Cisco UCSM Smart Plugin 2.3.1

For Windows

Operations Manual

Dec 24th, 2013

Table of Contents

1 Introduction

Cisco UCSM Smart Plugin provides the monitoring capability for Unified Computing System Manager (UCSM) nodes.

On integration of Cisco UCSM Smart Plugin with the Hewlett Packard Operations Manager (HPOM), you can use the HPOM console for managing the faults on UCSM. It enables you to view the service hierarchy of the UCS nodes being monitored and to view and acknowledge faults for the UCS node.

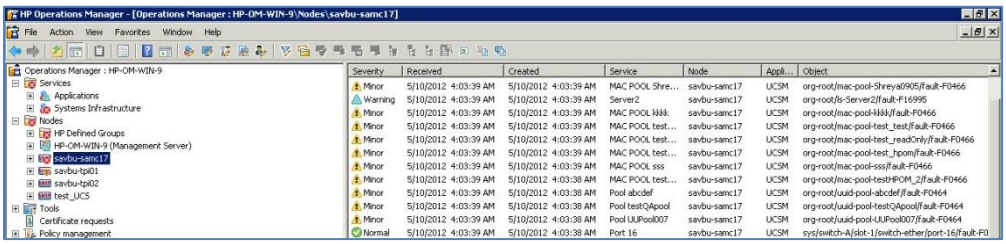
This Operations Guide describes the various operations which you can perform after installing the Cisco UCSM Agent Controller on the HPOM server.

1.1 Viewing Faults in HPOM

This section describes various ways of viewing the UCSM faults on HPOM.

To View all faults:

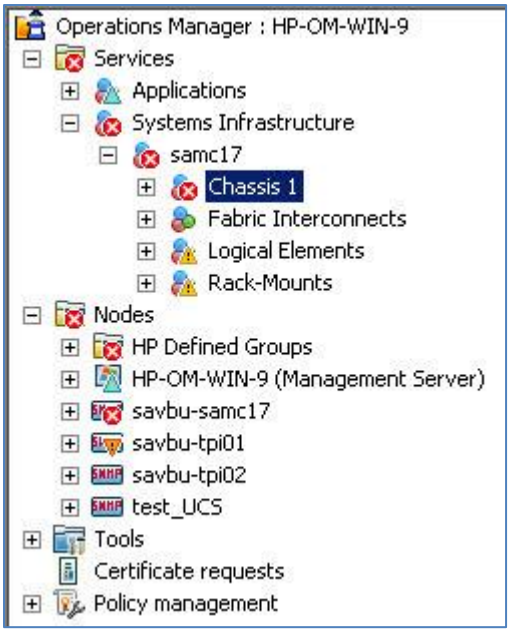
1. Select the node from Nodes list.
2. Select the UCSM node on the left panel in HPOM to see the faults.



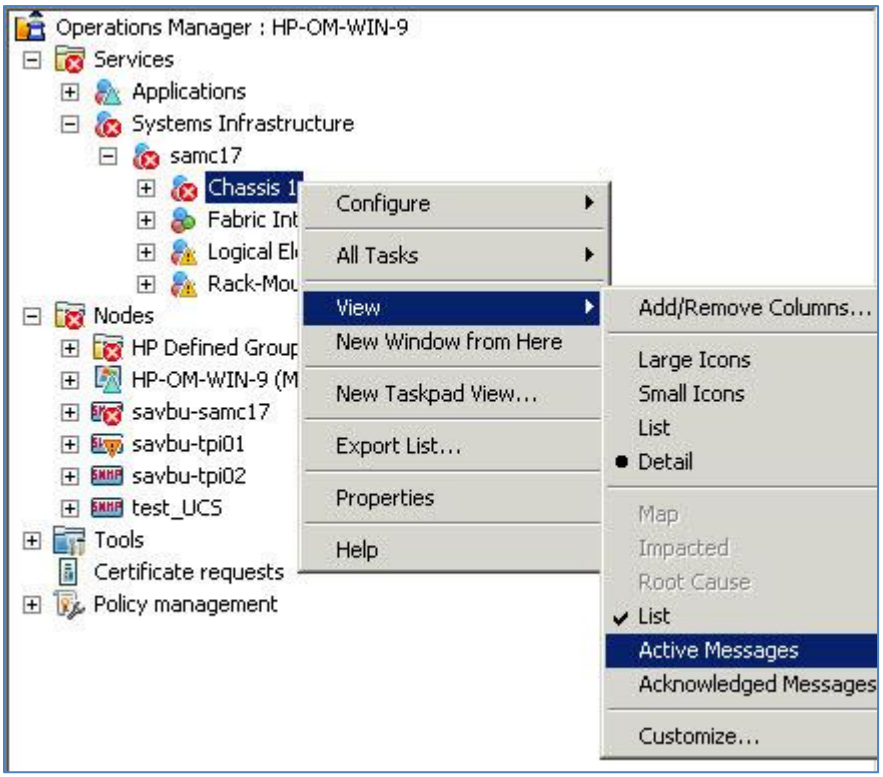
To View faults against a component:

You can also view only the faults against a particular component.

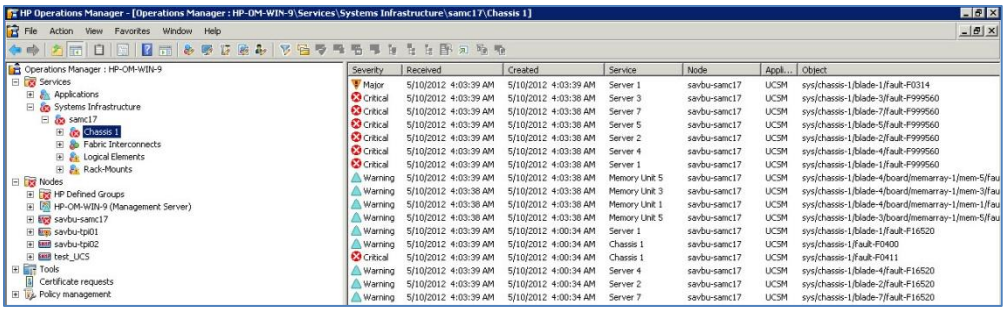
1. In the HPOM left panel, select the component and choose **Services > Systems Infrastructure > <UCSM node name>**.
   All the UCS components of the node appear.
2. Select the component for which the faults are to be viewed. Select **View** from the Right click menu.



