

# Troubleshoot the Cisco Security Agent Management Center Database

Document ID: 97206

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Cisco Security Agent MC Database is Full

- Problem

- Resolution

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document describes how to troubleshoot the database related problems in the Cisco Security Agent Management Center (CSA MC).

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the Cisco Security Agent Management Center (CSA MC).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Cisco Security Agent MC Database is Full

### Problem

An error message displays which states that the database primary file group is full and that it cannot be expanded any more because it has reached the limit of 2048 MB or 2 GB in the Microsoft SQL Desktop Edition (MSDE) database of the Cisco Security Agent MC.

```
1827 :  
CREATE/ALTER DATABASE failed because the resulting cumulative  
database size would exceed your licensed limit of 2048 MB per database.
```

```
Error: 1105, Severity: 17, State: 2
Could not allocate space for object 'formatted_event_log' in database
'csamc45' because the 'PRIMARY' filegroup is full.
```

## Resolution

Complete these two steps in order to resolve this issue.

1. Purge the Events
2. Enable Auto-pruning

### Purge the Events

Purge the events in such a way that it reduces or shrinks the size of the MSDE database as this procedure shows.

1. Access the Cisco Security Agent MC in the web browser.
2. Choose **Events > Event Log**. Note the total number of events. This number helps you gauge how many events are available for purging.
3. Choose **Events > Events Sets** and select **an existing event set or create a new one**.

An event set always provides a purge option. Event specification is based on the requirements in order to purge the desired events.

Refer to the Event Sets section of Using Management Center for Cisco Security Agent 5.2 Configuration Guide for more information.

#### **Example:**

**Events** > Event Sets > Critical events of all types

**Name**  
Critical events of all types

**Version**  
5.2 r119

**Description**  
Events with severity levels of Critical or higher

**Event Specification**

Include all event types

Include only the following selected **event types**:

- @DYNAMIC: file added
- @DYNAMIC: ip address added
- Access Control: Query action
- Administrator account created
- Administrator account deleted

Include all severity levels

Include only the following selected **severity levels**:

- Information
- Notice
- Warning
- Error
- Alert
- Critical
- Emergency

Include all hosts

Include only hosts in the following selected **groups**:

- <All Linux> [L]
- Desktops - All types [L, V5.2 r119]
- Servers - All types [L, V5.2 r119]
- Servers - Apache Web Servers [L, V5.2 r119]
- Servers - Externally deployed [L, V5.2 r119]

Include all policy rules

Include only rules in the following selected **rule modules**:

- Agent UI Module (Linux) [U, V5.2 r119]
- Agent UI Module (Solaris) [U, V5.2 r119]
- Apache Web Server (Generic Apache2 on Linux) [U, V5.2 r119]
- Apache Web Server (Red Hat Enterprise Linux) [U, V5.2 r119]
- Apache Web Server (Solaris) [U, V5.2 r119]

Include all timestamps

Include only these **timestamps**:

Custom      Custom start time

Today

Last 24 Hours      Custom end time

Last 7 Days

Last 30 Days

Save   View   **Purge events**   Delete   17 rule changes pending   Generate rules

4. Click the **Purge Events** button at the bottom of the window, and wait for the task to complete.
5. Repeat steps 3 and 4 until you purge all events that you do not need.
6. Once you have removed enough events, you can proceed with the database maintenance.

**OR**

The MSDE, which ships with the Cisco Security Agent MC, does not have a GUI. Therefore, database maintenance needs to be done through the command shell tool **osql -E**. Run these scripts via the command shell when you are ready to shrink the database:

Press **Enter** after each line:

- ◆ `osql -E`
- ◆ `use csamc`
- ◆ `backup log csamc with no_log`
- ◆ `go`
- ◆ `dbcc shrinkdatabase (csamc)`
- ◆ `go`
- ◆ At this point the Cisco Security Agent MC database should be compacted. You can exit out at this point. Check the sizes of the **mdf** and **ldf** files in the `C:/ProgramFiles/CSCOpX/CSAMC/db` folder.
- ◆ `update statistics host with fullscan`

- ◆ go
- ◆ update statistics group\_host with fullscan
- ◆ go
- ◆ update statistics event\_log with fullscan
- ◆ go
- ◆ update statistics formatted\_event\_log with fullscan
- ◆ go
- ◆ update statistics rule\_program\_distribution with fullscan
- ◆ go

## Enable Auto-Pruning

Complete these steps in order to configure the auto-pruning feature in the Cisco Security Agent MC:

1. Access the Cisco Security Agent MC in the web browser.
2. Choose **Events > Event Log Management > New** in order to create a new entry. This takes you to the auto-pruning configuration view.
3. Enter a Name for the auto-pruning task.
4. Enter a Description. This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.
5. Use the **Enabled** checkbox to enable this event auto-pruning configuration. (It is enabled by default.) If you do not select this checkbox, you can save this item, but it is not active.
6. Enter a value in the Delete Events – Older Than field. This is the value for which events, after being in the log for a specific number of days, are deleted. Before these events are removed, they must also match the parameters of the event set selected on this page.
7. From the And Matching the Following Event Set field, select the preconfigured event set for the event type you want to prune from the event log. When you configure event sets, it provides flexibility in the selection of the events for auto-pruning.
8. From the And The Database Size Exceeds <##> MB field, specify database size limits that should not be exceeded. Before events are removed due to size, they must also match the other parameters selected on this page.
9. Click the **Save** button.

**Note:** This purging of events occurs periodically based upon the configured auto-pruning items. Generally, this pruning takes place at a time when the least activity is registered on the MC. When event auto-pruning occurs, a message appears in the event log that notifies you of this action.

**Note:** An alternate solution is to upgrade the database to Microsoft SQL which does not have the 2 GB size limitation.

### Example:

**Events** > Event Managing Tasks > Configured auto-pruning

Name	Version
Configured auto-pruning	5.2 r119

**Description**  
Prune all events older than 90 days

Enabled

**Delete Events**

After  day(s)

**AND**

Matching the following event set  [New]

**AND**

The database size exceeds  MB

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

## Related Information

- [Cisco Security Agent Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 18, 2007

Document ID: 97206