External Web Authentication on Converged Access

The configuration procedure for the External Web Authentication on Converged Access is similar to the configuration procedure of Local Web Authentication with External RADIUS Authentication. However, to configure an External Web Authentication, in addition to configuring Local Web Authentication, you need to do the following:

- Add pre-authentication Access Control Lists (ACL)
- Change the Web Authentication parameter map

Note For information on Local Web Authentication with External RADIUS Authentication, refer to Local Web Authentication with External RADIUS Authentication.

The following example describes the parameter maps in global configuration mode:

```
parameter-map type webauth test_web
        type webauth
        redirect for-login https://192.168.154.119 : 8443
/guestportal/portals/external_webauth/portal.jsp -> ISE customguest portal
       redirect portal ipv4 192.168.154.119                                  -> Redirect
 to ISE banner
```

Note You can specify the redirect pages for success and failure scenario using the following commands:

- redirect on-success url
- redirect on-failure url

The following example describes the pre-authentication ACL in global configuration mode:

Note Preauth_ise is an optional configuration for external web authentication.

```
ip access-lists extended preauth_ise
10 permit udp any eq bootps any -> allow DHCP
20 permit udp any any eq bootpc -> allow DHCP
30 permit udp any eq bootpc any -> allow DHCP
```

```
40 permit udp any any eq domain -> allow DNS
50 permit udp any eq domain any -> allow DNS
60 permit ip any host 192.0.2.1 -> allow access to ISE
70 permit ip host 192.0.2.1 any -> allow ISE to talk back
```

Note On Converged Access, the traffic for Web Authentication, Service Set Identifier (SSID), DHCP, and Domain Name System (DNS) is not allowed, by default. You need to enable DHCP, DNS, and access to the external server.

Example: Configuring WLAN Commands

The following example describes how to configure WLAN commands:

```
wlan external_webauth 11 external_webauth
client vlan 263
ip access-group web preauth_ise          ----> applying preauth ACL
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 ext_ise
security web-auth parameter-map test_web
no shutdown
```

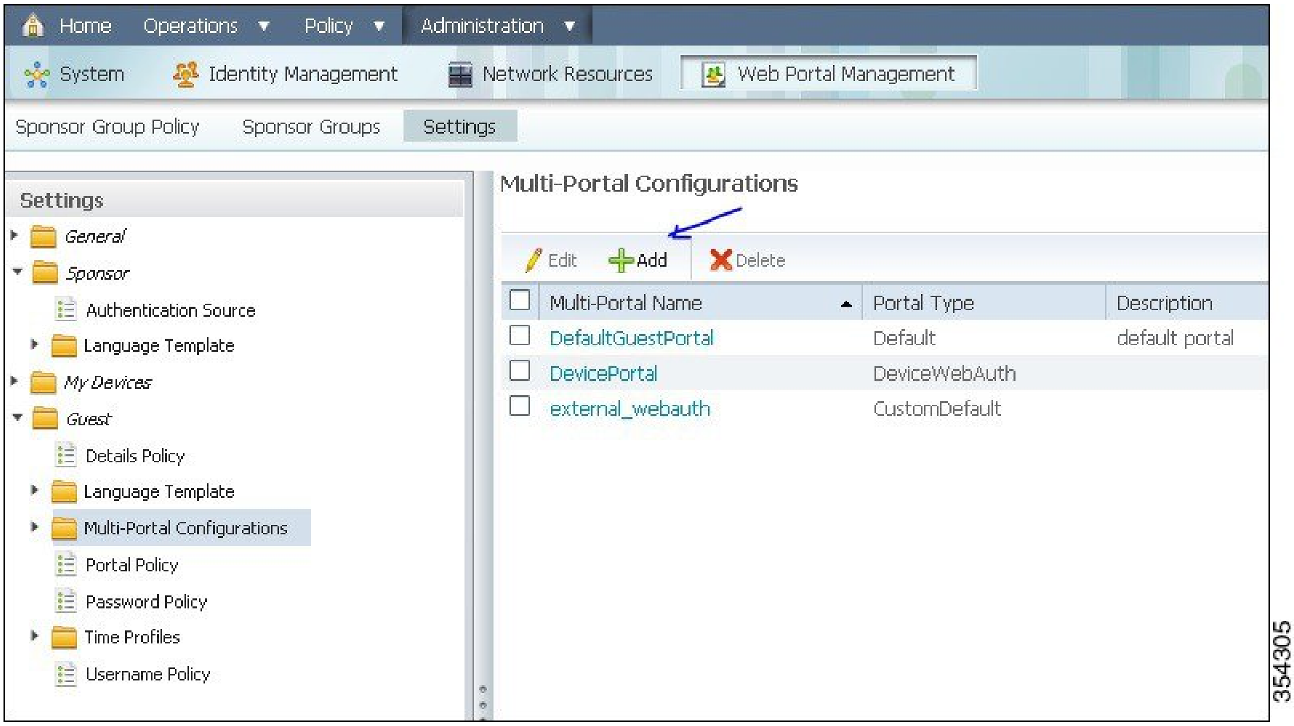
Configuring External Web Authentication with Custom Guest Portal page on ISE

