DEPLOYMENT BRIEF

SETUP IDM FOR CAPTIVE PORTAL

Meru Identity Manager is a Guest provisioning and management system that provides various levels of network access addressing BYOD challenges. Identity Manager works alongside any wireless controllers, LAN switches, firewalls or other network enforcement devices to provide secure network access. This Quick Deployment Guide explains basic configuration steps that are required for Identity Manager to integrate with Meru WLAN controllers.

IDENTITY MANAGER CONFIGURATION

The basic IDM configuration for captive portal involves the following steps that must be first completed in IDM and then in the System Director WebUI interface

IDM Configuration (*Complete these steps first before proceeding with System Director configuration***)**	**System Director Configuration (WebUI)**
1. Setup IDM and Add License 2. Create Sponsors 3. Add Guest Users 4. Add Meru WLAN controllers as RADIUS clients	1. Creating QoS rules 2. Creating RADIUS auth/accounting profiles 3. Captive Portal configuration settings 4. Creating Security Profile with Web auth enabled 5. Creating ESS with the security profile mapped to it

1. SETUP IDM AND ADD LICENSE

1. 1. Login to the console interface of IDM

1. 2. For username, enter **`root`**, and the system will prompt to configure a new password.

1. 3. After you have logged in, Select option 2 to configure the IP Address, Subnet Mask, Gateway, and DNS settings

1. 4. Restart the network service.

1. 5. Open a browser and provide the IP Address (from step 1.3) in https://192.168.10.10/admin format to access the IDM admin interface

1. 6. You will now see the system-ID. Use the System-ID to get license from Meru Support.

1. 7. After you get the license, upload it and login to IDM using the default credentials **`admin`** / **`admin`**.

1. 8. The initial login page will display the **Setup Wizard** allowing changes to the following parameters

   1. 8. a. Admin user password

   1. 8. b. Hostname / domain name / DNS

   1. 8. c. Date and time settings

   1. 8. d. Sponsor Authentication Options

   1. 8. e. Guest authentication options

Make required changes to steps 1.8.a, 1.8.b, 1.8.c. Steps 1.8.d and 1.8.e can be configured later.

ⓘ **IMPORTANT**	This document assumes that the initial installation is complete and the system console access is ready to start with configuration for the network placement.

2. CREATE SPONSORS

2. 1. From the IDM admin interface (*http://<idm-ip-address>/admin, see Step 1.5*) navigate to **Sponsor Portal** > **Internal Sponsor** > **Authentication**

2. 2. Select **Internal Sponsors** and click **Add User**

2. 3. Fill in the fields as appropriate and click **Save**.

Supported Hardware and SD Version

- Any Meru controller models
- Any IDM appliance models
- Tunnelled - Any Meru Access points
- Bridged - AP110, AP10xx, AP332, AP832, AP400
- System Director Version - 6.1 and above. **

(** Pre 6.0 integration procedures are not covered in this document)

PRE-REQUISITES

- Enable TCP 22 and 443 Identity Manager management access to Meru Controller
- Enable UDP 1812 and 1813 for RADIUS protocol between Meru Identity Manager and
- Enable UDP 3799 for RADIUS Change of Authorization (COA), used for user logout

3. ADD GUEST USERS

3. 1. Access the IDM sponsor interface, http://<idm-ip-address>/sponsor. (*Example: https:192.168.10.10/sponsor*)

3. 2. Enter username and password created in **Step 2.2** to login.

3. 3. Navigate to **Create Accounts** > **Create Guest Account**.

3. 4. Fill in the guest details in appropriate fields and click the **Add User** button.

3. 5. By default, the email address is the guest username and IDM will generate a random password.

4. ADDING MERU WLAN CONTROLLERS AS RADIUS CLIENTS

4. 1. From the IDM admin interface navigate to **Devices** > **Radius** clients and enter the name of the controller, IP-address, Secret and select Type as Meru SD 6.0 & Later. Provide the required description and enable the **Use CoA** check box

4. 2. Click **Save** to continue.

4. 3. Select the Automatic setup tab and fill in the hostname or IP-addresses for Identity Manager, Controller, and enter admin username & password

4. 4. Enable all the check boxes and click **Setup controller** button

SYSTEM DIRECTOR CONFIGURATION

Follow steps in this section after you have completed all of IDM configuration steps outline in sections 1 through 4.

ⓘ IMPORTANT	If "setup controller" is run from the IDM, manual configuration of step 5 to 8 is not required in controller.

When Captive portal is enabled, the pre-authentication traffic from clients is restricted by controller to allow only DNS and DHCP. The Firewall rules will help forward traffic to Identity Manager before authentication during the Captive Portal redirection. In the System Director WebUI, navigate to **Configuration** > **QoS Settings** > **QoS and Firewall Rules** and create the following rules.

