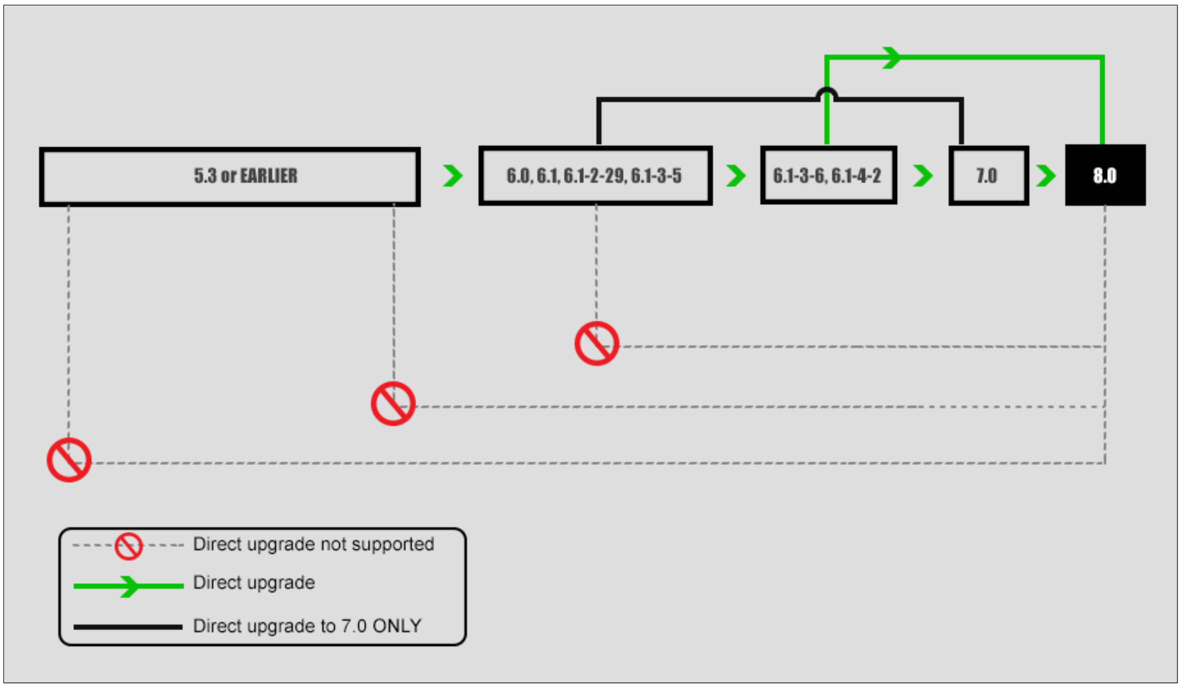
System Director

8.0-5-0
Release Notes

System Director 8.0-5-0 is released for general availability. This release introduces several new features and fixes to improve user experience and overall system performance.

Upgrade Path to 8.0



Before you Begin

The following mandatory steps must be performed before starting an upgrade. Upgrading a controller requires a serial or SSH2 connection for using the controller's CLI.

Free Space Requirements

Total free space required is the size of the image + 50MB (approximately 230 MB).

Serial Connection Settings

Ensure that your serial connection is set for the following options:

WARNING Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits

- Parity--None
- Stop Bit—1
- Flow Control—None

Upgrading Controllers to 8.0

1. Download controller image files from an FTP or TFTP server to the controller using one of the following commands:

```
# copy ftp://ftpuser:password@ext-ip-addr/meru-<release-version>-MC_MODEL-rpm.tar<space>. or
# copy tftp://ext-ip-addr/meru-<release-version>-MC_MODEL-rpm.tar<space>.
```

2. Disable AP auto upgrade and then upgrade the controller

```
# configure terminal
# auto-ap-upgrade disable
# upgrade controller <target version> (Example, upgrade controller 6.1-2-29)
```

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the `show controller` and `show ap` command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the `show running-config` command (if not, recover from the remote location). See the Backup Running Configuration step.

Upgrading New 802.11AC APs

New out of the box 802.11 ac access points require the following steps to upgrade and associate them to a controller running the latest SD 8.0 version. The following AP upgrade procedures lists two scenarios, when auto-ap-upgrade is ***ON*** and when auto-ap-upgrade is ***OFF***.

Upgrading if auto-ap-upgrade is ON

1. Copy the patch file to the controller via CLI (ftp/scp/tftp) or the WebUI

```
copy ftp://<user>:<password>@<Server-IP>/<path>/<Patch-File> .
```

2. Ensure the patch is copied using the show patch command

```
#show patch
8.0-5-0 patch
```

3. Install the copied patch using the `patch install <patch filename>`

```
#patch install 8.0-5-0 patch
```

4. Now, associate the new 802.11ac AP's to this controller. The new AP's will be upgraded to an intermediate patch (6.1-4-2 build) and subsequently to the SD8.0 build.

Upgrading if auto-ap-upgrade is OFF

1. Copy the patch image to controller via CLI (ftp/scp/tftp) or WebUI

```
copy ftp://<user>:<password>@<Server-IP>/<path>/<Patch-File> .
```

2. Ensure the patch image is properly copied using the 'show patch' command

```
#show patch

8.0-5-0 patch
```

3. Install the patch image `patch install <patch filename>`
4. Now, associate the 802.11ac AP's to controller.
   a) To upgrade single AP, Use the `upgrade ap 7istep < apID > force` command.
   b) To upgrade using the AP ID, use the `upgrade ap 7istep <apID> force` command
   c) To upgrade batch of APs, use the `upgrade ap 7istep <start-apID>-<end-apID> force` command
   d) To upgrade a APs in a specific range of AP ID (for example, AP ID 1 to AP ID 50), use the `upgrade ap 7istep 1-50 force` command.

Upgrading a Site Running N+1

To upgrade a site running N+1, all controllers must be on the same System Director version and the backup controller must be in the same subnet as the primary controllers. You can choose any of the following options to upgrade:

Option 1 - Just like you would upgrade any controller, you can upgrade an N+1 controller.

1. Upgrade master and then upgrade slave.
2. After upgrade enable master on slave using the `nplus1 enable` command.

Option 2 - Upgrade slave and then upgrade master.

After upgrade, enable master service on slave using the `nplus1 enable` command.

Option 3 - If there are multiple master controllers

1. Upgrade all master controllers followed by slave. After upgrade, enable all master controllers on slave controllers using the `nplus1 enable` command.
2. To enable master controller on slave controller, use the `nplus1 enable` command.
3. Connect all controllers using SSH or a serial cable.

IMPORTANT This must be done on the slave controller first, followed by the master controllers.

4. Use the `show nplus1` command to verify if the slave and master controllers are in the cluster. The output should display the following information:
   - Admin: Enable
   - Switch: Yes
   - Reason: -
   - SW Version: 7.0-1SR-0
5. If the configuration does not display the above settings, use the `nplus1 enable <master-controller-ip>` command to complete the configuration.
6. To add any missing master controller to the cluster, use the `nplus1 add master` command.

Restore Saved Configuration

1. Copy the backup configuration back to the controller:

```
# copy ftp://user:pswd@offbox-ip-address/runningconfig.txt orig-config.txt
```

2. Copy the saved configuration file to the running configuration file:

```
# copy orig-config.txt running-config
```

3. Save the running configuration to the start-up configuration:

```
# copy running-config startup-config
```

Features in this Release ...

- Captive Portal Profiles
- End of Support for AP320
- Patch Management
- Application Visibility (DPI)
- VLAN Pooling
- Support for VLAN Tagging in Bridge Mode for Wired Ports
- Enhancements to WAN Survivability
- Support for 802.11k/r Specifications
- Time Based ESS
- Remote RADIUS Server
- Support for VLAN in MESH
- 802.11w Support
- Support for Bluetooth Devices
- Context Sensitive Help

Captive Portal Profiles

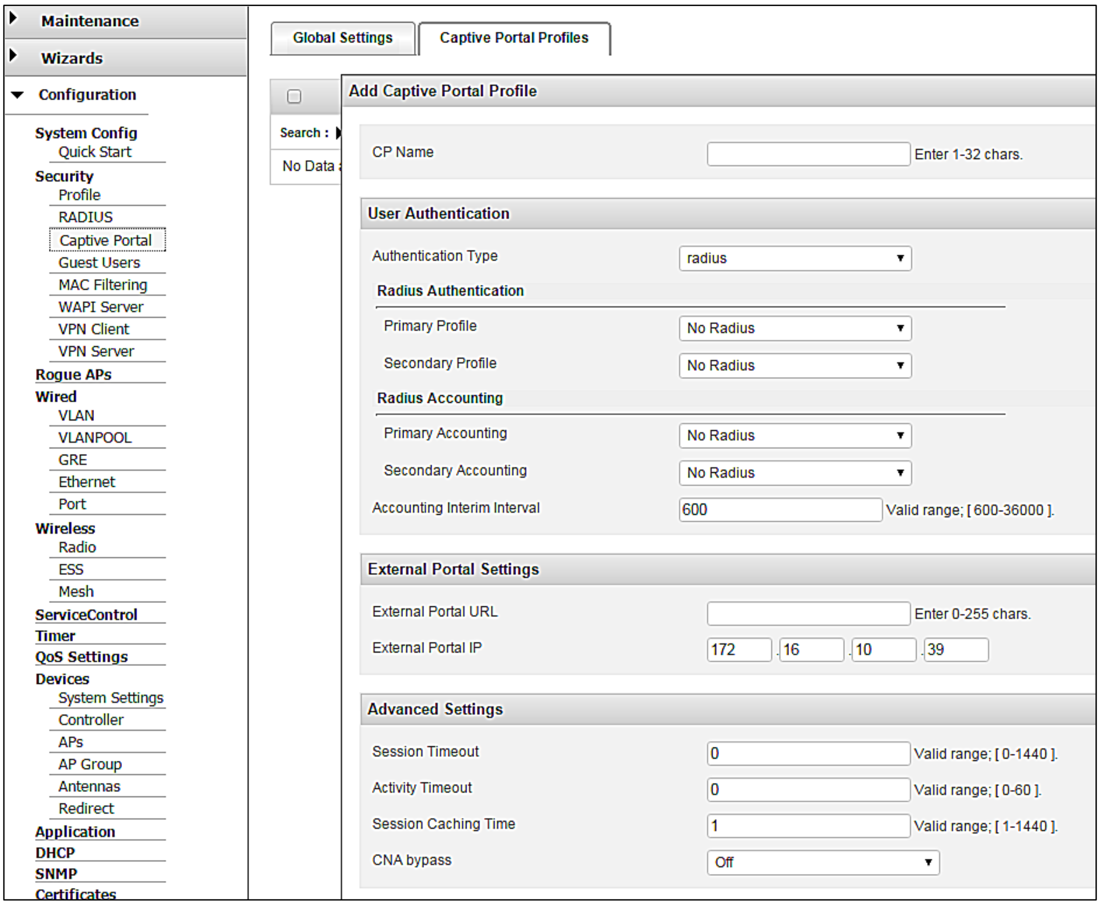
Until now, a captive portal setting was a single global configuration that was applied across multiple security profiles. This prevented fine control over captive portal user access.

System Director 8.0 introduces the captive portal profiles feature that allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access.

A captive portal profile is created from the **Configuration** > **Security** > ***Captive Portal*** page. With the introduction of this feature, a new tab, ***Captive Portal Profile*** is added to this page to specify the captive portal profile settings. Once created, this captive profile can be enabled in a security profile. The following screenshots illustrate the process.

NOTES	Maximum of 8 Captive profiles can be created.

Creating a Captive Portal Profile



Add Captive Portal Profile

CP Name: Enter 1-32 chars.

User Authentication

Authentication Type: radius ▾

Radius Authentication

Primary Profile: No Radius ▾

Secondary Profile: No Radius ▾

Radius Accounting

Primary Accounting: No Radius ▾

Secondary Accounting: No Radius ▾

Accounting Interim Interval: 600 Valid range; [600-36000].

External Portal Settings

External Portal URL: Enter 0-255 chars.

External Portal IP: 172 . 16 . 10 . 39

Advanced Settings

Session Timeout: 0 Valid range; [0-1440].

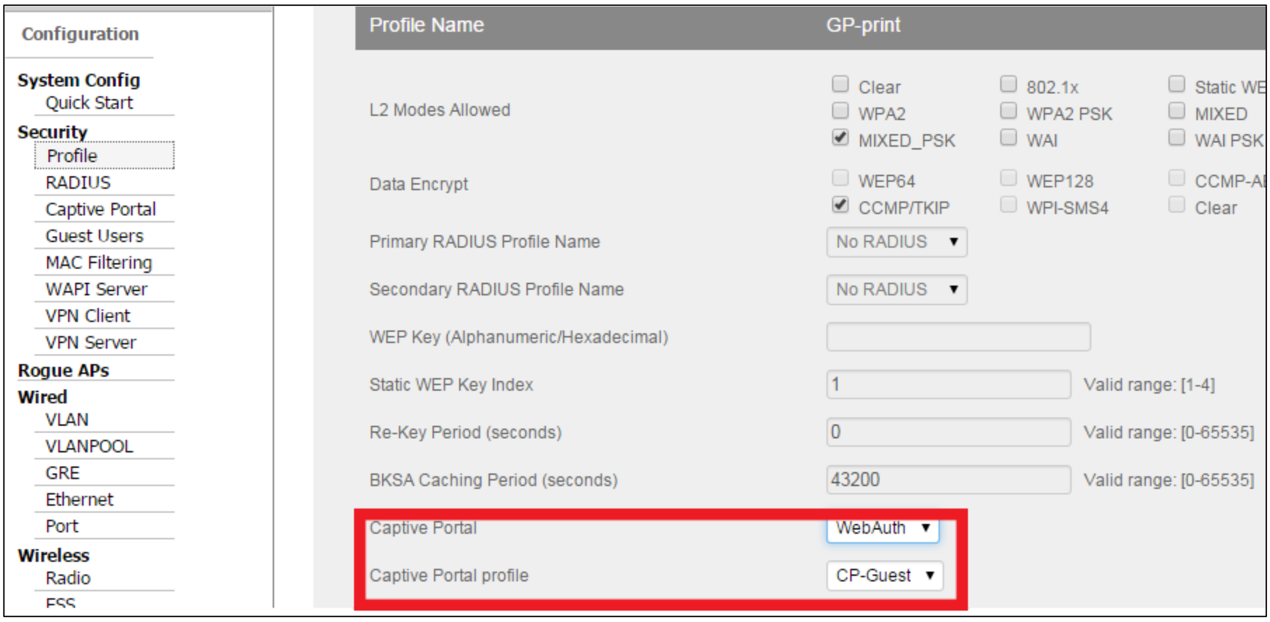
Activity Timeout: 0 Valid range; [0-60].

