WLC 5760/3850 로컬 인증 컨피그레이션이 포함된 사용자 지정 WebAuth 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[AAA(Authentication, Authorization, and Accounting)](#)
[매개변수 맵](#)
[무선 LAN(WLAN) 컨피그레이션](#)
[전역 구성](#)
[로컬 사용자 생성](#)
[파일 전송을 위한 FTP 구성](#)
[플래시에 업로드](#)
[샘플 Webauth_login HTML](#)
[스크린샷](#)
[다음을 확인합니다.](#)
[문제 해결](#)

소개

이 문서에서는 WLC(Wireless LAN Controller)에서 로컬 인증으로 사용자 지정 WebAuth를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

WebAuth를 구성하고 사용자 지정하기 전에 PC에 다음 정보가 있는지 확인합니다.

- 열려 있는 SSID(Service Set Identifier)에 IP 주소가 있음
- 기본 게이트웨이를 ping할 수 있습니다.
- DNS(Domain Name Server)(ipconfig**/all**)를 식별하고 찾을 수 있습니다.
- 이름 확인 가능(nslookup 사용)
- 인터넷에 액세스 가능

사용되는 구성 요소

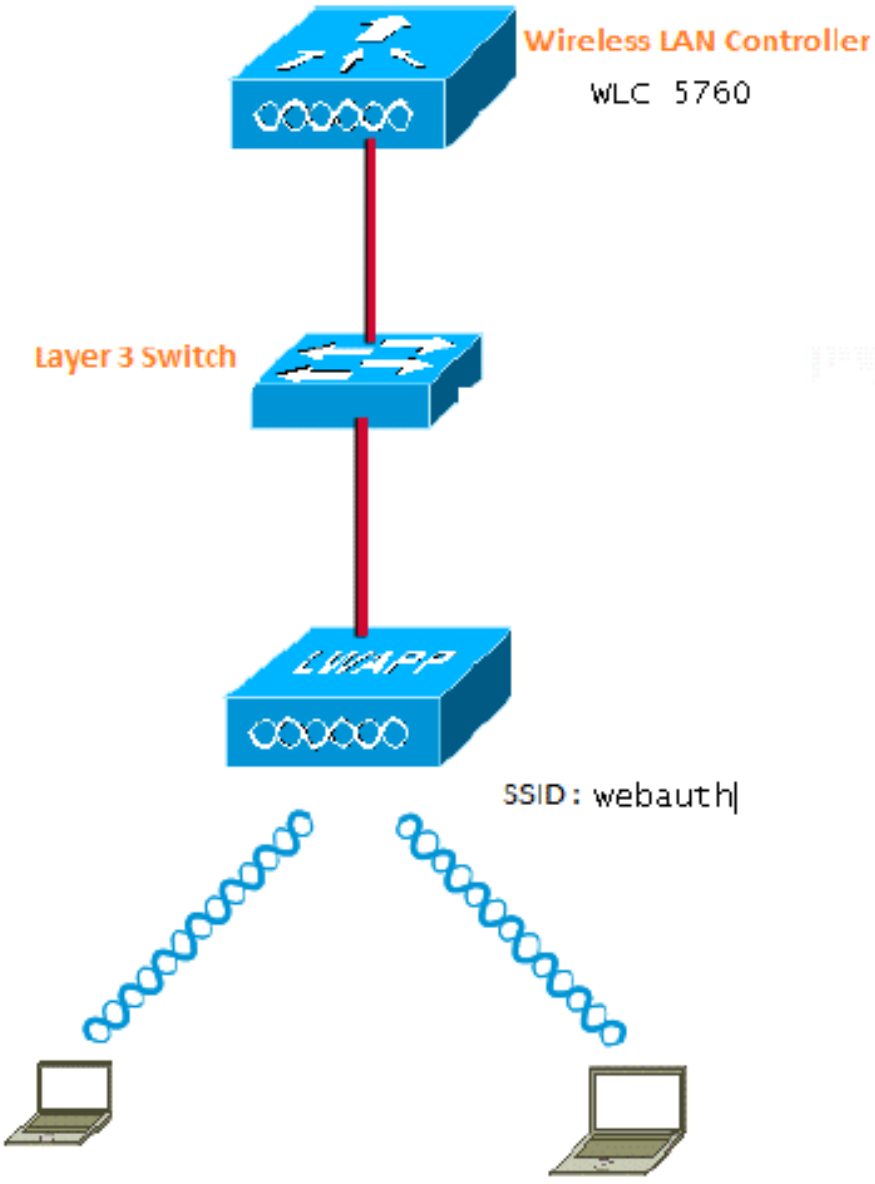
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 3.3 코드를 실행하는 5760 WLC
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows 7 기본 무선 서플리컨트

