



## Recommended Best Practices

---

This appendix provides the recommended best practices for increasing the disk space and system performance. It contains the following topics:

- [Basic Server and Client Requirements](#)
- [Best Practices to Reclaim Disk Space Using Purging Method](#)
- [Best Practices for Improving System Performance](#)
- [Best Practices for Performing Server Reboot](#)
- [Backing Up Data](#)
- [Handling Custom Telnet Prompts](#)
- [Best Practices for Software Image Upgrade](#)
- [FAQ](#)



**Note**

---

To avoid restarting daemons, you must ensure that device packages, point patches and software updates are updated (up-to-date) before network is down during planned network downtime.

---

## Basic Server and Client Requirements

Before installing LMS software, you must check if your system meets the recommended prerequisites. There are various factors that you must consider before installing LMS on Soft Appliance, Windows and Solaris systems. For more details, refer to [Prerequisites](#) in the *Installing and Migrating to Cisco Prime LAN Management Solution 4.2* guide.

Refer the following links to check if your system meets the recommended prerequisites:

- [System and Browser Requirements for Server and Client](#)
- [Terminal Server Support for Windows Server](#)
- [Solaris Patches](#)
- [LMS 4.2 Port Usage](#)
- [Required Device Credentials for LMS Functionalities](#)

# Best Practices to Reclaim Disk Space Using Purging Method

This section contains the list of best practices that are recommended when you want to reclaim disk space using purging method.

When data in your system increases and disk space decreases, purging helps you reclaim disk space. You can reclaim disk space using the following methods:

- [Purging Databases](#)
- [Purging Jobs](#)
- [Purging Archives](#)

## Purging Databases

To reclaim disk space by purging your system's database:

- Set the **Syslog Purge Settings** in such a way that syslog records do not pile up in the database. The following steps should be performed to set the **Syslog Purge Settings**:
  - Enable the **Syslog Backup Settings** by navigating to **Admin > Network > Purge Settings > Syslog Backup Settings**.
  - Set the purge policy date and schedule a job on daily/weekly basis by navigating to **Admin > Network > Purge Settings > Syslog Purge Settings**.
  - Perform a force purge job by navigating to **Admin > Network > Purge Settings > Syslog Force Purge**.
- Run the **DBSpaceReclaimer** tool after performing force purge job to reclaim disk space to a greater extent. The following steps should be performed:
  - Open `RMEDebugToolsReadme.txt` from `NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\debugtools`, where NMSROOT is the Cisco Prime installation directory.
  - Refer **Syslog DBSpaceReclaimer Tool** section in the `RMEDebugToolsReadme.txt` file and execute the perl script `DBSpaceReclaimer.pl`. For more details, refer [Syslog Administrative Tasks](#).

In Device Performance Management, if the size of the database remains the same after purging, the following steps should be performed to reclaim disk space:

- For Windows:
  - Stop the daemon using the `net stop crmdmgt` command.
  - Enter `dbunload -c "uid=DBA;pwd=<<password>>;dbf=<<upm_database_location>>" -ar`
  - For example: `dbunload -c "uid=DBA;pwd=admin;dbf=C:\Progra~2\CSCOpX\databases\upm\upm.db" -ar`
  - Start the daemon using the `net start crmdmgt` command.
- For Solaris:
  - Stop the daemon using the `/etc/init.d/dmgt stop` command.
  - If you get an error message regarding library path, enter `source /opt/CSCOpX/etc/install.cshrc`

- To get the library path LD\_LIBRARY\_PATH, navigate to **/opt/CSCOpX/lib/classpath/md.properties**.
- To set the library path, enter `setenv LD_LIBRARY_PATH <<PATH>>`
- To reload the database, enter `dbunload -c "uid=DBA;pwd=<<password>>;dbf=<<upm_database_location>>" -ar`  
*For example: dbunload -c "uid=DBA;pwd=welcome;dbf=/opt/CSCOpX/databases/upm/upm.db" -ar*

**Note**

Ensure that the file **/opt/CSCOpX/databases/upm/upm.db** has permission as: **-rw----- 1 casuser casusers upm.db**. You can change the permissions using the following commands:

- `chmod 600 upm.db`
- `chown casuser:casusers upm.db`

- Start the daemon using the `/etc/init.d/dmgttd start` command.
- For Linux:
  - Stop the daemon using the `/etc/init.d/dmgttd stop` command.
  - If you get an error message regarding library path, enter `source /opt/CSCOpX/etc/install.cshrc` from the `csH` shell.
  - To get the library path LD\_LIBRARY\_PATH, navigate to **/opt/CSCOpX/lib/classpath/md.properties**.
  - To set the library path, enter `setenv LD_LIBRARY_PATH <PATH>`
  - To reload the database, enter `dbunload -c "uid=DBA;pwd=<<password>>;dbf=<<upm_database_location>>" -ar`  
*For example: dbunload -c "uid=DBA;pwd=welcome;dbf=/opt/CSCOpX/databases/upm/upm.db" -ar*

**Note**

Ensure that the file **/opt/CSCOpX/databases/upm/upm.db** has permission as: **-rw----- 1 casuser casusers upm.db**. You can change the permissions using the following commands:

- `chmod 600 upm.db`
- `chown casuser:casusers upm.db`

- Start the daemon using the `/etc/init.d/dmgttd start` command.