Session Caching Time: 1 Valid range; [1-1440].

CNA bypass: Off ▾

Assigning a Captive Portal Profile to a Security Profile

NOTE The Captive Portal Profile option is enabled only if at least captive portal profile is created.



Configuration

System Config
- Quick Start

Security
- Profile
- RADIUS
- Captive Portal
- Guest Users
- MAC Filtering
- WAPI Server
- VPN Client
- VPN Server

Rogue APs

Wired
- VLAN
- VLANPOOL
- GRE
- Ethernet
- Port

Wireless
- Radio
- ESS

Profile Name	GP-print		
L2 Modes Allowed	□ Clear □ WPA2 ☑ MIXED_PSK	□ 802.1x □ WPA2 PSK □ WAI	□ Static WE □ MIXED □ WAI PSK
Data Encrypt	□ WEP64 ☑ CCMP/TKIP	□ WEP128 □ WPI-SMS4	□ CCMP-AE □ Clear
Primary RADIUS Profile Name	No RADIUS ▼		
Secondary RADIUS Profile Name	No RADIUS ▼		
WEP Key (Alphanumeric/Hexadecimal)			
Static WEP Key Index	1	Valid range: [1-4]	
Re-Key Period (seconds)	0	Valid range: [0-65535]	
BKSA Caching Period (seconds)	43200	Valid range: [0-65535]	
Captive Portal	WebAuth ▼		
Captive Portal profile	CP-Guest ▼		

End of Support for AP3xx

Starting with the 8.0 release, The following AP's are not supported.

- AP300
- AP310
- AP311
- AP320
- AP301
- AP302
- AP301i
- AP310i
- AP302i
- AP320i

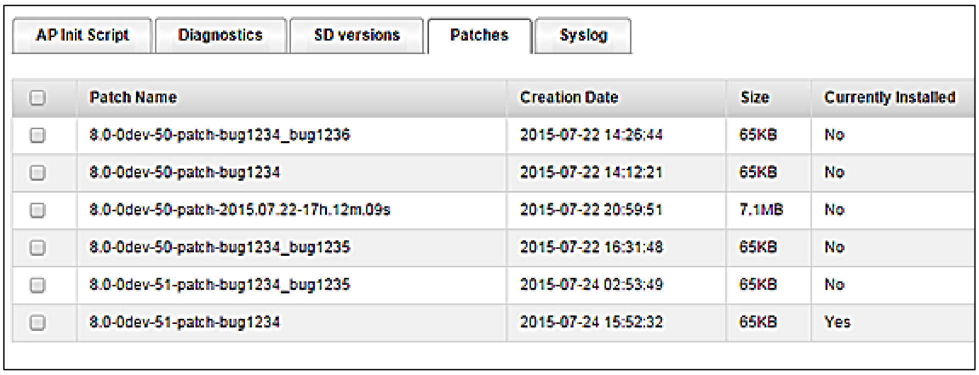
Patch Management

Patch management process in System Director 8.0 is significantly enhanced. In addition to providing options to install and uninstall patches, you can now easily view more details about the contents of a patch and also get history of patches installed in the controller. These new options are available via the controller WebUI and the CLI.

Using the WebUI

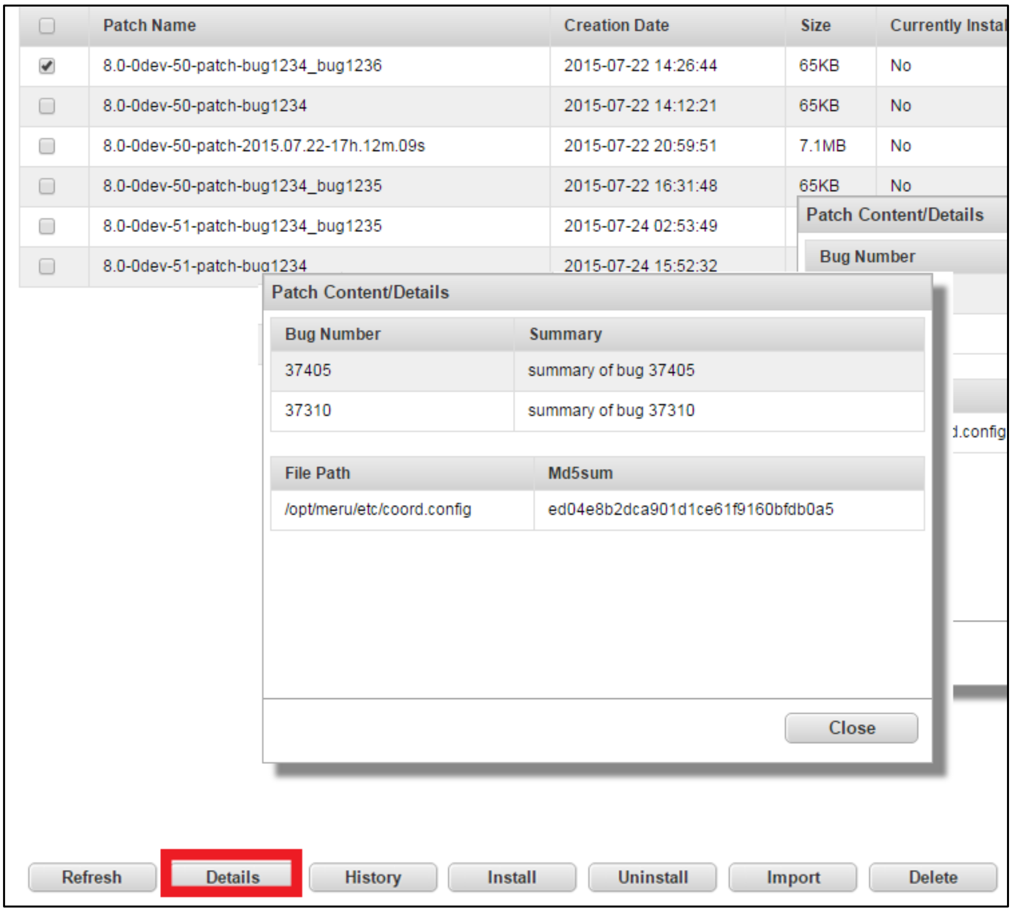
Patch management options are available via the **Maintenance** > **File Management** > **Patches** tab. If a patch build file is copied in the controller, they will be listed on this page. For specific options, select a patch file and click the option in the bottom of the page.

List of Patches



☐	Patch Name	Creation Date	Size	Currently Installed
☐	8.0-0dev-50-patch-bug1234_bug1236	2015-07-22 14:26:44	65KB	No
☐	8.0-0dev-50-patch-bug1234	2015-07-22 14:12:21	65KB	No
☐	8.0-0dev-50-patch-2015.07.22-17h.12m.09s	2015-07-22 20:59:51	7.1MB	No
☐	8.0-0dev-50-patch-bug1234_bug1235	2015-07-22 16:31:48	65KB	No
☐	8.0-0dev-51-patch-bug1234_bug1235	2015-07-24 02:53:49	65KB	No
☐	8.0-0dev-51-patch-bug1234	2015-07-24 15:52:32	65KB	Yes

Patch Details



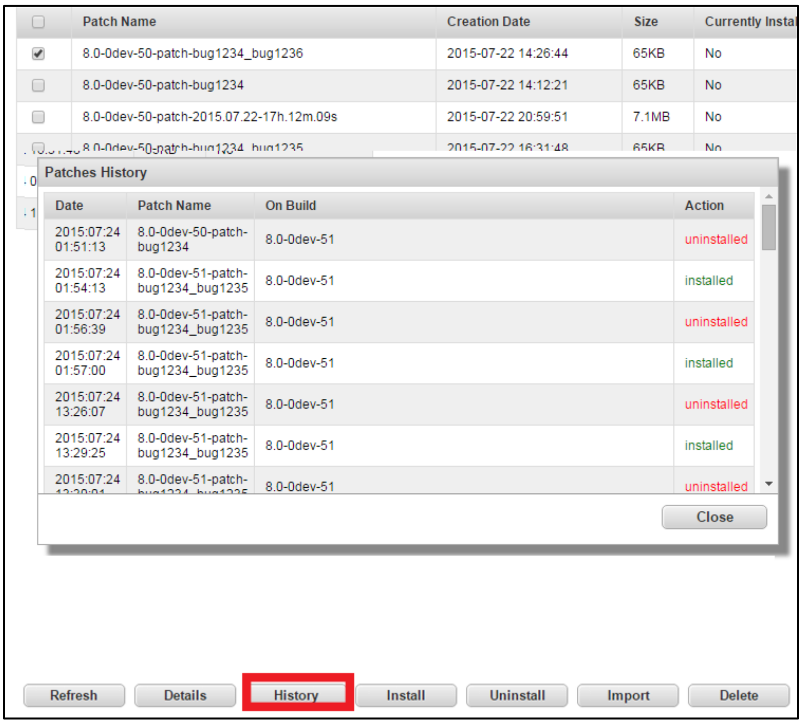
☐	Patch Name	Creation Date	Size	Currently Instal
☑	8.0-0dev-50-patch-bug1234_bug1236	2015-07-22 14:26:44	65KB	No
☐	8.0-0dev-50-patch-bug1234	2015-07-22 14:12:21	65KB	No
☐	8.0-0dev-50-patch-2015.07.22-17h.12m.09s	2015-07-22 20:59:51	7.1MB	No
☐	8.0-0dev-50-patch-bug1234_bug1235	2015-07-22 16:31:48	65KB	No
☐	8.0-0dev-51-patch-bug1234_bug1235	2015-07-24 02:53:49		
☐	8.0-0dev-51-patch-bug1234	2015-07-24 15:52:32		

Patch Content/Details

Bug Number	Summary
37405	summary of bug 37405
37310	summary of bug 37310

File Path	Md5sum
/opt/meru/etc/coord.config	ed04e8b2dca901d1ce61f9160bfdb0a5

Patch History

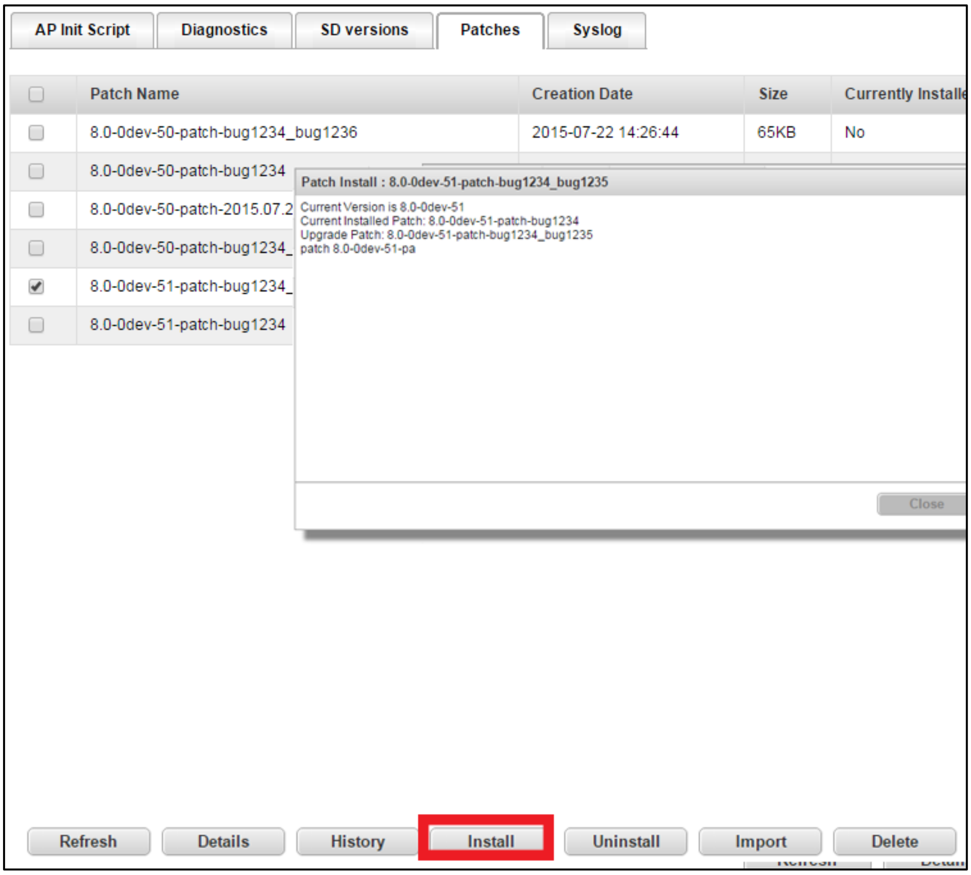


☐	Patch Name	Creation Date	Size	Currently Instal
☑	8.0-0dev-50-patch-bug1234_bug1236	2015-07-22 14:26:44	65KB	No
☐	8.0-0dev-50-patch-bug1234	2015-07-22 14:12:21	65KB	No
☐	8.0-0dev-50-patch-2015.07.22-17h.12m.09s	2015-07-22 20:59:51	7.1MB	No
☐	8.0-0dev-50-patch-bug1234_bug1235	2015-07-22 16:31:48	65KB	No