Perform the following steps to configure the External Web Authentication with a custom guest portal page on Identity Services Engine (ISE):

Note In the figure, the custom default portal is 'external webauth'.

Step 1 To add a custom default portal, click **Add**.

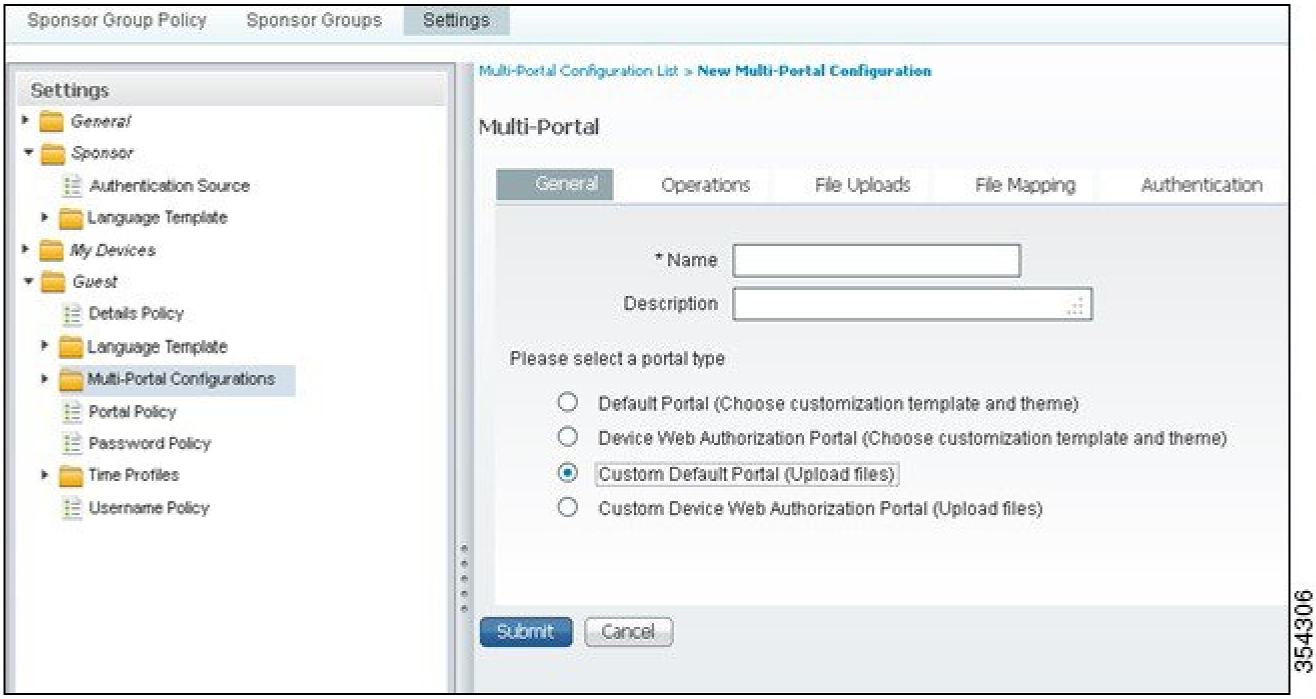
Figure 1: Multi Portal Configurations



□	Multi-Portal Name ▲	Portal Type	Description
□	DefaultGuestPortal	Default	default portal
□	DevicePortal	DeviceWebAuth	
□	external_webauth	CustomDefault	

Step 2 To upload files, choose **Custom Default Portal (upload files)**.

Figure 2: Custom Default Portal



Sponsor Group Policy | Sponsor Groups | Settings

Settings
- General
- Sponsor