3. Select the message type to view either **Active Messages** or **Acknowledged Messages** from the **View** menu.



4. The faults for the selected component appear in the HPOM window.



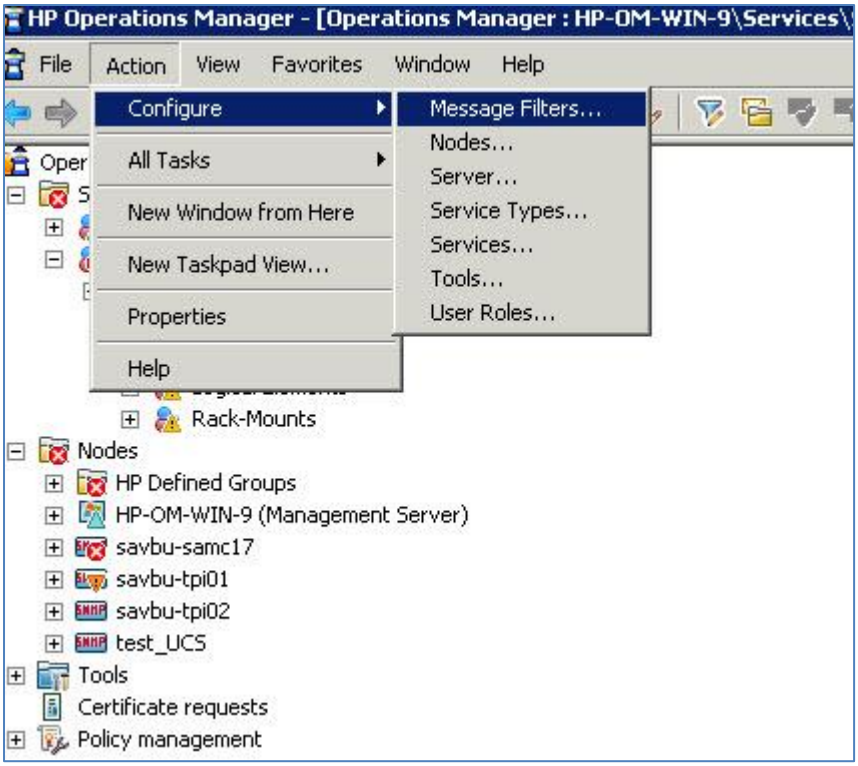
To View faults of a particular type:

You can view faults only of a particular type out of the below options:

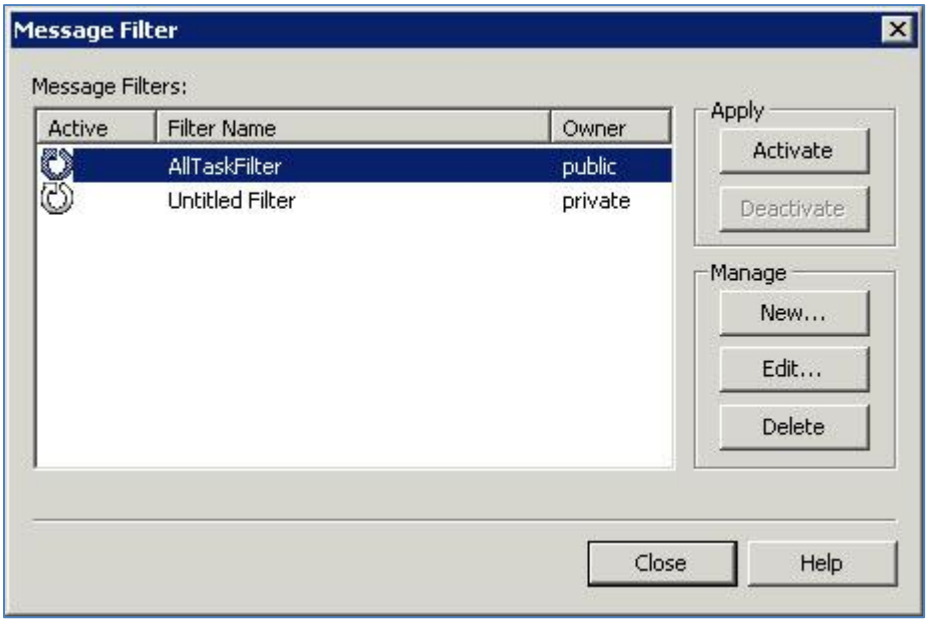
- generic
- equipment
- environmental
- management
- fsm
- sysdebug
- configuration
- server
- network
- connectivity
- operational

To do this, set Message Filters following the below steps:

1. In the **Action** tab, select **Configure** from the drop down menu. Select **Message Filters** from the Configure menu.