## Purging Jobs

You can configure LMS to periodically purge job data that you no longer need. This is done using Job Purge. For more details, refer [Performance Purge Jobs](#).

Refer the following links to configure the purge settings for all modules in LMS:

- [Purging Reports Jobs and Archived Reports](#)
- [Purging VRF Management Reports Jobs and Archived Reports](#)

- [Purging Configurations from the Configuration Archive](#)
- [Syslog Administrative Tasks](#)
- [Setting the Syslog Purge Policy](#)
- [Purging Configuration Management Jobs](#)
- [Performance Purge Jobs](#)
- [Performance Purge Data](#)
- [View Performance Purge Details](#)
- [IPSLA Data Purging Settings](#)
- [Configuring the Daily Fault History Purging Schedule](#)

**Note**

You can view the status of all the LMS admin-related Jobs in Job Browser. For more details, refer [Using Job Browser](#).

## Purging Archives

Purging archives frees disk space and maintains your archive at a manageable size. For more details, refer [Purging Configurations from the Configuration Archive](#).

**Note**

Log files can expand and fill up disk space. Log files disk space usage can be maintained by deleting the unwanted log files from the Cisco Prime installation directory. For more details, refer [Maintaining Log Files](#). Log Files can also be maintained by using the logrot functionality. For more details, refer [Configuring Log Files Rotation](#). Log files rotation can be also be scheduled. For more details, refer [Scheduling Log Files Rotation](#).

## Best Practices for Improving System Performance

System performance can be improved by setting the Performance Tuning Tool (PTT) and also by managing core devices in critical device poller.

### Improving System Performance Using PTT

PTT is a Command Line Interface (CLI) utility that enables you to apply and list various profiles available in LMS server. Profiles consist of configuration files, which are in the form of XML files whose values are based on the recommendations for various applications. There are two profiles shipped with LMS. You can use any of the profiles that matches the system. Parameters are tuned and available in each profile. You can apply the required profile to the system and improve performance. This is a major advantage of using PTT. For more details, refer to [Performance Tuning Tool](#) in the Configuration Management with Cisco Prime LAN Management Solution 4.2 guide. For Layer2 and topology related PTT, refer to [Performance Tuning Tool](#) in Appendix A.

### Improving System Performance Using Critical Device Poller

Data collection consumes significant system resources. The critical device poller allows you to view the device and link status without running Data Collection. You can simply poll the network and view the device and link status in Topology maps. Only core devices should be managed in critical device poller. For more details, refer [Data Collection Critical Device Poller](#).

### Suggestions for Better System Performance

Consider the following points for better system performance:

- Configure devices to send only the syslogs that you are working with. This practice will help you avoid server issues that occur due to huge amount of syslogs.
- Avoid running numerous scheduled jobs of the same type.
- When restarting the scanner, delay the anti-virus scan to avoid issues that could occur in upcoming processes. You can restart the scanner only after all processes are up again.
- Do not delete or move any files available in LMS-installed location, without confirming with the TAC engineer about the impact the action might cause.
- Related or critical jobs from the same application should not be triggered in a way that it conflicts with each other. For example: Inventory collection and Configuration collection should not be scheduled to run at the same time because doing so will create system issues. Similarly, Data Collection and User Tracking must not be scheduled to run simultaneously. You should identify priority of jobs based on use cases and schedule appropriate timings for those critical jobs to run. Unrelated jobs or non-critical jobs can run at a parallel or later time.