  - Authentication Source
  - Language Template
- My Devices
- Guest
  - Details Policy
  - Language Template
  - Multi-Portal Configurations
  - Portal Policy
  - Password Policy
  - Time Profiles
  - Username Policy

Multi-Portal Configuration List > New Multi-Portal Configuration

Multi-Portal

General | Operations | File Uploads | File Mapping | Authentication

* Name

Description

Please select a portal type

○ Default Portal (Choose customization template and theme)

○ Device Web Authorization Portal (Choose customization template and theme)

● Custom Default Portal (Upload files)

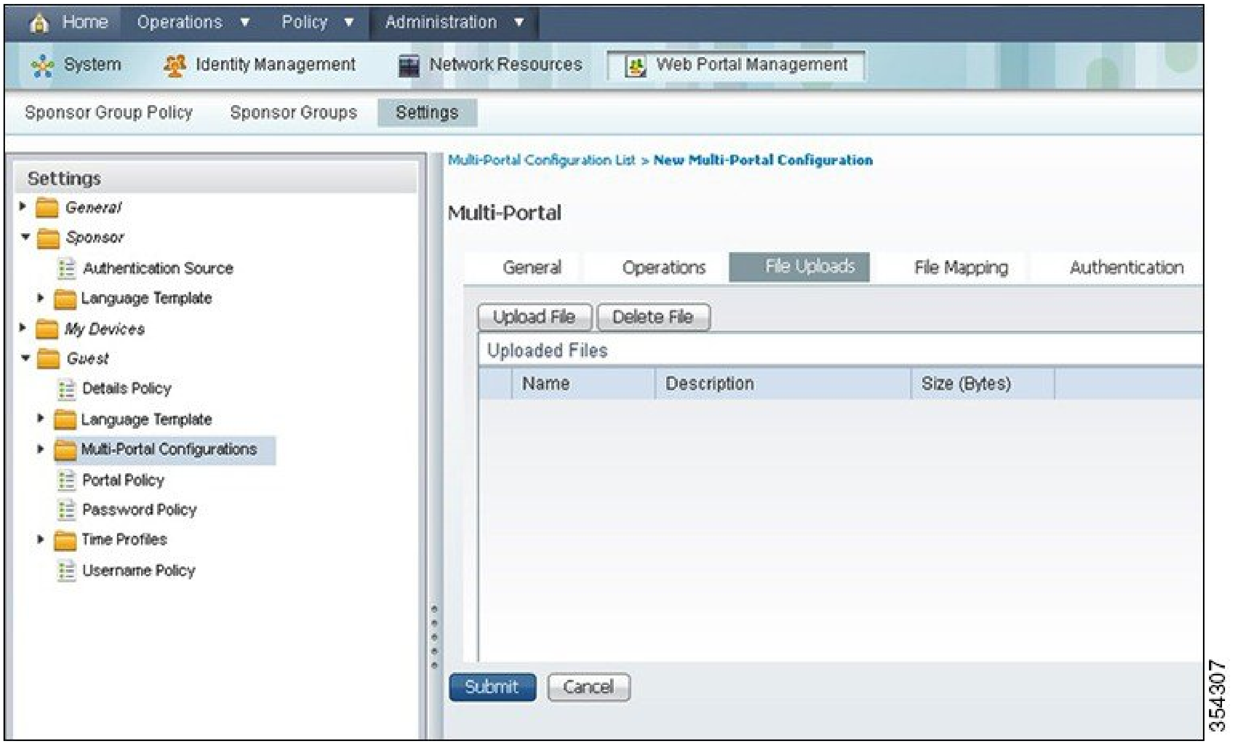
○ Custom Device Web Authorization Portal (Upload files)