Patches History

Date	Patch Name	On Build	Action
2015:07:24 01:51:13	8.0-0dev-50-patch-bug1234	8.0-0dev-51	uninstalled
2015:07:24 01:54:13	8.0-0dev-51-patch-bug1234_bug1235	8.0-0dev-51	installed
2015:07:24 01:56:39	8.0-0dev-51-patch-bug1234_bug1235	8.0-0dev-51	uninstalled
2015:07:24 01:57:00	8.0-0dev-51-patch-bug1234_bug1235	8.0-0dev-51	installed
2015:07:24 13:26:07	8.0-0dev-51-patch-bug1234_bug1235	8.0-0dev-51	uninstalled
2015:07:24 13:29:25	8.0-0dev-51-patch-bug1234_bug1235	8.0-0dev-51	installed
2015:07:24	8.0-0dev-51-patch-	8.0-0dev-51	uninstalled

Patch Install



☐	Patch Name	Creation Date	Size	Currently Installe
☐	8.0-0dev-50-patch-bug1234_bug1236	2015-07-22 14:26:44	65KB	No
☐	8.0-0dev-50-patch-bug1234			
☐	8.0-0dev-50-patch-2015.07.2			
☐	8.0-0dev-50-patch-bug1234_			
☑	8.0-0dev-51-patch-bug1234_			
☐	8.0-0dev-51-patch-bug1234			

Patch Install : 8.0-0dev-51-patch-bug1234_bug1235

```
Current Version is 8.0-0dev-51
Current Installed Patch: 8.0-0dev-51-patch-bug1234
Upgrade Patch: 8.0-0dev-51-patch-bug1234_bug1235
patch 8.0-0dev-51-pa
```

Using the CLI

`show patches:` Displays the list of patch builds copied to the controller.

```
#show patches
8.0-0dev-51-patch-bug1234 [installed]
8.0-0dev-50-patch-bug1234_bug1236
8.0-0dev-50-patch-bug1234
8.0-0dev-50-patch-2015.07.22-17h.12m.09s
8.0-0dev-50-patch-bug1234_bug1235
8.0-0dev-51-patch-bug1234_bug1235
8.0-0dev-51-patch-bug1234
```

`show patch installed:` Displays the patch currently installed in the controller.

```
controller(15)# show patch installed
8.0-0dev-51-patch-bug1234
```

`show patch history:` Displays the history of all the patches installed and uninstalled in the controller

```
controller(15)# show patch history
2015:07:24 01:51:13: uninstalled 8.0-0dev-50-patch-bug1234 on build 8.0-0dev-51
2015:07:24 01:54:13: installed 8.0-0dev-51-patch-bug1234_bug1235 on build 8.0-0dev-
51
2015:07:24 01:56:39: uninstalled 8.0-0dev-51-patch-bug1234_bug1235 on build 8.0-
0dev-51
--<snipped>---
2015:07:24 14:54:50: uninstalled 8.0-0dev-51-patch-bug1234 on build 8.0-0dev-51
```

`show patch details <patch-name>:` Displays the list of bug fixes available in this patch.

```
controller(15)# show patch details 8.0-0dev-50-patch-bug1234
8.0-0dev-50-patch-bug1234
patch is revertable
bugs:
  37405: summary of bug 37405
controller(15)#
```

`show patch contents <`*`patch-name`*`>:` Displays the md5 sum of the patch build.

```
controller(15)# show patch contents 8.0-0dev-50-patch-bug1234
8.0-0dev-50-patch-bug1234
files:
  /opt/meru/etc/coord.config: 3d4c720265e21a53dfafe2a484e8bf11
```

`patch uninstall <`*`patch-name`*`>:` To uninstall the patch build from the controller.

```
controller(15)# patch uninstall
Reverting from backup.
cp -f /data/.patch-backup//meru-8.0-0dev-51-patch-bug1234/coord.config
/opt/meru/etc/coord.config
Reverting from backup done.
```

Application Visibility (DPI)

System Director 8.0 allows you to monitor and/or block specific application traffic in your network. System Director can monitor and restrict access applications/services, as listed in the **Configuration** > **Application** > **Settings** tab > **System Defined Applications** and **Custom Applications**.

NOTE

- Feature is supported only on 11ac access points.
- Properties defined in a custom application will take precedence over system defined applications set up for blocking and monitoring.

Limitations and Recommendations

- To export DPI status to an EzRF server, the export destination port must be set to **4739**.
- If the total number of ESS profiles and the total number APs in the controller are the maximum allowed, then a policy cannot be created. When configuring each policy:
  - The total number of ESS that can be applied to is 64. ***Tip:*** To support this maximum, ensure that an ESS name is 15 characters or less.
  - The total number APs that can be applied are 186. To support this maximum, the AP IDs need to between the 1 to 500 AP ID range. ***Tip***: to maximize the coverage of APs, you can create AP groups and use this instead of listing individual APs.
- Advanced detection of sub-protocol traffic is a resource intensive task, so we recommend that you use it in moderation.
- A custom application is by default monitored even if it is not mapped to a policy. But for it to be blocked, it must be added to a policy.

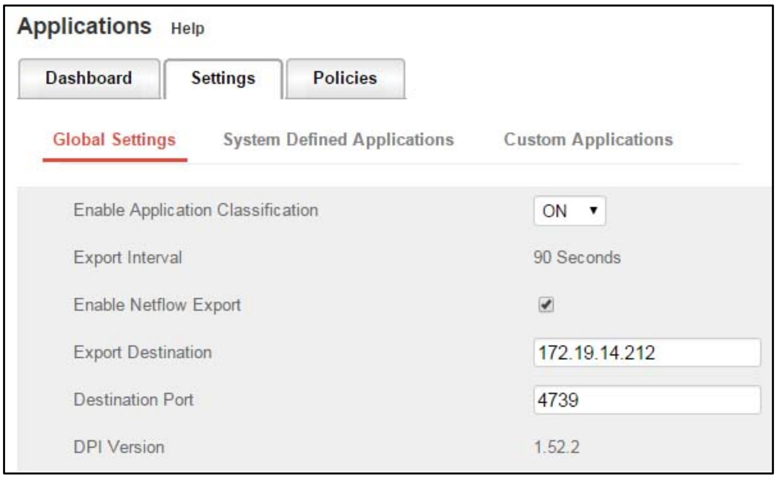
To set up and use the application monitoring:

1. Enable Application Visibility
2. Create Policies
3. Associate system defined and/or custom applications to policies

Enable Application Visibility

To enable DPI, go to **Configuration** > **Application** > **Settings** tab > ***Global Settings*** page and do the following:

1. Select **ON** for Enable Application Classification. This is a global setting and enables DPI on all APs (802.11ac)
2. Export Interval is a non-configurable field set at 90 seconds.
3. **Export Destination**: Specify or edit (if automatically pushed by *Network Manager*) the IP address of the correct *Network Manager* server. This is used to export stats to *Network Manager* server.
4. **Destination Port**: If the export destination is an EzRF server, the port must be set to 4739.



Enable Application Classification: ON

Export Interval: 90 Seconds

Enable Netflow Export: ☑

Export Destination: 172.19.14.212

Destination Port: 4739

DPI Version: 1.52.2

Figure 1 DPI - Enable DPI

Creating a Policy

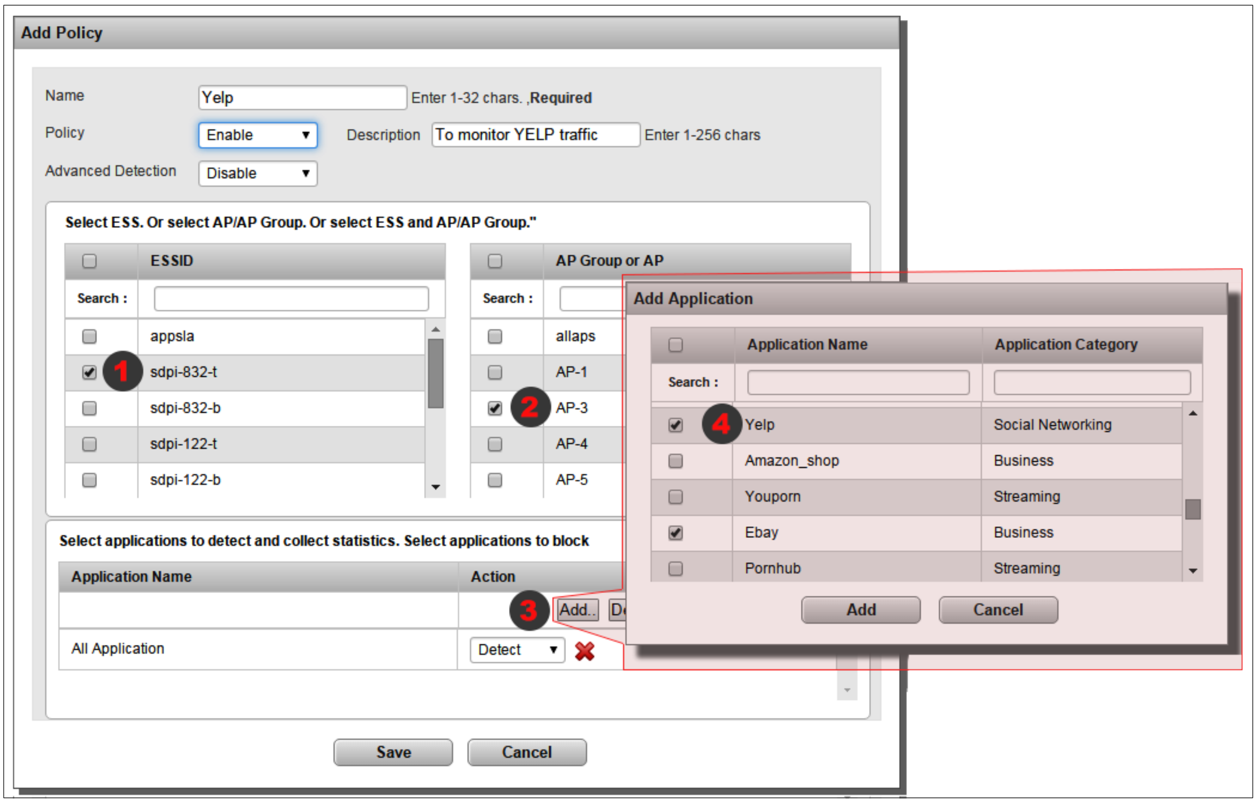
Policies are a collection of rules that monitor and block one or more application traffic. This can be done for any of the following condition:

- All ESS profiles
- Per ESS profile
- All APs
- Per AP
- Per AP Group
- ESS and AP Combination

Example

The following screenshots illustrate the procedure to create a policy to block *Yelp* traffic by clients that are connected to **sdpi-832-t** ESS profile via **AP-3**.

1. Select the ESS profile from the ESSID table.
2. Select the AP from the AP Group or AP table.
3. Click the **ADD** button to view application lists
4. Select the application from the list and click the **ADD** button
5. Select Block from the dropdown list and click the **SAVE** button



Add Policy

Name	Yelp	Enter 1-32 chars. ,**Required**	
Policy	Enable	Description	To monitor YELP traffic — Enter 1-256 chars
Advanced Detection	Disable		

Select ESS. Or select AP/AP Group. Or select ESS and AP/AP Group."

□	ESSID
Search :	
□	appsla
☑	sdpi-832-t
□	sdpi-832-b
□	sdpi-122-t
□	sdpi-122-b

□	AP Group or AP
Search :	
□	allaps
□	AP-1
☑	AP-3
□	AP-4
□	AP-5

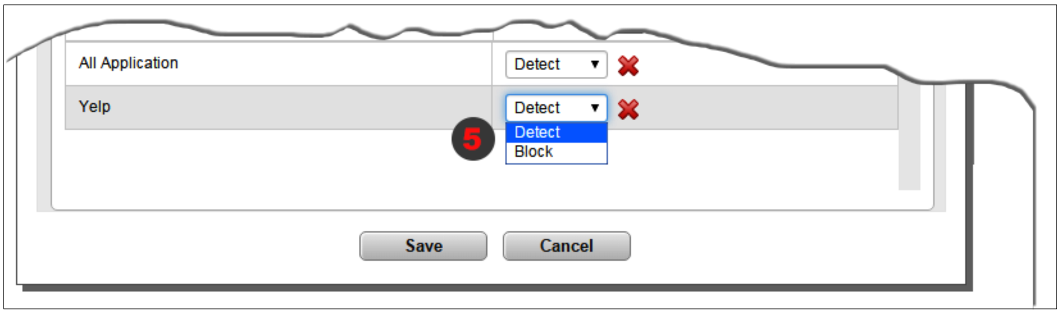
Select applications to detect and collect statistics. Select applications to block

Application Name	Action
	Add..
All Application	Detect ✖

Add Application

□	Application Name	Application Category
Search :		
☑	Yelp	Social Networking
□	Amazon_shop	Business
□	Youporn	Streaming
☑	Ebay	Business
□	Pornhub	Streaming

