



# Integrating Campus Manager With CiscoWorks Common Services

---

This chapter details the various CiscoWorks Common Services features that are integrated with Campus Manager 4.0.3. The features covered in this chapter are:

- [Understanding Common Services-ACS Integration, page 5-1](#)
- [Understanding DCR Integration, page 5-3](#)
- [Understanding Object Grouping Services Integration, page 5-8](#)
- [Understanding CiscoWorks Homepage Integration, page 5-8](#)
- [Understanding Device Center Integration, page 5-9](#)
- [Understanding Software Center Integration, page 5-9](#)
- [Understanding License Integration, page 5-10](#)

## Understanding Common Services-ACS Integration

Common Services 3.0.3 (CS) security model provides five standard roles:

- Help Desk
- Approver
- Network Operator
- Network Administrator
- System Administrator.

Campus Manager application features are mapped to CS User Roles. Campus Manager 4.0.3 integrates CS 3.0.3 security model with ACS (Access Control Server) to provide granular role definitions.

Campus Manager 4.0.3 application features are defined as a set of tasks. For a list of Campus Manager 4.0.3 tasks, see Common Services Permission Report. (**Common Services > Server > Reports > Permission Report**)

In CS mode, you can perform any operation on the device view as well as perform any operation on all the devices, if authorized for the corresponding tasks.

In ACS mode, you can view the devices. However, you are not allowed to perform a task for which you have no authorization. If you try to perform the task, Campus Manager displays an error message.

For example, in ACS mode, when you launch Topology Services window, you can view all the devices. All the devices includes devices whose groups you have not mapped to in the ACS server.

However, if you select a task that is related to configuration or IP change management on a device that you are not authorized to work on, an error message appears.

The following case applies when you select Per Network Device Group as the mode of authorization in the ACS server.

Suppose you (with Network Admin role in Common Services) are authorized to perform the following tasks in ACS mode. Let us assume that the same tasks are applicable to a user with Network Admin Role in Common Services.

- View\_topo
- View\_path
- View\_vpa
- View\_ut
- View\_Reports
- View\_AniAnalysis
- Config\_Vlan
- Config\_VlanPort
- Config\_UT
- Config\_MgmtIP
- Discover\_TopoDevices

- Discover\_UTEndHosts
- Export\_data

In ACS, assume that you are assigned to a device group with devices ip1, ip2, and ip3. You are not assigned to another device group that contains the devices ip4, ip5, and ip6.

If you launch Topology Services, you can view all the devices in the Topology Map window.

If you right-click and select **Change Management IP Address**, and the Change Management IP Address dialog box is launched since you are authorized for the task Config\_MgmtIP. You can perform the task.

If you right-click and select **Delete Device**, an authorization error appears, as you are not authorized for the task, Delete\_device.

## Understanding DCR Integration

Device and Credential Repository (DCR) is a set of tables that stores device information and their credentials. DCR Server, a Common Services component, is a daemon process.

Managing devices and end hosts in Campus Manager is a three-step process:

- Device Discovery
- Data Collection
- User and Host Acquisition

Device Discovery is a transient process initiated by the Campus Manager Server. This process discovers the devices in the network and collects basic information about devices in the network. Data Collection runs as a daemon.

It fetches data from devices and computes topology and network discrepancies. User and Host Acquisition is a transient process initiated by the Campus Manager Server. It discovers end hosts and IP phones in the network.

This section contains:

- [Role of CS Peer Server Account in ACS Mode, page 5-4](#)
- [Integration of Device Discovery With DCR, page 5-4](#)
- [Usage of Credentials, page 5-5](#)

- [Updating DCR, page 5-6](#)
- [Data Collection and DCR, page 5-6](#)
- [Handling DCR Events, page 5-7](#)

## Role of CS Peer Server Account in ACS Mode

Device Discovery and Data Collection get the devices from DCR with Peer Server Account privileges. The Peer Server Account should be allowed to perform Add, and View tasks of DCR.

In ACS mode, Data Collection is performed for all devices that are assigned to Peer Server Account in ACS. So all device groups in ACS that need Data Collection to be performed have to be mapped to Peer Server Account.

In other words, the Peer Server Account should be authorized for any network group, and should be provided with sufficient privileges to add and view devices in DCR.

