timeout file download 35791`	(Optional) Specifies how often the consent page file should be downloaded from the external TFTP server.
Step 8	**logging enabled** **Example:** `Router(config-profile)# logging enabled`	(Optional) Enables syslog messages.

	Command or Action	Purpose

Step 9	**exit**
	
	Example:
	`Router(config-profile )# exit`
	`Router(config)# exit`
		Returns to global configuration and privileged EXEC modes.

Step 10	**show parameter-map type consent** [*parameter-map-name*] **Example:** `Router# show parameter-map type consent`	(Optional) Displays all or a specified configured consent profiles.

Configuration Examples for Authentication Proxy Consent

This section contains the following configuration examples:

Ingress Interface ACL and Intercept ACL Configuration: Example

The following example shows how to define the ingress interface ACL (via the **ip access-list extended 102** command) to which the consent page policy ACEs will be dynamically appended. This example also shows how to define an intercept ACL (via the **ip access-list extended 103** command) to intercept the ingress interesting traffic by the IP admission consent rule.

```
ip access-list extended 102
 permit ip any 192.168.100.0 0.0.0.255
 permit ip any host 192.168.104.136
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any any eq www
 permit tcp any any eq 443
 permit udp any any eq 443
 exit
!
ip access-list extended 103
 permit ip any host 192.168.104.136
 permit udp any host 192.168.104.132 eq domain
 permit tcp any host 192.168.104.136 eq www
 permit udp any host 192.168.104.136 eq 443
 permit tcp any host 192.168.104.136 eq 443
 exit
!
```

Consent Page Policy Configuration: Example

The following example shows how to configure the consent page policy ACL and the consent page identity policy:

```
ip access-list extended consent-pg-ip-acc-group
 permit ip any host 192.168.104.128
 permit ip any host 192.168.104.136
 exit
!
identity policy consent_identity_policy
 description ### Consent Page Identity Policy ###
 access-group consent-pg-ip-acc-group
 exit
```

Parameter Map Configuration: Example

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map:

```
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
!
```

IP Admission Consent Rule Configuration: Example

The following example shows how to configure an IP admission consent rule, which includes the consent page parameter map as defined the in the "Parameter Map Configuration: Example" section:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 param-map
consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
 ip access-group 102 in
```

```
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
!
```

Additional References

The following sections provide references related to the Consent Feature for Cisco IOS Routers feature.

Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	The chapter "Configuring Authentication Proxy" in the *Cisco IOS Security Configuration Guide*

Standards

Standard	Title
None	—

MIBs

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

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

New Commands

- **authorize accept identity**
- **copy (consent-parameter-map)**
- **debug ip admission consent**
- **file (consent-parameter-map)**
- **ip admission consent banner**
- **logging enabled**
- **timeout file download**

Modified Commands

- **ip admission name**
- **parameter-map type**
- **show ip admission**

authorize accept identity

To configure an identity policy profile, use the **authorize accept identity** command in parameter-map-type consent configuration mode. To remove an identity policy profile, use the **no** form of this command.

authorize accept identity *identity-policy-name*

no authorize accept identity *identity-policy-name*

Syntax Description

identity-policy-name	Name of identify profile.

Command Default

An identity policy does not exist.

Command Modes

Parameter-map-type consent (config-profile)

Command History

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

Usage Guidelines

If an identity policy is not configured, the interface policy will be used.

Examples

The following example shows how to configure accept policies within the consent-specific parameter maps:

```
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
!
```

copy (consent-parameter-map)

To configure a consent page to be downloaded from a file server, use the **copy** command in parameter-map type consent configuration mode.

copy *src-file-name dst-file-name*

Syntax Description

src-file-name	Source file location in which the specified file will be retrieved. The source file location must be TFTP; for example, tftp://10.1.1.1/username/myfile.
dst-file-name	Destination location in which a copy of the file will be stored. The destination file should be copied to Flash; for example, flash.username.html.

Command Default

The consent page that is specified via the default parameter-map will be used.

Command Modes

Parameter-map-type consent (config-profile)

Command History

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

Usage Guidelines

Use the **copy** command to transfer a file (consent web page) from an external server to a local file system on a device. Thus, the file name specified via the **copy** command is retrieved from the destination file location and displayed to the end user as the consent page.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used.

Examples

In the following example, both parameter maps are to use the consent file "tftp://192.168.104.136/consent_page.html" and store it in "flash:consent_page.html":

