<HP>di cu
#
 version 5.20.109, Release 3507P35
#
 sysname HP
#
 dhcp relay server-group 1 ip 10.10.12.2
#
 radius log packet
 radius dynamic-author client trusted ip 10.10.13.185
#
 domain default enable ise-vm-4
#
 dns resolve
 dns proxy enable
 dns server 10.10.12.11
#
 telnet server enable
#
 port-security enable
#
 dot1x retry 3
 dot1x authentication-method eap
#
 portal server guest-cwa ip 10.10.13.188 port 8443 key cipher
c3$kIVB7ehITEMNgy0+uCI9/Qt7YzFhI5g= url https://ise-vm-
4.cisco.com:8443/portal/g?p=MQjNbbxj1vm7kCM1XdApWNmeJK server-type imc
 portal server ise-posture ip 10.10.13.188 port 8443 key cipher
c3$FYCmo6zdt58i6DXLHCWinERO5cexnyQ= url https://ise-vm-
4.cisco.com:8443/portal/g?p=94dzggNdwxpvQHrRbvqMKVZmXx server-type imc
 portal server ise-byod ip 10.10.13.188 port 8443 key cipher
c3$A2oQb0y7CSiHXk4J2M2oj0bUf25iAUg= url https://ise-vm-
4.cisco.com:8443/portal/g?p=7ROXzzoOP4pZmF9RJEVR4pzBEr server-type imc
 portal server guest-ise ip 10.10.13.188 port 8443 key cipher
c3$qey53G7774EInCyiHQrbonhBBzJO6E8= url https://ise-vm-
2.cisco.com:8443/portal/g?p=1kmBaaEqYZQLAIRZdDqOXOor1E server-type imc
 portal server guest-saml ip 10.10.13.188 port 8443 key cipher
c3$9Y5lCOYqB8FyBm6dKSbklsLABojid0U= url https://ise-vm-
4.cisco.com:8443/portal/g?p=8PoQlJYbGLZoyFXPQlEz6vPy9D server-type imc
 portal free-rule 0 source ip 10.10.54.4 mask 255.255.255.255 destination ip any
 portal free-rule 1 source ip 10.10.13.0 mask 255.255.255.0 destination ip any
 portal free-rule 2 source ip 10.10.54.253 mask 255.255.255.255 destination ip any
 portal free-rule 3 source ip 10.10.54.249 mask 255.255.255.255 destination ip any
 portal free-rule 4 source ip any destination ip 10.56.62.0 mask 255.255.255.0

```
 portal free-rule 5 source ip any destination ip 10.10.13.0 mask 255.255.255.0 tcp 80
 portal free-rule 6 source ip any destination ip 10.10.13.0 mask 255.255.255.0 tcp 8905
 portal free-rule 7 source ip any destination ip 10.10.13.0 mask 255.255.255.0 tcp 8443
 portal free-rule 8 source ip any destination ip 10.10.13.0 mask 255.255.255.0 tcp 8909
 portal free-rule 9 source ip any destination ip 10.10.54.0 mask 255.255.255.0
 portal free-rule 10 source ip any destination ip 10.10.12.2 mask 255.255.255.255
 portal free-rule 11 source ip any destination ip 10.10.12.11 mask 255.255.255.255
 portal free-rule 12 source ip any destination ip 10.10.12.11 mask 255.255.255.255 udp 53
 portal free-rule 13 source ip any destination ip 10.10.13.0 mask 255.255.255.255
 portal free-rule 14 source ip any destination ip 10.10.13.188 mask 255.255.255.255 tcp 80
 portal free-rule 20 source interface Bridge-Aggregation1 destination any
#
 ip http acl 199
#
 mac-authentication user-name-format mac-address with-hyphen
#
 oap management-ip 192.168.0.101 slot 0
#
 wlan country-code IL
#
 wlan auto-ap enable
#
 password-recovery enable
#
acl number 199
 rule 65534 deny
#
acl number 2000
 rule 0 permit
#
acl number 3000
 rule 0 permit ip destination 10.10.13.0 0.0.0.255
 rule 5 permit tcp destination 10.10.13.0 0.0.0.255
 rule 10 deny ip
acl number 3001
 rule 0 permit ip
#
vlan 1
#
vlan 13 to 14
#
vlan 54 to 55
#
vlan 111 to 112
```

```
#
radius scheme golan_49
 primary authentication 10.56.14.49 key cipher $c$3$Jewz/7z+HN++Wgm062NM+4FQJ3MmICE=
 key authentication cipher $c$3$IAh67E5MJfnVFVf3Vch1KpTTsqL9rs4=
 user-name-format without-domain