Consider the following points when you configure systems to manage a large number of devices:

- Device Discovery – Set up the discovery schedule to a less frequent one and choose the time most appropriate to you. You must select the discovery parameters most suitable to your environment so that it could speed up the discovery process, and discover and populate correct values.
- Data Collection Settings – The data collection is configured to run every four hours starting at midnight. Run discovery manually once to determine an appropriate polling cycle. The subsequent polls will be shorter in duration, but you should still give it a 20 percent buffer. For example, if it took four hours to poll the whole network the first time, you could set the frequency to five hours to make sure that there is no overlapping between the two consecutive data collection processes.
- User-Tracking Discovery – You must configure the time so that two consecutive schedules do not overlap. You could also filter subnets for which you do not want to perform end-host discovery or subnets where no end hosts are present. Configure subnets that you want excluded from doing a ping sweep before the discovery process.
- Fault Management Polling Parameters and Threshold – Default Cisco Prime fault management polling and threshold parameters are configured for Cisco Prime fault management system-defined groups; however, it is recommended that you look at these configurations based on critical and noncritical devices in your network.
- Cisco Prime Inventory, Configuration, and Image Management – In Cisco Prime LMS, you can create user-defined jobs for inventory polling and collection, and configuration collection and polling on a set of devices selected as part of the job creation process. You should consider this option when servers manage a large number of devices.
- Periodic Polling Versus Periodic Collection – Polling uses fewer resources than full scheduled collection because configuration files are retrieved only if the configuration MIB variable is set, so it is recommended that you enable the **Period Polling** option and disable the **Periodic Collection** option.



---

**Note**

All collection must be scheduled in a way that it does not conflict with each other.

---

### Recommendations on when to schedule various jobs

Consider the following points when scheduling jobs:

- Inventory/Config jobs can be scheduled to run on daily basis.

- Inventory/Config collection jobs can be scheduled to run on weekly basis.
- All Purge jobs (not specific to inventory and Config) can be scheduled to run on weekly basis.
- CDA Job can be scheduled to run on weekly basis.

**Note**

The UI performance of the application client can be improved by using device groups when executing application tasks, especially when a single server is managing a large number of devices.

## Best Practices for Performing Server Reboot

In windows, Security patches/OS updates requires server reboot. For performing server reboot, refer the following steps:

- 
- Step 1** Enter the following command to stop the Daemon Manager:
- ```
net stop crmdmgt
```
- Step 2** Change the startup type of the Daemon Manager to manual in Windows Services Control Panel.
- Step 3** Update the software on server or reload the server.
- Step 4** Change the startup type of the Daemon manager to automatic once the server comes up.
- Step 5** Enter the following command to start the Daemon manager and wait till all the services comes up.
- ```
net start crmdmgt
```
- 

**Note**

Don't restart the Daemon Manager when major collections like DC, UT, Inventory, Config is running to avoid database corruption problem.

**Note**

If you want to reboot the Windows, Solaris or VM server, you must do so only after stopping the daemons. You must not reboot the server while the daemons are running.

## Backing Up Data

Regular backup of data should be practiced on a daily/weekly basis to avoid data loss. To schedule system backups at regular intervals, select **Admin > System > Backup**. For more details, refer [Backing Up Data](#).

Consider the following points when backing up data:

- While scheduling or triggering a backup, if the backup time conflicts with any JRM job time (Jobs that is scheduled between backup time +/- one hr), then an error pops up displaying a list of job IDs. Similarly, when scheduling or triggering a JRM job, if the JRM job schedule time conflicts with any backup time (Backup time that is scheduled between JRM job time +/- one hr), then an error pops up displaying a list of backup time that runs around the same schedule as the JRM job.
- If you want to backup Config on a daily basis, the shadow directory option can be used.

**Note**

DiskWatcher is a back-end process that monitors disk space availability on LMS Server. This process calculates the disk space information of a drive (on Windows) or a file system (on Solaris/Soft Appliance) where Cisco Prime applications, are installed, and stores them in diskWatcher.log file. For more details, refer [Configuring Disk Space Threshold Limit](#).

**Note**

You should never backup data on the Cisco Prime Installation directories, such as, *NMSROOT* for Windows and */opt/CSCOPx* for Soft Appliance and Solaris; as well on */var/adm/CSCOPx*.

## Handling Custom Telnet Prompts

You can set the protocol order for Configuration Management features such as Archive Management, Config Editor, and NetConfig jobs to download configurations and to fetch configurations.

The configuration archive uses Telnet/SSH to collect the configurations from the devices. Make sure you enter the correct Telnet and Enable passwords.

If the device prompts for login credentials, you may experience problem in Telnet connection because LMS may fail to recognize the login credential prompt. To make your prompts recognizable, you must edit the TacacsPrompts.ini file. See the procedure given in the [Handling Custom Telnet Prompts](#).

## Best Practices for Software Image Upgrade

Software Distribution allows you to distribute images in your network and to analyze and determine the impact and prerequisites for new software images before distribution.

- Out of the four distribution methods available, Cisco recommends Remote Staging method because it is found to be the fastest while operating from a WAN network.
- A FTP server is found to be faster to stage an image temporarily.
- Perform image upgrade on one site at a time.
- Start with upgrading one device per each device type in the site, to uncover timeout or image related issues.
- On successful upgradation of one device, schedule the upgrade for rest of the devices in that site, grouping devices of the same type in a single job.

