WLC 5760/3850 Custom WebAuth with Local Authentication Configuration Example

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Authentication, Authorization, and Accounting (AAA)](#)
[Parameter-Map](#)
[Wireless LAN (WLAN) Configuration](#)
[Global Configuration](#)
[Create Local Users](#)
[FTP Configuration for File Transfer](#)
[Upload to Flash](#)
[Sample Webauth_login HTML](#)
[Screenshots](#)
[Verify](#)
[Troubleshoot](#)

Introduction

This document describes how to configure a custom WebAuth with local authentication on a Wireless LAN Controller (WLC).

Prerequisites

Requirements

Before you configure and customize WebAuth, ensure that your PC:

- Has an IP address on an open Service Set Identifier (SSID)
- Can ping the default gateway
- Can identify and locate the Domain Name Server (DNS) (**ipconfig/all**)
- Can resolve names (with **nslookup**)
- Can access the Internet

Components Used

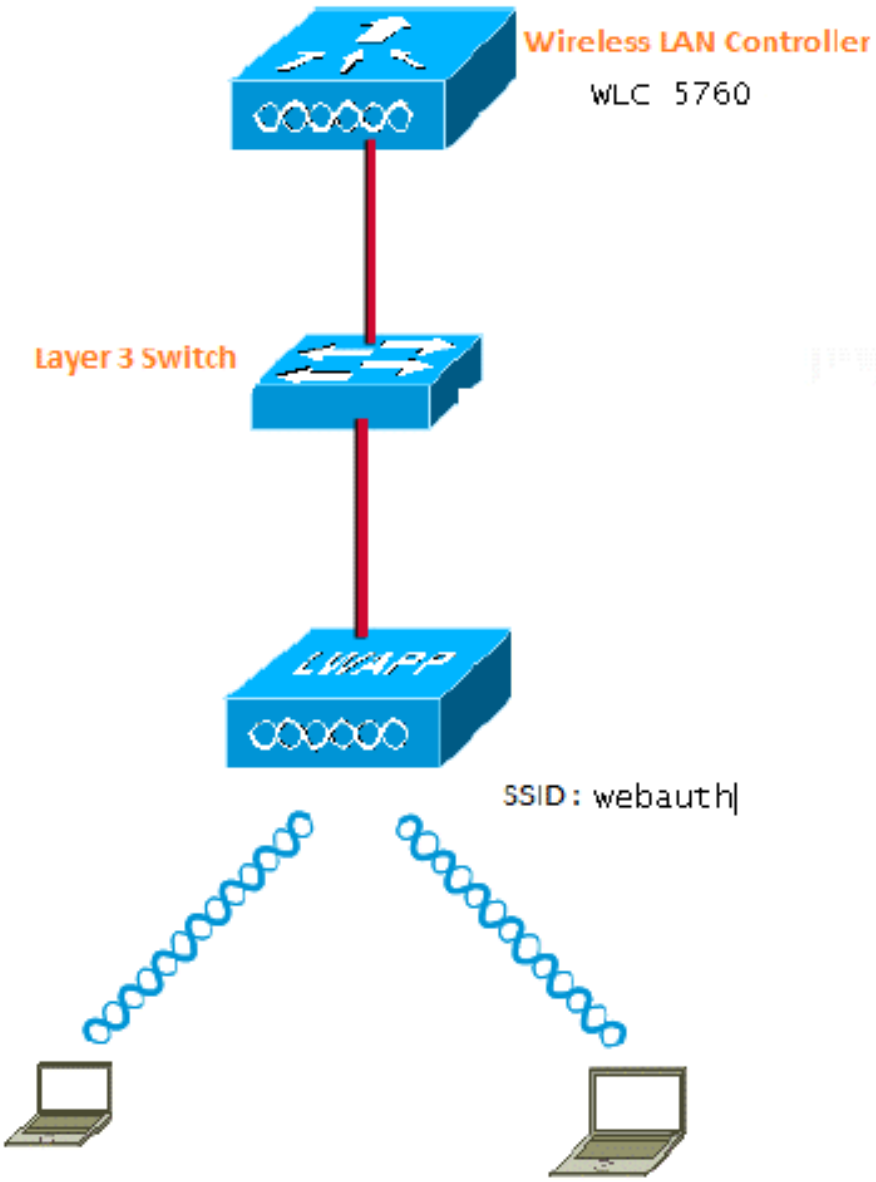
The information in this document is based on these software and hardware versions:

- A 5760 WLC that runs 3.3 code
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows 7 Native Wireless Supplicant

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



Authentication, Authorization, and Accounting (AAA)

Here is the configuration for AAA. This configures the authentication and the authorization profiles in such a way that the clients who connect are authenticated to the local WLC database.

```
aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local
```

Parameter-Map

Here is the configuration for the Parameter-Map. This section provides insight on the how to configure the Virtual IP address on the WLC and how to set the parameter type, which helps to specify the redirect URL, Login Page, Logout page, and Failure page. You must make sure that the flash has these files.

```
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1

parameter-map type webauth custom
type webauth
redirect on-success http://www.cisco.com
banner text ^C CC global ip for redirect ^C
 custom-page login device flash:webauth_login.html
 custom-page success device flash:webauth_success.html
 custom-page failure device flash:webauth_failure.html
 custom-page login expired device flash:webauth_expired.html
```

Wireless LAN (WLAN) Configuration

Here is the configuration for WLAN. The WLAN is configured for Layer 3 security. This configuration maps the authentication list to Local_webauth and ensures that the authentication is handled by the local net users. This calls the AAA configuration that is in the initial step.

```
wlan webauth 1 webauth

client vlan Vlanx
no security wpa
no security wpa akm dot1x

no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list local_webauth

security web-auth parameter-map custom

session-timeout 1800
no shutdown
```

Global Configuration

Use this for the global configuration. Ensure that you have HTTP/HTTPS and IP device tracking enabled. If you do not enable HTTP/HTTPS, you do not get the web page.

```
ip http server
ip device tracking
```

Create Local Users

Use this in order to create local users.

```
username <username> password 0 <password>
```

FTP Configuration for File Transfer

Use this for the FTP configuration for file transfer.

```
ip ftp username <username>
ip ftp password <password>
```

Upload to Flash

Use this in order to upload custom HTML files to the Flash: with command:

```
5760# copy ftp://x.x.x.x/webauth_login.html flash:
```

Here is an example of Flash content:

```
w-5760-2#dir flash:
Directory of flash:/
64649  -rw-        1164   Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654  -rw-        2047   Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655  -rw-        1208   Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656  -rw-         900   Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657  -rw-       96894   Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658  -rw-       23037   Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
64660  -rw-        2586   Oct 7 2013 13:31:27 +00:00  web_auth_aup.html
```

Sample Webauth_login HTML

If this needs any modification or customization, you must involve a developer who knows HTML, which is not covered by the Cisco Technial Assistance Center.

```
<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>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<style type="text/css">
body {
   background-color: #ffffff;
}
```