Submit Cancel

Step 3 Navigate to **File Uploads**. In the **File Uploads** area, click **Upload File** and select the relevant page.

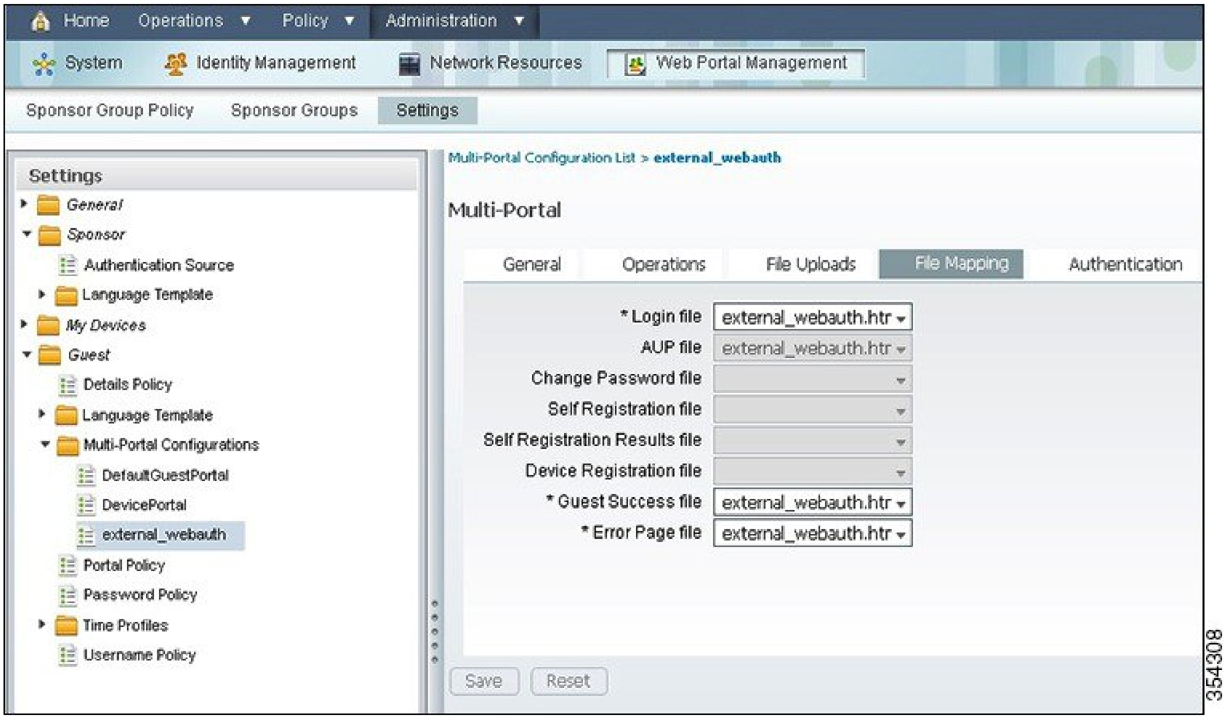
Note You can upload the login, success, and failure pages.