## FAQ

- Q. How can I exclude messages from Syslog Analyzer instead of performing a force purge?

**A.** Instead of reclaiming the disc space by performing a force purge, you can create Filters to either drop or keep the syslog messages. For a detailed procedure, go to [http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_lan\\_management\\_solution/4.0/user/guide/admin/useNotif.html#wp1074735](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/admin/useNotif.html#wp1074735)

**Q.** How can I avoid too many configuration archives in a single day?

**A.** If you feel that the archives are not required for that particular device category or device family or device type, you can add the respective command to the Config Compare Exclude Command Configuration list. For more information, go to [http://www.cisco.com/en/US/docs/net\\_mgmt/ciscoverks\\_lan\\_management\\_solution/4.0/user/guide/admin/collection.html#wp1092555](http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_lan_management_solution/4.0/user/guide/admin/collection.html#wp1092555)

You can also choose not to archive VLAN Config Collection by performing the following steps:

- a. Check the **Disable VLAN config collection** check box.
- b. Click Apply.

The VLAN config collection will be disabled for both manual and system config collection jobs. By default the Disable VLAN Config collection checkbox is unchecked.

**Q.** Why is Port Scanning not recommended in LMS?

**A.** Port Scanning is not recommended in LMS because,

- Processes such as User Tracking (UT) might hang
- Apache might crash
- Tomcat might stop responding.

Solution is to restart Daemon Manager and stop further scanning.

**Q.** How to reduce CPU/Memory consumption usage by sm\_server process?

**A.** CPU and Memory consumption of sm\_server process is influenced by various factors such as the components discovered in DFM, number of traps, polling interval, types of polling like fault and performance polling and so on. Hence, the maximum number of components that can be discovered in DFM is restricted to 40,000 per domain.

Type the command given below to know the number of components discovered in DFM.

```
CSCOPx/objects/smarts/bin/sm_tpmgr --server=<Domain Name> --sizes
```

Example:

```
CSCOPx/objects/smarts/bin/sm_tpmgr --server=DFM --sizes
```

To control the CPU or Memory usage by sm\_server processes refer the below approaches:

- Unmanage the components that need not be monitored by DFM from Detailed Device View. To manage or unmanage an interface or a port in DFM refer the steps given below:

- 
- Step 1** Log into LMS server using credentials.
  - Step 2** Go to **Monitor > Fault Settings > Setup > Fault Device Details**.
  - Step 3** Select the Device and Click View.
  - Step 4** Click the device name. Detailed Device View appears.
  - Step 5** Select Interface or Port.



- Step 6** To manage the Interface or Port, set the Managed State to True, and to unmanage the Interface or Port, set it to False.
- Step 7** Click Submit.
- Step 8** Go to **Monitor > Fault Settings > Setup > Apply Changes** and click **Yes apply change to fault engine**.

- Reduce the number of network adapters being discovered in DFM by filtering the components which need not be monitored.

We can avoid DFM discovery process to discover a particular type of interface or port by adding an IFDescrPattern or IFTypePattern in *CSCOp\objects\smarts\conf\discovery\tpmgr-param.conf*. You can find the instructions to create patterns in this file. After modifying tpmgr-param.conf file, we need to restart the daemon manager and rediscover the devices in DFM.

Examples:

```
IFDescrPattern-.1.3.6.1.4.1.9.1.110
~EFXS*|~*POTS*|~*Bearer*|~FXO*|~FXS*|~Voice*|~Foreign*
```

In this example, DFM discovery will not discover interfaces with description starting with EFXS, containing POTS, containing Bearer, starting with FXO, starting with FXS, starting with Voice or starting with Foreign for device having sysObjectId .1.3.6.1.4.1.9.1.110.

```
IFTypePattern-.1.3.6.1.4.1.164.6.1.3.83 ~80~81~82
```

In this example, DFM discovery will not discover ATMLogica(80), DS0 (81) and DS0Bundle(82) for device having sysObjectId .1.3.6.1.4.1.164.6.1.3.83

```
IFTypePattern-SwitchPort.1.3.6.1.4.1.9.12.3.1.3.380 ~56
```

In this example, DFM discovery will not discover Fibre channel (56) ports for device having sysObjectId .1.3.6.1.4.1.9.12.3.1.3.380

- Adjust the polling interval with proper values from LMS Polling Parameter Settings Screen.
- To reduce the number of traps received in LMS server, fine tune the trap configuration in devices such a way that the traps which need to be monitored alone are sent to the LMS server.

