

Instant 3.3: BYOD and Captive portal Enhancements

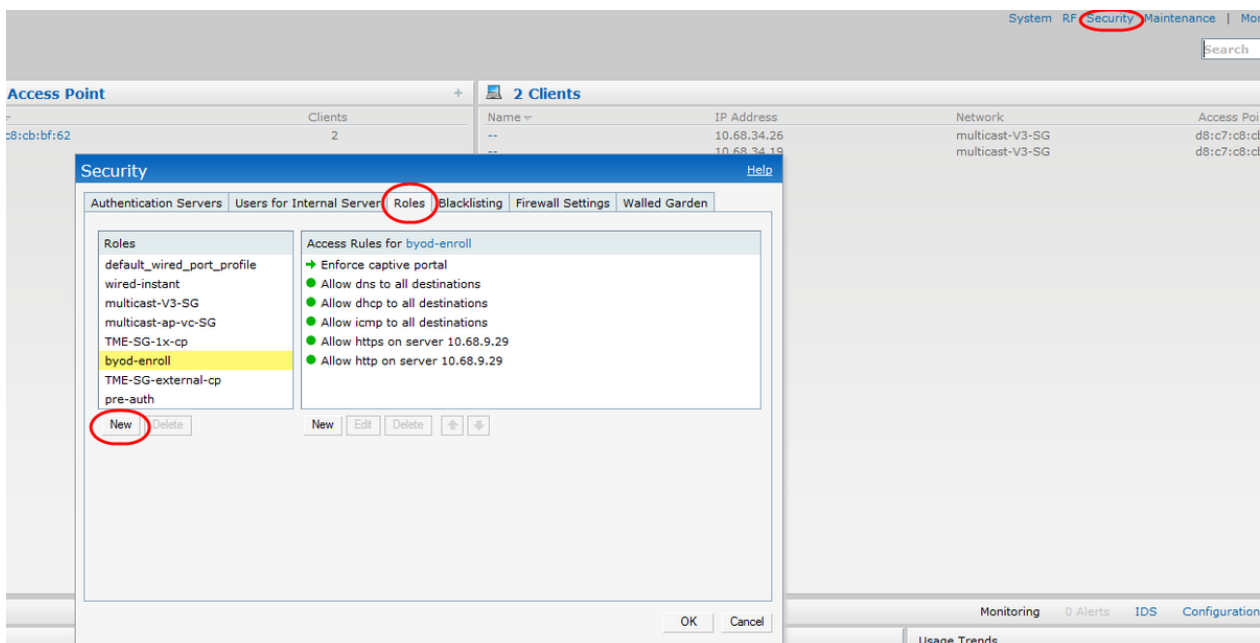
BYOD on a Single SSID

Instant OS 3.2 and earlier did not provide the ability to redirect a client to a captive portal page post 802.1X authentication. This limitation required the use of 2 SSIDs: 1) provisioning SSID 2) approved device SSID (802.1X) to provide a complete BYOD solution. In Instant OS 3.3, Aruba introduced the ability to redirect a client to a captive portal page after 802.1X authentication. This new enhancement provides the ability to append a captive portal redirection to a user role. This enhancement coupled with the ability to define a user role based on the EAP authentication type allows the use of a single SSID for a complete BYOD solution. The steps involved in configuring a single SSID for BYOD are these:

1. Create a user role with captive ported redirection
2. Create an employee SSID with WPA2_Enterprise authentication
3. In the employee SSID configuration create a derivation rule that assigns the captive portal user role based on 802.1X authentication type (Ex: EAP-PEAP MSCHAPv2)
4. Optionally, configure ClearPass to return non-captive user role for users authenticating using EAP-TLS . By default, a user authenticating with an EAP-method other than the one in Step 3 is assigned the default-role for the SSID.

