CHAPTER 13

System Maintenance

Much of the system maintenance information for the MARS Appliance is provided exclusively in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System.*

The MARS Appliance requires little maintenance. To perform maintenance tasks, you can use the CLI or the web interface, as needed. Some hardware maintenance tasks require physical access to the MARS Appliance.

Note For information on upgrading, backing up, and restoring data on the MARS Appliance, see the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X* and Migrating Data from Cisco Security MARS 4.x to 6.0.1.

This chapter contains the following topics:

Setting Runtime Logging Levels

To set the appliance's runtime logging levels, navigate to **Admin > System Maintenance > Set Runtime Logging Levels**. For typical use, it is best to leave this page set to its defaults.

When you have made your selections, click the **Change Logging Levels** button.

The following log levels are available:

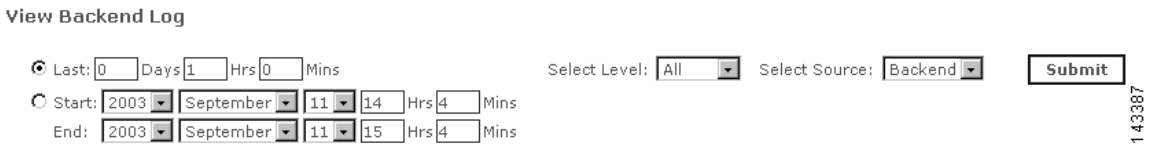
- **Fatal**—Enables fatal logging messages. Fatal messages record very severe error events that will likely lead the application to abort.
- **Error**—Enables error and fatal logging messages. Error messages record error events that might still allow the application to continue running.
- **Warn**—Enables warning, error, and fatal logging messages. Warning messages record potentially harmful situations.

- **Info**—Enables informational, warning, error, and fatal logging messages. Informational messages highlight the progress of the application at coarse-grained level.
- **Debug**—Enables debug, informational, warning, error, and fatal logging messages. Debug messages record fine-grained informational events that are most useful to debug an application.
- **Trace**—Enables trace, debug, information, warning, error, and fatal logging messages. Trace messages record finer-grained informational events than debug messages.

Viewing the MARS Backend Log Files

To view the appliance's log files or to change their levels or source, navigate to **Admin > System Maintenance > View Log Files**.

Figure 13-1 Backend log viewing options



You can view the appliance's backend logs either by selecting a number of days, hours, and minutes or you can view logs by selecting a start and ending date and time.

You can select the levels of logs that you want. Your choices are: All, Fatal, Error, Warn, Info, and Debug.

You can also choose the source of the files that you want to view. Select either Backend or GUI.

To view the backend log files, follow these steps:

Step 1 Click the appropriate radio button:

- **Last**—The present time minus the number of days, hours, and minutes entered.
- **Start/End**—Absolute literal time ranges defined by the date to the minute.

Step 2 Select user, group, and so on.

Step 3 Select the source.

Step 4 Click **Submit**.

Viewing the Audit Trail

You can track the activities of the appliance's users by analyzing the appliance's log files. To set the appliance's audit trail logs, navigate to **Admin > System Maintenance > View Audit Trail**. For typical use, it is best to leave this page set to its defaults.

You can view the user audit trails either by selecting a number of days, hours, and minutes, or you can view a specific interval by selecting a start and ending date and time.

To view the audit trail, follow these steps:

Step 1 Click the appropriate radio button:

- Last: DD-HH-MM
- Start/End: YY-MM-DD-HH-MM

Step 2 From the list, select the user or user group.

Step 3 Click **Submit**.

Retrieving Raw Messages

You can retrieve raw messages from either an archive server (see Configuring and Performing Appliance Data Backups) or from the local files running on the Local Controller. These two methods offer different advantages:

- **Archive server.** Retrieving raw messages, or event data, from an archive server is much faster than retrieving from the database. Therefore, it is the recommended option if it is available and it covers the time period you are investigating. However, this option is only available if you have enabled data archiving and waited the requisite time for the initial archival operation to occur; it is a scheduled operation that runs nightly around 2:00 a.m. After the initial archive is performed, the event data is written to the archive server frequently, often within 5 to 8 minutes after the MARS Appliance receives the message. That the data is not archived in real-time identifies another limitation to this option, and that is the historical period that can be studied. If you need to view data that is more current than an hour old, you should select the Database option to ensure that correct data is retrieved. For all other periods, the archive server option is recommended. To enable archiving, see Configuring and Performing Appliance Data Backups.
- **Local Files**. Retrieving event data from the local files provides slower performance than the archive server. However, it provides access to the most current data received. Local Files have the five tuples, whereas archived raw messages do not have the five tuples.