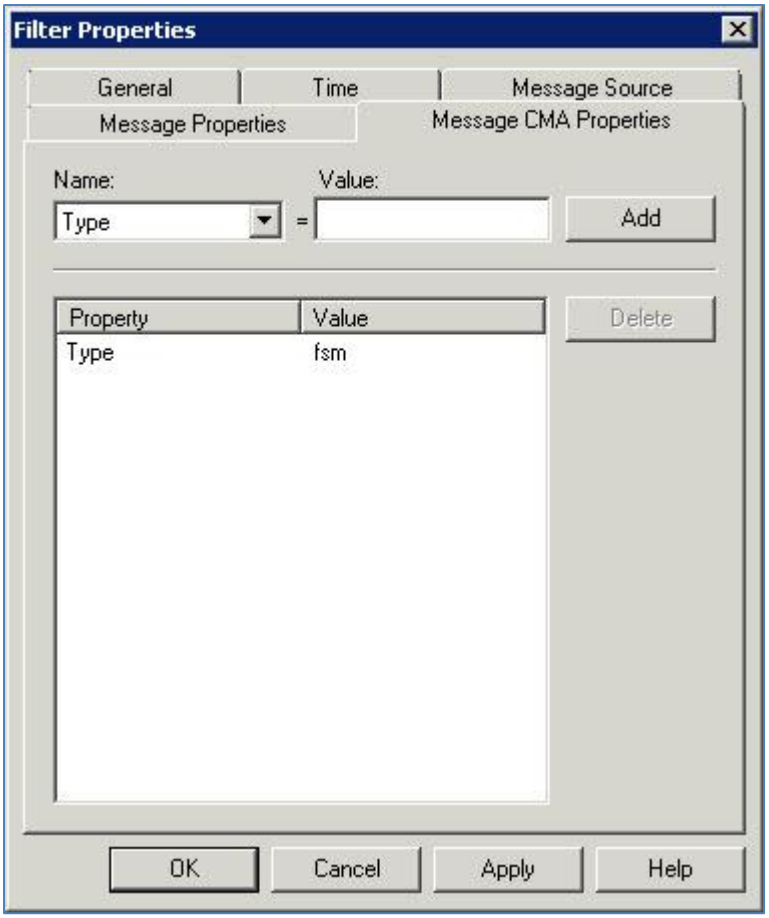


2. The **Message Filter** window appears.
   Click the **New** button.

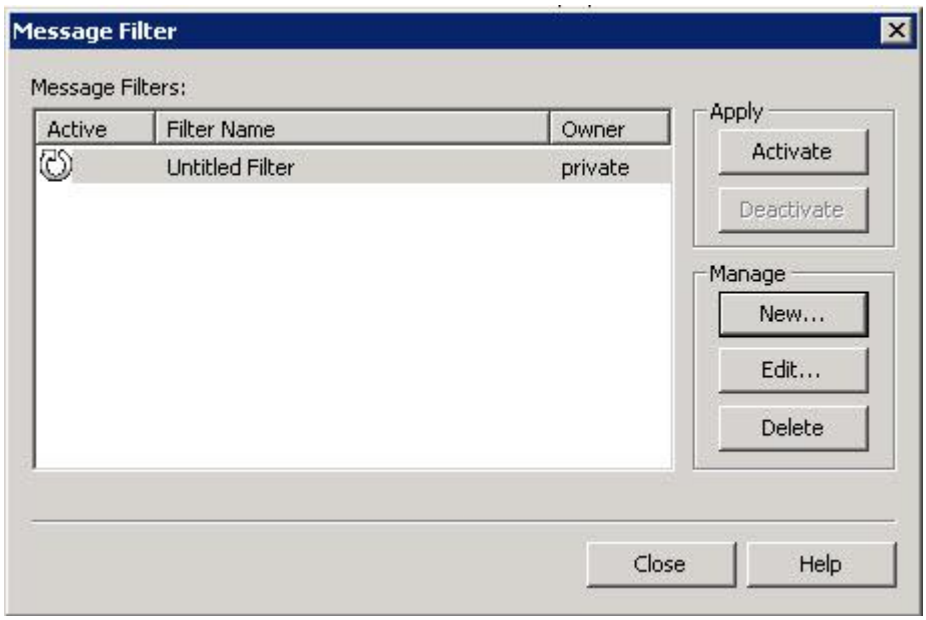


3. The **Filter Properties** window appears. In the **Message CMA Properties** tab, select the **Name** as **Type** from the drop-down menu. Specify a value like **fsm** in the Value textbox.

4. Click the **Add** button followed by the **OK** button.



5. The **Message Filter** window appears.
   Select the filter and click the **Activate** button.
   Note: In this scenario, only type 'fsm' faults will be available in the HPOM message browser.

