What’s New in Campus Manager 5.1

New Features in This Release

The following are the new features and enhancements available in Campus Manager 5.1:

- Auto Allocation of Devices
- MAC Detection and Reporting
- Integration with IPM, HUM and DFM for Topology Maps
- Enhanced Discrepancy and Best Practices Deviation Report
- Enhanced Topology in ACS Environment
- User Tracking Summary Portlet
- VSS Support

Note
ATM Management and Path Analysis that were supported in the previous releases of Campus Manager, has been removed in Campus Manager 5.1.

Auto Allocation of Devices

Devices can be added to Campus Manager in two modes:

- Auto
- Manual

In Auto Management mode, Campus Manager 5.1 allows you to manage devices in groups

There are two types of groups available:

- System-defined groups
  System-defined groups are automatically created, based on the information in DCR.
- User-defined Groups
  You can create User-defined groups based on your requirements.

  For example, if you want to manage only devices with IP address in the range 10.77.*.* in Campus Manager, create a group for those devices in Common Services and add it to Campus Manager in the Auto mode settings page. These devices will be managed in Campus Manager after you run Data Collection.

  For details, see Device Management.
MAC Detection and Reporting
Campus Manager 5.1 detects New MACs, Rogue MACs and Dormant MACs that are in the network.

- Dormant MAC
  MAC Addresses that are inactive for the specified number of days.
- New MAC
  MAC Addresses that are newly added to your network.
- Rogue MAC
  MAC Addresses that are not authorized to exist in your network.

This feature allows you to:
- Configure Campus Manager to send e-mails when New MACs are added to the network and Rogue MACs are detected in the network. For details, see Modifying Acquisition Settings.
- Define the list of MAC addresses are to be classified as unauthorized addresses in the network. For details, see Configuring Rogue MAC List.
- Generate reports to get information on the New MACs, Rogue MACs and Dormant MACs in the network. For details, see Viewing MAC Reports.

Integration with IPM, HUM and DFM for Topology Maps
From Topology Maps and N-Hop view Portlets, you can:
- View DFM information. If an alert is associated with a device, you can see icons displayed along with the devices. These icons indicate the severity of the alert.
- Launch the DFM report that displays information on the alerts and events that are associated with the device.
- Launch the Create Collectors page in IPM to create collectors on IPSLA capable devices.
- Launch the Collectors page in IPM to view details on collectors that have already been created.
- Launch the Device Dashboard page in HUM that provides the performance details of the device.
- Launch the Interface Report in HUM that displays the previous hour data for a link.

You can launch the application pages, if DFM, HUM, and IPM are installed on a local server or on a remote server with a Master-Slave setup.

For details see, Starting CiscoWorks Applications From Topology Views.

Enhanced Discrepancy and Best Practices Deviation Report
You can fix the following Best Practices Deviation through Campus Manager 5.1:
- Channel port in Auto mode
- Trunk ports in Auto mode
- Non-channel port in Desirable mode
- Non-trunk ports in Desirable mode

For details, see Interpreting Best Practices Deviations.
The following discrepancies are removed from Campus Manager 5.1:

- DRIP Enabled VLAN
- ATM-VLAN that do not have an entry in Lane Config server
- ATM-VLAN with Lane Server that do not have an entry in Config server
- Partitioned ATM-VLAN
- More than one Config server in single ATM-Fabric

Enhanced Topology in ACS Environment

Topology Maps normally display all the devices discovered by Campus Manager. When Campus Manager is integrated with the ACS server, you can set Topology Maps to display only the devices you are authorized to view.

For details, see Restricted Topology View.

User Tracking Summary Portlet

The User Tracking Summary Portlet displays the following data:

- Number of End hosts
  You can click the number link to launch the End Hosts Immediate Reports page.
- Number of Active End hosts
  End Hosts that are currently connected to the network are called Active End hosts. You can click the number link to launch the Active End Hosts Immediate Report page.
- Number of Dormant hosts in the last 12 days
  Displays the number of hosts that are inactive for 12 days. The number of days depends on the days configured in the Configuration screen.
- Number of New hosts in the last 12 days
  Displays the number of new hosts in the last 12 days. The number of days depends on the days configured in the Configuration screen.
- Number of Rogue hosts in the last 21 days
  Displays the number of rogue hosts in the last 21 days. The number of days depends on the days configured in the Configuration screen.

For more details, see the User Guide for LMS Portal 1.1.

VSS Support

The Virtual Switching technology is the process of combining two standalone distribution switches in the local distribution layer, into a single management point. The Virtual Switching System (VSS) functions and appears as a single switch to the wiring closet and the core layer.

See the User Guide for Resource Manager Essentials 4.2, for more details on:

- VSS Support
- Prerequisites for conversion to VSS
- VSS Configuration Process

Note

Only VSS-capable standalone Cisco Catalyst 6000 switches can be converted into a Virtual Switching System.
If the following devices are available in DCR, Campus Manager manages VSS as follows:

- **Device A**
  - IP Address—10.77.240.1
  - Display Name —Switch 1
- **Device B**
  - IP Address—10.77.240.2
  - Display Name —Switch 2

Campus Manager manages these devices as normal Catalyst 6000 devices.

You can configure the above devices as VSS through RME, with Device A as the Master and Device B as the Slave. After this configuration, RME adds another device in DCR with the following credentials:

- IP Address of the Master device—10.77.240.1
- sysOID of the VSS device—1.3.6.1.4.1.9.1.896
- Display name—VSS_10.77.240.1

Now DCR contains three devices instead of two:

- 10.77.240.1— Switch 1
- 10.77.240.2 — Switch 2
- 10.77.240.1—VSS_10.77.240.1

When Data Collection runs, the following occurs:

- 10.77.240.1 — Switch 1 will be deleted from Campus Manager
- 10.77.240.2 — Switch 2 will be managed in Campus Manager as an unreachable device
- 10.77.240.1—VSS_10.77.240.1 will be added to Campus Manager

With this VSS device, you can perform all Campus Manager operations that are applicable for normal Catalyst 6000 devices.

VSS re-configuration is not supported in RME. You have to manually reconfigure the devices to remove VSS. In that case, all the above mentioned three devices will be present in DCR. You must delete the VSS device from DCR before running Data Collection. Otherwise the results will be unpredictable.