This section contains the following topics:

About Raw Message Size Limitations and Storage Location

Before the 5.2.4 release, the storage of raw message data in the local database was restricted to 500 KB per message. Beginning with 5.2.4, the raw message size is stored in local files that can be up to 1.5 MB without being truncated. Each MARS Appliance model has dedicated disk space reserved for arbitrary-sized raw message files. When the upper limit of this storage size is reached, the pnarchiver process moves the raw messages and associated index files to the remote NFS server, if configured. If no NFS server is configured, then the raw message files are purged, oldest data first (first in, first out). When the database is purged, the corresponding raw message files are also purged.

The raw message files are archived under `/pnarchive/DATA_POOL`. The DATA_POOL directory contains a dated directories under which the raw message files created on that date are compressed and saved. An example `/pnarchive/DATA_POOL/<date>` directory listing follows:

```
2007-02-10
2007-02-11
```

The file names use the following format:

```
[dbversion]-[productversion]-[serialno]_[StartTime]_[EndTime].gz
```

For example, the ./pnarchive/DATA_POOL/2007-02-12/ES listing reveals:

```
ix-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
rm-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
```

Note Those files beginning with “ix” are index files, and those beginning with “rm” are the raw message files.

Retrieve Raw Messages

You can retrieve Raw Messages in any of four different modes, depending on the settings you configure on the Retrieve Raw Messages page for source and destination of the files. You can:

- Retrieve data from archived files to a local MARS cache.
- Retrieve data from archived files to a remote network file server (NFS).
- Retrieve data from the database to a local MARS cache.
- Retrieve data from archived files to a remote network file server (NFS).

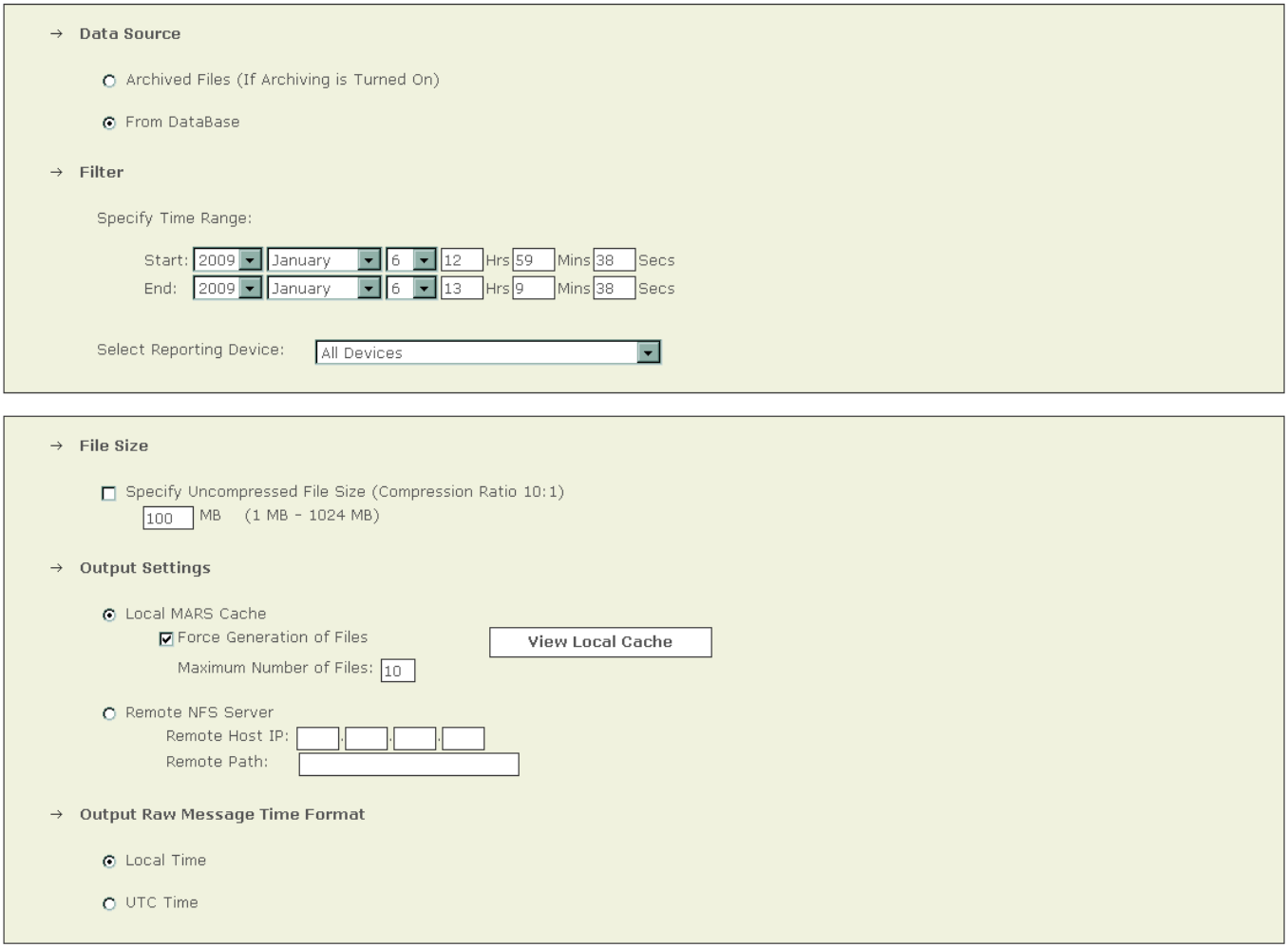
You can also filter the output according to time range, reporting device, and file size.

