

CSM Troubleshooting

Document ID: 108091

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Error:Policy or Assignment Locked when deleting devices associated with CSM

- Solution

Commands are removed from the PIX when CSM pushes additional changes

- Solution

Error when adding ASA running software version 8.2(1) to CSM

- Solution

Network configurations requesting more than 9 software licenses are blocked by SWIFT license server

- Solution

Error when trying to connect to CSM after a fresh installation

- Solution

Related Information

Introduction

This document describes how to resolve the error message that appears in the Cisco Security Manager (CSM).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the CSM 3.1.0 version.

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.

Error:Policy or Assignment Locked when deleting devices associated with CSM

This error message appears when you attempt to remove or delete the devices associated with CSM in order to

free up the CSM license:

Policy or Assignment Locked

Solution

Complete these steps in order to resolve this problem:

1. Make sure all users have either submitted or discarded their current activities and have logged out.
2. Login as a system admin and navigate to **Tools > Security Manager Administration > Workflow** in order to change the CSM to workflow mode.
3. Use **Tools/Activity Manager** to find any activities that are not in the **Approved** or **Discarded** state. In **Activity Manager**, you can click column head to sort the state column.
 - a. For activities in Edit or Edit Open state, open it and then discard.
 - b. For activities in Submitted state, reject it and then discard.
4. Change the CSM back to non-workflow mode.
5. Try to delete the devices again.

Commands are removed from the PIX when CSM pushes additional changes

Commands are removed from the PIX when CSM pushes additional changes.

Solution

This is the expected behavior for CSM. CSM will remove any out of band changes the next time it attempts to push changes to that device. It will query for the current configuration. However, you should only see this behavior in the transcript logs if you enable advanced debugging.

You can do this under **Tools--> Security Manager Administration --> Deployment --> Enable Advanced Debugging**. Remember, if you make any out of band changes for testing, you need to go back and make them in CSM as well. Otherwise, at the time of the next deployment, the changes will be lost.

Error when adding ASA running software version 8.2(1) to CSM

This error message is received when an ASA that runs the ASA software version 8.2.(1) is added to CSM:

```
Invalid device: The device combination of version "8.2(1) (N/A)"
and OS mode "ROUTER" and OS multiplicity "SINGLE" is not supported for
the device type of Cisco ASA-5520 Adaptive Security Appliance. Please
check if the image version is supported for this device type.
```

Solution

Support for ASA software versions 8.1(2) and 8.2(1) were first introduced in CSM version 3.3. This error occurs when the CSM version is earlier than 3.3. Upgrade CSM to version 3.3 in order to resolve this error message.

Network configurations requesting more than 9 software licenses are blocked by SWIFT license server

Network configurations requesting more than 9 software licenses within a 3-minute period may be blocked by the **SWIFT license server**. There are no indications in the CSM error log to indicate that access to the license server was blocked.

Solution

The Cisco software license server (SWIFT) contains safeguards to prevent high volumes of license requests from overloading the server. These safeguards currently permit a maximum of 9 license requests within a 3 minute interval for a given IP address. Enhancements provided in release 3.3 of the Cisco Security Manager (CSM) provide the capability to issue concurrent license requests from the SWIFT server. Some configurations of the **CSM 3.3** may result in requests for software licenses that exceed the SWIFT safeguard limitations and lead to the blocking of these requests. This action may prevent new software from being activated or result in the deactivation of software that requires license renewal.

The CSM product supports both manual (on-demand) and automatic modes for license verification. To reduce the chance that a license request is blocked by the SWIFT server when using manual (on-demand) mode, limit the license verification to no more than 9 devices per request. To reduce the chance that a license request is blocked by the SWIFT server when using automatic mode, it is recommended that the user reduce the thread count in the configuration file. This is accomplished by editing the `\MDC\ips\etc\sensorupdate.properties` file and changing the `licenseAutoUpdateThreadCount:50` entry to `licenseAutoUpdateThreadCount:5`. This will limit the number of concurrent license requests to five and help avoid overloading the license server. View Cisco bug ID CSCte83612 (registered customers only) in Bug Toolkit for more details.

Error when trying to connect to CSM after a fresh installation

After a fresh installation without any errors and reboot, could not connect to Cisco Security Manager 3.3.1. Noticed that Apache service is not starting after reboot. Started it manually, and this message appeared in Explorer:

```
Please wait..... System is still coming up. You will be
redirected to login page soon
```

Solution

This could be caused by the server having insufficient memory. Try to upgrade the memory on the server OR run this program on a machine that has sufficient memory.

Related Information

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