```
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
!
```

Related Commands

Command	Description
file (consent-parameter-map)	Specifies a local filename that is to be used as the consent webpage.

debug ip admission consent

To display authentication proxy consent page information on the router, use the **debug ip admission consent** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip admission consent [**events** | **errors** | **messages**]

no debug ip admission consent

Syntax Description

errors	(Optional) Displays only error messages.
events	(Optional) Displays only event-related messages.
messages	(Optional) Displays only packet-related messages.

Command Default

If an option is not selected, all debug messages are displayed.

Command Modes

Privileged EXEC

Command History

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

Examples

```
Router# debug ip admission consent errors
IP Admission Consent Errors debugging is on

Router# debug ip admission consent events
IP Admission Consent Events debugging is on

Router# debug ip admission consent messages
IP Admission Consent Messages debugging is on
Router#
Router# show debugging

IP Admission Consent:
IP Admission Consent Errors debugging is on
IP Admission Consent Events debugging is on
IP Admission Consent Messages debugging is on
```

file (consent-parameter-map)

To specify a local filename that is to be used as the consent webpage, use the **file** command in parameter-map-type consent configuration mode.

file *file-name*

Syntax Description

file-name	Filename that is to be used as the consent webpage.

Command Default

The consent page that is specified via the default parameter-map will be used.

Command Modes

Parameter-map-type consent (config-profile)

Command History

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

Usage Guidelines

If a file is already available on the router or if the file has already been transferred to a local system (via the **copy** command), use the **file** command to specify the local filename.

When a consent webpage is displayed to an end user, the filename specified via the **file** command is used. If the file command is not configured, the destination location specified via the **copy** command is used.

Examples

In the following example, both parameter maps are to use the consent file "tftp://192.168.104.136/consent_page.html" and store it in "flash:consent_page.html":

```
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
```

Related Commands

Command	Description
copy (consent-parameter-map)	Configures a consent page to be downloaded from a file server.

ip admission consent banner

To display a banner on the authentication proxy consent webpage, use the **ip admission consent banner** command in global configuration mode. To disable a display of the banner, use the **no** form of this command.

ip admission consent banner {**file** *file-name* | **text** *banner-text*}

no ip admission consent banner

Syntax Description

file *file-name*	Specifies a file that is to be shown as the consent webpage.
text *banner-text*	Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C *banner-text* C," where "C" is a delimiting character.

Command Default

A banner is not displayed on the authentication proxy consent webpage.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ip admission consent-banner** command allows users to configure one of two possible scenarios:

- The **ip admission consent-banner** command with a filename is enabled.

  In this scenario, the administrator supplies the location and name of the file that is to be used for the consent webpage.

- The **ip admission consent-banner** command with the banner text is enabled.

  In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text is displayed on the authentication proxy login page.

Note If the **ip admission consent-banner** command is not enabled, nothing will be displayed to the user on a consent login page except a text box to enter the username and a text box to enter the password.

Examples

The following example shows how to display the file "consent_page.html" located in flash:

```
ip admission consent-banner file flash:consent_page.html
```

The following example shows how to specify the custom banner "Consent-Page-Banner-Text" to be displayed in the authentication proxy consent webpage:

```
ip admission consent-banner text ^C Consent-Page-Banner-Text ^C
```

Related Commands

Command	Description
ip auth-proxy auth-proxy-banner	Displays a banner, such as the router name, in the authentication proxy login page.

ip admission name

To create an IP network admission control rule, use the **ip admission name** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]

no ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]

Syntax for Authentication Proxy Consent Webpage

ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

no ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).
bypass	(Optional) Admission rule bypasses EAPoUDP communication.
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag** {*policy name*} command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.
event	(Optional) Identifies the condition that triggered the application of the policy.
timeout aaa	(Optional) Specifies that the AAA server is unreachable.
policy identity	Configures the application of an identity policy to be used while the AAA server is unreachable.
identity-policy-name	Specifies the identity policy to apply.

consent	Associates an authentication proxy consent webpage with the IP admission rule specified via the *admission-name* argument.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
parameter-map	(Optional) A parameter map policy is to be associated with consent profile.
consent-parameter-map-name	Specifies the consent profile parameters to apply.

Command Default

An IP network admission control rule is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **bypass** and **service-policy type tag** keywords and *service-policy-name* argument were added.
12.4(11)T	The **event**, **timeout aaa**, and **policy identity** keywords and the *identity-policy-name* argument were added.
12.4(15)T	The following keywords and arguments were added: **consent**, **absolute-timer,** *minutes*, **inactivity-time**, *minutes,* **parameter-map**, and *consent-parameter-map-name*.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {*service-policy-name*} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the *identity-policy-name* argument allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

The **consent** keyword and the **parameter-map** *consent-parameter-map-name* keyword and argument allow you to associate the authentication proxy consent feature with an IP admission rule. The consent feature enables customers to display a consent webpage to an end user, providing access to wireless services only after the end user accepts the agreement.

Examples

"Tag and Template" Feature Examples

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

Class Map Definition for the "healthy class" Type Tag

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Class Map Definition for the "non_healthy_class" Type Tag

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Policy Map Definition

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
! The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router(config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Identity Policy Definition

```
Router (config)# identity policy healthy_policy
```

```
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy
Router (config-identity-policy)# end
```

Defining Access Lists

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end
```

Associating the Policy Map with the IP Admission Name

```
Router (config)# ip admission name greentree service-policy type tag global_class
! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

NAC—Auth Fail Open Feature Examples

The following example shows how to define an IP admission control rule named “samplerule” and attach it to a specific interface:

```
Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy
identity aaa_fail_policy
Router (config)# interface fastethernet 1/1
Router (config-if)# ip admission samplerule
Router (config-if)# end
```

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

Authentication Proxy Consent Webpage Example

The following example shows how to configure an IP admission consent rule and associate the consent rule with the definitions of the parameter map “consent_parameter_map”:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304
parameter-map consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
```

```
 ip access-group 102 in
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
!
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

logging enabled

To enable syslog messages, use the **logging enabled** command in parameter-map-type consent configuration mode.

logging enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Logging messages are not enabled.

Command Modes

Parameter-map-type consent (config-profile)

Command History

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

Usage Guidelines

After the **logging enabled** command is entered, a log entry (a syslog), including the client's IP address and the time, is created everytime a response is received for the consent web page.

Examples

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map. In both parameter maps, logging is enabled.

```
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
```

parameter-map type

To create or modify a parameter map, use the **parameter-map type** command in global configuration mode. To delete a parameter map from the configuration, use the **no** form of this command.

parameter-map type {**inspect** | **urlfilter** | **protocol-info** | **consent**} *parameter-map-name*

no parameter-map type {**inspect** | **urlfilter** | **protocol-info** | **consent**} *parameter-map-name*

Syntax Description

inspect	Defines an inspect type parameter map, which configures connection thresholds, timeouts, and other parameters pertaining to the **inspect** action.
urlfilter	Defines a URL-filter-specific parameter map.
protocol-info	Defines an application-specific parameter map. **Note** Protocol-specific parameter maps can be created only for Instant Messenger (IM) applications (AOL, MSN Messenger, and Yahoo Messenger).
consent	Defines an authentication proxy consent parameter map.
parameter-map-name	Name of the parameter map.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **protocol-info** keyword was added.
12.4(15)T	The **consent** keyword was added.

Usage Guidelines

A parameter map allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

There are currently four types of parameter maps:

- Inspect parameter map

  An inspect parameter map is optional. If you do not configure a parameter map, the software uses default parameters. Parameters associated with the inspect action apply to all nested actions (if any). If parameters are specified in both the top and lower levels, those in the lower levels override those in the top levels.

- URL filter parameter map

  A parameter map is required for URL filtering (via the URL filter action in a Layer 3 or Layer 4 policy map and the URL filter parameter map).

- Protocol-specific parameter map

  A parameter map is required for an IM application (Layer 7) policy map.
- Authentication proxy consent-specific parameter map.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and AOL traffic is allowed to pass through, while all MSN Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and AOL traffic on a more granular level.