To retrieve raw message event data, follow these steps:

Step 1 Click **Admin > System Maintenance > Retrieve Raw Messages**.

The Raw Message Files page appears.

Figure 13-2 Retrieve Raw Messages Page



Step 2 In the Data Source area, click to select the source as either: **Archived Files** or **From Database**.

Note Archiving must be turned on for you to select Archived Files as the data source.

Step 3 In the Filter area, specify the time range by specifying values in the Start and End fields.

Note The default specifies the last 10 minutes.

Step 4 In the File Size area, to specify a file size limit, select **Specify Uncompressed File Size (Compression Ratio 10:1)** and then type in the box the size limit you want. (The range is from 1 to 1024 MB.) The default size is 100 MB.

If you have specified *Archived Files*, and you do not specify a file size limit, links to all the files within the specified time limit are displayed.

Step 5 In the Output Settings area, select *one* of the following:

- **Local MARS Cache**—You are given the following options:

  - Deselect the **Force Generation of Files** option to negate forced generation of the files.
  - Click **View Local Cache** to view the cache.
  - Enter a number in the Maximum Number of Files field to increase or limit the number of files.
- **Remote NFS Server**—If you choose this option for output destination, you *must* specify the Remote Host IP and the Remote Path.

Step 6 Select the Output Raw Message Time Format as *one* of the following:

- Local Time (the output raw messages will be displayed in local time)
- UTC Time (the output raw messages will be displayed in UTC time)

Step 7 Click **Submit**.

Note While MARS is generating your files, you can still use the system for other tasks.

The `Retrieving Progress 0%` screen appears. When the operation is complete, the Raw Message Files screen appears, identifying a new Gzip archive file with a filename based on specified time range. The files are copied from the source (archive or database) to either the local cache in MARS or to the NFS specified, and links are displayed on the GUI to download files.

Step 8 To download and view the generated raw message file, click **Click Here to Download** next to the filename.

The filename adheres to the following syntax:
YYYY-MM-DD-HH-MM-SS_YYYY-MM-DD-HH-MM-SS.gz.

Step 9 Use WinZip or another archive expansion program to extract the contents of the Gzip archive file.

