Configuring Wireless Guest Access

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Guest Access

- All mobility peers should be configured for hierarchical mobility architecture.
- For Guest Controller Mobility Anchor configuration on WLAN is must on Mobility Agent and Guest Controller.
- Guest Access can be a 3 box solution or 2 box solution. The mobility tunnel link status should be up between:
  - Mobility Agent, Mobility Controller and Guest Controller.

  or
  - Mobility Agent/Mobility Controller and Guest Controller

Restrictions for Guess Access

Information about Wireless Guest Access

Ideally, the implementation of a wireless guest network uses as much of an enterprise's existing wireless and wired infrastructure as possible to avoid the cost and complexity of building a physical overlay network. Assuming this is the case, the following additional elements and functions are needed:

- A dedicated guest WLAN/SSID—Implemented throughout the campus wireless network wherever guest access is required. A guest WLAN is identified by a WLAN with mobility anchor (Guest Controller) configured.
- Guest traffic segregation—Requires implementing Layer 2 or Layer 3 techniques across the campus network to restrict where guests are allowed to go.
- Access control—Involves using imbedded access control functionality within the campus network or implementing an external platform to control guest access to the Internet from the enterprise network.
- Guest user credential management—A process by which a sponsor or lobby administrator can create temporary credentials in behalf of a guest. This function might be resident within an access control platform or it might be a component of AAA or some other management system.

Fast Secure Roaming

Fast secure roaming can be achieved by caching the Pairwise Master Key (PMK) information for Cisco Centralized Key Management (CCKM), and 802.11i clients. Cisco Centralized Key Management (CCKM) helps to improve roaming. Only the client can initiate the roaming process, which depends on factors such as:

- Overlap between APs
- Distance between APs
- Channel, signal strength, and load on the AP
- Data rates and output power

Whenever a fast-roaming client 802.11i, [CCKM]) roams to a new device, after fast-roaming the clients go through mobility "handoff" procedure. And new AAA attributes learned through mobility "handoff" procedure get re-applied.

Full L2 authentication must be avoided during roaming if the client uses the 802.11i WPA2, CCKM, to achieve the full requirements of fast secure roaming. The PMK cache (802.11i, CCKM) is used to authenticate and derive the keys for roaming clients to avoid full L2 authentication. This requires all Mobility Anchors (MA) and Mobility Controllers (MC) in the mobility group to have the same PMK cache values.

The session timeout defines when a PMK cache will expire. A PMK cache can also be deleted when a client fails to re-authenticate or when it is manually deleted them from the CLI. The deletion on the original controller or switch shall be propagated to other controllers or switches in the same mobility group.

How to Configure Guest Access

Creating a Lobby Administrator Account

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device (config)# user-name lobby`	Creates a user account.
Step 3	**type lobby-admin** **Example:** `Device (config-user-name)# type lobby-admin`	Specifies the account type as lobby admin.
Step 4	**password 0** *password* **Example:** `Device(config-user-name)# password 0 lobby`	Creates a password for the lobby administrator account.
Step 5	**end** **Example:** `Device (config-user-name)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config | section** *user-name* (or) **show running-config | section** *configured lobby admin username* **Example:** `Device # show running-config | section lobby`	Displays the configuration details.

Example

Configuring Guest User Accounts

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**user-name** *user-name* **Example:** `Device (config)# user-name guest`	Creates a username for the lobby ambassador account.
Step 3	**password** *unencrypted/hidden-password password* **Example:** `Device (config-user-name)# password 0 guest`	Specifies the password for the user.
Step 4	**type network-user description** *description* **guest-user lifetime year** *0-1* **month** *0-11* **day** *0-30* **hour** *0-23* **minute** *0-59* **second** *0-59* **Example:** `Device (config-user-name)# type network-user description guest guest-user lifetime year 1 month 10 day 3 hour 1 minute 5 second 30`	Specifies the type of user.
Step 5	**end** **Example:** `Device (config-user-name)# end`	Returns to privileged EXEC mode.
Step 6	**show aaa local netuser all** **Example:** `Device # show aaa local netuser all`	Displays the configuration details. After the lifetime, the user-name with guest type will be deleted and the client associated with the guest user-name will be de-authenticated.
Step 7	**show running-config | section***user-name* **Example:** `Device # show running-config | section guest`	Displays the configuration details.