## Integration of Device Discovery With DCR

Credentials are values that are used by applications to access and operate on devices. A device credential is used to access a managed device such as a switch or router. It is typically an SNMP community string or a user ID and password pair.

To discover the network, the Device Discovery process needs the SNMP credentials of the devices in the network. Campus Manager 4.x uses the `discoverysnmp.conf` file to store the credentials.

Similarly, other applications in the CiscoWorks suite have different ways of storing device credentials.

For easy management of device credentials, Common Services uses a new the Device and Credential Repository (DCR). DCR stores the list of devices and their credentials.

The Device Discovery process interfaces with DCR for credential information. Initially DCR could be empty. So, Device Discovery uses the credentials from `discoverysnmp.conf`, discovers the network and stores the list of devices and their credentials in DCR.

For further discoveries, all devices in DCR, and the devices configured in `DeviceDiscovery.properties` file, form the seed devices list.

## Usage of Credentials

The following scenarios are possible when Device Discovery tries to discover devices:

- DCR is empty (in cases where no other application has updated DCR)
- DCR already has the credential information for the devices in the network.
- Devices are running SNMPv2 or SNMPv3.

Considering these factors, the following logic is applied while using credentials:

### Case 1: Device is NOT in DCR

- Credentials from `discoverysnmp.conf` are used.
- If the credentials given in `discoverysnmp.conf` are wrong, the device is not discovered and is marked as unreachable.

### Case 2: Device is in DCR

- The credentials are taken from DCR.
- If the credentials in DCR are wrong, `discoverysnmp.conf` is searched for the correct credentials.
- If `discoverysnmp.conf` has SNMPv3 credentials for the device, Device Discovery discovers the devices with these credentials.
- If `discoverysnmp.conf` has SNMPv2 credentials for the device, Device Discovery discovers the devices with these credentials.
- If SNMPv2 and SNMPv3 credentials are available for a device (either in DCR or `discoverysnmp.conf`), only SNMPv3 credentials will be used. There is no fallback to SNMPv2.
- Multiple Community String feature is applicable only to SNMPv2.

After discovery completes, DCR is updated with the following SNMP credentials.

- SNMPv2 read-only community string (if SNMPv2 was used for communicating with the device)
- SNMPv3 userid, password, engineID, authorization algorithm (if SNMPv3 was used for communicating with the device).

Device Discovery does not update SNMPv2 write community string as it has no way of checking if the given write community string is valid or not.

## Updating DCR

When the network is discovered, Device Discovery updates the following device attributes in DCR:

- Host Name
- Domain Name
- Management IP Address
- Display Name
- SysObjectId
- MDF Device Type

## Data Collection and DCR

The information that is fetched during Device Discovery is minimal and is not specific to Campus Manager. Device Discovery does not compute topology, does not discover end hosts, and does not compute network discrepancies.

Hence, discovering devices using Device Discovery process does not mean managing devices in Campus Manager. Campus Manager has to perform Data Collection to manage devices. Data Collection Server does Data Collection, at scheduled intervals, on the devices in DCR.

Data Collection involves the following steps:

1. Data Collection Server gets the list of devices and their credentials from DCR.
2. It polls these devices, fetches information that is required for topology computation, reporting network discrepancies, and for various reports and device configurations.

If the credentials in DCR are incorrect for any reason, the devices are reported as unreachable in Campus Manager. For Data Collection, the credentials are never picked up from `discoverysnmp.conf`.

It is not mandatory that Data Collection be done for all devices in DCR. You can choose or restrict the devices to be managed by Campus Manager, using IP address or VTP domain filters. For more details, see [Setting up Data Collection Filters, page 4-22](#).

## Handling DCR Events

Data Collection Server gets the list of devices and credentials from DCR during every Data Collection. It is possible that other applications add new devices or update attributes of devices in DCR.

DCR Server provides an event mechanism to inform the applications about these changes. For Campus Manager to be in synchronization with DCR, Data Collection Server listens to update and delete events from DCR.

When Data Collection Server receives an update event for a device or a set of devices, it synchronizes the credential information for them.

When Data Collection Server receives a delete event for a set of devices, it deletes the devices from Campus Manager database. All Campus Manager views reflect this change immediately.