Step 10 After the textfile is extracted from the GNU Zip archive format, its contents resemble the following:

```
33750»Wed Jul 27 16:16:06 PDT 2005»BR-FW-1»10.1.2.4»9000»10.1.5.20»80»6»<134>Jan 06 2003
11:03:53: %PIX-6-302001: Built inbound TCP connection 21000 for faddr 10.1.2.4/9000 gaddr
10.1.5.20/80 laddr 10.1.5.20/80
```

where it reads: *Event ID >>date >>device name >>src IP >>src port >>dst IP >>dst port >>protocol number >>raw message*.

Note If you see Chinese or other unfamiliar characters in the resulting text file, please use Microsoft Internet Explorer to view the file and verify that the Western European ISO or Western European Windows encoding value is selected (View > Encoding). The "»" sign appears correctly as a separator when a compatible encoding is selected.

Change the Default Password of the Administrator Account

Good security practices require that you change the default password. We recommend using strong passwords for the MARS Appliance appliances.

Login names and passwords:

- Can be alphanumeric characters
- Are case sensitive
- Can contain special characters (!, @, #, etc.)
- *Cannot* contain single or double quotes (‘or “)

Login names can contain up to 20 characters. Passwords can contain up to 64 characters.

To change the default password and setup administrator notification, follow these steps:

Step 1 Click the **Management > User Management** tab.

Step 2 Check the box next to Administrator, and click **Edit**.

Step 3 Enter the new Administrator password and the Administrator e-mail address.

Step 4 Click **Submit**.

Understanding Certificate and Fingerprint Validation and Management

Many reporting devices use certificates or fingerprints to enable secure communications over SSL or SSH respectively. MARS performs a strict check of the certificate or fingerprint of the device or server to which it is attempting to connect.

Note Certificate validation does not follow the convention of presenting the client with a list of certificate authorities and using the selected one to validate individual certificates. Instead, the MARS Appliance compares the certificate presented by the reporting device with a previously stored instance of the certificate. If the two match, the presented certificate is considered valid. This approach allows MARS to validate certificates without knowledge of revocation lists and to operate in a network without an Internet connection.

Three options exist for specifying how MARS should respond during attempts to establish a secure connection. The three options are as follows:

- **Automatically always accept.** This option, which is compatible with previous releases, allows a MARS Appliance to connect to reporting devices regardless of how frequently the certificate or fingerprint changes because MARS automatically accepts and stores the replacement certificate or fingerprint for all devices. However, this option does not provide an opportunity to inspect and authorize the changes to the certificates or fingerprints. When a conflict is detected or when a new certificate or fingerprint is accepted, the event is logged to the internal log. The internal log entry includes the name of the process that detected the conflict and the IP address of the reporting device. The logs can be retrieved by queries and reports. See Monitoring Certificate Status and Changes, page 13-10 for more information on studying these events.

- **Accept first time and prompt on change (default).** This option accepts and stores a new certificate or fingerprint the first time MARS Appliance connects to a device. For subsequent connection attempts, the appliance checks the presented certificate or fingerprint against the stored value. If a conflict is detected, the session is refused unless the new certificate or fingerprint is manually accepted by the administrator. This option enables initial topology discovery to proceed without administrator intervention. Internal system logs of the initial acceptance, conflict detection, and acceptance of new change are created. The internal logs include the name of the process that detected the conflict, the IP address of the reporting device, and the username of the account used to accept the change.

  If, when a change is detected by a web interface process, the session times out before administrative intervention, the communication fails but no internal system log is generated to record the failure to accept the changed certificate or fingerprint. Also, if a back-end process initiates the request, such as auto discovery, then the session attempt always fails and no attempt to obtain administrative acceptance is initiated. In such cases, any data the MARS Appliance would normally ascertain from the device during such a session is not collected. This delay of data retrieval does not apply to syslogs forward to the MARS Appliance by the reporting device and it resumes once the new certificate is accept. The recommended method for manually kicking off the change detections is to use the Test Connectivity or Discover button on the reporting device.
- **Always prompt on new and changed.** This option requires an administrator to manually accept the certificate or fingerprint before MARS can establish the desired communications each time the certificate or fingerprint changes. During changes, the internal log includes the username of the account used to accept the change. If the communication times out before administrative intervention, the communication fails and an internal system log records the failure to accept the changed certificate or fingerprint.