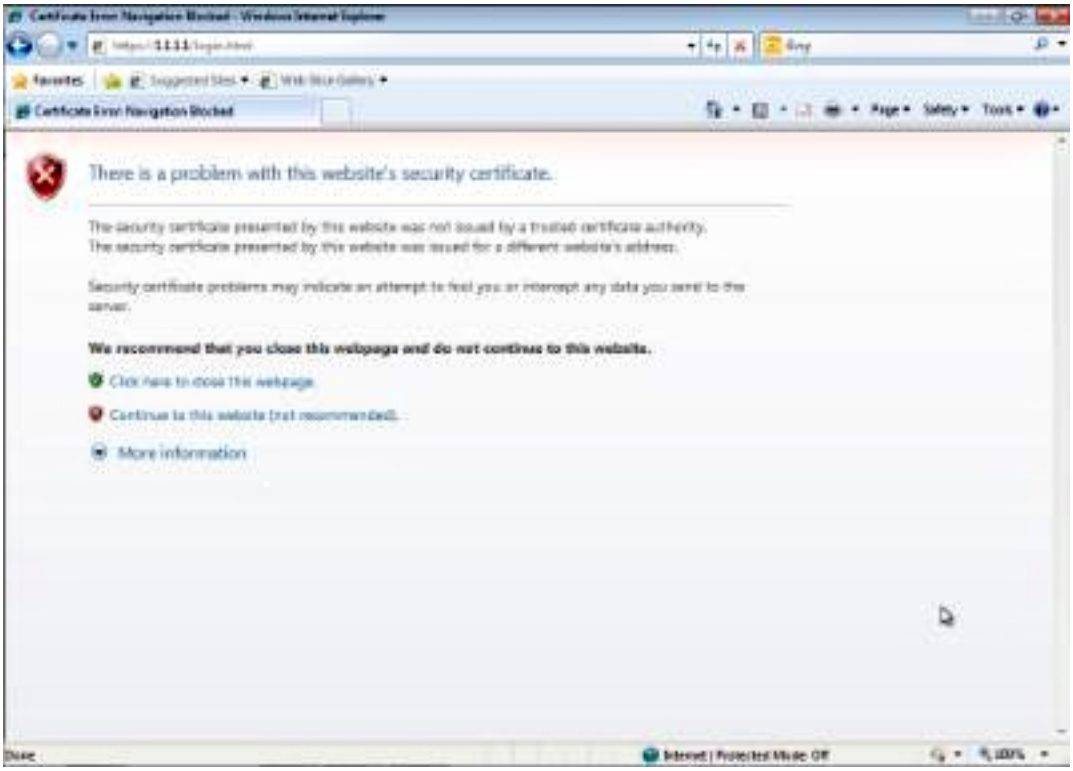
```
</style>
</HEAD>
<BODY>
<H1><img src="http://192.168.2.91/flash:web_auth_logo.png" width="75" height="50" alt="Cisco
Logo" longdesc="http://www.cisco.com"></H1>
<center>
<H2> Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http://192.168.2.91/flash:web_auth_aup.html" width="950" height="250"
scrolling="auto"></iframe><BR><BR>

<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>
<center>
<p> </p>
<img src="http://192.168.2.91/flash:web_auth_cisco.png" alt="Cisco Powered" width="215"
height="136" align="middle" longdesc="http://www.cisco.com">
</center>
</BODY></HTML>
```

