Contents

Introduction

This document describes the behavior change in Cisco Security Manager (CSM) services and the required permissions to execute them on CSM 4.8 or later releases.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Problem: Few CSM services fail to start automatically when it is upgraded to 4.8 or later versions.

Symptoms

1. Log in to Configuration Manager, it only shows a blank page under **Device view** tab, none of the devices are visible, as shown in the image.
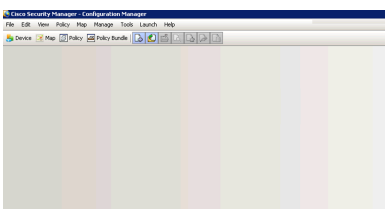
2. Few services show ./casuser under Log On As column, per the output of services.msc, as shown in the image.

Name ▲	Description	Status	Startup Type	Log On As
Cisco Security Manager AUS database engine	CiscoWorks Aus sybase database e...		Manual	.\casuser
Cisco Security Manager Daemon Manager	Administrative service for CiscoWork...	Started	Automatic	Local System

Services which would not start:

CmfDbEngine, rptDbEngine, AusDbEngine and vmsDbEngine

> **Note**: casuser- the casuer user account is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. You do not normally use this account directly.

3. Windows Event log:

Navigate to **Event Viewer > Windows Logs > System** (look for Error level)

```
The vmsDbEngine service was unable to log on as .\casuser with the currently configured password
due to the following error:
Logon failure: the user has not been granted the requested logon type at this computer.
```

Service: vmsDbEngine
Domain and account: .\casuser

```
This service account does not have the required user right "Log on as a service."
```

 User Action

```
Assign "Log on as a service" to the service account on this computer. You can use Local Security
Settings (Secpol.msc) to do this. If this computer is a node in a cluster, check that this user
right is assigned to the Cluster service account on all nodes in the cluster.

If you have already assigned this user right to the service account, and the user right appears
to be removed, check with your domain administrator to find out if a Group Policy object
associated with this node might be removing the right.
```
Similar events are observed for CmfDbEngine, rptDbEngine and

CSM 4.8 onwards, few CSM services are run by casuser and it is an expected behavior.

These are few of the services which are run by casuser :

```
CmfDbEngine, rptDbEngine, AusDbEngine and vmsDbEngine
```
Casuser requires permission to run the above services, therefore, it needs to be set for these Policy:

```
Log on as a service
```
View Permission Changes

The new installation or the upgrade to 4.8, automatically sets casuser for Log on as a service Policy.

Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.**

1) For a server with external Group Policy Object (GPO) set on it, check Resultant Set of Policy (rsop.msc).

2) For a server with local policies, gpedit.msc shows the change.

Trigger of the Issue

This issue is usually seen on a server which is a part of Domain Group and has an external GPO applied on it.

After a regular Group Policy update on the server, casuser might get removed from Log on a service Policy (set after the CSM 4.8 fresh install or upgrade), if the external GPO might not have an exemption for this policy.

Casuser is not removed Log on a service Policy

- After a server reboot
- After a DB Backup
- Anytime Daemon Manager is restarted

If casuser is removed from Log on as a service Policy, aforementioned four services (CmfDbEngine, rptDbEngine, AusDbEngine and vmsDbEngine) fails to start, since the casuser doesn't have the permission to Log on Or Start any of them.

Solution

Verify if casuser account is included for Log on as a Service.

1) Open rsop.msc and navigate to **Computer Configuration >Windows Settings > Security Settings > Local Policies > User Rights Assignment.**

As shown in the image,

2) If casuser is not present for Log on as a Service

As shown in the image,

The GPO is pushed as a regular update, once it is applied on the server, verify the services again.

A manual [Group Policy Refresh](#) can also be forced on the server.

Restart the Daemon Manager and verify the fix. Ensure that the aforementioned four services (CmfDbEngine, rptDbEngine, AusDbEngine and vmsDbEngine) are up and runs well.

Related information

- **[casuser account](#)**
- **[Permissions required for casuser](#)**
- **[Basics of Group Policy Objects](#)**
- **[Log on as a service](#)**
- **[Technical Support & Documentation - Cisco Systems](#)**