Example

Configuring Mobility Agent (MA)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility controller ip***mc-ipaddress* **public-ip** *mc-publicipaddress* **Example:** `Device (config) # wireless mobility controller ip27.0.0.1 public-ip 27.0.0.1`	Configures the Mobility Controller to which the MA will be associated.
Step 3	**wlan** *wlan-name wlan-id ssid* **Example:** `Device (config) # wlan mywlan 34 mywlan-ssid`	• For *wlan-name* enter, enter the profile name. The range is 1- 32 characters. • For *wlan-id*, enter the WLAN ID. The range is 1-512. • For *ssid*, enter the Service Set IDentifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 4	**client vlan id***vlan-group name/vlan-id* **Example:** `Device (config-wlan) # client vlan VLAN0136`	Configures the VLAN id or group of the WLAN.
Step 5	**no security wpa** **Example:** `Device (config-wlan) # no security wpa`	The security configuration must be the same for the WLAN created on the GC. This example is for open authentication. For other security types such as open and webauth, appropriate command should be provided.
Step 6	**mobility anchor** *ipaddress* **Example:** `Device (config-wlan) # mobility anchor 9.3.32.2`	Configures the Guest Controller as mobility anchor.
Step 7	**aaa-override** **Example:**	(Optional) Enables AAA override. AAA override is required for non open

	Command or Action	Purpose
	`Device (config-wlan) # aaa-override`	authentication in case AAA attributes are to be prioritized. It is required only in case guest user need to be deauthenticated after lifetime or have to give aaa-override attribute to the user.
Step 8	**no shutdown** **Example:** `Device(config-wlan) # no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device (config) # end`	Returns to privileged EXEC mode.
Step 10	**show wireless mobility summary** **Example:** `Device  # show wireless mobility summary`	Verifies the mobility controller IP address and mobility tunnel status.
Step 11	**show wlan name** *wlan-name/id* **Example:** `Device # show wlan name mywlan`	Displays the configuration of mobility anchor.

Example

Configuring Mobility Controller

Mobility Controller mode should be enabled using the **wireless mobility controller** command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**wireless mobility group member ip** *ip-address* **public-ip** *ip-address* **group** *group-name* **Example:** `Device (config) # wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test`	Adds all peers within the MC group. The *ip-address* should be the guest controller's IP address.
Step 3	**wireless mobility controller peer-group** *peer-group-name*	Creates the switch peer group.

	Command or Action	Purpose
	Example: `Device (config) # wireless mobility controller peer-group pg`	
Step 4	**wireless mobility controller peer-group** *peer-group-name* **member ip** *ipaddress* **public-ip** *ipaddress* **Example:** `Device (config) # wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip 9.7.136.10`	Adds the MA to the switch peer group.
Step 5	**end** **Example:** `Device (config) # end`	Returns to privileged EXEC mode.
Step 6	**show wireless mobility summary** **Example:** `Device # show wireless mobility summary`	Displays the configuration details.

Example

Obtaining a Web Authentication Certificate

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**crypto pki import** *trustpoint name* **pkcs12 tftp:** *passphrase* **Example:** `Device (config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco`	Imports certificate.
Step 3	**end** **Example:** `Device (config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	**show crypto pki** *trustpoints cert* **Example:** `Device # show crypto pki trustpoints cert`	Displays the configuration details.

Example

Displaying a Web Authentication Certificate

Procedure

	Command or Action	Purpose
Step 1	**show crypto ca certificate verb** **Example:** `Device # show crypto ca certificate verb`	Displays the current web authentication certificate details.

