



Authentication Proxy Configuration Guide, Cisco IOS Release 15E

First Published: January 16, 2013

Last Modified: December 10, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Web Authentication Enhancements—Customizing Authentication Proxy Web Pages 1

- Finding Feature Information 1
- Prerequisites for Customizing Authentication Proxy Web Pages 2
- Restrictions for Customizing Authentication Proxy Web Pages 2
- Information About Customizing Authentication Proxy Web Pages 2
 - Custom Authentication Proxy Web Pages 2
 - Images for Custom Web Pages 3
 - Result Display Enhancement 3
 - Custom Web Authentication Download Bundle 3
 - Virtual IP Support for Images 3
 - Parameter Map for Custom Authentication Proxy Web Pages 4
- How to Configure Custom Authentication Proxy Web Pages 4
 - Configuring Custom Authentication Proxy Web Pages 4
 - Specifying a Redirect URL for Successful Login 5
 - Configuring a Parameter Map for Custom Authentication Proxy Web Pages 6
 - Verifying the Configuration of Parameter Maps for Custom Authentication Proxy Web Pages 9
 - Verifying the Configuration of a Global Parameter Map 9
 - Verifying the Configuration of a Named Parameter Map 10
- Configuration Examples for Customization of Authentication Proxy Web Pages 11
 - Example: Configuring Custom Authentication Web Pages 11
 - Example: Configuring a Redirection URL for Successful Login 11
 - Example: Configuring Parameter Maps for Custom Authentication Proxy Web Pages 12
- Additional References 13
- Feature Information for Customization of Authentication Proxy Web Pages 14

CHAPTER 2

Webauth Sleeping Client 17

- Finding Feature Information 17

- Restrictions for Webauth Sleeping Client **17**
- Information About Webauth Sleeping Client **18**
 - Sleeping client cache **18**
- How to Configure Webauth Sleeping Client **18**
 - Configuring Sleeping Client Timer **18**
 - Verifying Sleeping Client Entries **20**
- Configuration Examples for Webauth Sleeping Client **21**
 - Example: Configuring Sleeping Client Timer **21**
- Additional References for Webauth Sleeping Client **21**
- Feature Information for Webauth Sleeping Client **22**



CHAPTER

1

Web Authentication Enhancements—Customizing Authentication Proxy Web Pages

The Web Authentication Enhancements—Customizing Authentication Proxy Web Pages feature allows you to display four HTML pages to users in place of the switch's internal default HTML pages during web-based authentication. The four pages are Login, Success, Fail, and Expire.

This module also describes the following enhancement features for the custom HTML pages:

- Custom Web Authentication Result Display Enhancement feature—ensures that the authentication results display on the main HTML page.
- Support for Custom Web Authentication Download Bundle feature—ensures that one or more custom HTML pages can be downloaded and configured from a single tar file bundle.
- Virtual IP Support for Images in Custom Web Authentication feature—ensures that users can configure a virtual IP address.
- [Finding Feature Information, page 1](#)
- [Prerequisites for Customizing Authentication Proxy Web Pages, page 2](#)
- [Restrictions for Customizing Authentication Proxy Web Pages, page 2](#)
- [Information About Customizing Authentication Proxy Web Pages, page 2](#)
- [How to Configure Custom Authentication Proxy Web Pages, page 4](#)
- [Configuration Examples for Customization of Authentication Proxy Web Pages, page 11](#)
- [Additional References, page 13](#)
- [Feature Information for Customization of Authentication Proxy Web Pages, page 14](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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 Customizing Authentication Proxy Web Pages

- To enable the custom web pages feature, you must specify all four custom HTML files.
 - If fewer than four files are specified, the internal default HTML pages are used.
 - The four custom HTML files must be present on the disk or flash of the switch.
- Any external link from a custom page requires the configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images requires the configuration of an intercept ACL within the admission rule to access a valid DNS server.

