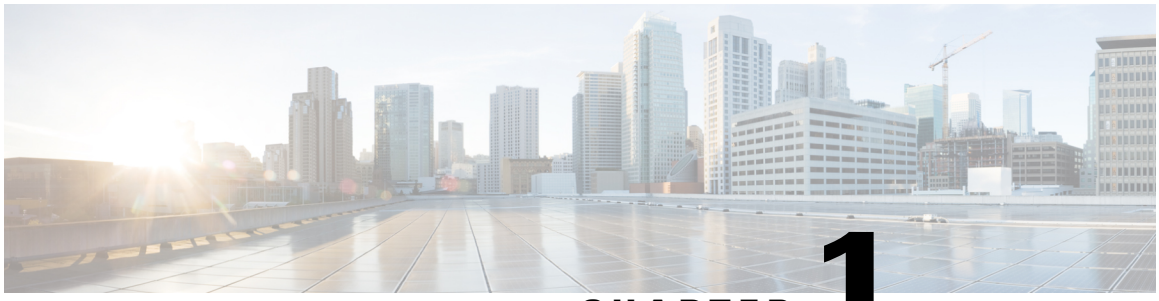
Authentication Proxy Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: January 16, 2013

Last Modified: January 16, 2013

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

CONTENTS



CHAPTER 1

Customizing Authentication Proxy Web Pages

The Customization of Authentication Proxy Web Pages feature allows you to provide four substitute 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.

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.

Information About Customization of Authentication Proxy Web Pages

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

- Login—The user's credentials are requested.
- Success—The login was successful.

- Fail—The 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 will be redirected upon successful authentication, effectively replacing the internal Success page.

How to Configure Custom Authentication Proxy Web Pages

Configuring the 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.

Before You Begin

Note 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 will be used.

- The four custom HTML files must be present on the disk or flash of the switch.
- 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”).
- All image file names must be less than 33 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.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.

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. • 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** *device:login-filename* **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. The device: is either disk or flash memory, such as disk0:.
Step 4	**ip admission proxy http success page file** *device:success-filename* **Example:** `Device(config)# ip admission proxy http success page file disk1:success.htm`	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** *device:fail-filename* **Example:** `Device(config)# ip admission proxy http failure page file disk1:fail.htm`	Specifies the location of the custom HTML file to be used in place of the default login failure page.

	Command or Action	Purpose
Step 6	**ip admission proxy http expired page file** *device:expired-filename* **Example:** `Device(config)# ip admission proxy http expired page file disk1:expired.htm`	Specifies the location of the custom HTML file to be used in place of the default login expired page.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Specifying a Redirection URL for Successful Login

To specify a redirection URL for successful login, perform this task.

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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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** *url-string* **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`	Returns to privileged EXEC mode.

Verifying the Configuration of Custom Authentication Proxy Web Pages

Perform this task to verify the configuration of custom authentication proxy web pages and the redirection URL for successful login:

SUMMARY STEPS

1. **enable**
2. **show ip admission configuration**
3. **show ip admission configuration**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show ip admission configuration**

Displays the configuration of custom authentication proxy web pages.

Example:

```
Device# show ip admission configuration

Authentication proxy webpage
 Login page           : disk1:login.htm
 Success page         : disk1:success.htm
 Fail Page            : disk1:fail.htm
 Login expired Page   : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Step 3 **show ip admission configuration**

Displays the configuration of custom authentication proxy web pages.

Example:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.company.com
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 disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication, authorization, and accounting	*Authentication, Authorization, and Accounting (AAA) Configuration Guide*
Access lists and the Cisco IOS Firewall	"Access Control Lists: Overview and Guidelines" module of the *Security Configuration Guide: Access Control Lists* publication.

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 XE Release 3.2SE	The Customization of Authentication Proxy Web Pages feature allows you to provide four substitute 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.