Whenever there is a change in Management IP address in Campus Manager, the Data Collection Server sends an event to DCR Server. DCR Server updates the Management IP address attribute accordingly.

# Understanding Object Grouping Services Integration

The Grouping Services is a framework for grouping arbitrary objects, including devices. Grouping Services helps in creating, managing, and sharing groups of objects.

Multiple applications share a group managed by Grouping Services. It provides tools that allow you to define groups useful to your application. After you have defined the groups you want, you can supply them in a predefined form with your application.

# Understanding CiscoWorks Homepage Integration

The CiscoWorks Homepage (CWHHP) for Common Services provides launch points for applications and their major functions. CWHHP is based on HTML and allows you to move among CiscoWorks Homepage and all other Product Homepages.

The Application Panel in the CiscoWorks HomePage serves as a top-level launch point for all Common Services applications installed on the local or remote server.

The Applications User Interface appears in a tree window component. By default, only the first level items are displayed when you log in. These first level items are in collapsed mode. Lower level navigations are displayed only if you manually expand a first level item.

The title of each Application Panel displays the application name and it serves as a link to the relevant Application Home Page. The Expand/Collapse icon next to the title expands or collapses the entire window component.

The Campus Manager application panel contains:

- Topology Services
- Path Analysis
- User Tracking
- VLAN Port Assignment
- Discrepancy Reports
- Administration

# Understanding Device Center Integration

Device Center provides a one-stop place where you can see a summary for a device and the various tools, reports, and tasks that you can perform on a selected device. Device Center helps you access device-centric features and information from a single location.

After launching Device Center, you can invoke many tools on the selected device from a single location. The various features in Device Center come from the CiscoWorks applications installed on the server.

The device details related to Campus Manager that are available in the various sections are:

- Summary
  - Device IP Address
  - Device Type
  - CDP Neighbors
- Reports
  - Switch Port Usage Report - Recently Down
  - Switch Port Usage Report - Unused Down
  - Switch Port Usage Report - Unused Up
  - UT End Host Report

# Understanding Software Center Integration

Campus Manager releases Service Packs (SP) every three months and these updates are available through Cisco.com. Campus Manager integrates with Software Center, also known as Package Support Updater (PSU), and uses its download service.

You can check the latest SP available for Campus Manager and download it, if required, using Software Center.

# Understanding License Integration

Campus Manager uses the Common Services licensing framework for licensing. Licensing is based on the number of devices.

Devices managed by Campus Manager are determined during Data Collection and not during Device Discovery. Therefore, Discovery might discover more devices than indicated by the Campus Manager license.

The license is validated while launching different applications of Campus Manager such as Topology Services. If the license is expired, or not valid, you are prompted to obtain a valid license.

The following are the use case scenarios for Campus Manager based on the Common Services licensing framework.

## Behavior prior to license expiration (nagging)

This behavior applies to all users:

- A Nag message appears 10 days before a license expires.
- A message appears before expiration of license and when the device limit is crossed.
- When you add devices, you are warned if the device count is close to the configured limit ( $\pm 10\%$  of limit or 100 whichever is lower).
- A message appears if the device limit is crossed. However, it allows up to 10% of additions to succeed (or 100, whichever is lower).

## Behavior when license period expires

This behavior applies to all users:

- Campus Manager displays the License Expired page after the license expires.
- User Tracking CLI and Data Extraction Engine (DEE) checks expiry and stops after displaying the License Expired message.
- User Tracking and Path Analysis do not allow any scheduled jobs in the system.
- Backup and Restore processes backup and restore the license file. The behavior is consistent with the bundle-level behavior.

**Impact of Licensing Device Limit.**

A network might have more devices than what is allowed by the product specific license. In such cases, Campus Manager manages only the number of devices allowed by the license.

For example, consider a network which has 1000 devices. Assume that the license is only for 300 devices.

In this case, Device Discovery discovers all the 1000 devices and stores the credentials in Device and Credential Repository. Campus Manager manages only the first 330 devices ( $\pm 10\%$  of the allowed license limit) in DCR. However, you are prompted to upgrade the license.

Since Data Collection is done on a partial set of devices, it is possible that some of the devices are placed under Topology Services Unconnected Views.

In this case, you have to either upgrade to the unrestricted version of the license or apply the IP Address / VTP Domain filters in order to manage only the devices within the current license limit.