```
! Define Layer 7 class-maps.
class-map type inspect ymsgr match-any l7-cmap-ymsgr
 match service text-chat
!
class-map type inspect aol match-any l7-cmap-aol
 match service text-chat
 match service any
!
! Define Layer 7 policy-maps.
policy-map type inspect im l7-pmap-ymsgr
 class-type inspect ymsgr l7-cmap-ymsgr
  allow
  alarm
!
!
policy-map type inspect im l7-pmap-aol
 class-type inspect aol l7-cmap-aol
  allow
  alarm
!
!
! Define parameter map.
parameter-map type protocol-info ymsgr
 server name sdsc.msg.yahoo.com
 server ip 10.1.1.1
!
parameter-map type protocol-info aol
 server name sdsc.msg.aol.com
 server ip 172.16.1.1.
```

The following example shows a typical URL filter parameter map configuration:

```
parameter-map type urlfilter eng-filter-profile
 server vendor n2h2 172.16.1.2 port 3128 outside log timeout 10 retrans 6
 max-request 80
 max-resp-pak 200
 cache 200
 exclusive-domain permit cisco.com
 exclusive-domain deny gaming.com
```

The following example shows a sample inspect type parameter map configuration:

```
parameter-map type inspect eng_network_profile
 audit-trail on
 alert off
 max-incomplete low 2000
 max-incomplete high 3000
 one-minute low 5000
 one-minute high 8000
 udp idle-time 75
 dns-timeout 25
 tcp idle-time 90
```

```
 tcp finwait-time 20
 tcp synwait-time 10
 tcp block-non-session
 tcp max-incomplete host 2000 block-time 120
```

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map:

```
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
!
```

show ip admission

To display the network admission (NAC) control cache entries or the running network admission control configuration, use the **show ip admission** command in privileged EXEC mode.

show ip admission {[**cache** [**consent**]] [**configuration**] [**eapoudp**]}

Syntax Description

cache	Displays the current list of network admission entries.
consent	Displays the authentication proxy consent webpage sessions.
configuration	Displays the running network admission control configuration.
eapoudp	Displays the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) network admission control entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	The **consent** keyword was added.

Usage Guidelines

Use **show ip admission cache eapoudp** to list the host IP addresses, the session timeout, and the posture state. If the posture statue is POSTURE ESTAB, the host validation was successful.

Examples

The following output displays all the IP admission control rules that are configured on the router:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name avrule
    eapoudp list not specified auth-cache-time 60 minutes
```

The following output displays the host IP addresses, the session timeout, and the posture states:

```
Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The following output displays a configuration that includes both a global and a rule-specific NAC Auth Fail Open policy:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 1 minutes
! The line below shows the global policy:
Authentication global AAA fail identity policy aaa_fail_policy
Authentication Proxy Rule Configuration Auth-proxy name greentree
    eapoudp list 101 specified auth-cache-time 60 minutes
! The line below shows the rule-specific AAA fail policy; the name changes based on what
the user configured.
    Identity policy name aaa_fail_policy for AAA fail policy
```

The field descriptions in the display are self-explanatory.

In the following example, a session has been initiated via https://192.168.104.136 from the client 192.168.100.132. After a successful session establishment, the output is as follows:

```
Router# show ip admission cache

Authentication Proxy Cache
 Client Name N/A, Client IP 192.168.100.132, Port 1204, timeout 204, Time Remaining 204,
 state ESTAB

Router# show ip admission cache consent

Authentication Proxy Consent Cache
 Client Name N/A, Client IP 192.168.100.132, Port 1204, timeout 204, Time Remaining 204,
 state ESTAB

Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 0 Init Sessions: 0
```

Related Commands

Command	Description
clear ip admission cache	Clears IP admission cache entries from the router.
ip admission name	Creates a Layer 3 network admission control rule.

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.

timeout file download *minutes*

Syntax Description

minutes	Specifies, in minutes, 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 ensurs that the consent file has the most current parameter map defintions.

Examples

In the following example, the file “consent_page.html” and the default 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
!
```

Feature Information for Authentication Proxy with Consent Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Authentication Proxy with Consent Support

Feature Name	Releases	Feature Information
Consent Feature for Cisco IOS Routers	12.4(15)T	This feature enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. This webpage lists the terms and conditions in which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent webpage.