Device and Credential Repository

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials. The Device and Credential Admin provides an interface to administer DCR. See, Administration Guide for Cisco Prime LAN Management Solution 4.2 for more information.

To access DCR, select Inventory > Device Administration > Add / Import / Manage Devices.

This section contains Understanding DCR.

For more information on:
- Discovering devices, see Discovering Devices.
- Managing devices, see Managing Devices and Credentials.
- AUS servers, see Managing Auto Update Servers.

Understanding DCR

DCR provides:
- A central place where you can add or import new devices.
- Easier and faster access to device and credential data.
- Secure data persistence, access and transport.
- Rationalized and controlled replication, with less user-level data reconciliation.
- Better integration with third-party and Cisco network-management applications.

DCR also:
- Stores device attributes and credentials, permits dynamic creation of attribute types, and permits default grouping and filtering.
- Supports proxy device attributes, unreachable devices, and pre-provisioning of devices.
- Allows you to populate the repository by importing devices from many sources. It also allows you to export device data to be used with third-party network management systems such as NetView and HP OpenView Network Node Manager.
- Uses a unique Internal Device Identifier to access device details, and detects duplicate devices based on specific attributes.
- Encrypts credential data stored in the repository. Access to device data is permitted only by secured channel and client authentication.
- Supports IPv6 and SNMP v3.
Understanding DCR

This section contains the following:

- Device Types
- Device Attributes
- Device Credentials
- DCR Architecture

### Device Types

DCR supports the following four types of device:

- **Standard type**
  Devices such as Routers, Switches, Hubs, and other common devices are managed using this management type.

- **AUS Managed devices**
  The Cisco Prime Auto Update Server is a web-based interface for upgrading device configuration files and software images on firewalls that use the auto update feature. You can use this interface to add, edit, and delete devices.

- **Cluster Managed devices**
  The Cisco clusters and their member devices are managed using this device management type.

- **CNS Managed devices**
  The CNS managed devices refer to the devices managed by Cisco Networking Services.

- **Non-Cisco Devices**
  Many Non Cisco devices are categorized as Non-Cisco Devices. The sysOIDs of the supported Non-Cisco Devices in LMS are available in the mdfdata_NonCisco.xml located at:
  - \NMSROOT\lib\classpath\com\cisco\nm\cwcs\mdf\mdfdata_NonCisco.xml (on Windows)
  - /opt/CSCOpx/lib/classpath/com/cisco/nm/cwcs/mdf/mdfdata_NonCisco.xml (on Solaris and Soft Appliance)

  The Non-Cisco Devices that are not listed in the above file will be classified as Unknown devices.
  - Non-Cisco Devices are not considered for license check in UDM. If these devices match the device management policy, they will be in managed state.
  - Once the Non-Cisco Devices are moved to the managed state, it triggers the MIB II level of inventory, Config and Image Management support and data collection.
  - Config and SWIM functionalities are not supported. Only system and interface information (MIB II) is collected for Non-Cisco devices through Inventory.
  - For IPSLA Performance Management, Target can be a non-Cisco device but responder should be a Cisco device.
  - For Device Performance Management:
    - Non-Cisco devices will be managed using MIB II variables automatically
    - Support for third party MIBs for Non-Cisco devices. The third party MIB file should have .my extension.
• Interface-related system-defined pollers will not work as Interface pollers are dependant on the Network Topology, Layer 2 Services and User Tracking module, and the Inventory, Config and Image Management module for getting the PMC port details. If you create a user-defined poller, devices can be polled using the Interface-related template.

• The following five system-defined templates can be used for Non-Cisco devices:
  - Device Availability
  - Interface Availability
  - Interface Utilization
  - Interface Errors
  - PoE PSE Consumption

• In LMS 4.2, for Fault Management, Non-Cisco devices will be moved to known state and trap support is provided for Non-Cisco devices.

The following are the list of events that are supported for Non-Cisco and Unknown devices:
  - Unresponsive
  - OperationallyDown
  - Flapping
  - Duplicate
  - HighBroadcastRate
  - HighDiscardRate
  - HighErrorRate
  - HighQueueDropRate
  - HighUtilization – On interfaces only
  - All Pass-Through Standard SNMP Traps

**Note**
For Non-Cisco and Unknown devices, only interface and ports details are managed.

• For CiscoView, Non-Cisco devices are not supported

• For Network Topology, Layer 2 Services and User Tracking:
  - Data collection will collect non-Cisco device detail like, sysOID, hostname, syslocation.
  - The device selector will not show the non-Cisco devices.
  - Topology services will show non-Cisco device in unconnected view.
  - The delete device, data collection, rediscover, telnet and SSH menu items will be enabled for non-Cisco devices.
  - User Tracking will not discover users and hosts in a network connected to non-CDP devices.
  - The device attributes, port attributes, VLAN report, Change Management IP, IVR configure and Add to critical poller menu item will be disabled for non-Cisco devices.
Device Attributes

Device attributes are unique to each device and are used to identify device properties, such as device name and host name. See Mandatory Device Attributes for more information on mandatory device attributes.