Figure 3: File Uploads



Step 4 To enter the file mapping details, navigate to **File Mapping** and enter the details, as required.

Figure 4: File Mapping



* Login file: external_webauth.htr

AUP file: external_webauth.htr

Change Password file:

Self Registration file:

Self Registration Results file:

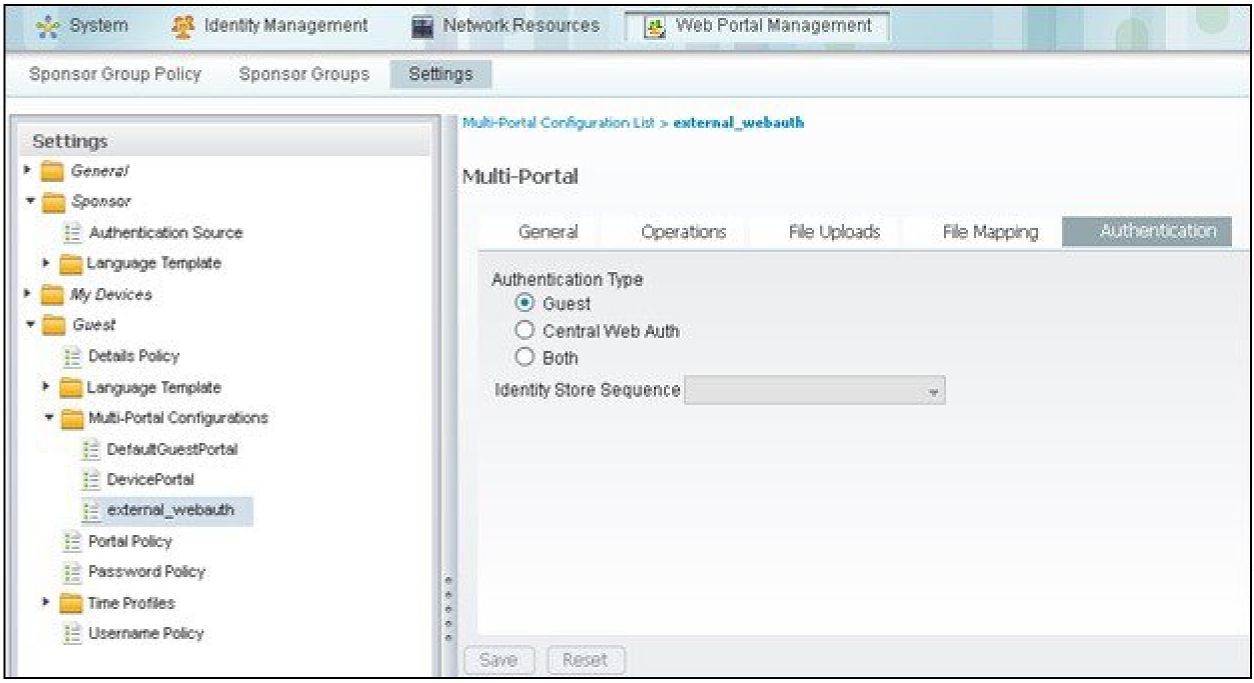
Device Registration file:

* Guest Success file: external_webauth.htr

* Error Page file: external_webauth.htr

Step 5 To enter authentication details, navigate to **Authentication** and enter the details, as required.

Figure 5: Authentication



Multi-Portal

Authentication Type

● Guest

○ Central Web Auth

○ Both

Identity Store Sequence

Step 6 The ISE Authentication success log is displayed. The authorization policy returns an access-accept.