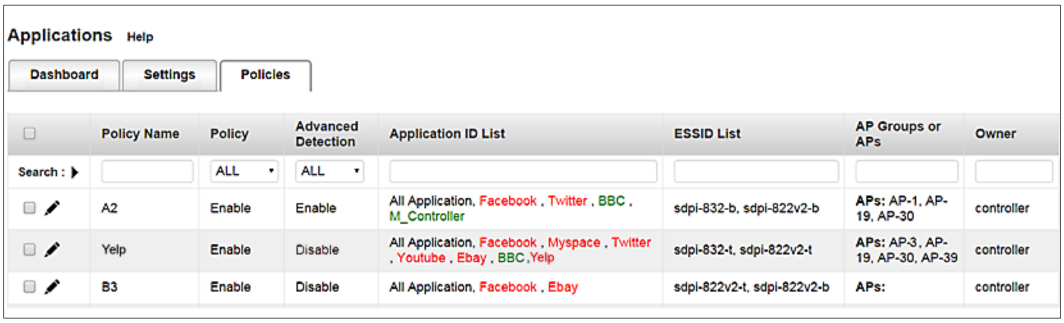
Figure 2 DPI - Adding Policy



All Application	Detect ✖
Yelp	Detect ✖

Figure 3 DPI - Policy Setting

List of policies



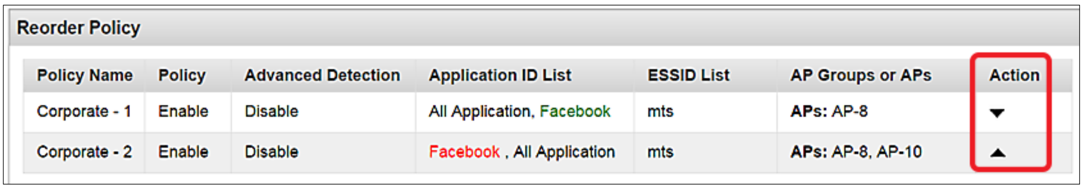
Applications Help

□	Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Owner
Search :		ALL	ALL				
□	A2	Enable	Enable	All Application, Facebook , Twitter , BBC , M_Controller	sdpi-832-b, sdpi-822v2-b	APs: AP-1, AP-19, AP-30	controller
□	Yelp	Enable	Disable	All Application, Facebook , Myspace , Twitter , Youtube , Ebay , BBC ,Yelp	sdpi-832-t, sdpi-822v2-t	APs: AP-3, AP-19, AP-30, AP-39	controller
□	B3	Enable	Disable	All Application, Facebook , Ebay	sdpi-822v2-t, sdpi-822v2-b	APs:	controller

Figure 4 DPI - Policy List

By default, the Policies tab displays the following:

- **Policy Name**: The name to identify the policy.
- **Policy**: The status of the policy
- **Advanced Detection**: Select *enable* to view sub-protocols for a system defined application and protocols.
- **Application ID List**: List of system defined application and /or custom applications that are blocked or monitored by the policy. Blocked applications are shown in red colour and applications that are only monitored are shown in green colour.
- **ESSID List**: The name of the ESS profile configured for this policy. Clients that connect using this ESSID profile and accessing the monitored application.
- **AP Groups or APs**: The list of APs that are configured for this policy. Clients that connected via these APs or AP groups and accessing the monitored application.
- **Owner**: The owner is either controller or NMS. If the policy is created in the controller the owner is listed as controller.
- **Search**: To locate a specific policy by Name, AP, ESS, or owner, enter the keyword in the search box and hit the **Enter** key. This will highlight the corresponding row that matches the keyword. To filter the display based on Status, select the status (from the dropdown) to highlight the corresponding rows.
- **Policy Reordering**: Policies are executed in the order they are displayed. To reorder policy priority, click the Reorder button and use the arrows in the action column to move them up or down the listing order. You **must save** this for the reorder changes to take effect.



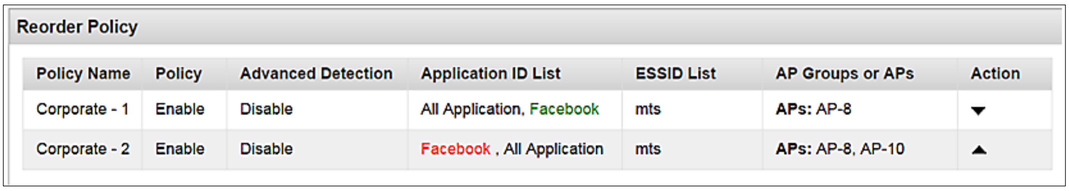
Reorder Policy

Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Action
Corporate - 1	Enable	Disable	All Application, Facebook	mts	**APs:** AP-8	▼
Corporate - 2	Enable	Disable	Facebook , All Application	mts	**APs:** AP-8, AP-10	▲

Figure 5 DPI - Policy Reorder

> **NOTE** If an ESS and AP combination appear in more than one policy, then the policy that is on top will be triggered.

In the following illustration, the ESSID **MTS** and APID **AP-8** appear in both *corporate-1* and *corporate-2* policies. The *corporate-1* policy allows Facebook traffic and *corporate-2* blocks Facebook traffic. Since *corporate-1* is higher in the order than *corporate-2*, Facebook will be allowed and not blocked. However, for AP-10 Facebook will be blocked as per *corporate-2* policy.



Reorder Policy

Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Action
Corporate - 1	Enable	Disable	All Application, Facebook	mts	**APs:** AP-8	▼
Corporate - 2	Enable	Disable	Facebook , All Application	mts	**APs:** AP-8, AP-10	▲

Figure 6 DPI - ESS-AP Combination Rule

Custom Applications

Custom applications are user-defined applications that are not part of the system defined applications. You can add a maximum of 32 applications in the controller and a maximum of 32 applications on Network Manager.

NOTE Protocol/sub-protocol detection/support for custom applications is not available.

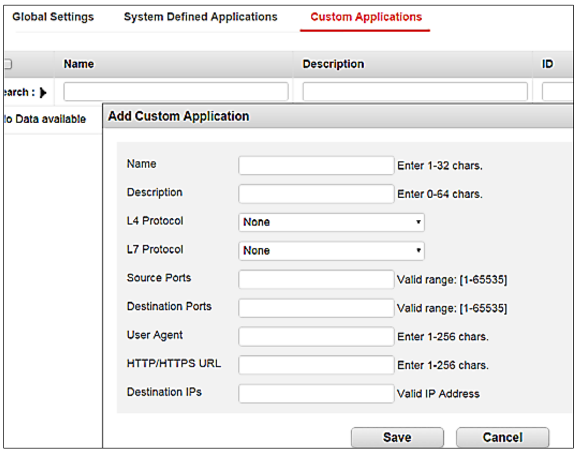
A custom application is a combination of one or more of the following:

- Predefined L4 and L7 protocols
- Source and/or Destination Ports
- User Agents
- Any HTTP/HTTPS URL
- Destination IP

IMPORTANT For a custom application to be monitored or blocked by a policy, all of its properties must match the traffic.

Creating a Custom Application and assigning it to a Policy

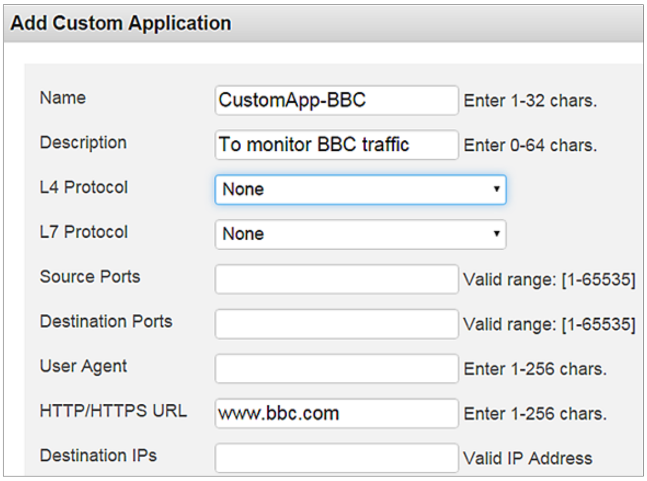
1. To create a custom application, go to **Application** > **Settings** > **Custom Applications** and click the **Add** button.



Add Custom Application

Name		Enter 1-32 chars.
Description		Enter 0-64 chars.
L4 Protocol	None	
L7 Protocol	None	
Source Ports		Valid range: [1-65535]
Destination Ports		Valid range: [1-65535]
User Agent		Enter 1-256 chars.
HTTP/HTTPS URL		Enter 1-256 chars.
Destination IPs		Valid IP Address

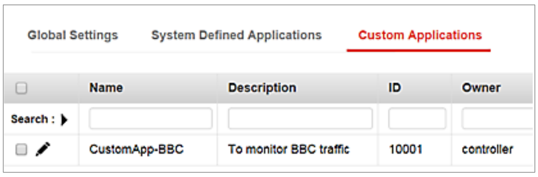
2. Enter properties for the custom application and click **Save**. In this simple example, traffic from www.bbc.com will be monitored.



Add Custom Application

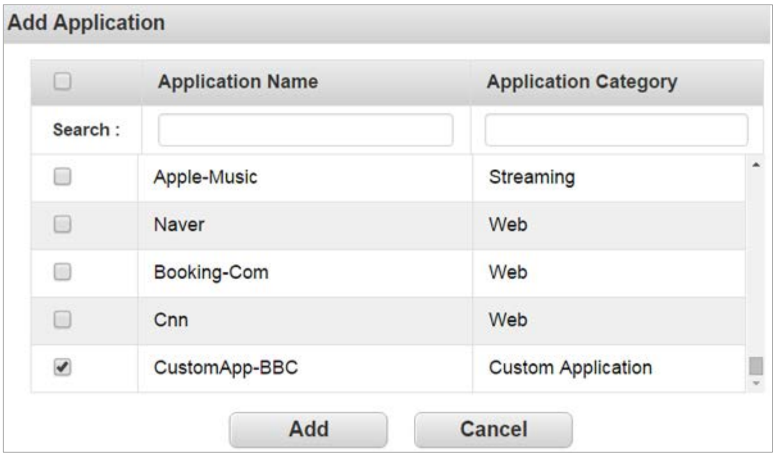
Name	CustomApp-BBC	Enter 1-32 chars.
Description	To monitor BBC traffic	Enter 0-64 chars.
L4 Protocol	None	
L7 Protocol	None	
Source Ports		Valid range: [1-65535]
Destination Ports		Valid range: [1-65535]
User Agent		Enter 1-256 chars.
HTTP/HTTPS URL	www.bbc.com	Enter 1-256 chars.
Destination IPs		Valid IP Address

3. Custom application listing



□	Name	Description	ID	Owner
Search :				
□	CustomApp-BBC	To monitor BBC traffic	10001	controller

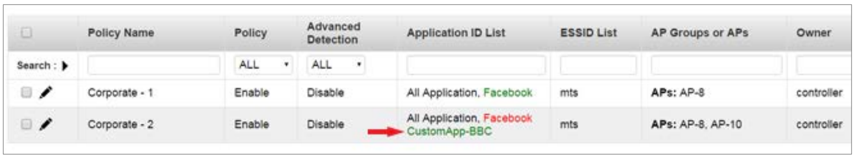
4. Add custom application to a policy. Use the same steps mentioned in Figure 2. But in the sub-step 4 of figure 2, scroll down to very end to location the custom application. Select the custom application and then select policy setting.



Add Application

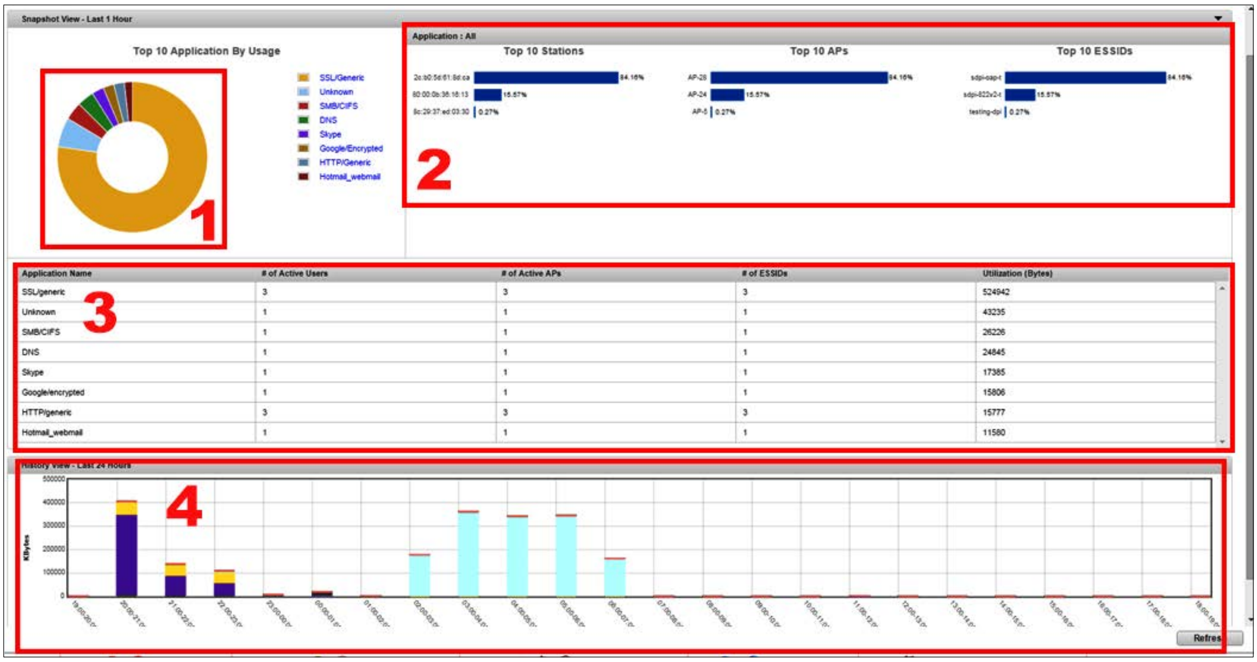
□	Application Name	Application Category
Search :		
□	Apple-Music	Streaming
□	Naver	Web
□	Booking-Com	Web
□	Cnn	Web
☑	CustomApp-BBC	Custom Application

5. Custom application is listed in the policy



□	Policy Name	Policy	Advanced Detection	Application ID List	ESSID List	AP Groups or APs	Owner
Search :		ALL	ALL				
□	Corporate - 1	Enable	Disable	All Application, Facebook	mts	**APs:** AP-8	controller
□	Corporate - 2	Enable	Disable	All Application, Facebook CustomApp-BBC	mts	**APs:** AP-8, AP-10	controller

DPI Dashboard



Application Name	# of Active Users	# of Active APs	# of ESSIDs	Utilization (Bytes)
SSL/generic	3	3	3	524942
Unknown	1	1	1	43235
SMB/CIFS	1	1	1	26226
DNS	1	1	1	24845
Skype	1	1	1	17385
Google/encrypted	1	1	1	15806
HTTP/generic	3	3	3	15777
Hotmail_webmail	1	1	1	11580

Figure 7 DPI - Dashboard

The DPI dashboard shows applications that are configured for monitoring (detect) only. Applications that are blocked are not displayed in the dashboard as they are dropped by the AP.