The implication of each option varies based on which MARS service is attempting the connection, not in the enforcement of the option, but in the ability of the service to prompt for immediate administrative intervention. In other words, if the service is a GUI-based services, you will be prompted to accept the changed certificate or fingerprint. If the service is a backend service, the communications with the target device will fail and the event will be logged.

The following services and operations are affected by the global certificate/fingerprint response setting:

- Upgrade (SSL). When MARS uses the HTTPS option to download the upgrade package from the remote server specified on the Admin > System Maintenance > Upgrade page.
- Discovery operation. (SSH)
- Test Connectivity operation. (SSL)
- Cisco IDS, IPS, and IOS IPS router Event Processing (RDEP or SDEE over SSH)
- CSM Policy Query Integration (SSL)
- Qualys Report Discovery. (SSL)
- Graphgen process for mitigation operation (SSH and SSL)
- Device Monitor process for resource monitoring feature (SSH)

Setting the Global Certificate and Fingerprint Response

The default response is to accept the certificate or fingerprint the first time MARS attempts to connect to the device, after which if a conflict is detected, then administrative intervention is required to update to the new certificate or fingerprint.

If this option is not the one that you wish to use, you can select from three options. The global setting for the conflict detection responses is located on the Admin > System Parameters > SSL/SSH Settings page.

To change the default certificate and fingerprint response, follow these steps:

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Parameters > SSL/SSH Settings** tab.

Step 3 Select one of the following options to define the global behavior that you require:

- Automatically always accept
- Accept first time and prompt when changed
- Always prompt on new and changed

For details on these options, see Understanding Certificate and Fingerprint Validation and Management, page 13-7.

Step 4 Click **Submit**.

Upgrading from an Expired Certificate or Fingerprint

If you have selected a global response option other than Automatically always accept (see Setting the Global Certificate and Fingerprint Response, page 13-8), you will at some time be required to update an expired certificate or fingerprint.

Two options exist for upgrading from an expired certificate or fingerprint. If you are logged in to the web interface when a GUI process detects a certificate or fingerprint conflict, you will be prompted to accept or reject the new value. Otherwise, if you are not logged in or a backend process detects the conflict, you must manually initiate a communication with the device. To determine the list of devices for which you must manually update the certificates or fingerprints, review the Activity: CS-MARS Detected Conflicting Certificates/Fingerprints report (see Monitoring Certificate Status and Changes, page 13-10).

The following procedures explain how to upgrade under the specific circumstances:

- Upgrade a Certificate or Fingerprint Interactively, page 13-9
- Upgrade a Certificate Manually, page 13-9
- Upgrade a Fingerprint Manually, page 13-10

Upgrade a Certificate or Fingerprint Interactively

An interactive upgrade refers to responding to a web interface prompt to update the certificate. This type of upgrade is available when you are logged into the GUI and a process, such as graphgen, prompts you to upgrade a certificate or fingerprint that conflicts with the previously accepted value. Click **Yes** to accept the new fingerprint or certificate.

Upgrade a Certificate Manually

A manual upgrade allows you to upgrade any certificate at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade to a new certificate, follow these steps:

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a certificate conflict. and click **Edit**.

Step 3 Click **Test Connectivity**.

The dialog box displays stating “Do you want to accept following certificate for the device named: <device_name>?.

Step 4 Verify the certificate value.

Step 5 If the value is correct. click **Yes**.

Upgrade a Fingerprint Manually

A manual upgrade allows you to upgrade any fingerprint at any time due to any reason: session time out during interactive prompt, user error, detection of conflict by a backend process.

To manually upgrade a fingerprint, follow these steps:

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Select the reporting device on the Admin > System Setup > Security and Monitor Devices page for which MARS has detected a fingerprint conflict and click **Edit**.

Step 3 Click **Discover**.

The dialog box displays stating “Do you want to accept following fingerprint for the device named: <device_name>?.”

Step 4 Verify the fingerprint value.

Step 5 If the value is correct, click **Yes**.