Restrictions for Customizing Authentication Proxy Web Pages

- If the custom web pages feature is enabled, a configured auth-proxy-banner cannot be used.
- If the custom web pages feature is enabled, the redirect URL for successful login feature is not available.

Information About Customizing Authentication Proxy Web Pages

Custom Authentication Proxy Web Pages

The switch's internal HTTP server hosts four custom HTML pages (in addition to the four default internal HTML pages) for delivery to an authenticating client during the web-based authentication process. These four pages allow the server to notify the user of the following four states of the authentication process:

- Login—User credentials are requested.
- Success—Login is successful.
- Fail—Login has failed.
- Expire—The login session has expired due to excessive login failures.

You can substitute your custom HTML pages for the four default internal HTML pages or you can specify a URL to which the user is redirected after a successful authentication; effectively replacing the internal success page.

This module describes two methods by which you can configure custom web pages:

- Using the **ip admission proxy** command.

- Using the **parameter-map type webauth** command for identity control policy-based access session management.

Images for Custom Web Pages

This section describes the guidelines for all images on the custom web pages:

- An image file has a size limit of 256 KB.
- All image files must have a filename that begins with “web_auth_” (such as “web_auth_logo.jpg” instead of “logo.jpg”).



Note The Virtual IP Support for Images in Custom Web Authentication feature supports image filenames that do not require any prefix. Users can specify any image name.

- All image filenames must be less than 63 characters.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.

Result Display Enhancement

The Custom Web Authentication Result Display Enhancement feature displays the authentication results on the main HTML page. There is no pop-up window to display the authentication results.

Custom Web Authentication Download Bundle

The Support for Custom Web Authentication Download Bundle feature ensures that one or more custom HTML pages can be downloaded and configured from a single tar file bundle. The images and the custom pages containing the images are also part of the same downloadable tar file bundle.

Virtual IP Support for Images

The Virtual IP Support for Images in Custom Web Authentication feature supports the following enhancements:

- Image filenames do not require any prefix. Users can specify any image name.
- Users need not specify the wireless management interface IP address to indicate the source of the image in the HTML code. Instead, users can configure the **virtual-ip** command in parameter-map webauth configuration mode (config-params-parameter-map) and specify a virtual IP address. For more information about the **virtual-ip** command, see the “Configuring a Parameter Map for Custom Authentication Proxy Web Pages” section or the *Cisco IOS Security Command Reference: Commands S to Z*.

Parameter Map for Custom Authentication Proxy Web Pages

A parameter map allows you to modify parameters that control the behavior of actions configured under a control policy. A parameter map for web-based authentication sets parameters that can be applied to subscriber sessions during authentication. If you do not create a parameter map, the policy uses default parameters.

How to Configure Custom Authentication Proxy Web Pages

Configuring Custom Authentication Proxy Web Pages

To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch's internal disk or flash memory and then perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file** *device:login-filename*
4. **ip admission proxy http success page file** *device:success-filename*
5. **ip admission proxy http failure page file** *device:fail-filename*
6. **ip admission proxy http expired page file** *device:expired-filename*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip admission proxy http login page file <i>device:login-filename</i> Example: Device(config)# ip admission proxy http login page file disk1:login.htm	Specifies the location in the switch memory file system of the custom HTML file to be used in place of the default login page. <ul style="list-style-type: none"> • The device: is either disk or flash memory, such as disk0:.

	Command or Action	Purpose
Step 4	ip admission proxy http success page file <i>device:success-filename</i> Example: <pre>Device(config)# ip admission proxy http success page file disk1:success.htm</pre>	Specifies the location of the custom HTML file to be used in place of the default login success page.
Step 5	ip admission proxy http failure page file <i>device:fail-filename</i> Example: <pre>Device(config)# ip admission proxy http failure page file disk1:fail.htm</pre>	Specifies the location of the custom HTML file to be used in place of the default login failure page.
Step 6	ip admission proxy http expired page file <i>device:expired-filename</i> Example: <pre>Device(config)# ip admission proxy http expired page file disk1:expired.htm</pre>	Specifies the location of the custom HTML file to be used in place of the default login expired page.
Step 7	end Example: <pre>Device(config)# end</pre>	Exits global configuration mode and returns to privileged EXEC mode.