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



AAA(Authentication, Authorization, and Accounting)

다음은 AAA에 대한 컨피그레이션입니다.이렇게 하면 연결하는 클라이언트가 로컬 WLC 데이터베이스에 인증되는 방식으로 인증 및 권한 부여 프로파일을 구성합니다.

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

매개변수 맵

다음은 매개변수 맵에 대한 컨피그레이션입니다.이 섹션에서는 WLC에서 가상 IP 주소를 구성하는 방법과 매개변수 유형을 설정하는 방법에 대한 정보를 제공합니다. 이 방법을 통해 리디렉션 URL, 로그인 페이지, 로그아웃 페이지 및 오류 페이지를 지정할 수 있습니다.플래시에 이러한 파일이 있는지 확인해야 합니다.

```
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
```

무선 LAN(WLAN) 컨피그레이션

다음은 WLAN에 대한 컨피그레이션입니다.WLAN은 레이어 3 보안을 위해 구성됩니다.이 컨피그레이션은 인증 목록을 Local_webauth에 매핑하고 로컬 네트워크 사용자가 인증을 처리하도록 합니다.이렇게 하면 초기 단계에 있는 AAA 컨피그레이션이 호출됩니다.

```
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
```

전역 구성

전역 컨피그레이션에 사용합니다.HTTP/HTTPS 및 IP 디바이스 추적이 활성화되었는지 확인합니다.HTTP/HTTPS를 활성화하지 않으면 웹 페이지가 표시되지 않습니다.

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

로컬 사용자 생성

로컬 사용자를 만들려면 이 옵션을 사용합니다.

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

파일 전송을 위한 FTP 구성

파일 전송을 위한 FTP 컨피그레이션에 사용합니다.

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

플래시에 업로드

사용자 지정 HTML 파일을 플래시에 업로드하려면 이 옵션을 사용합니다.명령 포함:

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

다음은 Flash 콘텐츠의 예입니다.

```
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
```

샘플 Webauth_login HTML

이를 위해 수정 또는 사용자 정의가 필요한 경우 Cisco Technical Assistance Center에서 다루지 않는 HTML을 알고 있는 개발자가 참여해야 합니다.

```
<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;
}
```