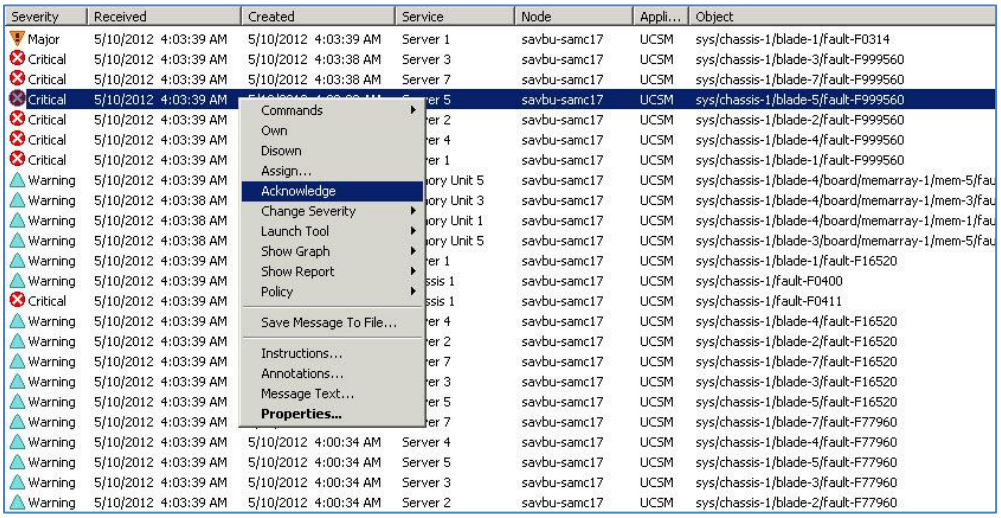


1.2 Acknowledging Faults in HPOM

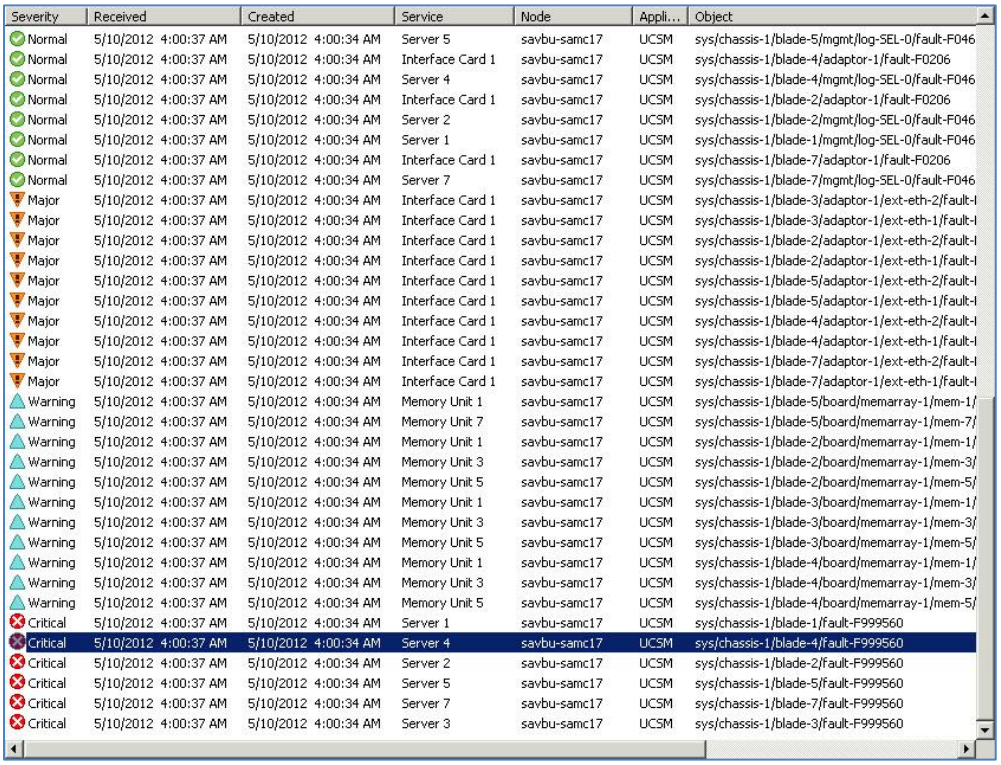
This feature enables you to acknowledge the faults in HPOM which are automatically synchronized with the selected UCSM node.

To acknowledge faults through HPOM:

1. Select the fault to be acknowledged and choose **Acknowledge** from the right click menu.



2. The fault moves from the list of Active Messages to the list of Acknowledged Messages in HPOM. The fault also gets acknowledged in the UCSM.



2 Plugin Features

This section describes various features provided with the Cisco UCSM Agent Controller like add and delete UCSM nodes for monitoring, start monitoring, stop monitoring, open the application logs, load a configuration file and provide server details.

2.1 Editing the Configuration File

This section describes the steps for editing the configuration file to add/delete the UCSM nodes or to edit an existing node.

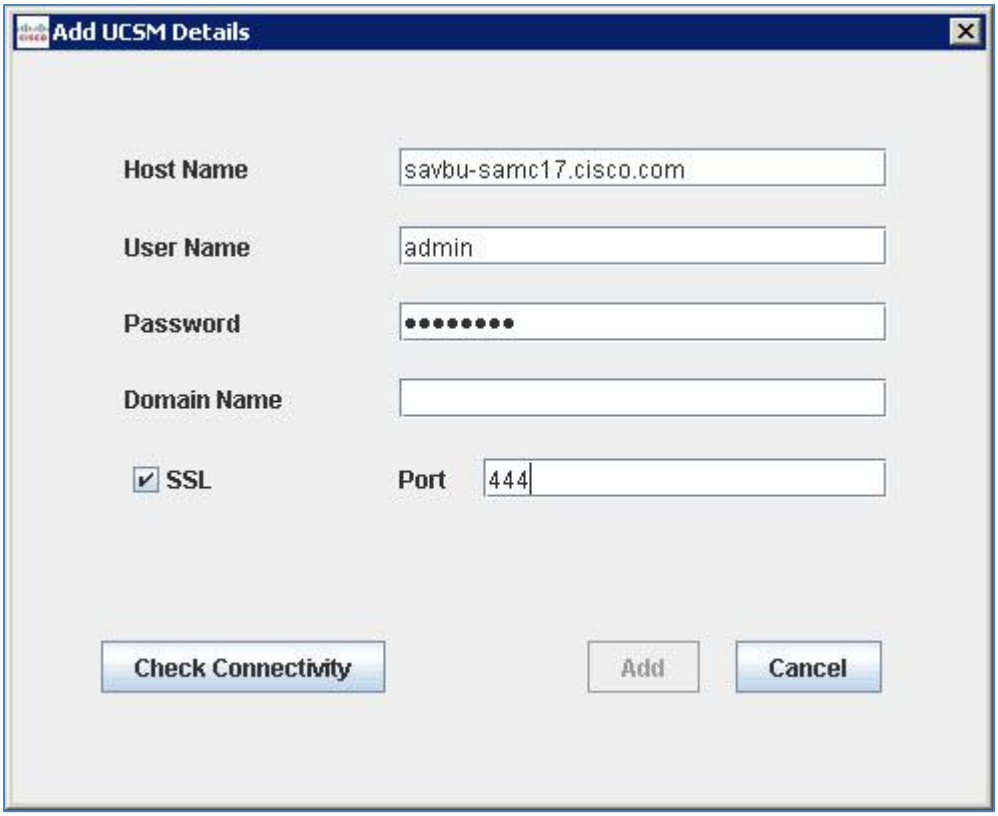
You can add/delete UCSM node entries in the configuration file while monitoring is in active state. However, while a UCSM node is in "Monitored" state, you cannot modify that node in the configuration table.

2.1.1 Adding UCS node details

To add the details of the UCSM nodes to be monitored:

1. On the Cisco UCSM Agent Controller window, click the **Add** button.

2. The **Add UCSM Details** window appears.
   Specify **Host Name, Username, Password** and **Port.**



Note: The SSL connection is checked by default. However, you can uncheck the SSL checkbox to change the connectivity to non-secure mode.