Example: External Web Authentication Page

The following code describes an external web authentication page:

```
<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>
<!--
// The form "action" url must be set to the webauth virtual-ip address
//
```

```
 -->
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<FORM method=post action="http://1.1.1.1/" 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>
```

Example: Configuring External Web Authentication on Converged Access

The following code describes the configuration of an external web authentication on converged access using **show run** command on Cisco Catalyst 3850 Series Switch:

```
Device# Device# show run
Building configuration...
Current configuration : 7946 bytes
!
! Last configuration change at 07:29:52 UTC Tue Apr 9 2013
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot system switch 1 flash:packages.conf
boot system switch 1 flash:cat3k_caa-universalk9.SSA.03.09.55.RDP.150-9.55.RDP.bin
boot-end-marker
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 4 EqmAkK0J3mSGO0ZICurjr4sQh0jNaaNBJAFiEDDLi1s
!
username admin privilege 15 password 0 ww-wireless
username 3850 password 0 3850
aaa new-model
```

```
!
!
aaa group server radius rad_ise
 server name ise
!
aaa authentication login wcm_local local
aaa authentication login ext_ise group rad_ise
aaa authorization network default local
!
!
!
!
!
aaa session-id common
switch 1 provision ws-c3850-24p
access-session mac-move deny
!
ip device tracking
ip dhcp snooping
!
!
qos wireless-default-untrust
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-0
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-0
 revocation-check none
 rsakeypair TP-self-signed-0
!
!
crypto pki certificate chain TP-self-signed-0
 certificate self-signed 01
  3082022C 30820195 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  28312630 24060355 0403131D 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 30301E17 0D313330 34303930 34343531 325A170D 32303031
  30313030 30303030 5A302831 26302406 03550403 131D494F 532D5365 6C662D53
  69676E65 642D4365 72746966 69636174 652D3030 819F300D 06092A86 4886F70D
  01010105 0003818D 00308189 02818100 A80E6C19 126053DC AF217458 7A9F5E74
  7E4FF6CB F0DA23BB 36603DC4 4418FA85 655F670C 38CDB836 497A3BCD 2ABF4A5C
  15F46CAB C503BD09 61AC0D7F C2F25DC0 670E30AD 926368BF 24BD0834 87750901
  5C2EA184 689700FE 10379C58 A9A778EA 88A05B32 AC2D7F6F BE90F6D1 C73625BA
  35F89D4F 633AC666 92B88255 094BF927 02030100 01A36630 64300F06 03551D13
  0101FF04 05300301 01FF3011 0603551D 11040A30 08820653 77697463 68301F06
  03551D23 04183016 801438DB 46071ACE AA940D18 EB943367 D62E08D7 93E1301D
  0603551D 0E041604 1438DB46 071ACEAA 940D18EB 943367D6 2E08D793 E1300D06
  092A8648 86F70D01 01040500 03818100 6039B3A8 BD78C3D3 3631D01D 44EE79FC
  5EE37CCD AC1244EF 97DC8B36 0D937D9F 6F965DCB 908ABBDC 8BBB7D10 3D7C1DE2
  0EC93557 2C162A8D 1EFB319D EF0E944D CEF2CC8E 5741ACD5 7C7E0B75 34C51700
  11ACDA36 A8968447 A86D6685 52277348 1EF6E60D BA7DD0B5 CB5A7264 B0CB7D1F
  E1AB1040 D580C937 CD227437 8695049A
   quit
dot1x system-auth-control
!
!
!
!
!
diagnostic bootup level minimal
service-template webauth-global-inactive
 inactivity-timer 3600
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode sso
!
!
parameter-map type webauth global
 virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
 type webauth
 redirect for-login https://192.0.2.1:8443/guestportal/portals/external_webauth/portal.jsp
 redirect portal ipv4 192.0.2.1
 banner
parameter-map type webauth webconsent
 type webauth
 banner
 custom-page login device flash:custom_login.html