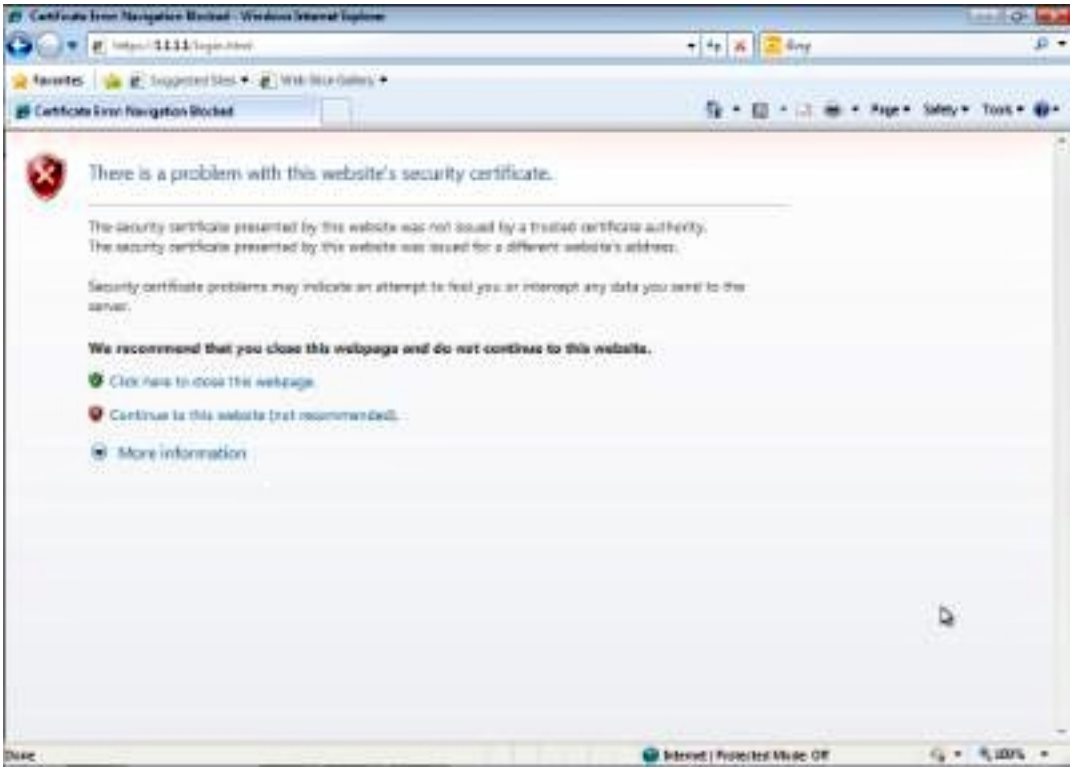
```
</style>
</HEAD>
<BODY>
<H1><img src="http://192.168.2.91/flash:web_auth_logo.png" width="75" height="50" alt="Cisco
Logo" longdesc="http://www.cisco.com"></H1>
<center>
<H2> Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http://192.168.2.91/flash:web_auth_aup.html" width