Custom Web Authentication Locally Hosted on WLC or an External Server

This document provides information on custom Web Authentication that is locally hosted on a Wireless LAN Controller (WLC) or an External server, such as, Identity Services Engine (ISE).

Configuring Custom Web Authentication Locally Hosted on WLC

The configuration for a Custom Web Authentication that is locally hosted on the WLC is similar to the Local Web Authentication and Local Web Authentication with External RADIUS Authentication. However, to configure a Custom Web Authentication, in addition to the above mentioned configuration methods, you need to download the custom page on flash and point the parameter map to use the custom pages.

Note For more information on Custom Web Authentication that is locally hosted on WLC and Local Web Authentication with External RADIUS Authentication, refer to the following:

- Web Authentication on Converged Access-Local Web Authentication.
- Web Authentication on Converged Access - Local Web Authentication with External RADIUS Authentication

To download the custom page on flash and point the parameter map to use the custom pages, use the following commands:

```
parameter-map type webauth WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page login expired device flash:webauth_expire.html
 custom-page failure device flash:webauth_fail.html
 custom-page success device flash:webauth_success.html
```

Note To use the Custom Web Authentication locally, define a custom page for the login page, expire page, login - success page, and login - fail page.

Configuring the Custom HTML pages

Web Authentication for Login Page

To configure the web authentication for the login page, use the following:

```
<HTML><HEAD><TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1',
'resizable=no,width=350,height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<FORM method=post action="/" target="pxywindow1">
  Username: <input type=text name=uname><BR><BR>
  Password: <input type=password name=pwd><BR><BR>
  <input type=submit name=ok value=OK   onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
     for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
      JavaScript if you would like to have JavaScript enabled
      for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
       disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web brower window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript></BODY></HTML>
```

Web Authentication for Success Page

To configure the web authentication for success page, use the following:

```
<HTML><HEAD>
<TITLE>Authentication Proxy Success Page</TITLE>
<script type="text/javascript">
    var donesubmitted = false;
    function DoneButton() {
        if (donesubmitted == false) {
            donesubmitted = true;
```

```
          window.opener.location.reload();
          window.close();
        }
    }
    setTimeout("DoneButton()", 5000);
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<p>Authentication Successful !</p>
<FORM>
  <input type=button name=enter value=DONE onClick="DoneButton();">
</FORM>
<noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
     for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
      JavaScript if you would like to have JavaScript enabled
      for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
       disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web brower window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript></BODY></HTML>
```

Web Authentication for Failure page

To perform the web authentication for failure page, use the following:

```
<HTML><HEAD>
<TITLE>Authentication Proxy Failed Page</TITLE>
<script type="text/javascript">
    var donesubmitted = false;
    function DoneButton() {
        if (donesubmitted == false) {
            donesubmitted = true;
          window.opener.location.reload();
          window.close();
        }
    }
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<p>Authentication Failed !</p>
<FORM>
  <input type=button name=enter value=DONE onClick="DoneButton();">
</FORM>
<noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
     for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
      JavaScript if you would like to have JavaScript enabled
      for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
       disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web brower window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
```

```
</UL>
</noscript></BODY></HTML>
```