1. The graphical chart displays the top 10 applications (by usage) and their statistics that are monitored in the last 1 hour. If application traffic is stopped, they will continue to be displayed in the top 10 list, until another application with more traffic gets listed or for an hour after it was stopped.
2. By default the dashboard lists top 10 stations, top 10 APs, and top 10 ESS profiles passing traffic from the top 10 monitored applications. To view application specific statistics, click the application name from the list or a segment in the doughnut chart.
3. This table lists the top 10 applications, numerical (integer) statistics about number of stations, ESS profiles, APs and bandwidth **utilization** (in Bytes). Clicking on a segment in the graphical chart highlights the corresponding row in the table.
4. This table shows historical data of all application traffic in the last 24 hours.

Using CLI

Creating a Policy

1. In the config mode, use the **`app-visibility-policy <policy-name>`** command.
2. Enable the status using the **`state enable`** command
3. Now, add applications, access points, ESS profile.
    a. Adding application: **`appids <application-ID>:<type>`**
    b. Adding access points: **apids “*<ap-id>*: A”**
    c. Adding access points groups: **apids “*<ap-group-name>*: L”**
    d. Adding ESS profiles: **essids *<essid-name>***

- See the Legends section for more information.

NOTE

- Application IDs are available in the **Configuration** > **Application** > **Settings** > ***System Defined Applications***.
- In a single policy you can add rules to monitor and block application traffic

```
mc1500(15)(config)# app-visibility-policy  CorpNet
mc1500(15)(config-app-visibility-policy)# description  ""
mc1500(15)(config-app-visibility-policy)# state  enable
mc1500(15)(config-app-visibility-policy)# appids  6:B
mc1500(15)(config-app-visibility-policy)# essids  stability
mc1500(15)(config-app-visibility-policy)# apids  "5:A"
mc1500(15)(config-app-visibility-policy)# owner  controller
mc1500(15)(config-app-visibility-policy)# version  0
mc1500(15)(config-app-visibility-policy)# exit
```

To view the list of policies and type configured, use the **`show application-visibility policy`** command.

```
PM-D2(15)# show application-visibility policy
Name            Policy         Adv Detection  Applications                    EssIds                          AP Groups
or APs

B1              enable         disable        *,2:B,32:B                      sdpi-822v2-t                    24:A
P3              enable         disable        2:B                             testing-dpi                     5:A
P6              enable         disable        2:B                             sdpi-oap-t                      28:A
P9              enable         disable        *                               sdpi-832-t                      5:A
        Application Visibility Policy(4)
```

Creating a Custom Application

```
(config)# app-visibility-custom-application CustomApp-BBC
(config-app-visibility-custom-application)# description  “To Monitor BBC traffic”
(config-app-visibility-custom-application)# url  www.bbc.com
(config-app-visibility-custom-application)# exit
# sh application-visibility custom-application
Name                    Description                     ID
CustomApp-BBC           To Monitor BBC traffic          10001
```

Monitoring Policies

```
mc1500(15)# sh service-summary Application-Visibility

Feature                 Type            Name                    Value   ValueStr

Application-Visibility  Application     myspace                 100     {"util":3006.76,"tx":6943001576,"rx":257651566}
Application-Visibility  Application     amazon_cloud            0       {"util":474.84,"tx":1093389603,"rx":43774451}
Application-Visibility  Application     facebook                0       {"util":184.00,"tx":421673492,"rx":18973696}
Application-Visibility  Application     twitter                 0       {"util":164.58,"tx":358628579,"rx":35513363}
… <snipped> …
Application-Visibility  Station         08:11:96:7d:cf:80       0       {"util":286.78,"tx":657504303,"rx":29271859}
Application-Visibility  Station         24:77:03:80:a4:40       0       {"util":281.94,"tx":646183947,"rx":29009375}
Application-Visibility  Station         24:77:03:80:5f:54       0       {"util":280.23,"tx":645624714,"rx":25475052}
Application-Visibility  Station         24:77:03:85:b4:50       0       {"util":279.89,"tx":641592459,"rx":28689908}
Application-Visibility  EssId           stability               100     {"util":4055.84,"tx":9313033268,"rx":399999526}
Application-Visibility  AP              AP-109                  100     {"util":4055.84,"tx":9313033268,"rx":399999526}
        Service Data Summary(20 entries)
mc1500(15)# sh application-visibility application-summary

APPID           Name                    Station Counts  AP Counts       ESS Counts      Tx Bytes        Rx Bytes
TxRx Bytes
```

```
5               myspace                 12              1               1               7274981850      269918317
7544900167
24              amazon_cloud            13              1               1               1149026229      45994062
1195020291
2               facebook                13              1               1               443832821       19962877
463795698
8               twitter                 13              1               1               375850987       37259491
413110478
0               unknown                 20              1               1               233565871       13899667
247465538
70              amazon_shop             13              1               1               170637983       25318821
195956804
41              linkedin                12              1               1               115430025       6896689
122326714
32              youtube                 13              1               1               3022484         304784
3327268
        Application Visibility Statistics Summary(8)

mc1500(15)# sh service-summary-trend Application-Visibility
Feature                 Type            Name                    StartTime            EndTime              Value
ValueStr

Application-Visibility  Application     myspace                 01/17/2009 01:00:00  01/17/2009 02:00:00  370191907
{"util":254501.59,"tx":3561906268,"rx":140012805}
Application-Visibility  Application     amazon_cloud            01/17/2009 01:00:00  01/17/2009 02:00:00  523131985
{"util":35964.57,"tx":502700232,"rx":20431753}
Application-Visibility  Application     twitter                 01/17/2009 01:00:00  01/17/2009 02:00:00  221967525
{"util":15259.95,"tx":202733592,"rx":19233933}
Application-Visibility  Application     facebook                01/17/2009 01:00:00  01/17/2009 02:00:00  220636588
{"util":15168.45,"tx":210304218,"rx":10332370}
Application-Visibility  Application     unknown                 01/17/2009 01:00:00  01/17/2009 02:00:00  113502079
{"util":7803.10,"tx":106412520,"rx":7089559}
Application-Visibility  Application     amazon_shop             01/17/2009 01:00:00  01/17/2009 02:00:00  106703142
{"util":7335.69,"tx":93322094,"rx":13381048}
Application-Visibility  Application     linkedin                01/17/2009 01:00:00  01/17/2009 02:00:00  58696435
{"util":4035.30,"tx":55165018,"rx":3531417}

… … . … <snipped> …. …

Application-Visibility  Application     linkedin                01/17/2009 03:00:00  01/17/2009 04:00:00  121917540
{"util":3824.43,"tx":114827231,"rx":7090309}
Application-Visibility  Application     youtube                 01/17/2009 03:00:00  01/17/2009 04:00:00  3187860
{"util":100.00,"tx":2879796,"rx":308064}
        Service Data Summary Trend(24 entries)
```

Legends

```
controller(15)# show application-visibility policy
Name            Enable          Applications                    EssIds                          AP Groups or APs
11              enable          2:A,3:B                         appsla                          3:A
123             enable          *                               appsla                          143:A
1232454         enable          2:A,3:B,4:B,5:B,6:A,7:A,8:A,9:A appsla                          145:A
ALL             enable          *                               appsla                          145:A
a               enable          *                               appsla                          123:L,143:A,145:A
rrer            enable          *                               appsla1                         1234:L
        Application Visibility Policy(6)
controller(15)#
```

Legend	Description
A	When used for an application, it means to allow, detect, and monitor the application traffic.
B	Used to detect and block the application traffic
A	When used as an AP-ID, refers to adding an individual AP.
L	Used to add an ap-group to a policy.

VLAN Pooling

To reduce big broadcast or risking a chance of running out of address space, you can now enable VLAN pooling in an ESS profile.

VLAN pooling essentially allows administrators to create a named alias using a subset of VLANs thereby creating a pool of address. By enabling VLAN pool, you can now associate a client/device to a specific VLAN. This allows you to effectively manage your network by monitoring appropriate or specific VLANs pools.

NOTE VLAN Pool is available only in tunnelled mode

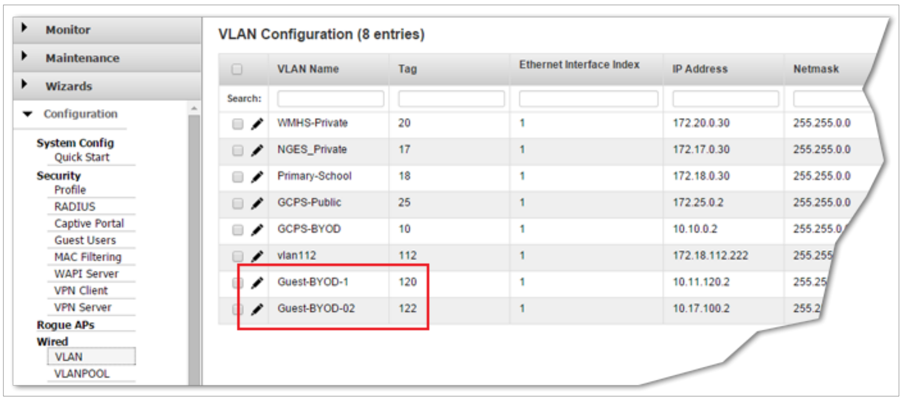
Features

- You can specify the maximum number of clients that can be associated to a VLAN.
- The client/device behaviour does not change after it is associates to a VLAN in a pool.
- If a VLAN is removed from a VLAN pool, clients/devices connected to the VLAN will continue to be associated to the VLAN. However, if the clients disconnect and reconnect the VLAN will change.

Configuration

Using WebUI

1. Create VLANs tags

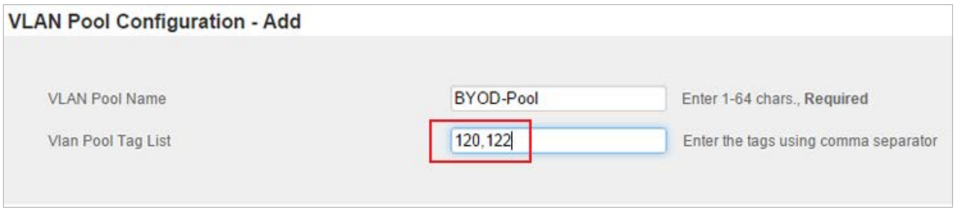


VLAN Configuration (8 entries)

VLAN Name	Tag	Ethernet Interface Index	IP Address	Netmask
WMHS-Private	20	1	172.20.0.30	255.255.0.0
NGES_Private	17	1	172.17.0.30	255.255.0.0
Primary-School	18	1	172.18.0.30	255.255.0.0
GCPS-Public	25	1	172.25.0.2	255.255.0.0
GCPS-BYOD	10	1	10.10.0.2	255.255.0
vlan112	112	1	172.18.112.222	255.255
Guest-BYOD-1	120	1	10.11.120.2	255.25
Guest-BYOD-02	122	1	10.17.100.2	255.2

2. Create a VLAN Pool and assign one or more VLAN tags

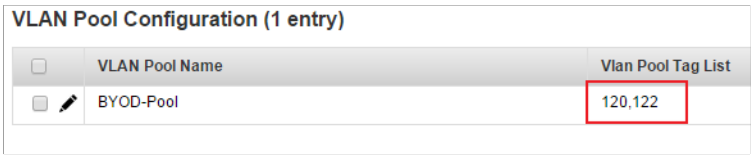
   Ensure that these VLAN tags are not in use by another profile.



VLAN Pool Configuration - Add

VLAN Pool Name	BYOD-Pool	Enter 1-64 chars., **Required**
Vlan Pool Tag List	120,122	Enter the tags using comma separator

3. VLAN Pool Listing



VLAN Pool Configuration (1 entry)

VLAN Pool Name	Vlan Pool Tag List
BYOD-Pool	120,122

Using CLI

1. Configure VLAN

```
default(config)# vlan vlan10 tag 10
default(config-vlan)# ip address 10.0.0.222 255.255.255.0
default(config-vlan)# ip default-gateway 10.0.0.1
default(config-vlan)# exit
default(config)# exit
default# sh vlan vlan10
VLAN Configuration
VLAN Name                              : vlan10
Tag                                    : 10
Ethernet Interface Index               : 1
IP Address                             : 10.0.0.222
Netmask                                : 255.255.255.0
IP Address of the Default Gateway      : 10.0.0.1
Override Default DHCP Server Flag      : off
DHCP Server IP Address                 : 0.0.0.0
DHCP Relay Pass-Through                : on
Owner                                  : controller
Maximum number of clients              : 253
default#
```

2. Configure VLAN Pool:

```
default(config)# vlan-pool vlangroup
default(config-vpool)# tag-list 10,36
default(config-vpool)# exit
default(config)# exit
default# sh vlan-pool
VLAN Pool Name            Vlan Pool Tag List
vlangroup                 10,36
VLAN Pool Configuration(1 entry)
default#
```

Support for VLAN Tagging in Bridge Mode for Wired Ports

You can now enable VLAN tagging for wired ports in bridged mode. VLAN tagging for wired ports provide four VLAN policies:

- **No VLAN**
- **Static VLAN**: VLAN tag shall be configured for a valid range of 0-4094.

NOTE Not supported in AP110 and 1014.

Enhancements to WAN Survivability

Starting with System Director 7.0, the following features are now available to tunnelled devices during a link outage to a controller in WAN deployment.

- ESS Profile is enhanced with additional option to specify a backup ESS profile for both bridge and tunnelled modes. This ESS profile is activated with the controller link is down.
- New devices connecting during the outage will connect using *clear* and *PSK profiles*.

The clients will now be serviced until the links up and all new devices that connected during outage will reconnect after the link is up.