="950"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

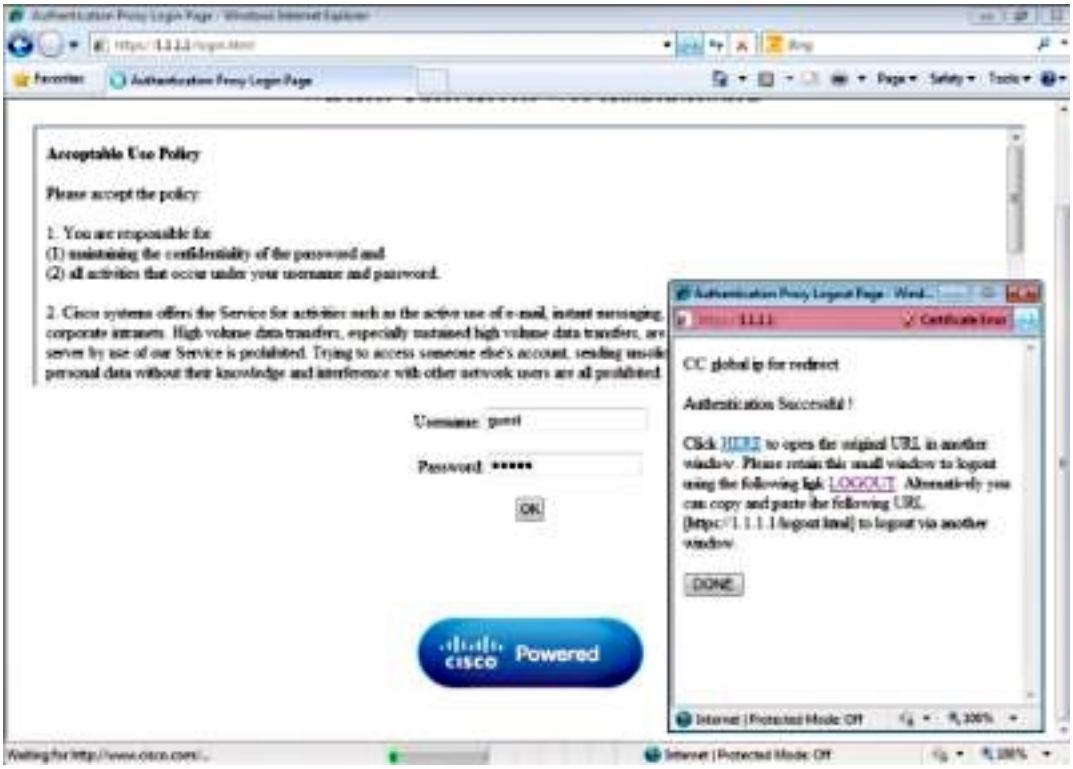
스크린샷

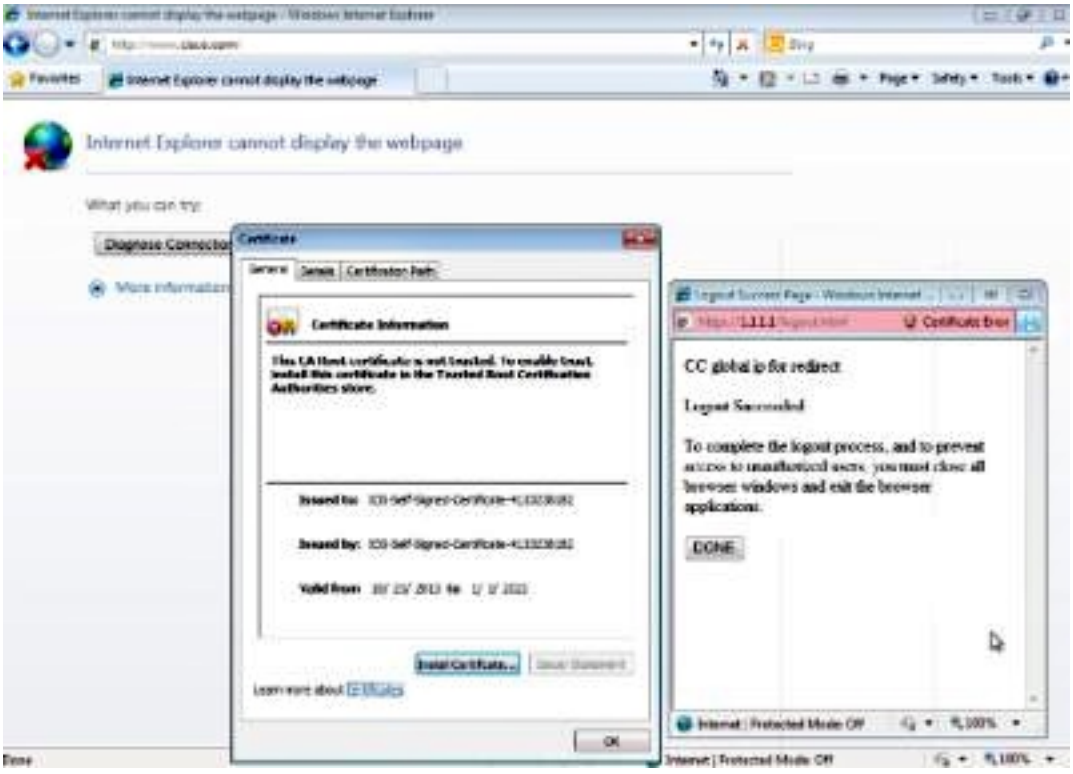
다음은 클라이언트의 스크린샷입니다.

클라이언트가 WLAN에 연결되고 자동으로 리디렉션됩니다.


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





다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.