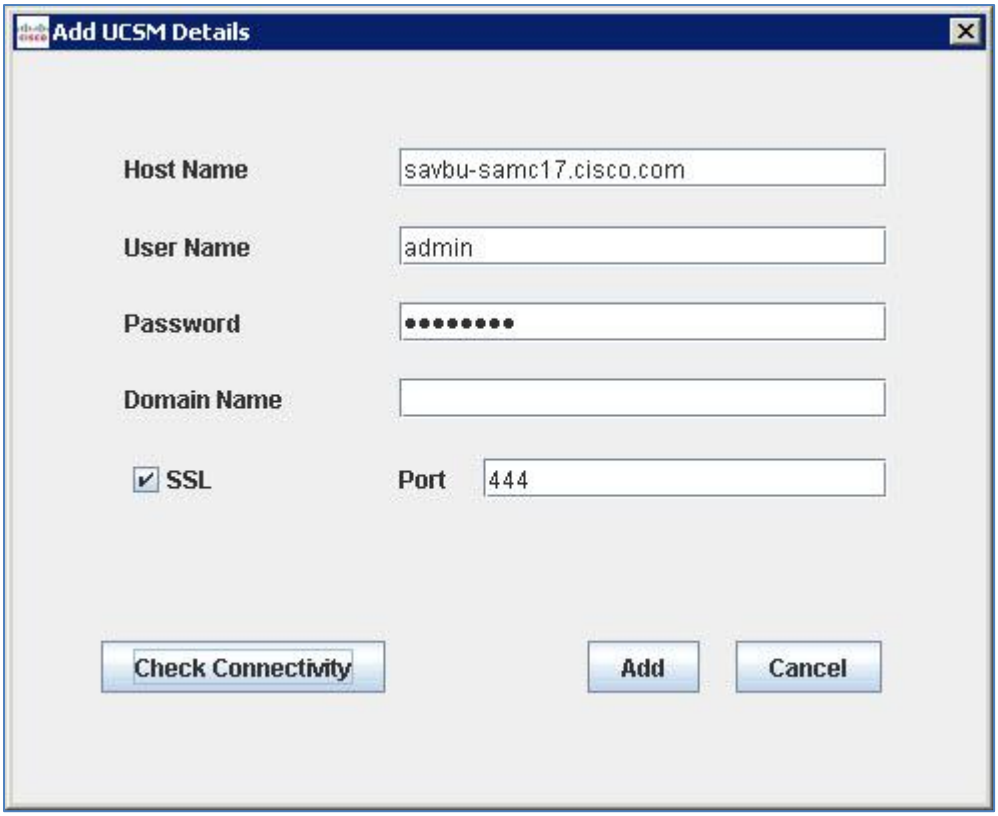
3. Click the **Check Connectivity** button to verify the connection to the UCSM and to enable Add button.
   The **Security Alert** window appears.

Note: In case of a secure connection (SSL checked), the server certificate check results appear.

4. To view the details of the certificate, click the **View Certificate** button.
   The **Details - Certificate** window appears.

5. Click the **Close** button.
   The **Security Alert** window appears.

6. Click the **Yes** button to accept the certificate.
   On successful connection, click the **Add** button in the **Add UCSM Details** window.

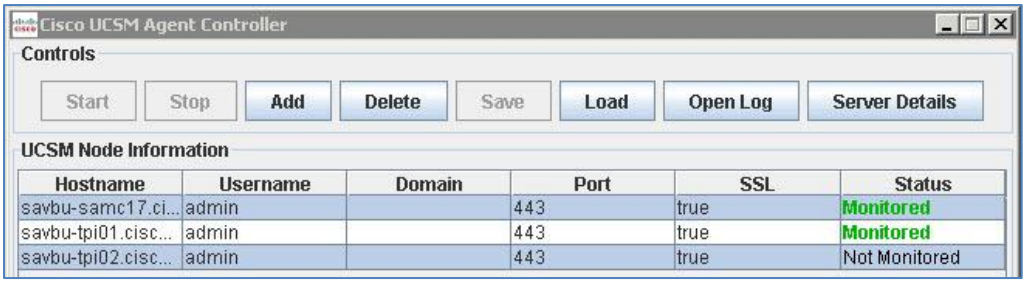


7. Click the **Save** button to save the node details in the application.
   The details are saved successfully.

2.1.2 Deleting an existing UCSM Node

To delete the UCSM nodes from the configuration file:

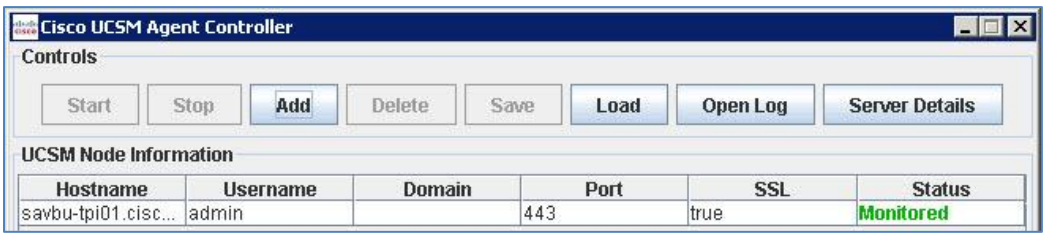
1. On the Cisco UCSM Agent Controller window, select the UCSM node(s) to be deleted from the configuration file. Click the **Delete** button.
   Note: The Delete button is enabled only when at least one row is selected from table.



2. A **Confirm Delete Message** dialog box appears.
   Click the **Yes** button.

3. Another **Confirm Delete Message** appears.

4. Click the **Yes** button.
   The **Save** button is enabled. Click the **Save** button.
   The UCSM Node Information table is updated with the remaining UCSM nodes and the status now changes to **Monitored**.