STEP 1: Create a user role with captive portal redirection

- Create a new role: byod-enroll



- Create a captive portal access rule

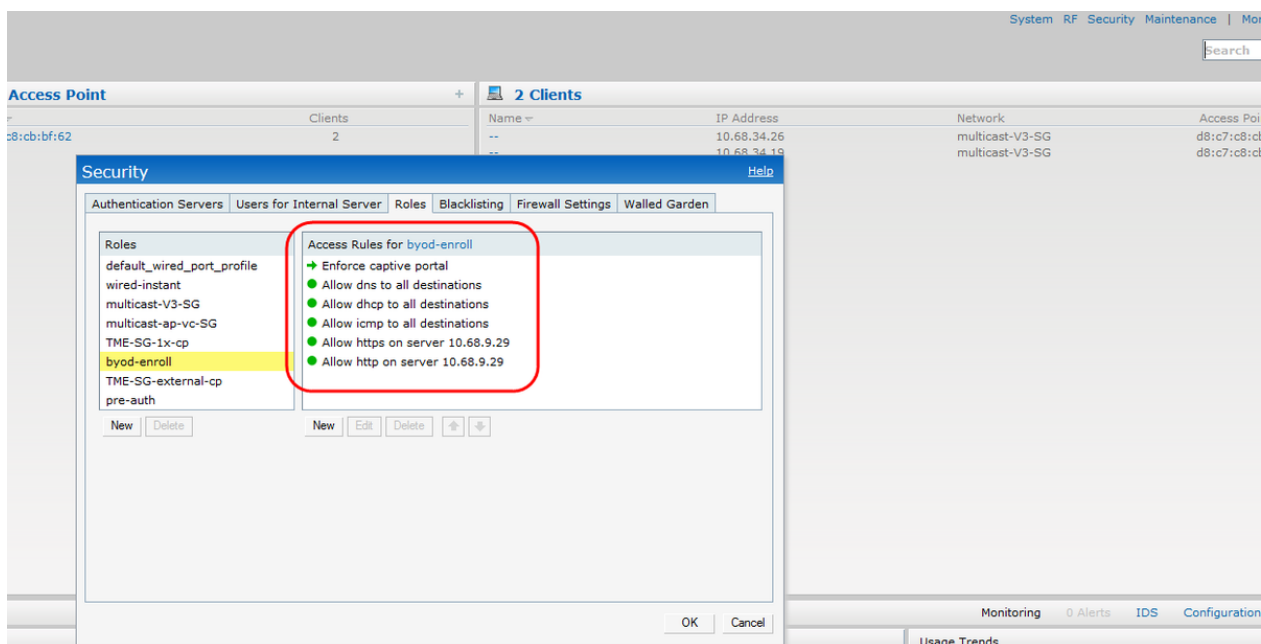
The first screenshot shows the 'Security' configuration window with the 'New Rule' dialog box open. The 'Rule type' dropdown menu is expanded, showing 'Access control', 'Access control', 'VLAN assignment', and 'Captive portal'. The 'Captive portal' option is selected and highlighted with a red circle. The 'Action' is set to 'Allow', 'Service' is 'any', and 'Destination' is 'to all destinations'. The 'Options' section includes checkboxes for 'Log', 'Blacklist', 'Classify media', 'Disable scanning', 'DSCP tag', and '802.1p priority'. The 'OK' and 'Cancel' buttons are at the bottom right.

The second screenshot shows the 'New Rule' dialog box with 'Captive portal' selected in the 'Rule type' dropdown. The 'Splash page type' dropdown is expanded, showing 'External', 'Internal', and 'External'. The 'External splash page' section is highlighted with a red circle and contains the following fields:

- IP or hostname: 10.68.9.29
- URL: /iap_test.php
- Port: 80
- Captive Portal failure: Deny internet
- Automatic URL Whitelisting: Enabled
- Auth text: (empty field)
- Redirect URL: (empty field) (Optional)

The 'OK' and 'Cancel' buttons are at the bottom right.