Specifying a Redirect URL for Successful Login

Before You Begin



Note You can specify a URL to which the user will be redirected upon successful authentication, effectively replacing the internal Success HTML page.

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available. You can perform redirection in the custom login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission proxy http success redirect *url-string***
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip admission proxy http success redirect <i>url-string</i> Example: Device(config)# ip admission proxy http success redirect www.company.com	Specifies a URL for redirection of the user in place of the default login success page.
Step 4	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Parameter Map for Custom Authentication Proxy Web Pages

Perform the following steps to define either a global or named parameter map for web-based authentication.

**Note**

The configuration commands available in the global parameter map differ from the commands available in a named parameter map.

Before You Begin

Ensure that you configure a parameter map for identity control policy-based access session management.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth** {*parameter-map-name* | **global**}
4. **banner** {**file** *location:filename* | **text** *banner-text*}
5. **consent email**
6. **custom-page** {**failure** | **login** [**expired**] | **success**} **device** *location:filename*
7. **max-http-conns** *number*
8. **redirect** {{**for-login** | **on-failure** | **on-success**} *url* | **portal** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}}
9. **timeout init-state** *sec seconds*
10. **type** {**authbypass** | **consent** | **webauth** | **webconsent**}
11. **timeout fin-wait** *msec milliseconds*
12. **virtual-ip** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*}
13. **watch-list** {**add-item** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} | **dynamic-expiry-timeout** *minutes* | **enabled**}
14. **end**
15. **show ip admission status** [**banners** | **custom-pages** | **parameter-map** [*parameter-map*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	parameter-map type webauth { <i>parameter-map-name</i> global }	Creates a parameter map and enters parameter-map webauth configuration mode. • The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the <i>parameter-map-name</i> argument.
Step 4	banner { file <i>location:filename</i> text <i>banner-text</i> }	(Optional) Displays a banner on the web-authentication login web page.
	Example: Device(config-params-parameter-map)# banner file flash:webauth_banner.html	

	Command or Action	Purpose
Step 5	<p>consent email</p> <p>Example: Device(config-params-parameter-map)# consent email</p>	<p>(Optional) Requests a user's e-mail address on the web-authentication login web page.</p> <ul style="list-style-type: none"> This command is supported in named parameter maps only.
Step 6	<p>custom-page {failure login [expired] success} device location:filename</p> <p>Example: Device(config-params-parameter-map)# custom-page login device flash:webauth_login.html Device(config-params-parameter-map)# custom-page login expired device flash:webauth_expire.html Device(config-params-parameter-map)# custom-page success device flash:webauth_success.html Device(config-params-parameter-map)# custom-page failure device flash:webauth_fail.html</p>	<p>(Optional) Displays custom authentication proxy web pages during web-based authentication.</p> <ul style="list-style-type: none"> You must configure all four custom HTML files. If fewer than four files are configured, the internal default HTML pages will be used.
Step 7	<p>max-http-conns number</p> <p>Example: Device(config-params-parameter-map)# max-http-conns 5</p>	<p>(Optional) Limits the number of HTTP connections for each web authentication client.</p>
Step 8	<p>redirect {{for-login on-failure on-success} url portal {ipv4 ipv4-address ipv6 ipv6-address}}</p> <p>Example: Device(config-params-parameter-map)# redirect portal ipv6 FE80::1 Device(config-params-parameter-map)# redirect on-failure http://10.10.3.34/~sample/failure.html</p>	<p>(Optional) Redirects users to a particular URL during web-based authentication.</p>
Step 9	<p>timeout init-state sec seconds</p> <p>Example: Device(config-params-parameter-map)# timeout init-state sec 60</p>	<p>(Optional) Sets the initial state timeout, in seconds, for web-based authentication sessions.</p>
Step 10	<p>type {authbypass consent webauth webconsent}</p> <p>Example: Device(config-params-parameter-map)# type consent</p>	<p>(Optional) Defines the methods supported by a web-based authentication parameter map.</p> <ul style="list-style-type: none"> This command is supported only for named parameter maps.
Step 11	<p>timeout fin-wait msec milliseconds</p> <p>Example: Device(config-params-parameter-map)# timeout fin-wait msec 30</p>	<p>(Optional) Sets the TCP finish (FIN) packet timeout for web-based authentication sessions.</p>