Example

Choosing the Default Web Authentication Login Page

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Device (config) # parameter-map type webauth test`	Configures the web-auth parameter-map.
Step 3	**wlan** *wlan-name* **Example:** `Device (config) # wlan wlan10`	For the wlan-name, enter the profile name. The range is 1- 32 characters.
Step 4	**shutdown**	Disables WLAN.

	Command or Action	Purpose
	Example: `Device (config) # shutdown`	
Step 5	**security web-auth** **Example:** `Controller (config-wlan) # security web-auth`	Enables web-auth on WLAN.
Step 6	**security web-auth authentication-list** *authentication list name* **Example:** `Controller (config-wlan) # security web-auth authentication-list test`	Allows you to map the authentication list name with the web-auth WLAN.
Step 7	**security web-auth parameter-map** *parameter-map name* **Example:** `Device (config) # security web-auth parameter-map test`	Allows you to map the parameter-map name with the web-auth WLAN.
Step 8	**no shutdown** **Example:** `Device (config) # no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device (config) # end`	Returns to privileged EXEC mode.
Step 10	**show running-config | section** *wlan-name* **Example:** `Device# show running-config | section mywlan`	Displays the configuration details.
Step 11	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Device# show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Choosing a Customized Web Authentication Login Page from an External Web Server

AAA override flag should be enabled on the WLAN for web authentication using local or remote AAA server.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `Device (config) # parameter-map type webauth global`	Configures a global webauth type parameter.
Step 3	**virtual-ip {ipv4 | ipv6}** *ip-address* **Example:** `Device (config-params-parameter-map) # virtual-ip ipv4 192.0.2.1`	Configures the virtual IP address.
Step 4	**parameter-map type webauth** *parameter-map name* **Example:** `Device (config-params-parameter-map) # parameter-map type webauth test`	Configures the webauth type parameter.
Step 5	**type {authbypass | consent | webauth | webconsent}** **Example:** `Device (config-params-parameter-map) # type webauth`	Configures webauth subtypes such as consent, passthru, webauth, or webconsent.
Step 6	**redirect [for-login|on-success|on-failure]** *URL* **Example:** `Device (config-params-parameter-map) # redirect for-login http://9.1.0.100/login.html`	Configures the redirect URL for the log in page, success page, and failure page.
Step 7	**redirect portal {ipv4 | ipv6}** *ip-address* **Example:** `Device (config-params-parameter-map) # redirect portal ipv4`	Configures the external portal IPv4 address.

	Command or Action	Purpose
Step 8	**end** **Example:** `Device (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 9	show running-config | section parameter-map **Example:** `Device # show running-config | section parameter-map`	Displays the configuration details.

Example

Assigning Login, Login Failure, and Logout Pages per WLAN

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth** *parameter-map-name* **Example:** `Device (config) # parameter-map type webauth test`	Configures the webauth type parameter.
Step 3	**custom-page login device** *html-filename* **Example:** `Device (config-params-parameter-map)# custom-page login device flash:login.html`	Allows you to specify the filename for web authentication customized login page.
Step 4	**custom-page login expired** *html-filename* **Example:** `Device (config-params-parameter-map)# custom-page login expired device flash:loginexpired.html`	Allows you to specify the filename for web authentication customized login expiry page.
Step 5	**custom-page failure device** *html-filename* **Example:** `Device (config-params-parameter-map)# custom-page failure device flash:loginfail.html`	Allows you to specify the filename for web authentication customized login failure page.

	Command or Action	Purpose
Step 6	**custom-page success device** *html-filename* **Example:** `Device (config-params-parameter-map)# custom-page success device device flash:loginsuccess.html`	Allows you to specify the filename for web authentication customized login success page.
Step 7	**end** **Example:** `Device (config-params-parameter-map)# end`	Returns to privileged EXEC mode.
Step 8	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Device (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Configuring AAA-Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device (config) # wlan ramban`	For *wlan-name*, enter the profile name. The range is 1- 32 characters.
Step 3	**aaa-override** **Example:** `Device (config-wlan) # aaa-override`	Enables AAA override on the WLAN.
Step 4	**end** **Example:** `Device (config-wlan) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section** *wlan-name* **Example:**	Displays the configuration details.