Support for 802.11k/r Specifications

Devices can now benefit from the 802.11r implementation to fast roam between best available access points within a controller domain. Additionally, with implementation of 802.11k specifications you can now calculate 802.11k neighbour and radio measurement reports. The exchange of 802.11k messages (Neighbour request/response, Beacon Report Request/Response, Channel report request/Response) between the Infrastructure (Controller + AP) and the wireless client helps the Infrastructure build

a) Neighbour List for that particular AP (as seen by the Client) and
b) Maintain client specific radio parameters (like Channel on which Client is communicating etc.)

The fast roaming capability and 802.11k is configurable in the ESS profile.

NOTE Supports backward compatibility for clients without 11k/r support.

Supported Access Points: AP122, AP822, AP832, OAP832

Limitations

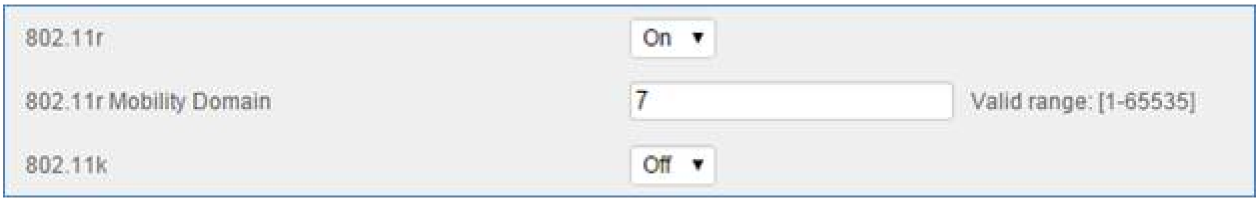
- Fast roaming is not available in inter-controller roaming.

Enabling 802.11k

Using WebUI

Go to **Configuration** > **Wireless** > **ESS** and in the ESS Profile tab, change the following:

- For 802.11r, select **On**.
- For 802.11r Mobility Domain, enter an integer value.
- For 802.11k, select **On** to perform radio measurements.



802.11r: On ▾

802.11r Mobility Domain: 7 Valid range: [1-65535]

802.11k: Off ▾

Using CLI

```
default(15)# configure terminal
default(15)(config)# essid fastroam-1
default(15)(config-essid)# 802.11r on
default(15)(config-essid)# 802.11k on
default(15)(config-essid)# 802.11r-mobility-domain-id 100
```

Time Based ESS

You can schedule the availability of an ESS based on pre-define time intervals. By default, ESS profiles are always ON and available to clients/devices. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days.

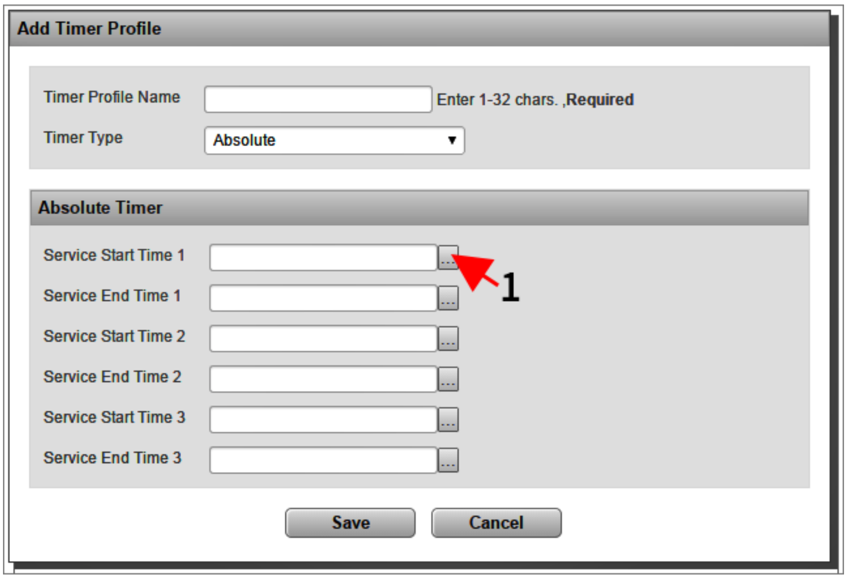
To create a time based ESS profile, you must first create a timer profile and then associate the timer profile to the ESS profile.

Creating a Timer Profile

You can create timer profile using WebUI or CLI.

Using WebUI

1. Go to **Configuration** > **Timer** and click the **Add** button.
2. In the **Add Timer Profile** pop up window, enter *Timer Profile Name* and select *Timer Type*:



Add Timer Profile

Timer Profile Name: Enter 1-32 chars. ,Required

Timer Type: Absolute

Absolute Timer

Service Start Time 1

Service End Time 1

Service Start Time 2

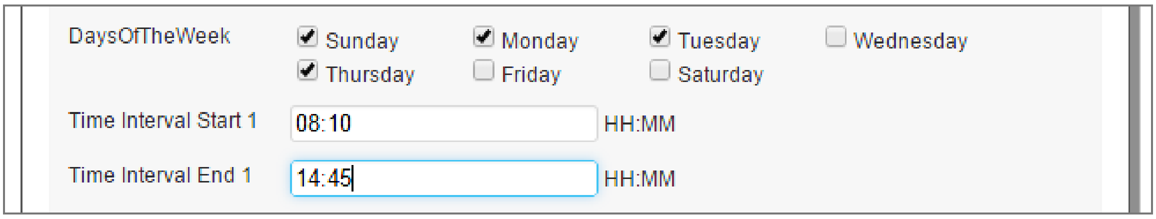
Service End Time 2

Service Start Time 3

Service End Time 3

Figure 8

- **Absolute** timer profiles can enable and disable ESS visibility for time durations across multiple days. You can create up to 3 specific start and end time per timer profile. To enter start of the end time, click the Date picker box. See **label 1** in figure 1.
- **Periodic** timer profiles are a set of start and end timestamp that can be applied across multiple days of a week. To create a period timer profile, enter the time in *hh:mm* format. Where ***hh***, represent hours in 2-digits and ***mm*** represent minutes in 2-digits. Figure 2, illustrates a timer profile that will be applied on Sunday, Monday, Tuesday, and Thursday from 08:10 a.m. or 14:45 (2.45 p.m).



DaysOfTheWeek ☑ Sunday ☑ Monday ☑ Tuesday ☐ Wednesday ☑ Thursday ☐ Friday ☐ Saturday

Time Interval Start 1: 08:10 HH:MM

Time Interval End 1: 14:45 HH:MM

Figure 9

Using CLI

A new CLI command **`timer-profile`** with various options is available to create a timer profile.

Syntax

```
#(config-mode) timer-profile <profile-name>

#(timer-config-mode) <timer-type> <timer-slot> start-time <”mm/dd/yyyy hh:mm”> end-time <”mm/dd/yyyy hh:mm”>
```

- timer-type is either absolute-timer or periodic timer
- Absolute timer profile allows creation of 3 timer slots.
- Time must be specified within double quotes in this format: **mm/dd/yyyy** <space> **hh:mm**

Example: Creating an absolute timer profile

```
default# configure terminal
default (config)# timer-profile monthly-access
default (config-timer)# absolute-timer time-slot-1 start-time "01/01/2014 10:10" end-time "02/02/2014 08:45"
```

Remote RADIUS Server

Network deployments with remote sites that are physically away from their head-quarter (or master data center –***DC***) can use remote RADIUS server in each of the remote sites for local authentication purposes.

In a typical scenario, a RADIUS server is usually co-located in the DC. Remote sites that required AAA services to authenticate their local clients use the RADIUS server in the DC. This in most cases introduces among other issues high latency between the remote site and its DC. Deploying a RADIUS server within a remote site alleviates this problem and allows remotes sites or branches to use their local AAA services (RADIUS) and not rely on the DC.

Before you Begin

Points to note before you begin deploying a remote RADIUS server:

1. Ensure that the Controller and site AP communication time is less than RADIUS timeout.
2. Provision for at least one AP that can be configured as a relay AP.
3. Only 11ac APs (AP122, AP822, AP832, and OAP832) in L3-mode can be configured as a relay AP.
4. In case of WAN survivability, no new 802.1x radius clients will be able to join, until relay AP rediscovers the controller.

Upgrade Note After upgrade two new fields `RemoteRadiusServer` & `RadiusRelayApId` are added to the Radius Profile. By default the `RemoteRadiusServer` field is set to ***OFF*** and `RadiusRelayApId` will not point to any AP ID.

How It Works

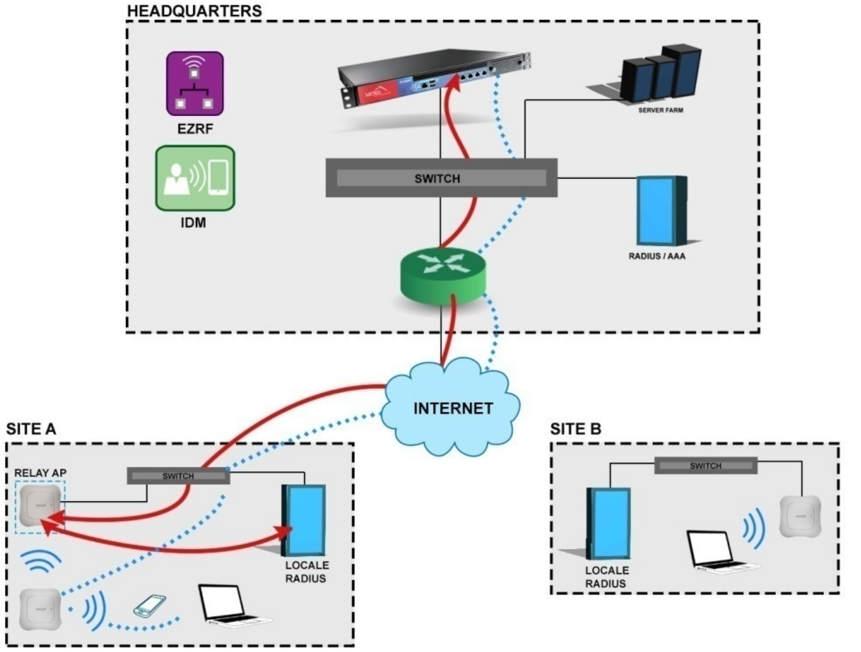
This feature provides local authentication (.1x, Captive Profile, and mac-filtering) services using a RADIUS server set up in the remote site. In addition to the RADIUS server, the remote site must also configure a 11ac AP as a **relay AP.** The remote RADIUS profile can be created per ESS profile using the controller's WebUI (**Configuration** > **RADIUS**) or CLI. A remote RADIUS profile works like a regular profile and can be used as primary and secondary RADIUS auth and accounting servers.

IMPORTANT High latency between the remote site and DC can cause client disconnections and sluggish network experience.

About Relay AP

- The **relay AP** is used for communicating between the RADIUS server (in the remote site) and the controller in the head-quarters.
- An AP is set as a relay AP only when it is assigned in the RAIDUS profile. Once an AP is assigned as a relay AP It is recommended that you do not overload the relay AP with client WLAN traffic. This can result in communication issues between the relay AP and DC. For regular client WLAN services, we recommend the use of a different access point.
- For a remote RAIDUS profile, you cannot configure a secondary relay AP. However, for resilience purposes, we recommend configuring an alternate (backup) RADIUS profile and assigning another AP as a relay AP to this backup RAIDUS profile. In the security profile, set this RADIUS profile as the secondary RADIUS server.

The following figure illustrates a simple scenario with local RADIUS deployment



The red line indicates the communication between the remote RADIUS server > Relay AP > Controller in headquarters.

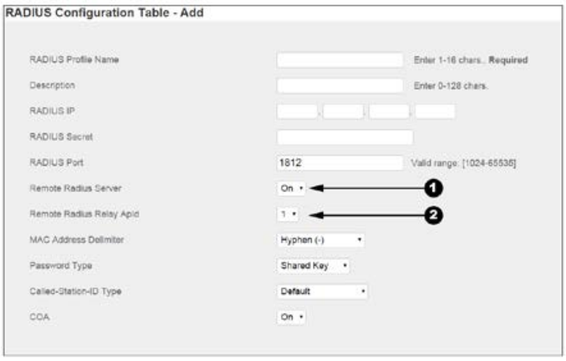
The blue dotted line indicates regular communication (WLAN traffic) between clients, AP, and the controller in headquarters.

Figure 10 Deployment Example

Configuring Using WebUI

To configure remote RADIUS via WebUI,

1. In the **Configuration** > **RADIUS** > **RADIUS Configuration Table – ADD** page, set Remote Radius Server to ON (see **1** in *Figure 2*).
2. Select the AP (**Remote Radius Relay ApId**) to be used as the relay AP (see **2** in *Figure 2*).



RADIUS Configuration Table - Add

RADIUS Profile Name		Enter 1-16 chars., Required
Description		Enter 0-128 chars.
RADIUS IP		
RADIUS Secret		
RADIUS Port	1812	Valid range: [1024-65535]
Remote Radius Server	On	1
Remote Radius Relay Apid	1	2
MAC Address Delimiter	Hyphen (-)	
Password Type	Shared Key	
Called-Station-ID Type	Default	
COA	On	

Figure 11 WebUI Configuration

Configuring Using CLI

```
# configure terminal
(config)# radius-profile RemoteRadius
(config-radius)# remote-radius-server on
(config-radius)# radius-relay-apid XXX
XXX is the AP ID of the relay AP in the remote site.
# configure terminal
(config)# radius-profile RemoteRadius
(config-radius)# no remote-radius-server
```

```
# show radius-profile <remoteRadius-profile-name>
EXAMPLE
# show radius-profile site-a
RADIUS Configuration Table
RADIUS Profile Name      : site-a
Description              : Remote radius profile for Site-A
RADIUS IP                : 172.18.1.8
RADIUS Secret            : *****
RADIUS Port              : 1812
Remote Radius Server     : on
Remote Radius Relay ApId : 2
MAC Address Delimiter    : hyphen
Password Type            : shared-secret
Called-Station-ID Type   : default
Owner                    : controller
COA                      : on
```

Support for VLAN in MESH

Mesh APs now supports VLAN trunking. Enabling VLAN trunking on the G2 port of a mesh AP allows you to pass traffic using the mesh backhaul via the G1 port of the gateway AP.