	Command or Action	Purpose
Step 12	virtual-ip { ipv4 <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } Example: Device(config-params-parameter-map)# virtual-ip ipv6 FE80::1	(Optional) Specifies a virtual IP address for web-based authentication clients. <ul style="list-style-type: none"> This command is supported only for global parameter maps.
Step 13	watch-list { add-item { ipv4 <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } dynamic-expiry-timeout <i>minutes</i> enabled } Example: Device(config-params-parameter-map)# watch-list enabled Device(config-params-parameter-map)# watch-list dynamic-expiry-timeout 20 Device(config-params-parameter-map)# watch-list add-item ipv6 FE80::1	(Optional) Enables a watch list of web-based authentication clients. <ul style="list-style-type: none"> This command is supported only for global parameter maps.
Step 14	end Example: Device(config-params-parameter-map)# end	(Optional) Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
Step 15	show ip admission status [banners custom-pages parameter-map [<i>parameter-map</i>]] Example: Device# show ip admission status custom-pages	(Optional) Displays information about configured banners and custom pages.

Verifying the Configuration of Parameter Maps for Custom Authentication Proxy Web Pages

Verifying the Configuration of a Global Parameter Map

Perform this task to verify the configuration of a global parameter map for custom authentication proxy web pages.

SUMMARY STEPS

- enable
- show parameter-map type webauth global

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show parameter-map type webauth global**

Displays the configuration of a global parameter map for custom authentication proxy web pages.

Example:

```
Device# show parameter-map type webauth global

Parameter Map Name      : global
Type                    : none
Custom Page:
  Auth-proxy login      : flash:login.html
Auth-proxy Init State time : 120 sec
Auth-proxy Fin Wait time : 3000 milliseconds
Webauth max-http connection : 30
Webauth logout-window   : Enabled
Consent Email           : Disabled
Virtual-ipv4            : 3.3.3.10
Webauth intercept https : Disabled
Watch-list:
  Enabled                : no
Webauth login-auth-bypass:
```

Verifying the Configuration of a Named Parameter Map

Perform this task to verify the configuration of a named parameter map for custom authentication proxy web pages.

SUMMARY STEPS

1. **enable**
2. **show parameter-map type webauth *parameter-map-name***

DETAILED STEPS

Step 1

enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 `show parameter-map type webauth parameter-map-name`

Displays the configuration of a named parameter map (webauth-name1) for custom authentication proxy web pages.

Example:

```
Device# show parameter-map type webauth webauth-name1

Parameter Map Name           : webauth-name1
Type                         : webauth
Auth-proxy Init State time   : 120 sec
Auth-proxy Fin Wait time     : 3000 milliseconds
Webauth max-http connection  : 30
Webauth logout-window        : Enabled
Consent Email                 : Disabled
Webauth login-auth-bypass:
```

Configuration Examples for Customization of Authentication Proxy Web Pages

Example: Configuring Custom Authentication Web Pages

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http login page file disk1:login.htm
Device(config)# ip admission proxy http success page file disk1:success.htm
Device(config)# ip admission proxy http failure page file disk1:fail.htm
Device(config)# ip admission proxy http expired page file disk1:expired.htm
Device(config)# end
```

Example: Configuring a Redirection URL for Successful Login