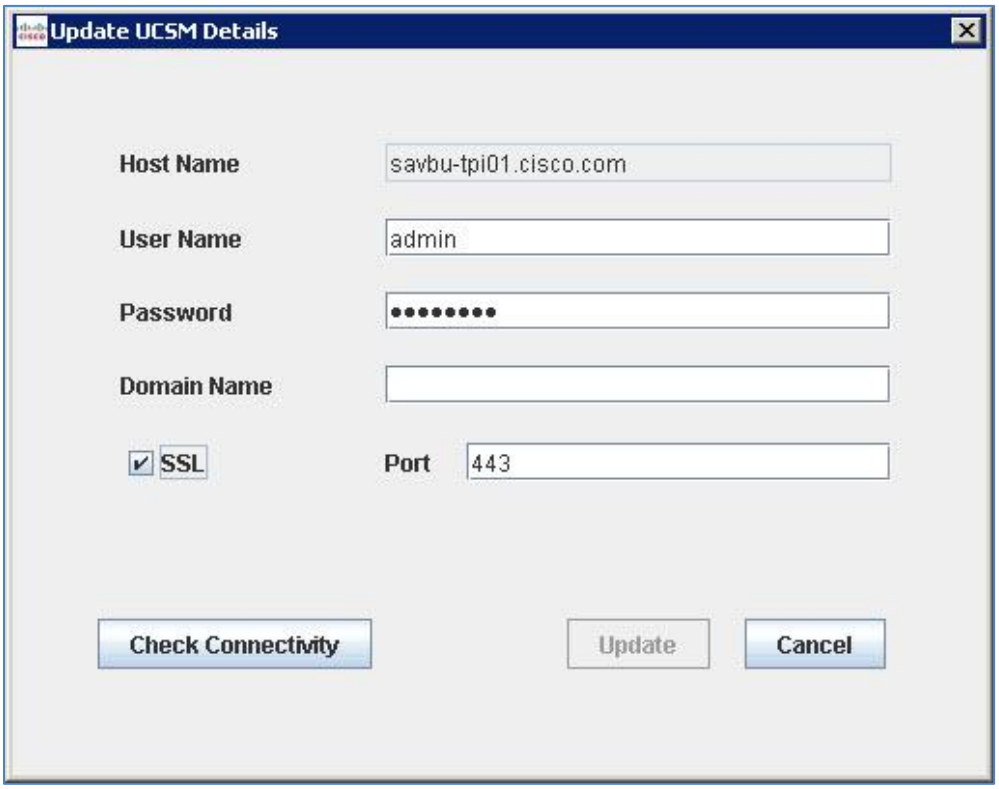
Note: Add/delete UCSM nodes in parallel on the HPOM, to reflect the changes made in the Cisco UCSM Agent Controller. To know more refer Section 2.3 (Configure HPOM) of Cisco UCSM Smart Plugin Install Guide_Windows.pdf.

2.1.3 Updating an existing UCSM Node

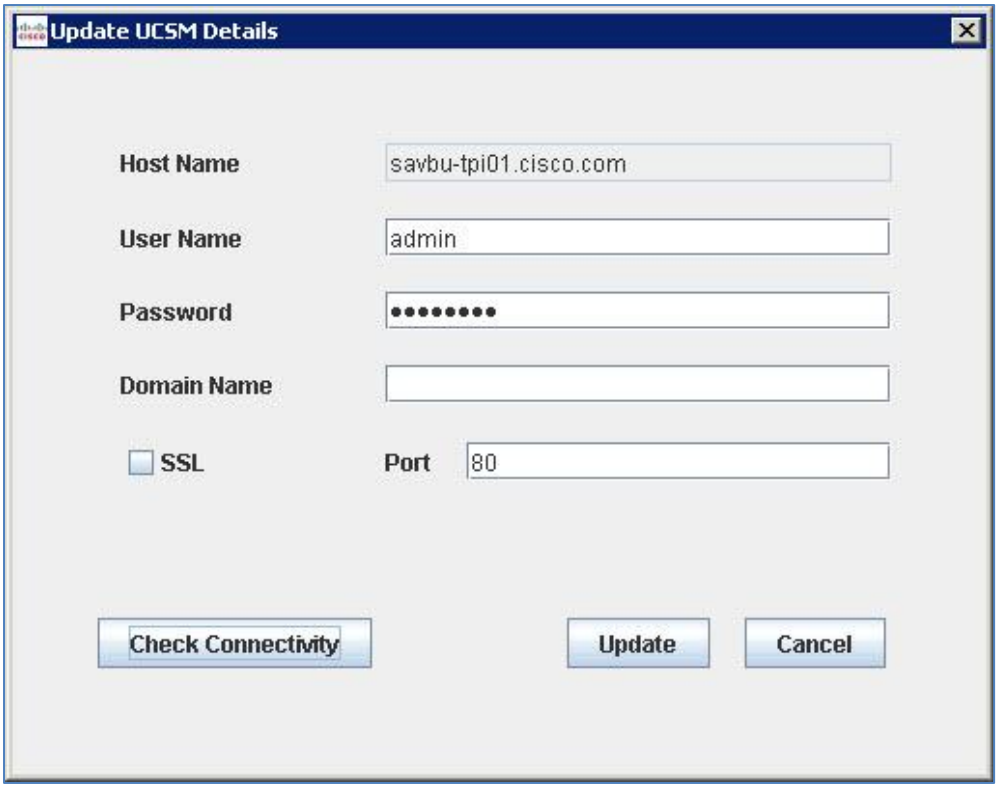
You can edit the UCSM nodes with status as Not Monitored or Faulted. The UCSM nodes with status as Monitored cannot be edited.

To update an existing UCSM Node:

1. Double click on Username/Domain/Port/SSL column of the appropriate row. The **Update UCSM Details** window appears.
2. Update any of the details in **User Name, Password, Domain Name, SSL** or **Port**. Click the **Check Connectivity** button.



3. After the connection successful message appears, the **Update** button is enabled on the **Update UCSM Details** window.



4. Click the **Update** button.
   The changes are reflected in the UCSM Node Information table.

5. Click the **Save** button.
   The changes are saved to the Configuration file.

2.1.4 Saving Configuration File

The Save button is enabled whenever following actions are performed on UCSM Node Information table:

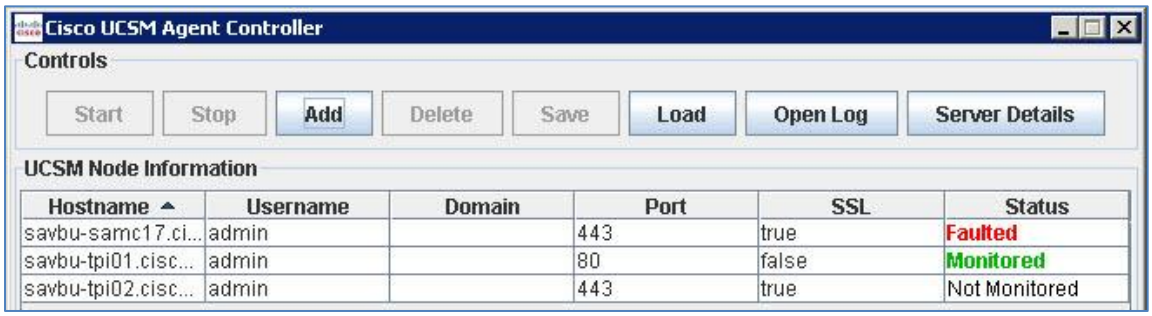
1. A new UCSM node is added in table.
2. One or more UCSM nodes are deleted from table.
3. A UCSM node in “Not Monitored” or “Faulted” state is edited.