Monitoring Certificate Status and Changes

To support the certificate management features in MARS, the following system inspection rule exists:

- **System Rule: CS-MARS Failure Saving Certificates/Fingerprints.** This inspection rule indicates that MARS has failed to save a new or changed device SSL certificate or SSH key fingerprint based on either explicit user action or automatic accept as specified on the SSL/SSH Settings page.

In addition, the following reports appear under the System: CS-MARS Issue category.

- Activity: CS-MARS Accepted New Certificates/Fingerprints
- Activity: CS-MARS Accepted Conflicting Certificates/Fingerprints
- Activity: CS-MARS Detected Conflicting Certificates/Fingerprints
- Activity: CS-MARS Accepted New Certificates/Fingerprints’
- Activity: CS-MARS Failure Saving Certificates/Fingerprints
- Activity: CS-MARS Device Connectivity Errors

Database Tuning and Query Optimization

When you run a query from the MARS GUI and specify a large time range, it may take a long time to complete the query even though the returned results may include only a few entries. Such long-term queries require the database to perform a full table scan, even when you employ query filters.

To vastly improve the speed of query execution, we recommend that you create and employ database indexes of the filtering columns. Database query performance, of course, still depends on the amount of data that must be returned, and a query that returns thousands of rows of data will still take significantly longer than a query that returns only dozens of rows.

The performance improvement achieved is not subject to the number of indexes created, rather, the degree of performance improvement is subject to the following three conditions:

- The query has at least one filter
- All the filters are indexed (the number of filters do not matter, one filter may be as good as many filters)
- The query returns a small amount of data after the filtering.

About Database Indexing

Although a series of database indexes can significantly improve response time, creating additional indexes can also, depending on the particular circumstances, have the reverse effect. To effectively optimize query operations, MARS helps to determine the nature and scope of database indexing you should perform.

MARS stores security events in 10 database tables, *pn_event_session_0*, …, *pn_event_session_9*. Each of the tables is about the same size, and the size is predefined based on the CS-MARS model. A MARS-25, for example, has approximately 70 percent fewer rows in each table than a MARS-55. When the current table is full of data, the system truncates the table that contains the oldest data and starts storing data there.

An index is a special database table that stores the location of particular data in a database table. Looking up an entry in the index table is usually faster because it is organized, while looking up an entry directly from the data table is sequential and usually much slower.

MARS employs both bitmap and B-tree indexes. Bitmap indexes are preferred when the cardinality of a database table column is low. Cardinality expresses the number of distinct values in a column. For example, a column that held only *true|false* values would have a cardinality of 2 and would be a prime candidate for a bitmap index. For this reason, proper database indexing begins with determining the cardinality of all database columns.

Note B-tree indexes use many more system resources and may severely impact system performance. Use B-tree indexing prudently when the index is not recommended, and drop the index if you find it impacts your system performance.

Keep the following considerations for database optimization in mind:

- Calculating the cardinality is best done on a full table.
- You should only have to calculate cardinality once or twice a year.
- Calculate cardinality before creating indexes.

- Create indexes on columns that best reduce the scope of the data returned.
- Monitor system performance and test queries using the indexed columns as filters.
- Drop an index if you find it degrades system performance. (A dropped index can always be reactivated.)
- Keep an index, even if it is rated as "Not Recommended," if you determine it works well.

Understanding the Data Indexing/Query Optimization Page

The Data Indexing/Query Optimization page, which you can view by selecting **Admin > System Maintenance > Database Tuning / Query Optimization,** enables you to view index configuration information and to perform index-related functions.

Figure 13-3 shows the Data Indexing/Query Optimization page of the System Maintenance tab.

Note The table on the Data Indexing/Query Optimization page presents each database table column that can be indexed on a separate row.