5. QOS RULE #1

Create a rule by entering the following details

5. 1. **Destination IP**- IP-address of the Identity Manager

5. 2. **Destination Net Mask –** Subnet mask which of the Identity Manager IP –address

5. 3. **Destination Port** --443

5. 4. **Network Protocol** -6

5. 5. **Firewall Filter ID** - <any string>. (By default Identity manager configures a string named "***IDMPREAUTH***")

5. 6. Set **Action** as forward.

Make sure the *Match* check box is enabled against all above fields. The **Rule ID** should be unique and all the other fields are optional.

6. QOS RULE #2

6. 1. **Source IP**- IP-address of the Identity Manager

6. 2. **Source Net Mask –** Subnet mask which of the Identity Manager IP –address

6. 3. **Source Port** --443

6. 4. **Network Protocol** -6

6. 5. **Firewall Filter ID** - <any string>. (By default Identity manager configures a string named "***IDMPREAUTH***")

6. 6. Set **Action** as forward.

Make sure the *Match* check box is enabled against all above fields. The **Rule ID** should be unique and all the other fields are optional. Both rules should have the same ***Firewall Filter ID*** string.

ⓘ NOTE	**IDMPREAUTH** is Firewall Filter ID that is automatically generated if controller was set up with RADIUS profiles via the Automatic Setup tab in **IDM** > **Devices** > **RADIUS Clients** > **Automatic Setup**.

7. CREATE RADIUS PROFILES FOR AUTHENTICATION AND ACCOUNTING

You can choose the create RADIUS profiles manually or use the options in Automatic Setup tab (IDM > Device > RADIUS Clients > Automatic Setup). This following are manual steps to create RADIUS profiles. In the System Director WebUI, navigate to **Configuration** > **Security** > **RADIUS** and do the following:

7. 1. Rule for authentication.

7. 1. a. Give a name and description for the RADIUS profile.

7. 1. b. Fill in the RADIUS server IP field. This is the Identity Manager IP Address

7. 1. c. Enter the RADIUS secret. The secret key should be matching the Identity Manager configuration.

7. 1. d. Fill in the RADIUS port, 1812 or 1645. (1812 is default)

Leave all the other fields as default.

7. 2. Rule for accounting.

7. 2. a. Give a name and enter description for the RADIUS profile.

7. 2. b. Fill in the RADIUS server IP field. This is the Identity Manager IP Address

7. 2. c. Enter the RADIUS secret. The secret key should match the Identity Manager configuration.

7. 2. d. Fill in the RADIUS port, 1813 or 1646.

Leave all the other fields as default.

8. CAPTIVE PORTAL SETTINGS

From the Configuration tab in the WebUI, navigate to **Security** > **Captive Portal** to make the following changes.

8. 1. Under **Internal Portal Settings**, Under User Authentication, Set Authentication Type to **RADIUS**.

8. 2. Select the primary profile (*see section 7.1.b*) under RADIUS Authentication.

8. 3. Select the primary profile (*see section 7.2.b*) under RADIUS Accounting.

8. 4. Under External Portal Settings, Configure the External Portal URL in the following format, https://<IDM-IP-Addr>/portal/<Controller-IP-Addr>?meruInitialRedirect.

8. 5. If the controller is behind NAT, enter the public IP-address of controller in the External Portal IP field.

Leave all other fields with default settings.

9. CREATE A SECURITY PROFILE WITH CAPTIVE PORTAL

From Configuration navigate to security and profile. Click on Add button.

9. 1. Provide a name for the Security Profile

9. 2. In the L2 Modes Allowed, select **Clear**.

9. 3. Select **Web Auth** in Captive Portal field

9. 4. Select **External** option in the Captive Portal Authentication Method.

9. 5. Enter the Firewall Filter ID string that was created in step 5.5 in the Pass-through Firewall Filter ID field.

10. CREATE AN ESS PROFILE AND MAP THE CAPTIVE PORTAL ENABLED SECURITY PROFILE

From the configuration tab navigate to Wireless – ESS and click on Add.

10. 1. Give a name for ESS profile and SSID

10. 2. Click the drop down against the Security Profile tab and select the Security profile created on step 4.

Leave all other fields as default.

TEST AND VERIFY

1. Connect a wireless client to the ESS profile created in step 10 under controller configuration
2. Once connected successfully, open a browser and type any public URL (Example, www.merunetworks.com) and see if it's redirected to IDM portal.
3. Provide the guest username and password created in Step 3 and see if the user is successfully authenticating.

SUPPORT

Visit the Meru Support Portal (***http://support.merunetworks.com***) for any additional information or support.

For more information about Meru Networks, visit www.merunetworks.com or email your questions to:
meruinfo@merunetworks.com

Meru Networks
894 Ross Drive, Sunnyvale, CA 94089
T +1.408.215.5300
F +1.408.215.5301
E meruinfo@merunetworks.com