radius scheme ise-vm-4
 server-type extended
 primary authentication 10.10.13.188 key cipher $c$3$yxd5fD1+GCFVP+enPjnkJcjpKb5D21s=
 primary accounting 10.10.13.188 key cipher $c$3$mNOXEKmMoi7MQz7vxW6gFyzs+a0Yv9Q=
 secondary authentication 10.10.13.185 key cipher $c$3$nlGNndqEDDFJ6PmEvcAGJxAsCjnVfew=
 key authentication cipher $c$3$SpU9Vk2qRnw5GPAO2T6nGGwt6hRUhTw=
 key accounting cipher $c$3$osheV0g/3GRkOSrJsaNElmvPlxYOPd0=
 user-name-format without-domain
 nas-ip 10.10.54.249
 accounting-on enable
radius scheme ise-vm-2
 server-type extended
 primary authentication 10.10.13.186 key cipher $c$3$kw6Vyevj4Wq9+EaqHUW3/4rL7WiUlfg=
 primary accounting 10.10.13.186 key cipher $c$3$7VxLB1upDCl+6aXeE1eygtXkGyRnj5M=
 key authentication cipher $c$3$3bMsiEToKU6t72FhtvoeCfxPB/yqN+0=
 key accounting cipher $c$3$FiqhBVak5HjreN5boi0PZSxGiaH6wF4=
 user-name-format without-domain
 nas-ip 10.10.54.249
 accounting-on enable
#
domain cu
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain guests
 authentication lan-access none
 authorization lan-access none
 accounting lan-access none
 authentication portal local
 authorization portal none
 accounting portal none
 access-limit disable
 state active
 idle-cut enable 480 10240
 self-service-url disable
domain ise-vm-2
 authentication lan-access radius-scheme ise-vm-2
 authorization lan-access radius-scheme ise-vm-2
```

```
 accounting lan-access radius-scheme ise-vm-2
 authentication portal radius-scheme ise-vm-2
 authorization portal radius-scheme ise-vm-2
 accounting portal radius-scheme ise-vm-2
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain ise-vm-4
 authentication lan-access radius-scheme ise-vm-4
 authorization lan-access radius-scheme ise-vm-4
 accounting lan-access radius-scheme ise-vm-4
 authentication portal radius-scheme ise-vm-4
 authorization portal radius-scheme ise-vm-4
 accounting portal radius-scheme ise-vm-4
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 accounting optional
domain test
 authentication default radius-scheme ise-vm-4
 authorization default radius-scheme ise-vm-4
 accounting default radius-scheme ise-vm-4
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 accounting optional
#
dhcp server ip-pool ap_1
 static-bind ip-address 10.10.54.240 mask 255.255.255.0
 static-bind mac-address 4431-92f6-fbc0
 gateway-list 10.10.54.253
#
dhcp server ip-pool clients extended
 network ip range 10.10.112.40 10.10.112.50
 network mask 255.255.255.0
 gateway-list 10.10.54.253
```

```
 dns-list 10.10.12.11
#
user-group system
 group-attribute allow-guest
user-group employee
 authorization-attribute acl 2000
user-group authenticated
 authorization-attribute acl 2000
#
local-user admin
 password cipher $c$3$5m3rnNpP9UM9nP9CKihiTNnubYBNQlFZ
 authorization-attribute level 3
 service-type ssh telnet
 service-type web
local-user guest
 password cipher $c$3$kQXQM3nr6oCjMxPUop0U5ZW7xr08
 authorization-attribute user-role guest
 service-type portal
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan hotspot-policy 1
 policy-name hotspot_hp
 authentication-type 2 redirect-url https://10.56.14.188:8443
#
wlan service-template 1 clear
 ssid HP-Guest
 bind WLAN-ESS 0
 service-template enable
#
wlan service-template 2 clear
 ssid HP-Open
 bind WLAN-ESS 1
 service-template enable
#
wlan service-template 3 crypto
 ssid HP-Dot1x