The following attributes are stored in the repository:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_name</td>
<td>Device Host name.</td>
</tr>
<tr>
<td>domain_name</td>
<td>Domain name of the device.</td>
</tr>
<tr>
<td>management_ip_address</td>
<td>IP Address used to access the device. Both IPv4 and IPv6 address types are supported.</td>
</tr>
<tr>
<td>device_identity</td>
<td>Identifies pre-provisioning devices. The value is application specific.</td>
</tr>
<tr>
<td>display_name</td>
<td>Device name, as you want it to be represented in reports or graphical displays. Can be derived from Host Name, Management IP Address or Device Identity.</td>
</tr>
<tr>
<td>sysObjectID</td>
<td>sysObjectID value of Cisco or non-Cisco devices. It may be UNKNOWN if the facility that populates the repository is not aware of the value.</td>
</tr>
<tr>
<td>mdf_type</td>
<td>Normative name for the device type as described in Cisco’s Meta Data Framework (MDF) database or other vendor’s MDF database. Each device type has a unique normative name defined in MDF.</td>
</tr>
<tr>
<td>DCR Device ID</td>
<td>Internally generated unique sequential number that identifies the device record in the DCR database. The DCR clients should know the value to access device details from the repository.</td>
</tr>
</tbody>
</table>

User Defined Fields (UDF)

- DCR Administration, by default, provides four UDFs. These fields are used to store additional user-defined data for a device.
- DCR supports a maximum of ten UDFs.
- You can add six more UDFs to DCR Administration. You can rename or delete all the UDFs including the four default UDFs provided by DCR Administration.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_mode</td>
<td>Current transport mode.</td>
</tr>
<tr>
<td>http_port</td>
<td>The HTTP Port.</td>
</tr>
<tr>
<td>https_port</td>
<td>The HTTPS Port.</td>
</tr>
<tr>
<td>cert_common_name</td>
<td>Certificate Common Name.</td>
</tr>
</tbody>
</table>

Individual applications interact with the repository to get the device list, device attributes, and device credentials.

Mandatory Device Attributes

The mandatory attributes are:

- Management IP Address or Host Name or Device Identity.
• Device Name.

Apart from these attributes, there are few attributes that are mandatory for each management type of devices. They are:

• CNS managed devices — CNS Server is mandatory.
• AUS managed devices — Auto Update Device ID and Auto Update Server fields are mandatory.
• DSBU Cluster managed devices — DSBU member number is sufficient.

The Device Name and the Host Name/Domain Name combination must be unique for each device in DCR. A device will be considered duplicate if:

• The Device Name of a device is the same as the Device Name of any other device.
• The Host Name/Domain Name combination of a device is the same as that of any other device.
• Auto Update Device ID is the same as Auto Update Device ID of any other device (when the device is AUS managed)
• Cluster and Member Number, together is the same as that of any other device (when the device is Cluster managed)

Note: DFM is the only application in LMS that does not consider the device name configured in DCR. Instead, DFM does its own resolution on the IP address to get a hostname. Ensure that DNS or host file is properly configured so that the IP address being managed by DFM resolves to a hostname, and that hostname resolves back to that IP address.

Device Credentials

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

Credentials are encrypted and stored in DCR. The maximum length of a credential after encryption is 128 characters and credentials must not exceed this limit.

This section contains the following:

• Device Credentials in DCR
• Secondary Credentials
• SNMP Credentials
• Device Credentials of Other Management Types

Device Credentials in DCR

The following credentials can be associated with a device in DCR:

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary_username</td>
<td>Primary username used to access the device.</td>
</tr>
<tr>
<td>primary_password</td>
<td>Password for the Primary username.</td>
</tr>
</tbody>
</table>
### Understanding DCR

