Applicable Version: 10.00 onwards

Overview

Cyberoam Captive Portal authenticates users for Internet access. When users attempt to access the internet, a default Captive Portal is presented to authenticate the users. The default Captive Portal display can be customized in terms of organization name, logo, page - title, header, footer, background and font colours or links. Additionally, the default Captive Portal Settings can be changed as per the requirement.

Scenario

Customize the default Captive Portal display and other settings in Cyberoam.
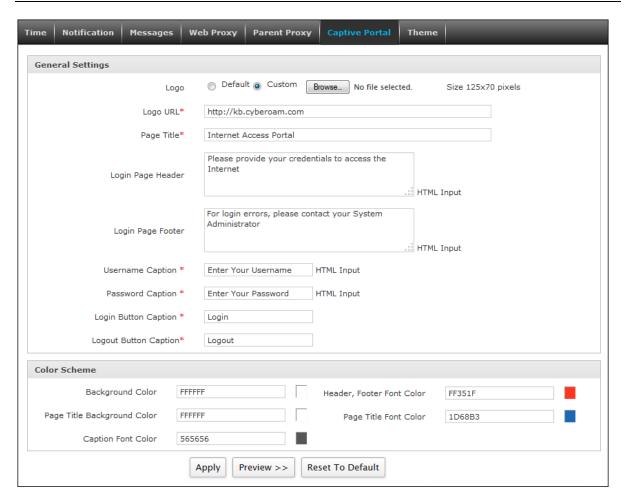
Configuration

You must be logged on to the Web Admin Console as an administrator with Read-Write permission for relevant feature(s).

Customize Captive Portal Display

a.   Change Text, Captions, Logo

Go to **System > Configuration > Captive Portal** to Customize the Captive Portal display. Refer the sample custom configuration shown in the table below.

Parameters	Value	Description
Logo	**Custom**	Select **Custom** and click **Browse** to select your custom Logo. The image size should not exceed 125 X 70 pixels.
Logo URL	**http://kb.cyberoam.com**	Specify a URL to be redirected to on clicking the Logo.
Page Title	**Internet Access Portal**	Specify the page title.
Login Page Header	**Please provide your credentials to access the Internet**	Specify the page header to be displayed at the top of the page.
Login Page Footer	**For Login Errors, please contact your System Administrator**	Specify the page footer to be displayed at the bottom of the page.
Username Caption	**Enter Your Username**	Specify label for the username textbox.
Password Caption	**Enter Your Password**	Specify label for the password textbox.
Login Button Caption	**Login**	Specify label for the Login button.
Logout Button Caption	**Logout**	Specify label for the Logout button.

b. Change Color Scheme

You can customize the colour scheme of the Captive portal as per your preference. Specify the colour code or click the square box against page item to pick the colour.
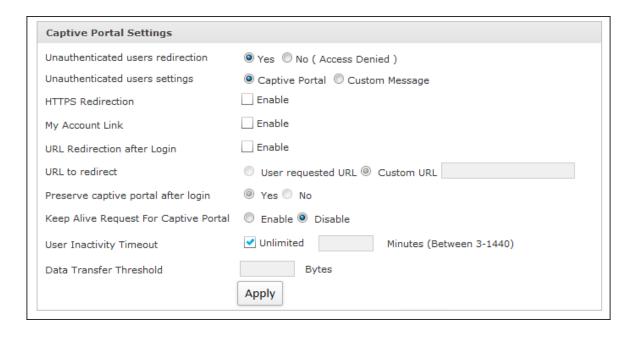

Click **Apply** to apply the configuration. You can also preview the configuration by clicking **Preview**.

Please provide your credentials to access the Internet

Internet Access Portal

Knowledge Base

Enter Your Username

Enter Your Password

Login

For Login Errors, please contact your System Administrator

c. Captive Portal Settings

The default settings of Captive Portal can be changed to further customize the Captive Portal. Go to **Identity > Authentication > Firewall** and under the **Captive Portal Settings**, set the following options as per the requirement.

Captive Portal Settings

Unauthenticated users redirection	◉ Yes ○ No (Access Denied)
Unauthenticated users settings	◉ Captive Portal ○ Custom Message
HTTPS Redirection	☐ Enable
My Account Link	☐ Enable
URL Redirection after Login	☐ Enable
URL to redirect	○ User requested URL ◉ Custom URL
Preserve captive portal after login	◉ Yes ○ No
Keep Alive Request For Captive Portal	○ Enable ◉ Disable
User Inactivity Timeout	☑ Unlimited ____ Minutes (Between 3-1440)
Data Transfer Threshold	____ Bytes

Apply

Unauthenticated users redirection

Unauthenticated users redirection is used to configure the redirection of user access request to Captive portal page or Custom page.

Select **No** if you want to completely restrict Internet Access to the users. The user request will be dropped and the browser will display the default message for loss of Internet connectivity.

By default, **Unauthenticated users redirection** is set to **Yes** to redirect user access requests. The following options are applicable only if **Unauthenticated users redirection** is enabled**.**

1. **Unauthenticated users settings**

Unauthenticated users settings is used to redirect user requests to the Captive Portal or Custom Message page. By default, the Unauthenticated user settings is set to **Captive Portal**.

Select **Custom Message** to redirect unauthenticated user request to the Custom Message page. To configure the Custom Message Page, refer Articles, Serve a Custom Page to unauthenticated users instead of Captive portal and Customize a Denied Message.

2. **HTTPS Redirection**

Check **Enable** to provide access of the Captive portal page through HTTPS or secure channel.

3. **My Account Link**

My Account Link provides user information like personal details, Internet usage or quarantined virus/spam mails. It is present on the Captive Portal by default. To disable My Account Link, check **Disable**.

4. **URL Redirection after Login** and **URL to redirect**

After successful authentication, the user requested URL opens, to change the URL redirection, refer article Configure Captive Portal URL Redirection.

5. **Preserve captive portal after login**

Select **Yes** to preserve the Captive Portal page after successful logon, where the user-requested/custom URL opens in a new page.

If you don't want to preserve the Captive Portal page, select **No**, where the user-requested/custom URL opens in the same page as the Captive Portal page. If the Captive Portal is not preserved, the user will not be able to log out and his login session remains active until the user is idle. In this case, administrators can enable **Keep Alive Request for Captive Portal** or configure **User Inactivity Timeout** or **Data Transfer Threshold** to disconnect idle users.

6. **Keep Alive Request For Captive Portal**

Keep-Alive request is constantly exchanged between the appliance and the user to check whether user has logged out or idle. If the appliance does not receive the response, user is logged out automatically. To set keep-alive request active, select **Enable**.

Select **Disable** to configure **User Inactivity Timeout** or **Data Transfer Threshold** to logout the user.

   User Inactivity Timeout

Specify the time after which the user will be logged off. Check **Unlimited** to allow permanent logon. To specify a finite duration, uncheck Unlimited and specify the duration in minutes. (3 to 1440)

Data Transfer Threshold

Specify threshold value for Data Transfer in Bytes. If the specified data is not transferred within the Inactivity Timeout period, the user will be marked as inactive and logged out.

Note:

Cyberoam Captive Portal can also be used to create Guest Users. To configure guest user creation through Captive portal, refer article Guest User Creation using Captive Portal.

Document Version: 1.0 – 24 June, 2014