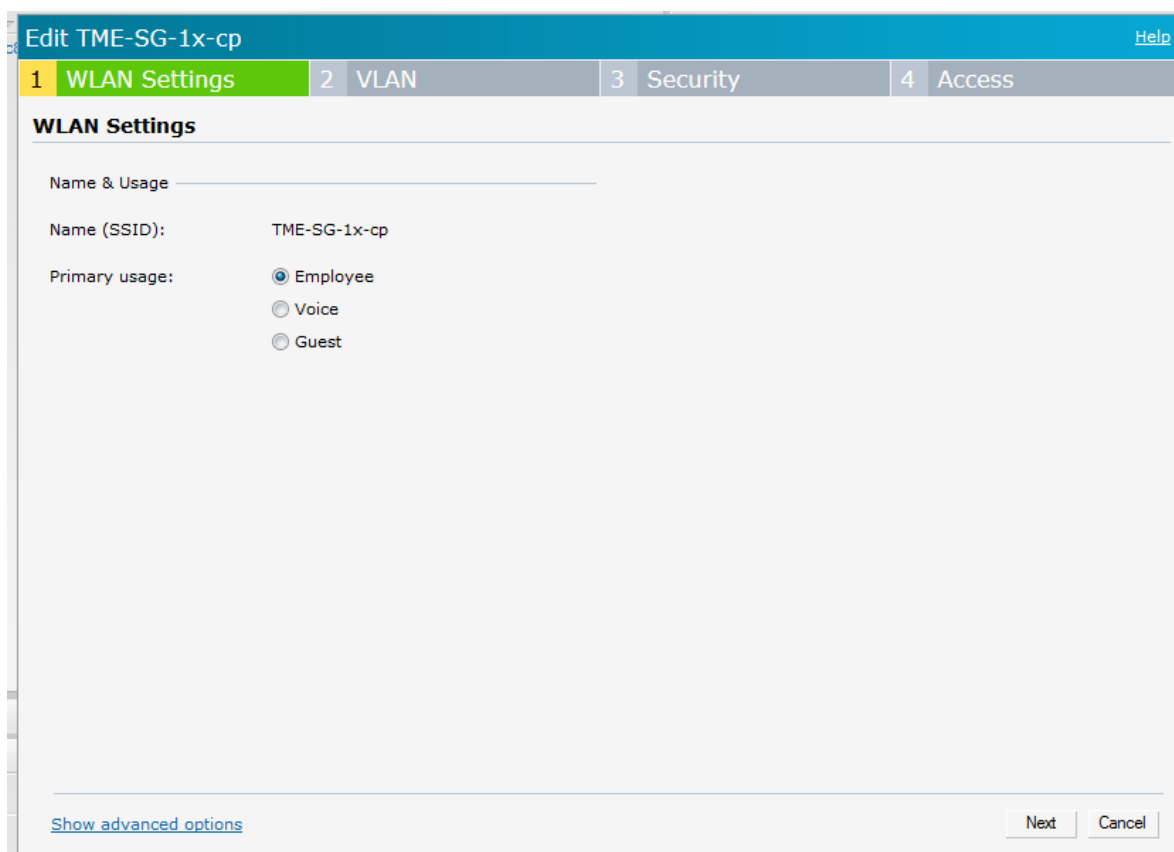
- Allow DNS, DHCP to all destinations and HTTP/HTTPS access to ClearPass server.



Note: Ensure that the appropriate servers and URLs are whitelisted. See *Amigopod ClearPass Guest Whitelist Reference* for details.

STEP 2: Create an Employee SSID

- Configure SSID name and VLAN



Edit TME-SG-1x-cp [Help](#)

1 WLAN Settings 2 VLAN 3 Security 4 Access

Client IP & VLAN Assignment

Client IP assignment: ☐ Virtual Controller assigned
☒ Network assigned

Client VLAN assignment: ☐ Default
☒ Static
☐ Dynamic

VLAN ID:

Back Next Cancel

- Configure WPA2-Enterprise security on the SSID

Edit TME-SG-1x-cp [Help](#)

1 WLAN Settings 2 VLAN 3 Security 4 Access

Security Level

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: clearpass Edit

Authentication server 2: -- Select Server --

Reauth interval: hrs.