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary_enable_password</td>
<td>Console-enabled password for the device. Allows you to make configuration changes and provides access to a larger set of commands. Without the enable password, users are restricted to read-only operations.</td>
</tr>
<tr>
<td>secondary_username</td>
<td>Secondary username used to access the device, when device access using the primary credentials fails.</td>
</tr>
<tr>
<td>secondary_password</td>
<td>Password for the secondary username.</td>
</tr>
<tr>
<td>secondary_enable_password</td>
<td>Console-enabled secondary password for the device. Allows you to make configuration changes and provides access to a larger set of commands, when device access using the primary console-enabled password fails. Without the enable password, you cannot make any configuration changes. You can perform read-only operations.</td>
</tr>
<tr>
<td>rxboot_mode_username</td>
<td>Special case username (for example, RxBoot mode in 2500).</td>
</tr>
<tr>
<td>rxboot_mode_password</td>
<td>Password for the Rx Boot Mode user.</td>
</tr>
<tr>
<td>snmp_v2_ro_comm_string</td>
<td>SNMP V2 read-only community string of the device.</td>
</tr>
<tr>
<td>snmp_v2_rw_comm_string</td>
<td>SNMP V2 read/write community string of the device.</td>
</tr>
<tr>
<td>snmp_v3_user_id</td>
<td>SNMP V3 user ID of the device.</td>
</tr>
<tr>
<td>snmp_v3_password</td>
<td>SNMP V3 password of the device.</td>
</tr>
<tr>
<td>snmp_v3_engine_id</td>
<td>SNMP V3 engine ID of the device.</td>
</tr>
<tr>
<td>snmp_v3_auth_algorithm</td>
<td>SNMP V3 authentication algorithm used. Can be MD5 or SHA-1.</td>
</tr>
<tr>
<td>snmp_v3_priv_algorithm</td>
<td>SNMP V3 privacy algorithm used in AuthPriv mode. Can be DES, 3DES, AES128, AES192, and AES256.</td>
</tr>
<tr>
<td>snmp_v3_priv_password</td>
<td>SNMP V3 privacy password of the device in AuthPriv mode.</td>
</tr>
<tr>
<td>http_username</td>
<td>HTTP-interface user ID of the device.</td>
</tr>
<tr>
<td>http_password</td>
<td>HTTP-interface password of the device.</td>
</tr>
<tr>
<td>secondary_http_username</td>
<td>HTTP-interface secondary user ID of the device.</td>
</tr>
<tr>
<td>secondary_http_password</td>
<td>HTTP-interface password for the secondary user ID of the device.</td>
</tr>
</tbody>
</table>

### Additional Credentials for Cluster Managed Devices

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsbu_member_number</td>
<td>Number of the Cluster member. This number represents the order in which the device was added to the cluster.</td>
</tr>
<tr>
<td>parent_dsbu_id</td>
<td>DCR Device ID of the parent Cluster device.</td>
</tr>
</tbody>
</table>

### Auto Update Server Specific Credentials

<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aus_url</td>
<td>URL for the AUS device.</td>
</tr>
<tr>
<td>aus_port</td>
<td>Port number of the AUS service running on the AUS device.</td>
</tr>
<tr>
<td>aus_username</td>
<td>User login providing access to the AUS device.</td>
</tr>
<tr>
<td>aus_password</td>
<td>Password for the corresponding aus_username.</td>
</tr>
</tbody>
</table>
Chapter 2  Device and Credential Repository

Understanding DCR

Secondary Credentials

DCR stores both the primary and secondary device credentials. Secondary credentials comprise a username, a password and a console-enabled password for the devices. You can use the secondary credentials as a fallback to access the devices if you cannot access them using primary credentials.

For example, assume you have configured devices in your network to be in TACACS mode and you have stored the TACACS credentials as the primary credentials. The local username and password are stored as secondary credentials to access devices. If the AAA server is not running, you cannot access the devices using primary TACACS credentials. Instead, you can use the secondary credentials as a fallback to access the devices in your network.
SNMP Credentials

The SNMP credentials are used to access the devices in the network.

DCR stores both:
- SNMPv2 credentials
- SNMPv3 credentials for all security levels.

The SNMPv3 protocol provides the security features such as message integrity, authentication, and encryption based on the security levels.

The following table lists the SNMP security levels and the SNMP credentials stored in DCR for each level:

<table>
<thead>
<tr>
<th>SNMP Version</th>
<th>Security Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>SNMP Credentials in DCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2</td>
<td>NoAuthNoPriv</td>
<td>Uses a community string match for authentication</td>
<td>Not Supported</td>
<td>• snmp_v2_ro_comm_string</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• snmp_v2_rw_comm_string</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>NoAuthNoPriv</td>
<td>Uses a username match for authentication</td>
<td>Not Supported</td>
<td>• snmp_v3_user_id</td>
</tr>
<tr>
<td>AuthNoPriv</td>
<td></td>
<td>Provides authentication based on the</td>
<td>Not Supported</td>
<td>• snmp_v3_user_id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authentication algorithms (MD5 or SHA)</td>
<td></td>
<td>• snmp_v3_password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides authentication based on the</td>
<td>Provides encryption</td>
<td>• snmp_v3_auth_algorithm</td>
</tr>
<tr>
<td>AuthPriv</td>
<td></td>
<td>authentication algorithms (MD5 or SHA)</td>
<td>on the privacy algorithm</td>
<td>• snmp_v3_auth_algorithm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>such as DES, 3DES, AES128, AES192, and AES256</td>
<td>• snmp_v3_password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• snmp_v3_priv_algorithm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• snmp_v3_priv_password</td>
</tr>
</tbody>
</table>

1. SNMPv2 supports only the NoAuthNoPriv security level.

During the configuration of SNMP credentials, if you:
- Specify only SNMPv3 username, this denotes that the SNMPv3 security level is NoAuthNoPriv.
- Specify SNMPv3 username, SNMPv3 password and SNMPv3 authentication algorithm, this indicates that the SNMPv3 security level is AuthNoPriv.
- Specify SNMPv3 username, SNMPv3 password, SNMPv3 authentication algorithm, SNMPv3 privacy algorithm, and SNMPv3 privacy password, this indicates that the security level is AuthPriv.
Device Credentials of Other Management Types

DCR supports Cisco Cluster Management Suites, Auto Update Servers and the managed devices, CNS Configuration Engine and CNS Managed devices, using a mix of standard and additional attributes and credentials.

- Clusters: All the attributes of the Cluster are the same as a normal DCR device.
- Cluster Members: Each cluster member has its own Host Name, sysObjectID, and MDF type, and uses the same Telnet credentials as the Cluster. Each cluster member has the following additional attributes:
  - Member Number: Number of the Cluster member. This number represents the order in which the device is added into the cluster.
  - Device ID of the Parent Cluster record.
- Auto Update Server: This has the following attributes and credentials:
  - URN
  - Username
  - Password
- Auto Update Server managed devices: Apart from having its own attributes and credentials as normal DCR devices in DCR, each Auto Update Server managed device has the following additional attributes:
  - Device Identity: String value that uniquely identifies this device in the parent Auto Update Server.
  - DCR Device ID of the Parent Auto Update Server record.

DCR Architecture

The sharing of device list and credentials among various network management products is achieved through a Client-Server mechanism. The clients are network management applications that use DCR. The server is called the DCR Server.

DCR works based on a Master-Slave model. The DCR mode is set to Standalone, by default.

This section contains:

- Master DCR
- Slave DCR
- Standalone DCR

Master DCR

Refers to the master repository of device list and credential data. The Master hosts the authoritative, or a master-list of all devices and their credentials. All other DCRs in the same management domain that are running in Slave mode, normally shares this list.

There is only one Master repository for each management domain, and it contains the most up-to-date device list and credentials.
DCR Master Server communicates with its Slaves through the HTTPS port. If there is a firewall in between the LMS Servers of the same DCR management domain, you must:

- Open the HTTPS port of LMS Servers for communication.
- Permit the ICMP requests and responses between the LMS Servers.

Only then the peer certificates can be exchanged and the communication could happen between the DCR Master and Slave servers.

Changes to the repository data in DCR Master are properly propagated to Slaves although you block or close the HTTPS port of DCR Slave Server in firewall. However the DCR status of Slave server is displayed as Unreachable in DCR Master.

But you should never block the HTTPS port of DCR Master Server in firewall. Otherwise communication between the servers in the same management domain will not happen.

**Note**

The default HTTPS port is 443. You can change the default HTTPS port number to some other port number.

**Slave DCR**

Refers to a repository that is an exact replica of the Master.

DCR Slaves are slave instances of DCR in other servers and provide transparent access to applications installed in those servers.

Any change to the repository data occurs first in the Master, and those changes are propagated to multiple Slaves. There can be more than one Slave in a management domain.

The Slave:

- Maintains an exact replica of the data managed by the Master for the management domain.
- Has a mechanism to keep itself synchronized with the Master.
- Will first update Master and then update its own repository data. This is in case of repository data updates.

DCR running in Master or Slave mode always has an associated DCR Group ID that indicates the Server's management domain. This Group ID is generated when a DCR is set to Master mode, and communicated to all Slaves assigned to that Master.

**Standalone DCR**

In Standalone mode, DCR maintains an independent repository of device list and credential data. It does not participate in a management domain and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other Master, Slave, or Standalone DCR.

The DCR mode is set to Standalone, by default, after a fresh installation of Cisco Prime.