Intelbras Zeus OS

Especificações do Captive Portal Externo v2.0

O Zeus OS suporta a funcionalidade de Captive Portal usando um servidor de Radius externo opcional para autenticação. Para permitir a integração, algumas especificações são necessárias.

Logon

Quando um cliente quer acessar a Internet, o seguinte cenário ocorre:

1. O cliente Wireless associa-se à rede sem fio **SSID;**
2. O usuário faz uma solicitação inicial para uma URL em seu navegador;
3. O Access Point (AP) rodando **Zeus OS** redireciona o usuário para uma página de autenticação (splash page) externa, através da qual o usuário deve autenticar para ter acesso à Internet.
   A página splash page é solicitada através de uma solicitação http ou https **GET,** incluindo os seguintes parâmetros **HTTP:**

Parâmetro	**Descrição**
continue	URL que o usuário solicitou originalmente
ip	Endereço IP do access point
ap_mac	Endereço MAC do access point
mac	Endereço MAC do cliente Wireless
radio	Nome do rádio Wireless ao qual o cliente está conectado
ssid	Nome do SSID Wilress ao qual o cliente se conectou
ts	Timestamp do requisição
redirect_uri	URL para a qual o cliente deve ser redirecionado para continuar o processo de autenticação
user_hash	Usado para identificar cada solicitação do usuário

Exemplo:

http://my_captive.com.br?continue=www.intelbras.com.br&ip=10.0.0.1&mac=00:11:22:33:44:55&ap_mac=00:11:22:33:44:66&radio=radio0&ssid=MY_CAPTIVE&ts=1573052168&redirect_uri=http%3A%2F%2F10.0.0.1%3A2061%2Fcp%2Fitbcaptive.cgi&user_hash=0123456abcdefg

Etapas quanto utilizado Captive Portal Externo

4. O usuário deve autenticar na página de autenticação; a página de autenticação deve conter um formulário que solicita os seguintes campos para o usuário:

   username e **password**

5. A forma da página splash deve ser submetida a uma página do lado do servidor (pode ser a mesma página), incluindo as informações solicitadas ao usuário**(nome de usuário/senha)**e os seguintes parâmetros especificados na etapa 3: **continuar** (opcional) e **user_hash**.
6. A página do lado do servidor que recebe o formulário enviado, usa os parâmetros recebidos para conceder/negar acesso. Uma vez concedido o acesso, ele deve redirecionar o navegador do usuário para a URL especificada na etapa 3 (**redirect_uri**) usando http **GET** ou http **post** solicitação:

   http://10.0.0.1:2061/cp/itbcaptive.cgi

   com os seguintes parâmetros:

   continue=**[continue]**&nome deusuário=**[username]**&senha=**[password]**&user_hash=**[user_hash]**

   onde:

parâmetro	**descrição**
continue (opcional)	URL para a qual o usuário será redirecionado após autenticação bem sucedida
username	Nome de usuário para autenticação no servidor Radius
password	Senha para autenticação do usuário no servidor Radius
user_hash	Usado para identificar cada solicitação do usuário

7. O AP irá autenticar o usuário através do servidor Radius, e, em seguida, redirecionará o navegador do usuário para a URL passada no campo **continue.**

Etapas ao usar o Captive Portal Externo (as etapas anteriores 1 a 3 permanecem as mesmas)

4. O usuário deve autenticar ou preencher quaisquer parâmetros necessários na página de autenticação (Veja o exemplo: **captive_login.php**);
5. A página de autenticação deve ser submetida do lado do servidor (pode ser a mesma página), incluindo todas as informações solicitadas ao usuário e os seguintes parâmetros especificados na etapa **3**: **continue** (opcional), **ts** e **user_hash**.
6. A página do lado do servidor que recebe o formulário enviado, usa os parâmetros recebidos para conceder/negar acesso. Uma vez concedido o acesso, ele deve redirecionar o navegador do usuário para a **URL** especificada na etapa **3** (**redirect_uri**) usando http **GET** ou http **post** solicitação (Veja o exemplo: **captive_auth.php**):

   http://10.0.0.1:2061/cp/itbcaptive.cgi

   com os seguintes parâmetros:

   ts=**[ts]**&user_hash=**[user_hash]**&continue=**[continue]**&token=**[token]**&session_timeout=**[session_timeout]**&idle_timeout=**[idle_timeout]**&download_kbps=
   [download_kbps]&upload_kbps=**[upload_kbps]**

   onde:

Parâmetro	**Descrição**
ts	Timestamp da requisição
user_hash	Usado para identificar cada solicitação do usuário
continue (opcional)	URL para a qual o usuário será redirecionado após autenticação bem sucedida
token (opcional)	Parâmetro opcional para aumentar a segurança. Este é o resultado de um **HMAC SHA-256** usando uma chave **secret** compartilhada configurada no **AP**. Exemplo usando função **php:** $token = hash_hmac('sha256', "$user_hash|$ts", $secret, false);
session_timeout (opcional)	Duração (em segundos) da sessão que o usuário autenticou
idle_timeout (opcional)	Duração (em segundos) que o usuário autenticado permanece autorizado após desconectar da rede WiFi

download_kbps (opcional)	Limite de velocidade de download (tanto o download/upload precisam ser preenchidos)
upload_kbps (opcional)	Limite de velocidade de upload

7. O AP redirecionará o navegador do usuário para a URL passada no campo **continue.**

Logoff

O usuário pode fazer uma solicitação HTTP **GET** ou HTTP **POST:**

http://10.0.0.1:2061/cp/itbcaptive.cgi

com os seguintes parâmetros:

action=logoff&user_hash=**[user_hash]**&ts=**[ts]**&token=**[token]**

onde:

Parâmetro	**Descrição**
user_hash	Usado para identificar cada solicitação do usuário
ts	**Não usado com Radius**
token (opcional)	Token SHA-256 HMAC. **Não usado com Radius**

Walled Garden

Zeus OS inclui automaticamente o domínio de sua página de autenticação externa no Walled Garden. Caso você precise que o usuário acesse qualquer outro domínio, antes da autenticação, é obrigatório que você adicione todos os domínios necessários manualmente. Caso contrário, o usuário não poderá acessar.

Controle de largura de banda

Atualmente, o **Zeus OS** suporta atributos de Radius **WISPr** para controle de largura de banda:

WISPr-Bandwidth-Max-Down e **WISPr-Bandwidth-Max-Up**

Quando não utilizado Radius, os valores de controle de largura de banda são passados como parâmetros de URL (GET) ou valores de formulário HTML (POST).

O QoS (limite de largura de banda) deve ser habilitado no AP para fazer uso desses atributos e ambos precisam ser definidos.

Gerenciamento de Sessões

Existem dois intervalos que podem ser configurados a partir do Zeus OS: **Session Timeout** e tempo **idle timeout**. Ambos podem ser especificados manualmente.

O Session Timeout de sessão pode ser recebido como um atributo Radius ou um parâmetro URL (quando o Radius não é usado). **O idle timeout** pode ser recebido como um parâmetro de URL (quando o Radius não é usado).

O **Session Timeout** de sessão define a duração da sessão em segundos; este tempo limite não é renovável e quando expira, a sessão é encerrada.

O **idle timeout** define o tempo de inatividade do cliente (quando ele se desconecta do AP) em segundos após o qual o cliente é considerado desligado.

Scripts PHP como exemplo

Land page (captive_login.php)

```
<?php
  /*
    These parameters are sent by the AP to this portal page:
      ap_mac - MAC address of the AP
      ip - IP address of the AP
      mac - MAC address of the client device
      radio - Name of Wireless Radio which the client is connected to
      continue - Original requested url by the client, ie:
http://www.intelbras.com.br
      ts - Request timestamp
      user_hash - Unique client device identifier
      ssid - SSID the client device is connected to
      redirect_uri - url to forward the client to in order to release
Internet access

    If you want to send the guest to a content page after authorization,
configure the $desired_url instead of using the valued that is passed as a
parameter.
  */

  $ap_mac = $_GET['ap_mac'];
  $ap_ip = $_GET['ip'];
  $ap_radio = $_GET['radio'];
  $client_mac = $_GET['mac'];
  $desired_url = $_GET['continue'];
  $timestamp = $_GET['ts'];
  $user_hash = $_GET['user_hash'];
  $ssid = $_GET['ssid'];
  $redirect_uri = $_GET['redirect_uri'];
?>

<html>
  <body>
      <form action="captive_auth.php" method="post">
          <input type="hidden" name="ap_mac" value="<?php echo($ap_mac) ?>"
/>
          <input type="hidden" name="ap_ip" value="<?php echo($ap_ip) ?>"
/>
          <input type="hidden" name="ap_radio" value="<?php echo($ap_radio)
?>" />
          <input type="hidden" name="client_mac" value="<?php
echo($client_mac) ?>" />
          <input type="hidden" name="timestamp" value="<?php
echo($timestamp) ?>" />
          <input type="hidden" name="user_hash" value="<?php
echo($user_hash) ?>" />
          <input type="hidden" name="desired_url" value="<?php
echo($desired_url) ?>" />
          <input type="hidden" name="redirect_uri" value="<?php
echo($redirect_uri) ?>" />
          <input type="hidden" name="ssid" value="<?php echo($ssid) ?>" />
```

```
          <table>
              <tr>
                  <td><b>Your Login</b></td>
                  <td><input type="text" name="username" /></td>
              </tr>
              <tr>
                  <td><b>Your Password</b></td>
                  <td><input type="text" name="password" /></td>
              </tr>
              <tr>
                  <td><input type="submit" value="Login" /></td>
              </tr>
          </table>
      </form>
  </body>
</html>
```