The changes can be saved in configuration file by clicking Save on the Cisco UCSM Agent Controller window. After a successful save operation, a message box displays the status of saving the configuration file.

2.2 UCSM Node Monitoring Status

You can check the status of the UCSM nodes being monitored in Status column of UCSM Node Information table. The UCSM nodes for which monitoring are active are shown with status as Monitored in green color. If the monitoring has been stopped for some UCSM nodes due to some error condition or when you try to start monitoring but monitoring cannot be started, the status is shown as Faulted.

When a new UCSM node is added through Add button, or when the Stop operation is manually performed on a UCSM node, then status will be Not Monitored.



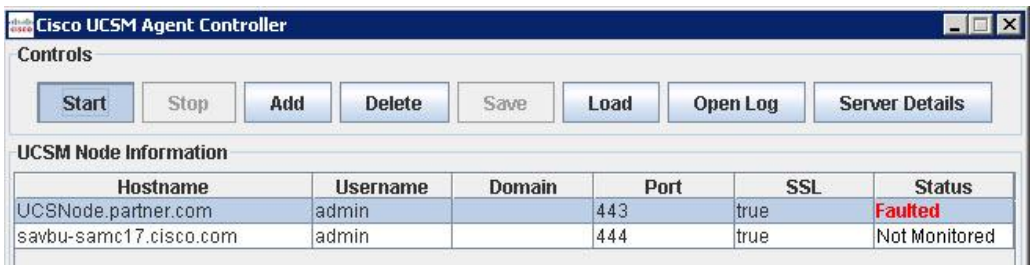
Note: On moving the mouse cursor over the Faulted status, a tooltip appears specifying one of the probable reason for "Faulted" state.

2.3 Loading UCSM Node Configuration File

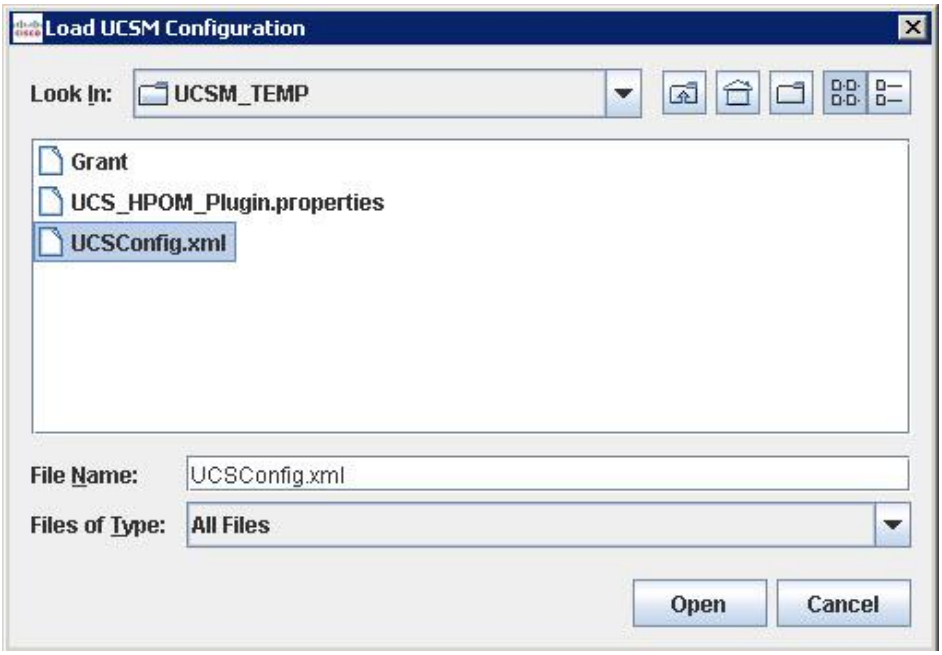
To load a UCSM Node Configuration File:

A Prerequisite for loading the UCSM node configuration file is to stop all the monitored UCSM nodes, before beginning the process of loading the node configuration file.

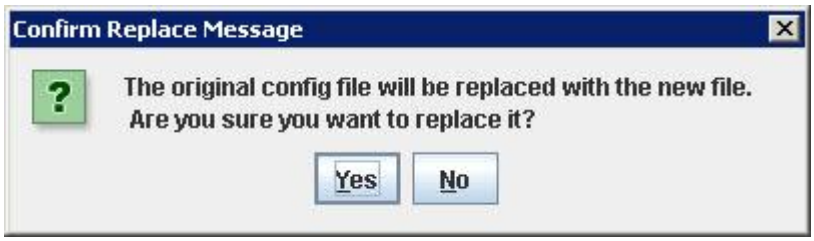
1. On the Cisco UCSM Agent Controller window, click the **Load** button.



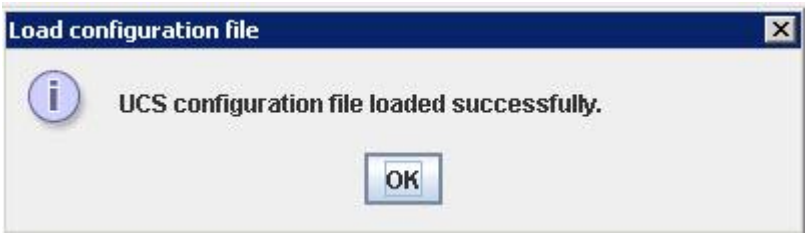
2. A **Load UCSM Configuration** dialog box appears.
   Select a valid UCSM Node configuration file (.xml) to be loaded and Click the **Open** button.