Authentication survivability: Disabled

MAC authentication: ☒ Perform MAC authentication before 802.1X
☐ MAC authentication fail-thru

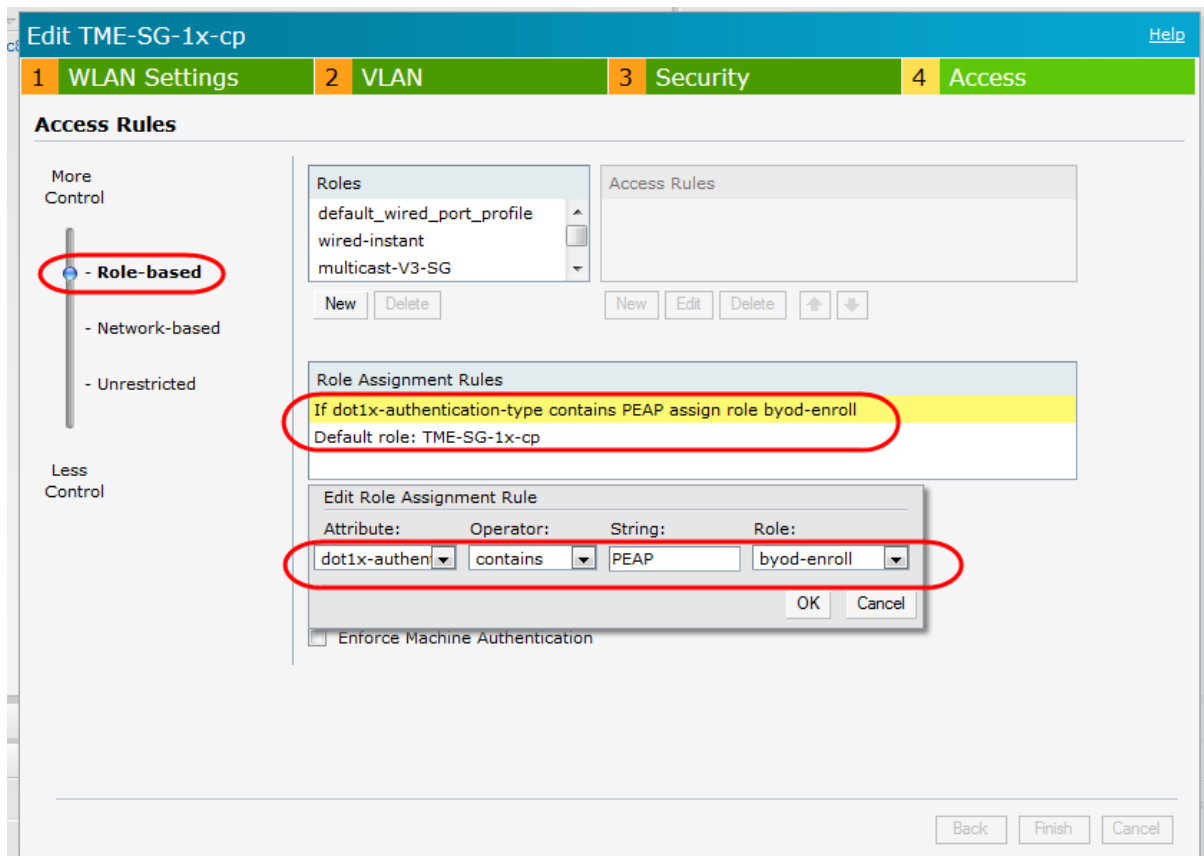
Accounting: Disabled

Blacklisting: Disabled

Back Next Cancel

STEP 3: Configure the access settings of the SSID with appropriate 802.1X authentication type based derivation rule

