Consent Feature for Cisco IOS Routers

Last Updated: January 18, 2012

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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

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

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).

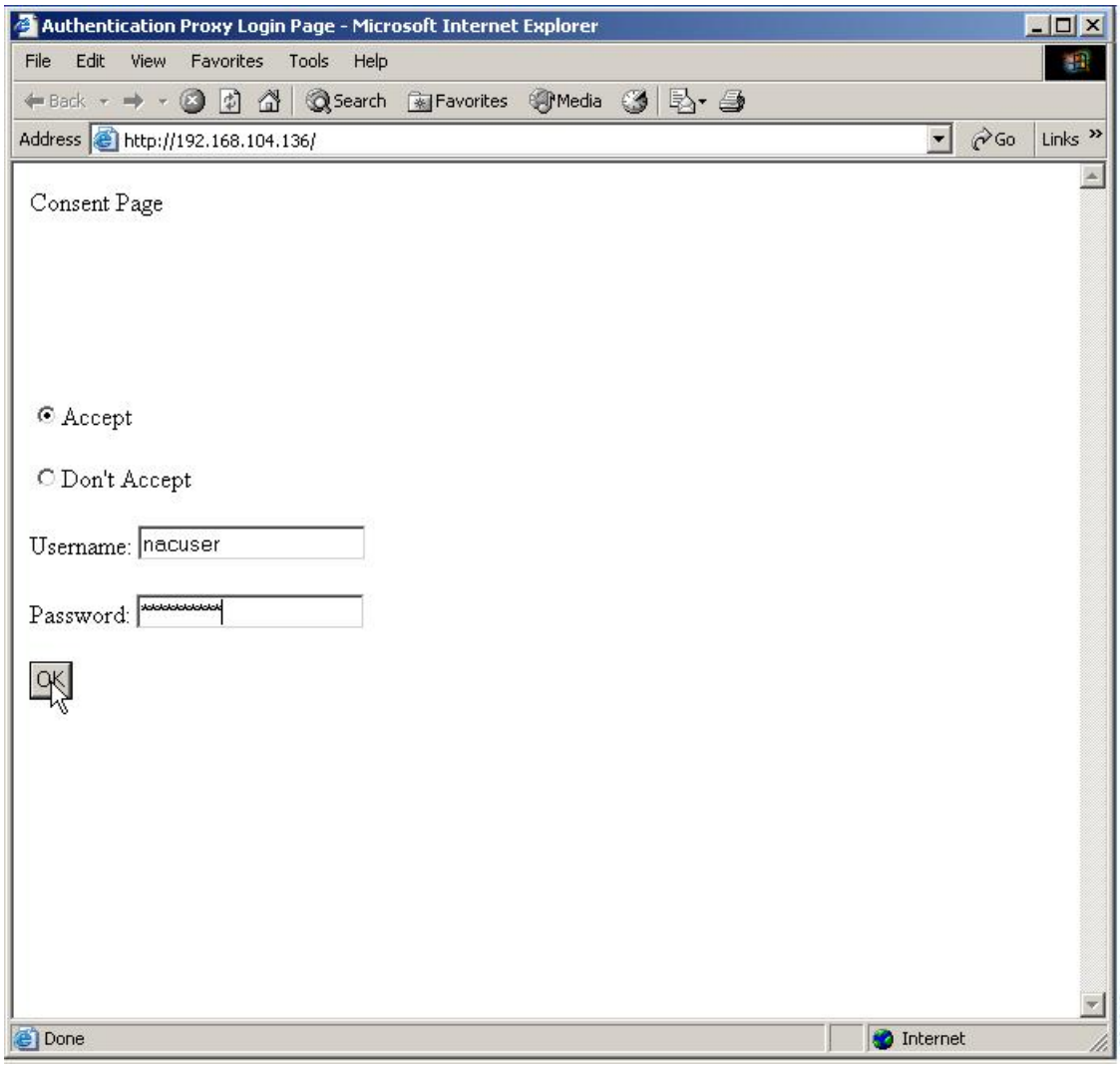
When an end user posts an HTTP(S), FTP, or Telnet request on a router's authentication-proxy-enabled ingress interface, the Network Authenticating Device (NAD) verifies whether or not the same host has already been authenticated. If a session is already present, the ingress request is not authenticated 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 the figure below.)

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.



Note When HTTP authentication proxy is configured together with the Consent feature, any HTTP authentication proxy-related configurations or policies will override the Consent Page-related configurations or policies. For example, if the **ip admission name** *admission-name* **consent**command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is shown.

How to Configure Authentication Proxy Consent

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, page 5

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.

	Command or Action	Purpose
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.

Step 9	**exit**
	
	Example:
	`Router(config-profile )# exit`
	
	Example:
	`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

- Ingress Interface ACL and Intercept ACL Configuration Example, page 8

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	See the Configuring Authentication Proxy feature module

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

Feature Information for Consent Feature for Cisco IOS Routers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for Consent Feature for Cisco IOS Routers

Feature Name	Releases	Feature Information
Consent Feature for Cisco IOS Routers	12.4(15)T	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. In Cisco IOS Release 12.4(15)T, this feature was introduced. The following commands were introduced or modified: **authorize accept identity**, **copy (consent-parameter-map)**, **debug ip admission consent**, **file (consent-parameter-map)**, **ip admission consent banner**, **ip admission name**, **logging enabled**, **parameter-map type**, **show ip admission**, **timeout file download**