	Command or Action	Purpose
	`Device # show running-config | section ramban`	

Example

Configuring Client Load Balancing

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Device (config-wlan)# shutdown`	Disables WLAN.
Step 4	**mobility anchor** *ip-address1* **Example:** `Device (config-wlan) # mobility anchor 9.7.136.15`	Configures a guest controller as mobility anchor.
Step 5	**mobility anchor** *ip-address2* **Example:** `Device (config-wlan) # mobility anchor 9.7.136.16`	Configures a guest controller as mobility anchor.
Step 6	**no shutdown wlan** **Example:** `Device (config-wlan) # no shutdown wlan`	Enables the WLAN.
Step 7	**end** **Example:** `Device (config-wlan) # end`	Returns to privileged EXEC mode.
Step 8	**show running-config | section** *wlan-name* **Example:**	Displays the configuration details.

	Command or Action	Purpose
	`Device # show running-config | section ramban`	

Example

Configuring Preauthentication ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name* **Example:** `Device (config)# wlan ramban`	For *wlan-name*, enter the profile name.
Step 3	**shutdown** **Example:** `Device (config-wlan)# shutdown`	Disables the WLAN.
Step 4	**ip access-group web** *preauthrule* **Example:** `Device (config-wlan)# ip access-group web preauthrule`	Configures ACL that has to be applied before authentication.
Step 5	**no shutdown** **Example:** `Device (config)# no shutdown`	Enables the WLAN.
Step 6	**end** **Example:** `Device (config-wlan)# end`	Returns to privileged EXEC mode.
Step 7	**show wlan name** *wlan-name* **Example:** `Device# show wlan name ramban`	Displays the configuration details.

Example

Configuring IOS ACL Definition

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *access-list number* **Example:** `Device (config) # ip access-list extended 102`	Configures extended IP access-list.
Step 3	**permit udp any eq** *port number* **any** **Example:** `Device (config-ext-nacl) # permit udp any eq 8080 any`	Configures destination host.
Step 4	**end** **Example:** `Device (config-wlan) # end`	Returns to privileged EXEC mode.
Step 5	**show access-lists** *ACL number* **Example:** `Device # show access-lists 102`	Displays the configuration details.

Example

Configuring Webpassthrough

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device # configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *parameter-map name* **Example:** `Device (config) # parameter-map type webauth webparalocal`	Configures the webauth type parameter.
Step 3	**type consent** **Example:** `Device (config-params-parameter-map) # type consent`	Configures webauth type as consent.
Step 4	**end** **Example:** `Device (config-params-parameter-map) # end`	Returns to privileged EXEC mode.
Step 5	**show running-config | section parameter-map type webauth** *parameter-map* **Example:** `Device (config) # show running-config | section parameter-map type webauth test`	Displays the configuration details.

Example

Configuration Examples for Guest Access

Example: Creating a Lobby Ambassador Account

This example shows how to configure a lobby ambassador account.

```
Device# configure terminal
Device(config)# user-name lobby
Device(config)# type lobby-admin
Device(config)# password 0 lobby
Device(config)# end
Device#  show running-config | section lobby
    user-name lobby
    creation-time 1351118727
    password 0 lobby
    type lobby-admin
```

Example: Obtaining Web Authentication Certificate

This example shows how to obtain web authentication certificate.

```
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Device# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
```

```
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

Example: Displaying a Web Authentication Certificate

This example shows how to display a web authentication certificate.

```
Device# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
    Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
    X509v3 extensions:
    X509v3 Key Usage: F0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
      Data Encipherment
    X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
    X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
    Authority Info Access:
    Associated Trustpoints: CISCO_IDEVID_SUDI
    Key Label: CISCO_IDEVID_SUDI
```

Example: Configuring Guest User Accounts

This example shows how to configure a guest user account.

