Guidelines for Configuring Web-Based Authentication

Guidelines for Setting Custom Web Authentication Pages

Read the following guidelines before you configure custom web authentication pages for login, succesful login, failed login and expired login pages.

- Ensure that the custom pages are in HTML format .
- You must configure all four custom HTML files. If fewer than four files are configured, the internal default HTML pages will be used.
- You must copy the four custom HTML files to the disk or flash of the switch. When you are using a switch stack, you can copy the pages on to the flash on the active and member switches. For example, the login page can be on the flash on the active switch, and the success and failure pages can be on the flash on a member switch.

Note When using the CLI, you must manually copy the custom HTML files on to the flash of the active and standby swithces. However, when you upload the customer web auth bundle file in tar format through the Web UI, the system will untar and place the custom HTML files on both the active and standby switches.

- You must include an HTML redirect command in the success page to access a specific URL.
- You must configure a virtual IP in the global parameter map.
- If you configure custom web pages for HTTP authentication, they must also include the HTML commands to set the page time out, hidden password, or to confirm that the same page is not submitted twice.
- You cannot configure web authentication banners after configuring custom web authentication pages.

- All of the logo files such as image, flash, audio, video, and so on that are stored in the system directory (for example, flash, disk0, or disk) and that must be displayed on the login page must use *web_auth_<filename>* as the file name.

Guidelines for Setting Redirection URL

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used.
- To remove the specification of a redirection URL, use the **no** form of the command.
- If the redirection URL is required after the web-based authentication client is successfully authenticated, then the URL string must start with a valid URL (for example, http://) followed by the URL information. If only the URL is given without http://, then the redirection URL on successful authentication might cause page not found or similar errors on a web browser.

Guidelines for Configuring Secure HTTP Access

With the introduction of **webauth-http-enable** and **secure-webauth-disable** commands, you can control how HTTP and HTTPS requests are handled for web authentication. Earlier, with **ip http server** and **ip http secure-server** global commands, you could configure HTTP and secure HTTP access only for the web user interface and not specifically for web authentication.

By default, **ip http secure-server** command enables secure access globally for accessing the web user interface and for web authentication. Enabling HTTPS globally secures the data to and from an HTTP server by encrypting the data before transmitting over the Internet. However, in situations where you want to disable secure HTTP access for web authentication, and still want to enable secure access for the user interface, you must run **secure-webauth-disable** command. Configuring **secure-webauth-disable** overrides the global **ip http secure-server** command and lets you disable HTTPS for web authentication.

Alternatively, in certain situations, you might have to disable HTTP access for port 80 in order to disable accessing the web user interface through port 80 and still enable the port for web authentication. You can achieve this by disabling port 80 using the global command, **no ip http server** and enable web authentication on port 80 using the **webauth-http-enable** command.

The **secure-webauth-disable** and **webauth-http-enable** commands are not enabled by default; you must configure them explicitly.

The following are the allowed CLI combinations and respective system behaviour while connfiguring HTTP/HTTPS access for web authentication and device management using the web user interface.

Table 1: CLI Combinations

Required Configurations		Device Management		Web Authentication	
Device Management	**Web Authentication**	**HTTP Access**	**HTTPS Access**	**HTTP Access**	**HTTPS Access**

`no ip http server`
 	
`ip http secure-server`
	`no ip http server`
	`ip http secure-server`
	
	`parameter-map type webauth global`
	
	`webauth-http-enable`
		No	Yes	Yes	Yes

`no ip http server`
 	
`ip http secure-server`
	`no ip http server`
	`ip http secure-server`
		No	Yes	No	Yes

`no ip http server`
`ip http secure-server`
	`no ip http server`
	`ip http secure-server`
	
	`parameter-map type webauth global`
	
	`webauth-http-enable`
	
	`secure-webauth-disable`
		No	Yes	Yes	No

`no ip http server`
`ip http secure-server`
	`no ip http server`
	`ip http secure-server`
	
	`parameter-map type webauth global`
	
	`secure-webauth-disable`
		No	Yes	No	No

`no ip http server` `no ip http secure-server`	Not Supported	No	No	No	Yes

`no ip http server`
`no ip http secure-server`
	`no ip http server`
	`no ip http secure-server`
	
	`parameter-map type webauth global`
	
	`webauth-http-enable`
		No	No	Yes	No

`ip http server` `no ip http secure-server`	`ip http server` `no ip http secure-server`	Yes	No	Yes	No

Required Configurations		Device Management		Web Authentication	
Device Management	**Web Authentication**	**HTTP Access**	**HTTPS Access**	**HTTP Access**	**HTTPS Access**

`ip http server`
`ip http secure-server`
	`ip http server`
	`ip http secure-server`
	
	`parameter-map type webauth global`
	
	`secure-webauth-disable`
		Yes	Yes	Yes	No