```
Device> enable
Device# configure terminal
Device(config)# ip admission proxy http success redirect www.company.com
Device(config)# end
```

Example: Configuring Parameter Maps for Custom Authentication Proxy Web Pages

Global Parameter Map

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# timeout init-state sec 60
Device(config-params-parameter-map)# logging enabled
Device(config-params-parameter-map)# watch-list enabled
Device(config-params-parameter-map)# virtual-ip ipv6 FE80::1
Device(config-params-parameter-map)# redirect on-failure
Device(config-params-parameter-map)# http://10.10.3.34/~sample/failure.html
Device(config-params-parameter-map)# max-http-conns 100
Device(config-params-parameter-map)# watch-list dynamic-expiry-timeout 5000
Device(config-params-parameter-map)# banner file flash:webauth_banner.html
Device(config-params-parameter-map)# end
```

Named Parameter Map for Web Authentication Using Custom Pages

The following example shows how to configure a named parameter map for web authentication that defines custom pages for the login process, along with a control policy that uses the parameter map.

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type webauth CUSTOM-WEBAUTH-MAP
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# custom-page login device flash:login_page.html
Device(config-params-parameter-map)# custom-page success device flash:success_page.html
Device(config-params-parameter-map)# custom-page failure device flash:fail_page.html
Device(config-params-parameter-map)# custom-page login expired device flash:expire_page.html
Device(config-params-parameter-map)# exit
Device(config)# policy-map type control subscriber CUSTOM-WEBAUTH-POLICY
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using webauth parameter-map
CUSTOM-WEBAUTH-MAP retries 2 retry-time 0
Device(config-action-control-policymap)# end
```

Named Parameter Map for Consent Using Custom Pages

The following example shows how to configure a named parameter map for custom consent, along with the corresponding control policy that uses the parameter map:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type webauth CUSTOM-CONSENT-MAP
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# custom-page login device flash:consent_login_page.html
Device(config-params-parameter-map)# custom-page success device
flash:consent_success_page.html
Device(config-params-parameter-map)# custom-page failure device flash:consent_fail_page.html
Device(config-params-parameter-map)# custom-page login expired device
flash:consent_expire_page.html
Device(config-params-parameter-map)# end
Device(config)# ip access-list extended GUEST-ACL
Device(config-ext-nacl)# permit ip any 172.30.30.0 0.0.0.255
Device(config-ext-nacl)# permit ip any host 172.20.249.252
```



```

Device(config-ext-nacl)# exit
Device(config)# service-template GUEST-POLICY
Device(config-service-template)# access-group GUEST-ACL
Device(config-service-template)# exit
Device(config)# policy-map type control subscriber CUSTOM-CONSENT-POLICY
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using webauth parameter-map
CUSTOM-CONSENT-MAP
Device(config-action-control-policymap)# exit
Device(config-event-control-policymap)# event authentication-success match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 activate service-template GUEST-POLICY
Device(config-action-control-policymap)# end