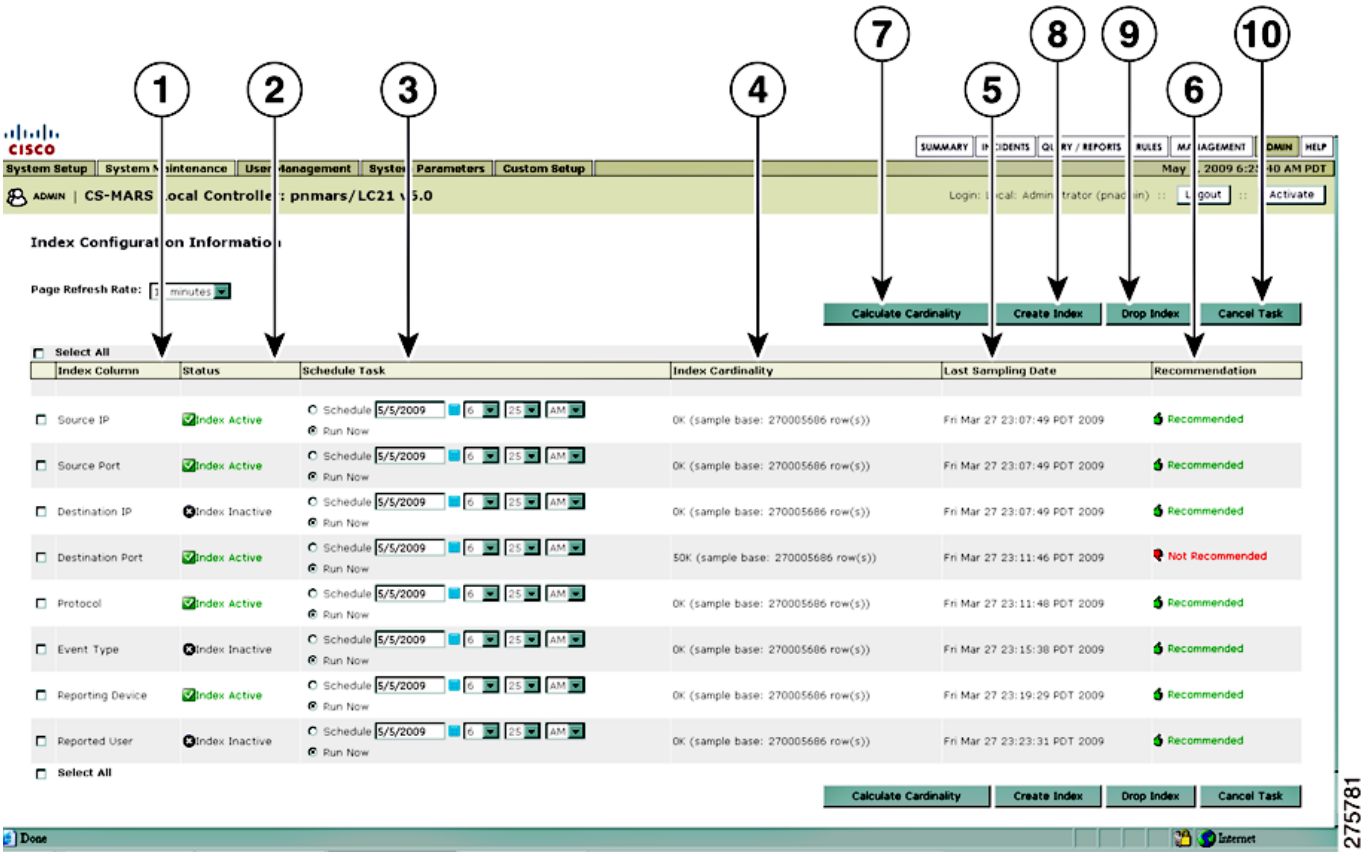


Figure 13-3 Data Indexing/Query Optimization Page

1	**Index Column**: Lists which database columns can have indexes created.	2	**Status**: For a each index column, indicates index status. Displays a green, square, check icon for active indexes or a black, round, X icon for inactive indexes.
3	**Schedule Task**: For a each index column, two radio buttons enable you to determine whether an operation on an index is scheduled or run immediately. Four date and time fields enable you to specify schedule time.	4	**Index Cardinality**: For a each index column, displays the size of the last sampled cardinality in thousands and, in parentheses, displays the sample base size.
5	**Last Sampling Date**: For a each index column, displays the date of the most recent cardinality calculation sampling.	6	**Recommendation**: For a each index column, indicates recommendations for whether a particular index: • ***should be*** activated (green, thumb up icon with text reading “Recommended”), or • ***may be*** activated (green, thumb up icon with the text "Not Ideal"), or • ***should not be*** activated (red, thumb down icon).
7	**Calculate Cardinality Button**: Clicking this button requests that cardinality calculations be performed on the selected database columns, either immediately, or by the specified schedule.	8	**Create Index Button**: Clicking this button requests that the selected database columns be indexed (or re-indexed), either immediately, or by the specified schedule.
9	**Drop Index Button**: Deletes selected index.	10	**Cancel Task Button**: Cancels requested actions on the selected database columns.