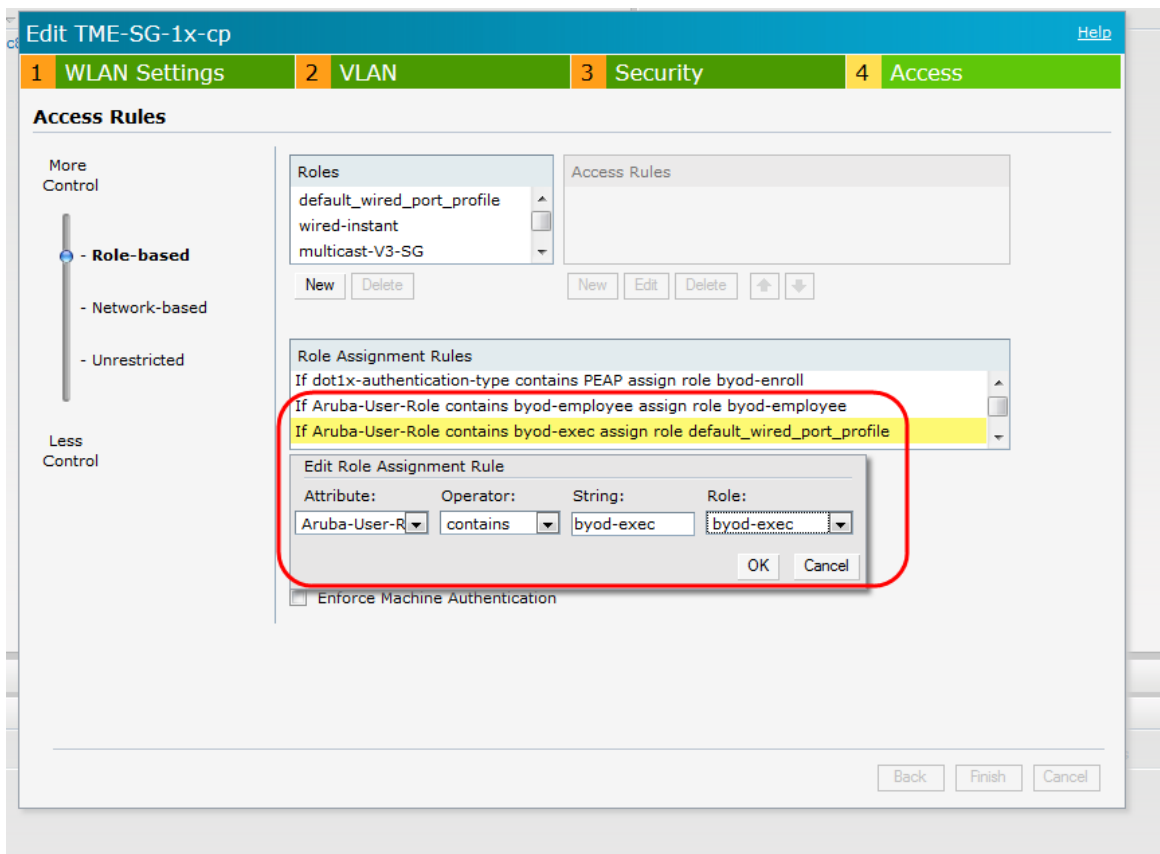
- Configure a derivation rule based on the EAP-type. If the user authenticates with PEAP-MACHAPv2 assign the byod-enroll. This will redirect the users to provisioning page.



- User authenticates with EAP types other the PEAP-MSCHAPv2 will be assigned the default role for the SSID. The provisioning process on ClearPass will install certificates and configure the client's wireless supplicant for EAP-TLS.
- When the client reconnects to the SSID during the final step of the provisioning process it uses EAP-TLS. This will assign the default SSID role to the client.

STEP 4: If required configure IAP for server derived rules

- Using the Aruba-User-Role VSA, ClearPass can push user roles to IAP. The accomplish this, the IAP should be configured with the appropriate user role definition ad server derived rule.



Article Sources and Contributors

Instant 3.3: BYOD and Captive portal Enhancements *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?oldid=44409> *Contributors:* Sathyang, Tbrophy

Image Sources, Licenses and Contributors

Image:New-role.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:New-role.png> *License:* unknown *Contributors:* Sathyang

Image:Cp-rule-1.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:Cp-rule-1.png> *License:* unknown *Contributors:* Sathyang

Image:Cp-rule-2.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:Cp-rule-2.png> *License:* unknown *Contributors:* Sathyang

Image:3.3-byod-role.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:3.3-byod-role.png> *License:* unknown *Contributors:* Sathyang

Image:New-SSID.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:New-SSID.png> *License:* unknown *Contributors:* Sathyang

Image:Vlan-config.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:Vlan-config.png> *License:* unknown *Contributors:* Sathyang

Image:Wpa2-ent.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:Wpa2-ent.png> *License:* unknown *Contributors:* Sathyang

Image:Ssid-access.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:Ssid-access.png> *License:* unknown *Contributors:* Sathyang

Image:3.3-cp-server-derived.png *Source:* <http://arubapedia.arubanetworks.com/arubapedia/index.php?title=File:3.3-cp-server-derived.png> *License:* unknown *Contributors:* Sathyang