Before you enable VLAN trunking on a mesh network, follow the recommendations listed below:

1. Redundancy is available only via mesh rediscovery.
2. The gateway AP in a VLAN mesh should use ESS and port profiles in tunnel mode if the profiles contain VLAN tags.

Enabling VLAN Trunk

Using CLI

```
controller(15)# configure terminal
controller(15)(config)# port-profile vlantrunk
controller(15)(config-port-profile)# enable
controller(15)(config-port-profile)# vlantrunk enable
controller(15)(config-port-profile)# multicast-enable
controller(15)(config-port-profile)# end
controller(15)(config)# mesh vlantest
controller(15)(config-mesh)# admin-mode enable
controller(15)(config-mesh)# psk key 12345678
controller(15)(config-mesh)# meshvlantrunk enable
controller(15)(config-mesh)# end
controller(15)#
controller(15)# sh mesh-profile
Name              Description       Admin Mode     PlugNPlay Status VLAN Trunking St
vlantrunk                           enable         disable          enable
testvlan                            enable         disable          enable
vlantest                            enable         disable          enable
        Mesh Configuration(3)
controller(15)# configure terminal
controller(15)(config)# mesh-profile vlantest
controller(15)(config-mesh)# mesh-ap 65
controller(15)(config-mesh-mesh-ap)# end
controller(15)#
controller(15)# sh port-profile
Profile Name                     Enable/Disable VlanTrunk      Dataplane Mode VLAN Name   Security
Profile Allow Multicast IPv6 Bridging
default                          enable         enable         bridged
on              off
vlantrunk                        enable         enable         bridged
off             off
        Port Table(2)
```

802.11w Support

You can now enable 802.11w support to protect WLAN management frames. Protection can be enabled for all clients or specifically for 802.11w capable clients.

Support for Bluetooth Devices

AP832 running System Director 8.0 enables support for BLE devices.

Context Sensitive Help

This release introduces context sensitive help on all screens of the System Director WebUI. For information on any screen, click the Help link available next to the respective page title. The global help link is deprecated.

Known Issues

Bug ID	Description
49154	Ping drops observed on a bridge profile with static VLAN and LACP configured on the AP.
49232	Occasionally Skype calls are detected incorrectly by the DPI engine.
49828	Custom applications created with L4 protocols cannot be blocked completely.
49997	Newly added applications are detected only if application visibility is restarted or added to a policy.
49232	Occasionally Skype voice calls are incorrectly identified as video calls.
49041	Clients authenticated with custom captive profile do not get the successful page.
49346	Master controller is not reachable if the network cable is unplugged and plugged in from the active slave.
49571	OAP832 reboots when there is heavy video traffic.
49773	iPhone6 (iOS9 devices) unable to connect to WPA2 CCMP-AES (PEAP) security profiles, when 11W is enabled-capable.
49787, 49789	CP Authentication does not happen, when same RADIUS Profile is used for both MAC Filtering & CP Auth & Accounting. This results in same session ID in both MAC Filtering Accounting & CP Accounting
49828	Policies created for custom applications using URL does not always block traffic.

Fixed Issues

Bug ID	Description	Scenario
39763	Fixed issues that caused packets to be incorrectly ordered in t-shark captures.	The issue was seen on MC3200, MC4200 and MC6000 controllers (running 5.3-132, 5.3-143, 5.3-154, 6.1-1-25) which have multi-core processors.
41307	Disabling multicast to unicast conversion with WPA2PSK profiles does not affect Airplay services.	This issue affected AP332 and AP832 running SD 6.0-2-0, 6.0-10-0, 6.1-0-3, 6.1-2-28. It is now fixed.

Bug ID	Description	Scenario
42952	The "Rogue detected on the wire" field in the Monitor > Rogue Devices page in WebUI has been removed since System Director (post 4.0 release) does not support this notification.	N.A.
43751	Fixed connections issues with Ascom i62 phones that occurred due to force sync while roaming.	The issue affected SD 5.3-154, 6.1-2-29.
44191	Fixed master ownership issues that occurred after active slave failover. After active slave failover, passive master takes over as master from active slave.	Issue was seen in SD 6.1-2-28,6.1-2-29
44255	Fixed issues to prevent nplus1 revert command from triggering automatic failover on active slave controller.	Issue was found in SD 6.1-2-29,8.0-0-2,7.0-0SR-2,7.0-0SR-11
44706	AP reboots due to softlock up has been fixed.	The issue affected AP 832 running 6.1-2-29,6.1-1-25,7.0-7-0
44816	Fixed connection issues for clients that had both Ipv4 and Ipv6 stack enabled.	Issue affected MC4200, AP 832e running 6.1-2-29,6.1-2-28 and clients with Intel(R) Centrino(R) Advanced-N 6250 AGN running driver version 15.7.0.3.
45073	Fixed graph for station & throughput to accommodate daylight time offset.	The issue affected MC3200 and AP310,AP320i,AP832 running 6.1-2-29
45290	Fixed client upstream throughput issues when connected to AP822i and AP832i.	The issue affected AP822/832 running 6.1-2-29 and if the number of wireless clients (Intel client: Intel(R) Centrino(R) Advanced-N 6235) where more than 8.
45377	Fixed issues that resulted in "bonding: bond0: Error: Couldn't find a slave to tx on for aggregator ID 1" error message.	With this error, the clients had connectivity issues. The issue was seen in SD 6.1-3-3 6.1-3-5
45892	Issues causing AP832 to send incorrect beacons have been fixed.	This issue affected AP832 running 6.1-2-29.
46082	The leaf AP displays its parent/gateway AP ID.	Issue was found in 6.1-2-29.
46215	Fixed client to AP assignment issues.	Issue was seen in SD 6.1-2-29.
46285	Fixed issue that prevented APs from passing downstream traffic.	Issue was seen in SD 6.1-2-29.
46427	Fixed downstream throughput issues faced by Blackberry Z10 connected to AP1014.	Issue affected MC3200 and AP1014 running SD 6.1-2-29.

Bug ID	Description	Scenario
46899	Fixed incorrect output results for the "show interfaces Ethernet controller 1" command and for the display in the "configuration - Ethernet - controller - "show detail info"" page.	Issue affected SD 6.1-2-28 , 6.1-2-29.
47069	Fixed controller reboot issues.	Issue affected MC 4200 running SD 6.1-2-29.
47223	Fixed lost and found issues that prevented clients from connecting to the network.	The issue affected clients connected to MC4200, AP320s running SD 6.1-2-29.
47237	Fixed incorrect authentication statistics.	Issue was found in MC4200 running 6.1-3-5.
47282	Fixed Apache server crashes and webGUI accessibility issues.	The issue affected MC 4200 running SD 6.1-2-29.
47299	Fixed issues that resulted in false nplus1 failovers.	The issue affected SD 8.0-0-1,6.1-2-28
47357	Fixed issues that resulted in controller losing its gateway after controller reload.	Issue was seen in SD 6.1-3-5, 6.1-2-29
47369	The "DHCP Address pool exhausted" alarm is cleared after the DHCP lease time is released.	Issue was seen in 8.0-0-2, 6.1-1-25 , 7.0-4-0
47587	Fixed client station age issues.	Issue was seen in SD 6.1-2-29
47623	Fixed issues related to RADIUS services not starting after reloading controller with factory defaults.	Issue was see in SD 6.1-3-5
47626	Fixed AP reboot issues.	The issue affected MC1500 (4GB) and AP332e running SD 6.1-2-29.
47692	Fixed issues that resulted in "Client moved to Wired" error in a VDS based Virtual environment	The issue affected virtual controllers running 6.1-2-29,6.1-1-25.
47729	Fixed issue with swap ap command that resulted in duplicate entries of new MAC across old mac entries.	Issue was seen in SD 6.1-3-5
47754	Fixed AP node mismatch issues.	This issue occurred when an AP node had a wrong AP MAC address. Issue was seen in SD 6.1.2.29.
47764	Fixed issues that caused the controller to lose AP config changes.	The issue affected SD 6.1-2-29.
47817	Fixed issue that resulted in AP's not in enabled online state after reboot.	Issue was found in SD 6.1-3-5,6.1-3-6,6.1-4-2
47821	Fixed issues that resulted in high CPU usage by XEMS process.	Issue was noticed in SD 6.1-3-6.
47844	Fixed connectivity issues with Wivia wireless client.	Issue affected AP1020i and AP822i running SD 6.1-3-5
47854	Fixed AP reboot issues.	Issue affected 4200 Virtual Controller with AP 1010/1020 running 6.1-2-29.

Bug ID	Description	Scenario
47856	Issues that caused delayed connection by APs after a network outage has been fixed.	This issue was seen in SD 6.1-2-29 and affected AP320, 332.
47857	Fixed L3 time out issues that caused users to enter the credentials for captive portal within the timeout period.	Issue affected SD 6.1-2-29
47878	Fixed controller crash issues due to hostapd service.	Issue was seen in SD 6.1-3-6,7.0-7-0
47887	Fixed connection issues faced by users connected to AP1010e/AP1020e/AP1010/AP110.	This issue was occasionally seen on AP1010e/AP1020e/AP1010/AP110 running 6.1-2-29, where users could get connected to an SSID but could pass traffic.
47932	VAP entries can be deleted after deleting an ESSID.	This issue affected SD 7.0-0SR-13,6.1-3-6
47935	A regular reboot of the controller will not trigger a failover.	The issue was seen in SD 6.1-2-29 and7.0-0SR-13 where the reboot of the controller using GUI triggered failover. This is now fixed.
48092	Fixed Ascom I62 phone connection issues.	This issue was seen after upgrading from SD 6.1-2-28 to 6.1-3-6
48095	Fixed wncagent restart issues.	The issue was seen in SD 6.1-3-6.
48096	Fixed incorrect serial number issues with AP 822v2 and 122.	This issue was seen after upgrading MC3200 controller to 6.1-3-5, where an AP-822i shows up as AP-822e. This is now fixed.
48102	Fixed controller crash due to coordinator process issues.	The issue was found in 612me-9
48124	Fixed captive portal redirection issues.	The issue was found in SD 6.1-2-29. It affected captive portal pages served via HTTP. Users were unable to get past captive portal page after entering credentials. This is now fixed.
48208	Fixed issues causing incorrect display of AP alarm status.	The issue was seen in SD 6.1-2-29
48233	Fixed issues that resulted in Service control to unresponsive.	Issue was seen in SD 6.1-2-29,6.1-2-28, 7.0-7-0
48322	Fixed issues that resulted in controller loosing running configuration.	Issue was seen in SD 6.1.3.5
48326	Fixed AP1020 reboot issues.	Issue was in SD 6.1-2-29
48345	Fixed AP832 reboot issues.	AP832 reboot happening with "NIP [c0077408] smp_call_function_single+0x158/0x184" has been fixed. This was seen in 6.1-3-5.

Bug ID	Description	Scenario
48428	Fixed network issues when multicast to unicast conversion is ON in a bridge profile.	This issue was seen when multiple clients (connected to AP832) are connected on a bridge profile with multicast-unicast ON, resulting in client communication failure. Issue was seen in SD 6.1-2-29
48442	Fixed unresponsive controller issues due to high CPU usage.	Issue affected MC4200V running SD 7.0-4-0
48467	The controller will now display the uploaded certificates and not the default certificates.	Issue affected SD 6.1-2-9
48497	Capturing packets via tshark command does not crash controller.	Issue was seen in SD 6.1-2-29
48543	Fixed power consumption issues by AP832 connected to an HP Poe+ switch.	Issue was noticed after upgrading to SD 7.0-5.
48573	Fixed AP433 crash issues with NIP [c0008fa4] cpu_idle+0xcc/0xdc	Issue was seen in SD 6.1-3-5, 7.0-5-0.
48574	Fixed AP832e crash issues with NIP [c000d514] e500_idle+0x90/0x94	Issue was seen in SD 6.1-3-5, 7.0-5-0.
48593	Fixed wncagent crashes that resulted in missing license file.	Issue was seen in SD 6.1-3-5
48673	Fixed wireless connectivity issues for client connected to AP832 running SD 6.1-3-5.	Issue was seen in SD 6.1.3.5
48699	Fixed client connectivity issues due to hostapd crash.	Issue was see in SD 7.0-5, 6.1-4-2
48760	Backup folder is now set to /opt/meru/var/upgrade to avoid disk space issues.	The was seen in SD 6.1-3-6 where full disk space in /opt/meru/var/run resulted in wncagent issues.
48784	Fixed upgrade issue while upgrading AP from 5.3.132 to 7.0.7.0 or 7.0.6.0	Issue was seen while upgrading 5.3.132 to SD 7.0.6.0, 7.0.7.0. The APs would fall back as disabled online to 5.3-132
48944	Fixed wncagent process crash issues.	Issue was seen in SD 7.0.5.0
49128	After upgrading a controller with LACP set up, the operational status now correctly shows ENABLED state.	Issue was seen in SD 7.0-7-0
49137	Fixed wncagent crash issues.	Issue was seen in SD MC4200-VE controller running SD7.0-7-0.
48851	Fixed issues that delayed leaf AP from immediately connecting to gateway AP.	Issue was seen in SD 8.0 Beta.
49022	Fixed throughput issues for clients connected to BGN radio with DPI ON.	The issue was seen in SD 8.0 Beta
49188	Internal captive portal is supported when DPI is enabled in tunnelled or bridged mode ESS profile.	The issue was seen in SD 8.0 Beta

Bug ID	Description	Scenario
43606	Fixed discovery process deadlock issues that caused APs to show up as Online/Enabled even though they not and the users are unable to connect.	This issue affected MC4200, AP320,AP832, and AP332i running SD 6.1-3-5.
48124	Fixed captive portal redirection issues.	The issue was found in SD 6.1-2-29. It affected captive portal pages served via HTTP. Users were unable to get past captive portal page after entering credentials. This is now fixed.
48258	Fixed show command access issues.	NA
48674	Fixed captive portal authentication issues.	There was an issue where users were not being authenticated after the pre-defined timeout setting. This is now fixed. Issue was seen in SD 6.1-3-6.
48921	Fixed network sluggish issues.	This issue was seen in a situation where a proxy server used 8080 as proxy port and the controller used 8080 for internal captive portal redirection. The issue was seen in SD 6.1-3-6, 6.1-4-2, 7.0-7-0.