The performance of an indexed database to a query depends on three factors:

- At least one filter is employed
- The filter(s) used is indexed
- The query returns a small of amount of data after the filtering

Data Indexing/Query Optimization Procedures

Procedures that you perform from the Data Indexing/Query Optimization page include the following:

- Calculate Cardinality, page 13-14
- Create Database Index, page 13-14
- Schedule Database Optimization, page 13-15
- Drop Index, page 13-15

Calculate Cardinality

You can calculate the cardinality of any database table column to better understand whether that column is suitable for bitmap indexing. This calculation also helps the system determine the best type of index to create (cardinality values less than a few thousand typically employ a bitmap index and larger cardinality values dictate the use of a B-tree index.) This operation can be scheduled to run during off-peak hours to minimize system impact.

Keep the following considerations in mind:

- Calculating the cardinality is best done on a full table.
- You should only have to calculate cardinality once or twice a year.

Warning **To prevent overwhelming system resources, you should always calculate a database column's cardinality prior to creating its index.**

To calculate a database column's cardinality, follow these steps:

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select the database columns for which you want to calculate cardinality by clicking to select their corresponding checkbox on the left of the table.

Tip Typically you will want to calculate cardinality for all your indexes close to the same time. However, to lessen system impact, you may want to run a few calculations one night and the rest on the next night.

Step 4 Select when to run the calculation by doing one of the following:

- To run the calculation immediately, select the default, Run Now.
- To schedule the calculation to run later, specify the time by selecting values for the date, hour, minute and AM/PM fields.

Tip Clicking the blue calendar icon next to the date field simplifies selecting a date. Alternatively you can enter a date in mm/dd/yyy format.

Step 5 Click Calculate Cardinality.

Create Database Index

Any database column that you use to perform queries should be indexed.

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select the database columns for which you want to create an index by clicking to select their corresponding checkbox on the left of the table.

Tip Typically you will want to create your indexes at close to the same time. However, to lessen system impact, you may want to create your indexes one at a time and on weekends.

Step 4 Select when to create the index by doing one of the following:

- To create the index immediately, select the default, Run Now.
- To schedule the index creation to run later, specify the time by selecting values for the date, hour, minute and AM/PM fields.

Tip Clicking the blue calendar icon next to the date field simplifies selecting a date. Alternatively you can enter a date in mm/dd/yyy format.

Step 5 Click Create Index.

Schedule Database Optimization

This procedure enables you to schedule the update of one or more database tables. To lessen system impact, you may want to optimize your indexes one at a time and on weekends.

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select a database column for which you want to schedule an update.

Tip If you previously scheduled a particular index for optimization, eliminate that task request by selecting that index and clicking Cancel Task.

Step 4 Specify a time by selecting values for the date, hour, minute and AM/PM fields.

Step 5 Click Create Index.

Step 6 Repeat Step 3 through Step 5 for each database column to be updated.

Drop Index

Too many active indexes can cause system performance issues and impact the event rate. The system warns you of this when you have compiled three database indexes or more. When you find an index affects your system's performance, you should drop it.

Step 1 Log in to the web interface using an account with Administrative privilege.

Step 2 Click the **Admin > System Maintenance > Database Tuning / Query Optimization**

The Index Configuration Information page appears.

Step 3 Select the checkbox of any database column whose index status is listed as Index Active.

Step 4 Select when to drop the index by doing one of the following:

- To drop the index immediately, select the default, Run Now.
- To schedule the index to be dropped later, specify the time by selecting values for the date, hour, minute and AM/PM fields.

Step 5 Click Drop Index.