```

Named Parameter Map for Web Authentication with Consent Using Custom Pages

The following example shows how to configure a named parameter map for web authentication with custom consent, along with the corresponding control policy that uses the parameter map:

```

Device> enable
Device# configure terminal
Device(config)# parameter-map type webauth CUSTOM-WEBAUTH-CONSENT-MAP
Device(config-params-parameter-map)# type webconsent
Device(config-params-parameter-map)# custom-page login device
flash:webauth_consent_login_page.html
Device(config-params-parameter-map)# custom-page success device
flash:webauth_consent_success_page.html
Device(config-params-parameter-map)# custom-page failure device
flash:webauth_consent_fail_page.html
Device(config-params-parameter-map)# custom-page login expired device
flash:webauth_consent_expire_page.html
Device(config-params-parameter-map)# exit
Device(config)# ip access-list extended GUEST-ACL
Device(config-ext-nacl)# permit ip any 172.30.30.0 0.0.0.255
Device(config-ext-nacl)# permit ip any host 172.20.249.252
Device(config-ext-nacl)# exit
Device(config)# service-template GUEST-POLICY
Device(config-service-template)# access-group GUEST-ACL
Device(config-service-template)# exit
Device(config)# policy-map type control subscriber CUSTOM-WEBAUTH-CONSENT-POLICY
Device(config-event-control-policymap)# event session-started match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 authenticate using webauth parameter-map
CUSTOM-WEBAUTH-CONSENT-MAP
Device(config-action-control-policymap)# exit
Device(config-event-control-policymap)# event authentication-success match-all
Device(config-class-control-policymap)# 10 class always do-until-failure
Device(config-action-control-policymap)# 10 activate service-template GUEST-POLICY
Device(config-action-control-policymap)# end

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Authentication, authorization, and accounting	<i>Authentication, Authorization, and Accounting (AAA) Configuration Guide</i>
Access lists and the Cisco IOS Firewall	“Access Control Lists: Overview and Guidelines” module of the <i>Security Configuration Guide: Access Control Lists</i> publication
Configuring identity control policies	<i>Identity-Based Networking Services Configuration Guide</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Customization of Authentication Proxy Web Pages

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 Customization of Authentication Proxy Web Pages

Feature Name	Releases	Feature Information
Web Authentication Enhancements—Customization of Authentication Proxy Web Pages	Cisco IOS 15.0(1)EX	The Customization of Authentication Proxy Web Pages feature allows you to provide four HTML pages to be displayed to the user in place of the switch's internal default HTML pages during web-based authentication. The four pages are Login, Success, Fail, and Expire.
Custom Web Authentication Result Display Enhancement	Cisco IOS 15.2(2)E	<p>The Custom Web Authentication Result Display Enhancement feature displays the authentication results on the main HTML page. There is no pop-up window to display the authentication results.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"> • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches
Support for Custom Web Authentication Download Bundle	Cisco IOS 15.2(2)E	<p>The Support for Custom Web Authentication Download Bundle feature ensures that one or more custom HTML pages can be downloaded and configured from a single tar file bundle. The images and the custom pages containing the images are also part of the same downloadable tar file bundle.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"> • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches

Feature Name	Releases	Feature Information
Virtual IP Support for Images in Custom Web Authentication	Cisco IOS 15.2(2)E	<p>The Virtual IP Support for Images in Custom Web Authentication feature supports image filenames without prefixes and removes the requirement of users having to specify the wireless management interface IP address to indicate the source of the image in the HTML code.</p> <p>In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none">• Catalyst 3560-X Series Switches• Catalyst 3750-X Series Switches



Webauth Sleeping Client

The Webauth Sleeping Client feature allows successfully authenticated devices to stay logged in for a configured period without re-authentication.

This module describes how to add a parameter map to configure the time until which the access switch remembers the sleeping client.

- [Finding Feature Information, page 17](#)
- [Restrictions for Webauth Sleeping Client, page 17](#)
- [Information About Webauth Sleeping Client, page 18](#)
- [How to Configure Webauth Sleeping Client, page 18](#)
- [Configuration Examples for Webauth Sleeping Client, page 21](#)
- [Additional References for Webauth Sleeping Client, page 21](#)
- [Feature Information for Webauth Sleeping Client, page 22](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

Restrictions for Webauth Sleeping Client

- The MAC address of the device and the username or password is mapped. Once an entry is added to sleeping-client cache, all users of the device get the same policies that are stored in the cache. To use different policies, a user can force normal authentication by logging out. To log out, use `http[s]://<Virtual IP/Virtual Host>/logout.html`.

- Mobility is not supported. If a device sleeps, wakes up, and gets associated with a different foreign controller, the device undergoes normal authentication on the foreign controller.

Information About Webauth Sleeping Client

Sleeping client cache

The Webauth Sleeping Client feature enables users to login once and not be disturbed with login forms for a configurable period. The details of the devices (sleeping clients) that need to be remembered are stored in the sleeping client cache.

Once a user authenticates successfully for the first time, an entry is added to the sleeping client cache and the sleeping client timer starts. If the authenticated device goes to sleep and wakes up, the service manager uses the web authentication method to check if there is an entry in the sleeping client cache for the mapped MAC address. If the entry is found, the authentication is run in the background using the stored credentials. If the authentication is successful, the sleeping client cache is updated and a logout access control list (ACL) is added. The logout ACL helps the client force normal authentication by logging out. In case the authentication fails with the stored credentials, the entry is deleted from the sleeping client cache.

If the service manager does not find any entry in the sleeping client cache for the mapped MAC address, normal authentication is performed. After successful authentication, an entry is added to the sleeping client cache and the sleeping client timer starts.

How to Configure Webauth Sleeping Client

Configuring Sleeping Client Timer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type webauth** *{parameter-map-name | global}*
4. **sleeping-client** [*timeout time*]
5. **end**
6. **clear ip admission sleeping client** *{* | mac-address}*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>parameter-map type webauth {<i>parameter-map-name</i> global}</p> <p>Example:</p> <pre>Device(config)# parameter-map type webauth global</pre>	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 4	<p>sleeping-client [timeout <i>time</i>]</p> <p>Example:</p> <pre>Device(config-params-parameter-map) # sleeping-client timeout 60</pre>	<p>Configures the sleeping client timeout in minutes. Available range for the <i>time</i> argument is from 60 to 35791.</p> <p>Note If you do not use the timeout keyword, the sleeping client is configured with the default timeout value of 720 minutes.</p>
Step 5	<p>end</p> <p>Example:</p> <pre>Device(config-params-parameter-map) # end</pre>	Exits parameter-map webauth configuration mode and returns to privileged EXEC mode.
Step 6	<p>clear ip admission sleeping client {<i>*</i> <i>mac-address</i>}</p> <p>Example:</p> <pre>Device# clear ip admission sleeping client *</pre>	Deletes all or specific MAC entries from the sleeping client cache.
Step 7	<p>exit</p> <p>Example:</p> <pre>Device# exit</pre>	Exits privileged EXEC mode and returns to user EXEC mode.

Verifying Sleeping Client Entries

SUMMARY STEPS

1. **enable**
2. **show ip admission sleeping-client**
3. **show ip admission cache**

DETAILED STEPS

Step 1

enable

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2

show ip admission sleeping-client

Displays the sleeping client database.

Example:

```
Device# show ip admission sleeping-client

Sleeping-Client Cache
Total number of sleeping-client entries: 1
Client-mac Time-Remaining(min)
00e1.e1e1.0001 59
```

Step 3

show ip admission cache

Displays the sleeping client and normal client details. The sleeping client entries are prefixed with ^.

Example:

```
Device# show ip admission cache

^Client MAC 00e1.e1e1.0001 Client IP 2001:DB8::1 IPv6 ::, State AUTHZ, Method Webauth
```

Configuration Examples for Webauth Sleeping Client

Example: Configuring Sleeping Client Timer

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# sleeping-client timeout 60
Device(config-params-parameter-map)# end
Device# clear ip admission sleeping client *
Device# exit
```

Additional References for Webauth Sleeping Client

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Web authentication process	"Managing Web Authentication" chapter in <i>Cisco Wireless LAN Controller Configuration Guide</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Webauth Sleeping Client

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 2: Feature Information for Webauth Sleeping Client

Feature Name	Releases	Feature Information
Webauth Sleeping Client	Cisco IOS 15.2(3)E	<p>The Webauth Sleeping Client feature allows successfully authenticated devices to stay logged in for a configured period without re-authentication.</p> <p>The following commands were introduced or modified: clear ip admission sleeping-client, show ip admission sleeping-client, show ip admission cache and sleeping client timeout.</p>