Supported Upgrade Releases

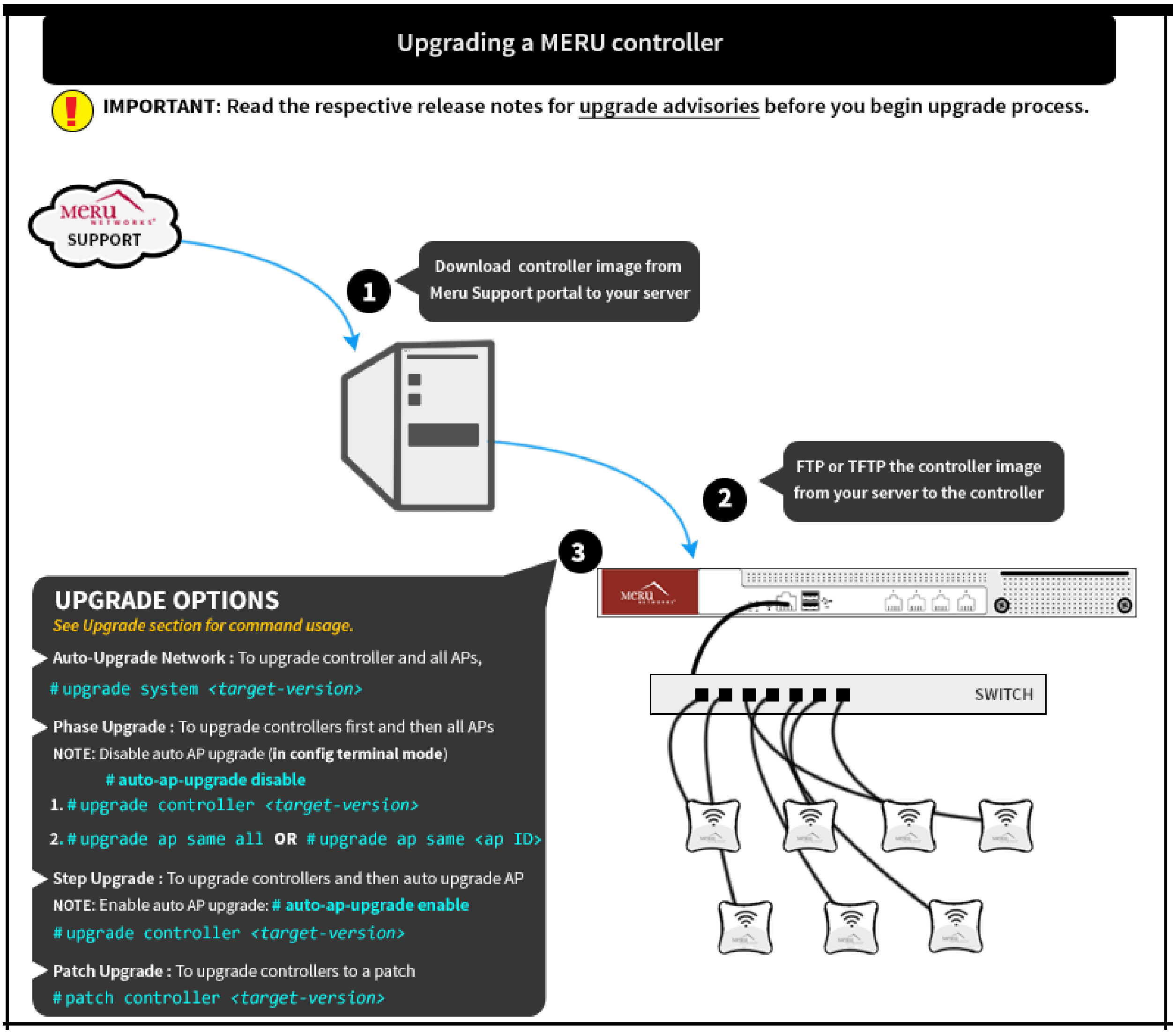
Release	GoTo Release Numbers
5.3	5.3-50, 5.3-132, 5.3-149, 5.3-153, 5.3-158, 5.3-164
NOTE	Release 5.3 requires a minimum flash size of 2GB installed in the controller. Flash sizes smaller than this will display an error message during installation.
6.0	6.0-1-0, 6.0-2-0, 6.0-10-0
6.1	6.1-0-3, 6.1-1-25, 6.1-2-28, 6.1-2-29
7.0	7.0-1-0, 7.0-2-0, 7.0-3-1, 7.0-4-0

Supported Hardware and Software

Hardware and Software	Supported	Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i AP332e, AP332i* AP433e, AP433i, OAP433e* AP433is* AP1010e, AP1010i* AP1020e, AP1020i* AP1014i* AP110* OAP832 PSM3x*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
	*Cannot be configured as a relay AP	
Controllers	MC6000	MC 5000

Hardware and Software	Supported	Unsupported
	MC4200 (with or without 10G Module) MC4200-VE MC3200 MC3200-VE MC1550 MC1550-VE	MC 4100 MC 1500 MC 1500-VE
Network Manager	8.0-7-0	
Meru Connect	15.10	
Browsers		
System Director WebUI	Internet Explorer 9 (Vista and Win XP) Mozilla Firefox 25+ (Vista and Win XP) Google Chrome 31+	
NOTE	A limitation of Firefox 3.0 and 3.5+ prevents the X-axis legend of dashboard graphs from being displayed.	
Captive Portal	Internet Explorer 6, 7, 8, and 9 Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)	

Upgrade Process



Upgrading a MERU controller

IMPORTANT: Read the respective release notes for upgrade advisories before you begin upgrade process.

1 Download controller image from Meru Support portal to your server

2 FTP or TFTP the controller image from your server to the controller

3 UPGRADE OPTIONS

See Upgrade section for command usage.

- **Auto-Upgrade Network :** To upgrade controller and all APs,

```
# upgrade system <target-version>
```

- **Phase Upgrade :** To upgrade controllers first and then all APs

NOTE: Disable auto AP upgrade (**in config terminal mode**)

```
# auto-ap-upgrade disable
1. # upgrade controller <target-version>
2. # upgrade ap same all OR # upgrade ap same <ap ID>
```

- **Step Upgrade :** To upgrade controllers and then auto upgrade AP

NOTE: Enable auto AP upgrade: **# auto-ap-upgrade enable**

```
# upgrade controller <target-version>
```

- **Patch Upgrade :** To upgrade controllers to a patch

```
# patch controller <target-version>
```

Upgrade Advisories

The following are some upgrade advisories, which you should note before you begin upgrading your network. For further assistance, please contact your customer support representative.

iOS 9 Devices

iOS 9 Devices have the following connectivity issues:

- Connectivity issues while associated to vPort enabled AP320.
- Connecting to 11w enabled security profiles.

vPort Support

The following access points **do not support** vPort:

- AP10xx
- 322

- 122
- 8xx

Devices with Intel Chipset 62xx

Wireless devices with Intel chipset 62xx series must upgrade its firmware to version 15.x.x.x.

Mesh Deployments

When attempting to upgrade a mesh deployment, it is strongly recommended that users upgrade the mesh APs individually, starting with the outermost APs and working inwards towards the Gateway APs, prior to upgrading the controller itself. Be sure to disable the auto-ap-upgrade feature when performing this task. The following procedure is recommended for optimal operation:

1. Disable the **`auto-ap-upgrade`** feature.
2. Copy the running-config to startup-config.
3. Upgrade the APs manually using `upgrade ap same all` command.

In order to prevent IP assignment problems after the upgrade, if your network utilizes VLAN configurations, ensure that the DHCP Relay Pass-through option is enabled in the following two locations:

- Configuration > Devices: Controller
- Configuration > Wired: VLAN > [Select VLAN]

Captive Portal and Meru Connect Deployment Recommendations

DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

External Portal IP Configuration:

If a NAT device is located between the controller and the MERU Connect, the IP address with which MERU Connect sees the controller, should be configured under Device > RADIUS Clients page in Meru Connect Admin portal (*http://<idm-ip-address>/admin*), . Select the RADIUS client and enter the controller IP address in the Client tab. The Meru Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Meru Connect.

Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if that fails try the MAC address" option. This removes dependency on the client's browser and security settings.

SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If you have uploaded all the certificates in the chain (from root to server), then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, goto **Server** > **SSL Settings** > **Server Certificate** tab.
- To upload rest of the chain, goto **Server** > **SSL Settings** > **Trusted CA Certificates** tab.

CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

In the WebUI

Go to **Configuration** > **Captive Portal** > **Advanced Settings** section and set **Apple Captive Network Assistant (CNA) Bypass** to **ON**.

Using CLI

Use the ssl-**server cna-bypass ON** command in config mode.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all AP's or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration** > **Devices** > **System Settings** > **Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

NOTE Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and these results in a noticeable reduction of throughput in data traffic.

IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

AP Survivability

When a bridged AP loses contact with its host controller, it will provide uptime for a default period of 120 minutes or for the time specified in controller's Link Probe (1 - 32000 minutes) setting. During this time existing clients will function normally but cannot roam between APs. New clients cannot join a bridged AP during this time.

NOTE This is not supported for APs in tunnelled mode.

Noise Level for AP332

A limitation in the driver resulted in incorrect reporting of AP332 noise levels. To avoid further confusion and till a driver fix (from chip manufacturer) is available, the noise levels for AP332 will be displayed as 0 (zero) in the output of `sh interfaces Dot11Radio statistics` command and in the **Monitor** > **Diagnostics** > **Radio** page.

WPA Modes Not Available

As per WiFi alliance regulation, the WPA modes are not displayed while creating or editing security profiles. In the WebUI, **Configuration** > **Security** > **Profiles** page has been updated and the WPA options in the L2 mode has been removed.

QoS Rules

QoS rules with no matching criteria when Match is checked will abort an upgrade. To prevent this, check QoS rules to ensure that at least one matching criteria is set for each rule if Match is set.

Downgrade Procedure

NOTE	Any controller that has been upgraded to 6.1-2 can only be downgraded to the previous release from which it was originally upgraded.

Obtain a Meru-signed image file for a downgrade from the Meru FTP site and install it on the controller before the downgrading. To downgrade to an earlier release, use the upgrade procedure.

Several configuration changes have been observed after downgrading to previous release builds. Before downgrading to any release, save your configuration to a backup file and store it on a server accessible by FTP. The saved configuration can then be used to restore your configured parameters if needed. There are two upgrade command options.

You can upgrade the controller first using the **`upgrade controller`** command and then upgrade APs using the **`upgrade ap same all`** command. You can also use the **`upgrade system`** command; this downgrades the APs first, then the controller.

NOTE	Downgrading a deployment utilizing APs specifically supported by this release (such as AP1014i) to an earlier release will result in the APs being disabled. After upgrading such a deployment back up to 6.1-2, the radio band on each AP must be reset.

Troubleshooting Upgrade Issues

Issues	Summary
Package security check failed - image controller not installed. If the target release package is prior to 3.6, you need to obtain a signed version and try again	This message can appear due to one of four problems: - As mentioned in ***Before You Begin*** section, this may indicate that the date is incorrect on the controller. Try resolving this and re-run the upgrade command. - You are attempting to upgrade from a build that is not supported for direct upgrade. Refer to the sections detailed regarding your current installed version earlier in this document to perform incremental upgrades. - You are attempting to install 5.x on an unsupported system (such as an MC3000). Contact Meru Sales for additional details regarding controller upgrade or replacement. - The download was incomplete or invalid. Delete the image and download it again to verify that it has no errors.
QoS Rule <X> matching is inconsistent	- The indicated QoS rule has no set match criteria and matching is enabled (on) for that rule. If you upgrade without correcting this, the QoS rule will be lost. - Modify the indicated QoS file by adding a matching criteria for that rule. To do this, click *Configuration > QoS > System Settings > QoS and Firewall Rules > select a rule and make changes > OK* . - Possible matching criteria are dstip-match, dstport-match, firewall-filter-id-match, netprotocol-match, packet-min-length-match, srcip-match, srcport-match.

Issues	Summary
ESS < name > is missing a < name > profile	- The indicated ESS is missing the indicated profile (security, VLAN, GRE, primary accounting server, or secondary accounting server). Add the missing profile by clicking *Configuration > Wireless > ESS > select an ESS and make changes > OK* . - If you upgrade without correcting this, the ESS will be lost.

Support and Contact

In addition to the release notes, the following documentation is available.

- System Director Getting Started Guide
- System Director Command Reference
- System Director Configuration Guide
- Controller Installation Guide
- Access Point Installation Guides

RMA Procedures

Contact Customer Services and Support for a Return Material Authorization (RMA) for any equipment. Please have the following available when making the call:

- Company and contact information
- Equipment model and serial numbers
- Software release and revision numbers
- Description of the symptoms

Contact

For the first 90 days after you buy a Meru product, you have access to the online support. If you have a support contract, you have access for the length of the contract. See the web site http://support.merunetworks.com for information such as:

- Knowledge Base (Q&A)
- Downloads
- Open a ticket or check an existing one
- Customer Discussion Forum

For assistance, contact Customer Services and Support 24 hours a day toll-free at 888-637-8952 or at 650-385-3144. Send email to csm@fortinet.com.

Customer Services and Support provide end users and channel partners with the following:

- Telephone technical support
- Software update support
- Spare parts and repair service