 custom-page success device flash:custom_success.html
 custom-page failure device flash:custom_fail.html
 custom-page login expired device flash:custom_fail.html
parameter-map type webauth localweb
 type webauth
 banner text ^C test webauth ^C
!
!
vlan 254,263
!
!
class-map match-any non-client-nrt-class
  match non-client-nrt
!
policy-map port_child_policy
 class non-client-nrt-class
    bandwidth remaining ratio 10
!
!
!
!
!
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 no ip route-cache
 negotiation auto
!
interface GigabitEthernet1/0/1
 switchport access vlan 263
 switchport mode access
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
 switchport access vlan 263
 switchport mode access
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
 switchport mode trunk
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
```

```
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan263
 ip dhcp relay information trusted
 ip address 192.0.2.2 192.0.2.254
 ip helper-address 192.0.2.25
 no ip route-cache
!
ip default-gateway 192.0.2.1
ip http server
ip http authentication local
ip http secure-server
!
!
ip access-list extended ACL-REDIRECT
 deny   udp any eq bootps any
 deny   udp any any eq bootpc
 deny   udp any eq bootpc any
 deny   ip any host 192.0.2.5
 deny   ip any host 192.0.2.6
 deny   ip any host 192.0.2.6
 permit tcp any any eq www
ip access-list extended ACL_Provisioning
 permit udp any eq bootpc any eq bootps
 permit udp any host 192.0.2.25 eq domain
 permit udp any host 192.0.2.119 eq domain
 permit ip any host 192.0.2.14
ip access-list extended ACL_Provisioning_Web
 permit ip any host 192.0.2.250
 permit udp any eq bootpc any eq bootps
 permit udp any host 192.0.2.25 eq domain
 permit tcp any host 192.0.2.119 eq 443
 permit tcp any host 192.0.2.119 eq 8443
 permit tcp any host 192.0.2.119 eq www
ip access-list extended ACL_Redirect
 deny   ip any 198.51.100.1 198.51.100.2
 deny   ip any 198.51.100.5 198.51.100.9
 deny   ip any 198.51.100.15 198.51.100.20
 deny   ip any 198.51.100.30 198.51.100.40
 deny   ip any 198.51.100.50 198.51.100.60
 deny   ip any 198.51.100.70 198.51.100.80
 deny   ip any 198.51.100.80 198.51.100.90
 deny   ip any host 198.51.100.95
 permit tcp any any eq www
 permit tcp any any eq 443
 permit tcp any any eq 8443
ip access-list extended preauth_ise
 permit udp any eq bootps any
 permit udp any any eq bootpc
 permit udp any eq bootpc any
 permit ip any host 192.0.2.251
 permit ip host 192.0.2.250 any
 permit ip any host 192.0.2.249
 permit ip host 192.0.2.245 any
!
ip radius source-interface Vlan263
!
!
!
radius server ise
 address ipv4 192.0.2.240 auth-port 1812 acct-port 1813
 key Cisco123
!
!
!
banner motd ^Citen login
^C
!
line con 0
 login authentication console
 stopbits 1
line aux 0
 stopbits 1
line vty 5 15
!
wireless mobility controller
wireless management interface Vlan263
wireless security dot1x radius call-station-id ap-macaddress-ssid
wlan ua-web1 11 ua-web1
 client vlan 263
 ip access-group web preauth_ise
 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 ext_ise
 security web-auth parameter-map test_web
 no shutdown
ap dot11 24ghz rrm channel dca 1
ap dot11 24ghz rrm channel dca 6
ap dot11 24ghz rrm channel dca 11
ap dot11 5ghz rrm channel dca 36
ap dot11 5ghz rrm channel dca 40
ap dot11 5ghz rrm channel dca 44
ap dot11 5ghz rrm channel dca 48
ap dot11 5ghz rrm channel dca 52
ap dot11 5ghz rrm channel dca 56
ap dot11 5ghz rrm channel dca 60
ap dot11 5ghz rrm channel dca 64
ap dot11 5ghz rrm channel dca 149
ap dot11 5ghz rrm channel dca 153
ap dot11 5ghz rrm channel dca 157
ap dot11 5ghz rrm channel dca 161
ap group default-group
end
```