 bind WLAN-ESS 2
```

```
 cipher-suite ccmp
 security-ie rsn
 security-ie wpa
 service-template enable
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 54
 dhcp-snooping trust
#
interface NULL0
#
interface Vlan-interface1
 shutdown
 ip address 192.168.1.1 255.255.255.0
 undo dhcp select server global-pool
#
interface Vlan-interface14
 ip address 10.56.14.63 255.255.255.0
#
interface Vlan-interface54
 ip address 10.10.54.249 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
 dhcp relay information enable
 portal server guest-cwa method direct
#
interface Vlan-interface112
 ip address 10.10.112.238 255.255.255.0
 dhcp server apply ip-pool clients
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 54
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 54
 port link-aggregation group 1
#
```

```
interface WLAN-ESS0
 port link-type hybrid
 port hybrid vlan 1 54 untagged
 port hybrid pvid vlan 54
 port-security port-mode mac-authentication
 mac-authentication domain ise-vm-4
#
interface WLAN-ESS1
 port link-type hybrid
 port hybrid vlan 1 54 112 untagged
 port hybrid pvid vlan 54
 mac-vlan enable
 port-security port-mode mac-authentication
 mac-authentication domain ise-vm-4
#
interface WLAN-ESS2
 port link-type hybrid
 port hybrid vlan 1 54 untagged
 port hybrid pvid vlan 54
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain ise-vm-4
 undo dot1x multicast-trigger
#
interface WLAN-ESS3
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 55 untagged
 port hybrid pvid vlan 55
 mac-vlan enable
 port-security port-mode mac-authentication
 mac-authentication domain ise-vm-4
#
interface WLAN-ESS4
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 54 to 55 untagged
 port hybrid pvid vlan 54
 mac-vlan enable
 port-security port-mode mac-authentication
 mac-authentication trigger after-portal
 mac-authentication guest-vlan 55
 mac-authentication domain guests
```

```
#
wlan ap-group default_group
 country-code IL
 dot11a service-template 1
 dot11a service-template 2
 dot11a service-template 3
 dot11bg service-template 1
 dot11bg service-template 2
 dot11bg service-template 3
 dot11a radio enable
 dot11bg radio enable
#
wlan ips
 malformed-detect-policy default
 signature deauth_flood signature-id 1
 signature broadcast_deauth_flood signature-id 2
 signature disassoc_flood signature-id 3
 signature broadcast_disassoc_flood signature-id 4
 signature eapol_logoff_flood signature-id 5
 signature eap_success_flood signature-id 6
 signature eap_failure_flood signature-id 7
 signature pspoll_flood signature-id 8
 signature cts_flood signature-id 9
 signature rts_flood signature-id 10
 signature addba_req_flood signature-id 11
 signature-policy default
 countermeasure-policy default
 attack-detect-policy default
 virtual-security-domain default
  attack-detect-policy default
  malformed-detect-policy default
  signature-policy default
  countermeasure-policy default
#
 dhcp-snooping
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.54.253
#
 info-center source DHCP channel 0
 info-center logbuffer channel 0
 info-center synchronous
 info-center monitor channel 0
#
 dhcp server detect
```

```
#
 dhcp enable
#
 ssh server enable
#
 ip https acl 199
 ip https enable
#
user-interface con 0
user-interface vty 0 4
 acl 199 inbound
 authentication-mode scheme
 user privilege level 3
#
return
<HP>
```