Authorization Page (captive_auth.php)

```
<?php
  $secret = 'test_key';  // Secret key configured at the AP (optional)
  $ap_mac = $_POST['ap_mac'];
  $ap_ip = $_POST['ap_ip'];
  $ap_radio = $_POST['ap_radio'];
  $client_mac = $_POST['client_mac'];
  $user_hash = $_POST['user_hash'];
  $timestamp = $_POST['timestamp'];
  $ssid = $_POST['ssid'];
  $redirect_uri = $_POST['redirect_uri'];
  $desired_url = $_POST['desired_url']; // URL the user is forwarded to
after authorization
  $username = $_POST['username'];
  $password = $_POST['password'];

  // Optional parameters
  $session_timeout = 300;  // Duration (in seconds) the guest user is
authorized before they are redirected back to the portal page.
  $idle_timeout = 60;  // Duration (in seconds) the guest user remains
authorized after disconnecting from the WiFi network.
  $download_kbps = 0;  // Download limit (in kbps). 0 = unlimited.
  $upload_kbps = 0;  // Upload limit (in kbps) per client. 0 = unlimited.

  // Token - Only needed when using $secret
  $user_context = sprintf('%s|%d', $user_hash, $timestamp);
  $token = hash_hmac('sha256', $user_context, $secret, false);

  $params = 'continue=' . urlencode($desired_url);
  $params .= '&ts=' . $timestamp;
  $params .= '&token=' . $token;
  $params .= '&user_hash=' . $user_hash;
  $params .= '&session_timeout=' . $session_timeout;
  $params .= '&idle_timeout=' . $idle_timeout;
  $params .= '&download_kbps=' . $download_kbps;
```

```
  $params .= '&upload_kbps=' . $upload_kbps;

  $final_url = sprintf('%s?%s', $redirect_uri, $params);

  /*
    Debug code used for testing purposes only
    If set to true, display the variable details without authorizing the
guest
  */
  $debugging = false;
  if ($debugging) {
    header('Content-Type: text/plain');
    echo sprintf('redirect_uri : %s', $redirect_uri) . PHP_EOL;
    echo sprintf('URL          : %s', $final_url) . PHP_EOL;
    echo PHP_EOL;
    echo sprintf('desired_url  : %s', $desired_url) . PHP_EOL;
    echo PHP_EOL;
    echo sprintf('token (%d)   : %s', strlen($token), $token) . PHP_EOL;
    echo sprintf('client_mac   : %s', $client_mac) . PHP_EOL;
    echo sprintf('ap_ip    : %s', $ap_ip) . PHP_EOL;
    echo sprintf('ap_mac       : %s', $ap_mac) . PHP_EOL;
    echo sprintf('ap_radio     : %s', $ap_radio) . PHP_EOL;
    echo sprintf('user_hash    : %s', $user_hash) . PHP_EOL;
    echo sprintf('timestamp    : %s', $timestamp) . PHP_EOL;
    echo sprintf('ssid         : %s', $ssid) . PHP_EOL;
    echo sprintf('username     : %s', $username) . PHP_EOL;
    echo sprintf('password     : %s', $password) . PHP_EOL;
    return 0;
  }

  // Login process. If OK, then forward back to AP to release.
  if (username && password) {
    header('Location: ' . $final_url);
  } else {
    // Guest is redirected for authorization.
    header('Location: captive_login.php');
  }
?>
```