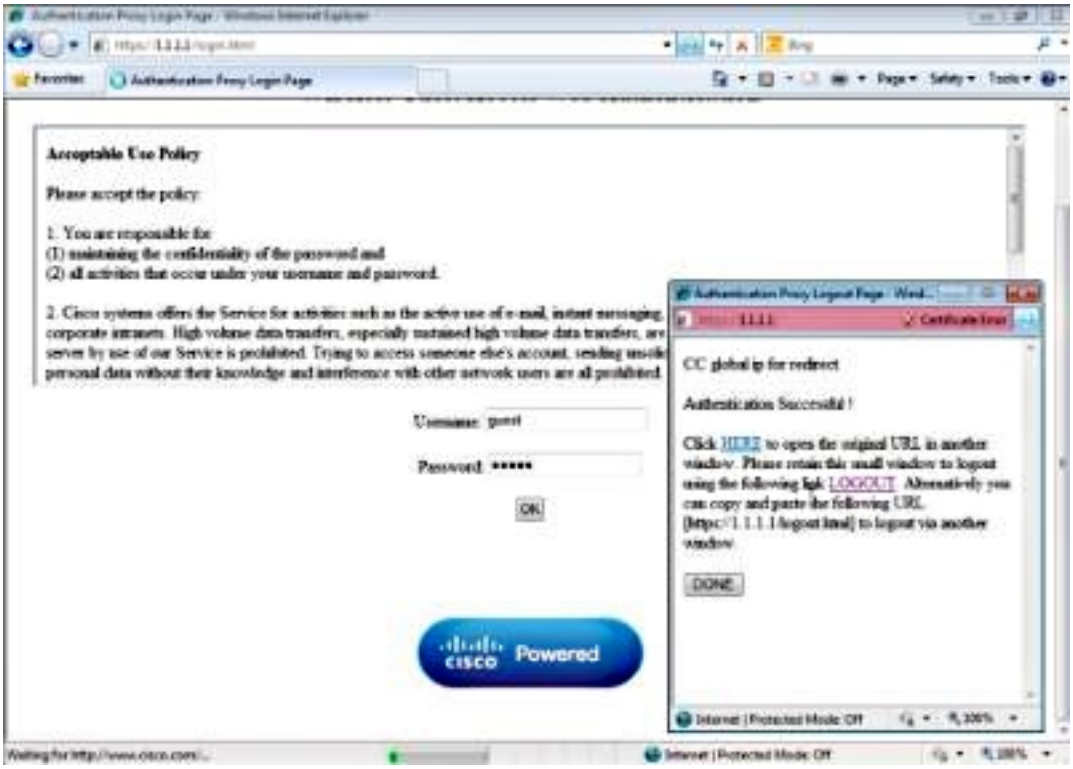
Screenshots

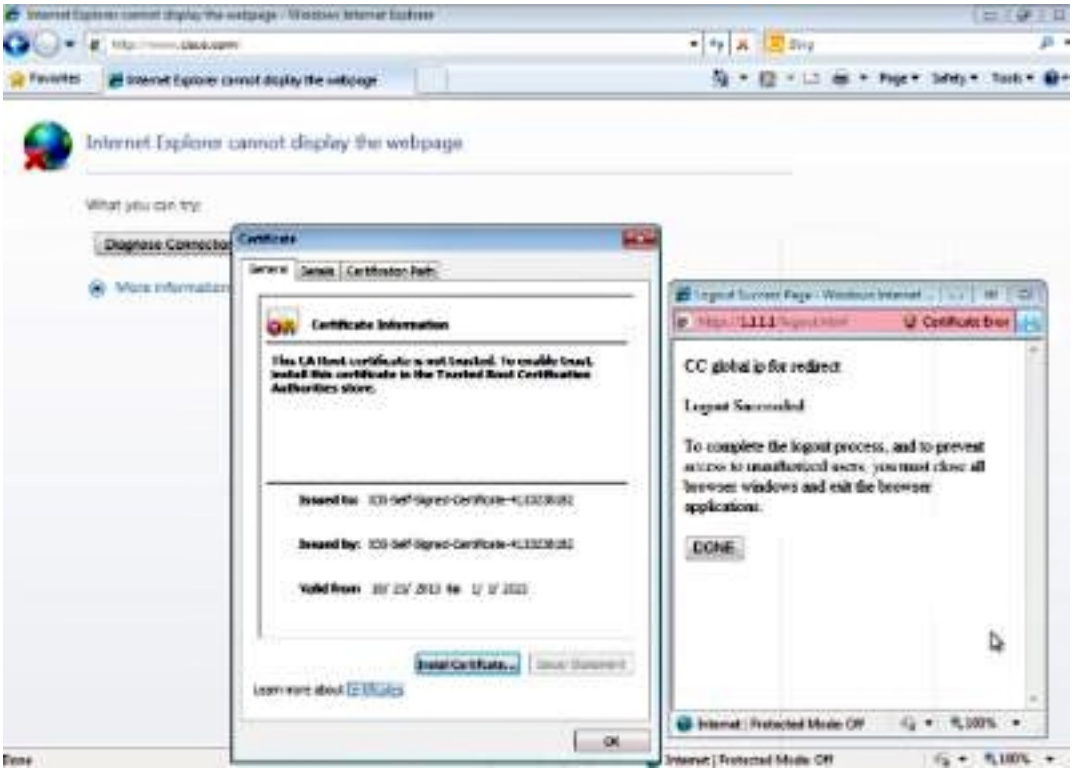
Here are some screenshots from the client:

Client connects to WLAN and is automatically redirected:


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Wireless Guest Access Web Authentication
Acceptable Use Policy
Please accept the policy:
1. You are responsible for
(1) maintaining the confidentiality of the password and
(2) all activities that occur under your username and password.
2. Cisco systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.
Username: guest
Password:
OK





Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.