```
Device# configure terminal
Device(config)# user-name guest
Device(config-user-name)# password 0 guest
Device(config-user-name)# type network-user description guest guest-user lifetime year 1
month 10 day 3 hour 1 minute 5 second 30
Device(config-user-name)# end
Device# show aaa local netuser all
```

```
User-Name           : guest
Type                : guest
Password            : guest
Is_passwd_encrypted : No
Descriptio          : guest
Attribute-List      : Not-Configured
First-Login-Time    : Not-Logged-In
Num-Login           : 0
Lifetime            : 1 years 10 months 3 days 1 hours 5 mins 30 secs
Start-Time          : 20:47:37 chennai Dec 21 2012
```

Example: Configuring Mobility Controller

This example shows how to configure a mobility controller.

```
Device# configure terminal
Device(config)# wireless mobility group member ip 27.0.0.1 public-ip 23.0.0.1 group test
Device(config)# wireless mobility controller peer-group pg
Device(config)# wireless mobility controller peer-group pg member ip 9.7.136.10 public-ip
9.7.136.10
Device(config)# end
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : default
Mobility Oracle                                 : Enabled
DTLS Mode                                       : Enabled

Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 7
Mobility Domain Member Count                    : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP               Public IP        Group Name       Multicast IP     Link Status
-----------------------------------------------------------------------------------
9.9.9.2          -                default          0.0.0.0          UP   : UP
12.12.11.11      12.13.12.12      rasagna-grp                       DOWN : DOWN
27.0.0.1         23.0.0.1         test                              DOWN : DOWN

Switch Peer Group Name            : spg1
Switch Peer Group Member Count    : 0
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

Switch Peer Group Name            : pg
Switch Peer Group Member Count    : 1
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

IP               Public IP             Link Status
--------------------------------------------------
9.7.136.10       9.7.136.10            DOWN : DOWN
```

Example: Choosing the Default Web Authentication Login Page

This example shows how to choose a default web authentication login page.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their CPL
control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

Example: Choosing a Customized Web Authentication Login Page from an IPv4 External Web Server

This example shows how to choose a customized web authentication login page from an IPv4 external web server.

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

Example: Assigning Login, Login Failure, and Logout Pages per WLAN

This example shows how to assign login, login failure and logout pages per WLAN.

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

Example: Configuring AAA-Override

This example shows how to configure aaa-override.

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# aaa-override
Device(config-wlan)# end
Device# show running-config | section fff
 wlan fff 44 fff
 aaa-override
 shutdown
```

Example: Configuring Client Load Balancing

This example shows how to configure client load balancing.

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# mobility anchor 9.7.136.15
Device(config-wlan)# mobility anchor 9.7.136.16
Device(config-wlan)# no shutdown wlan
Device(config-wlan)# end
Device# show running-config | section fff
wlan fff 44 fff
 aaa-override
 shutdown
```

Example: Configuring Preauthentication ACL

This example shows how to configure preauthentication ACL.

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff
```

Example: Configuring IOS ACL Definition

This example shows how to configure IOS ACL definition.

```
Device# configure terminal
Device(config)# ip access-list extended 102
Device(config-ext-nacl)# permit udp any eq 8080 any
Device(config-ext-nacl)# end
Device# show access-lists 102
 Extended IP access list 102
    10 permit udp any eq 8080 any
```

Example: Configuring Webpassthrough

This example shows how to configure webpassthrough.

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

Additional References for Guest Access

Related Documents

Related Topic	Document Title
Mobility CLI commands	*Mobility Command Reference, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE 3SE (Cisco WLC 5700 Series)*
Security CLI commands	*Security Command Reference, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*
Configuring web-based authentication on the Catalyst 5700 Series Wireless Controller	*Security Configuration Guide, Cisco IOS Release 3SE (Cisco WLC 5700 Series)*

Related Topic	Document Title
Wired guest access configuration and commands	*Identity Based Networking Services*

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information for Guest Access

Releases	Feature Information
Cisco IOS XE Release 3.2SE	This feature was introduced.