3. A **Confirm Replace Message** appears.
   Click the **Yes** button to replace the original configuration file with the new file.



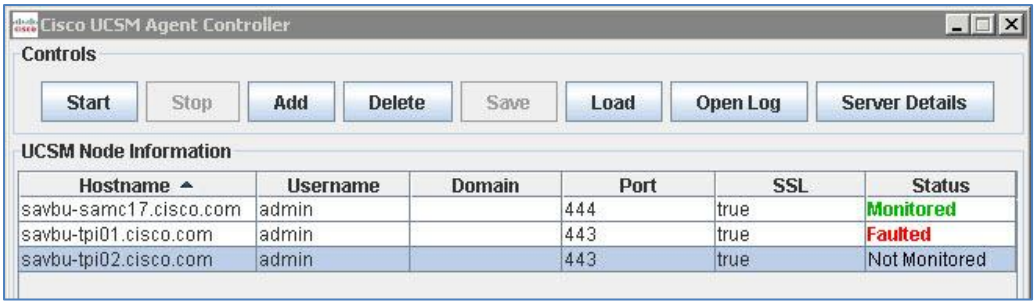
4. A **Load Configuration File** dialog box appears.
   Click the **OK** button to exit.



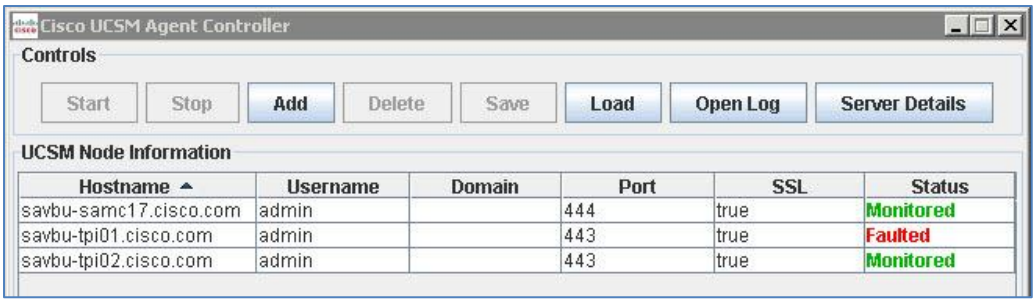
2.4 Start Monitoring

To start monitoring for multiple UCSM nodes in UCSM Node Information table:

1. Select multiple rows in the UCSM Node Information table, with status as **Not Monitored** or **Faulted**. The **Start** button is enabled.



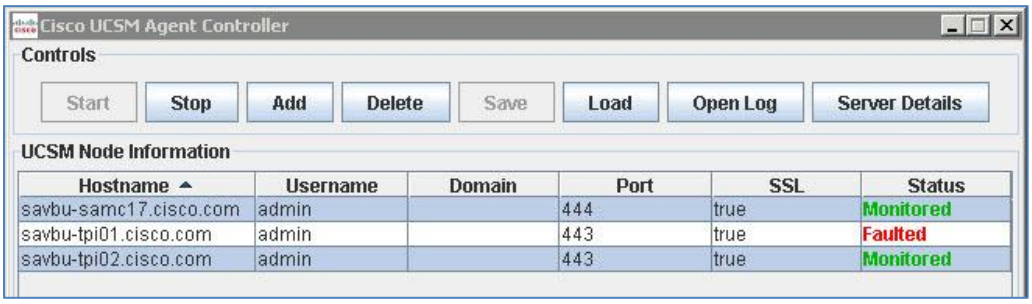
2. Click the **Start** button. The status of the selected nodes changes to **Monitored**.



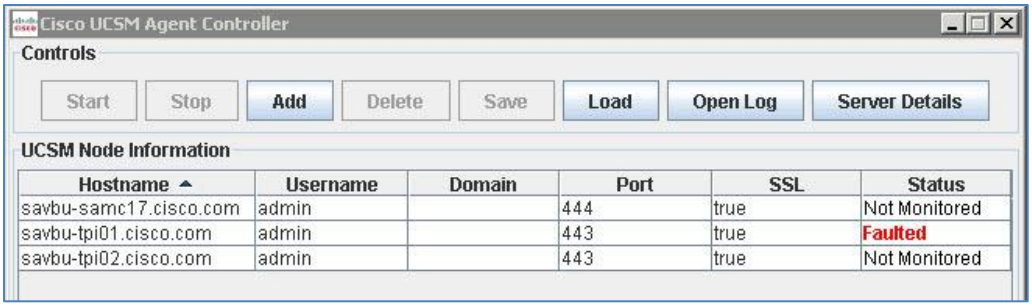
2.5 Stop Monitoring

To stop monitoring for multiple UCSM nodes in UCSM Node Information table:

1. Select multiple rows in the UCSM Node Information table, with status as **Monitored**. The **Stop** button is enabled.



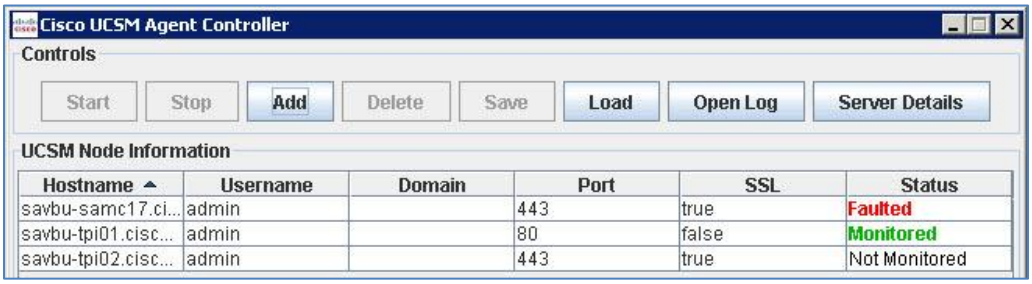
2. Click the **Stop** button. The status of the selected nodes changes to **Not Monitored**.



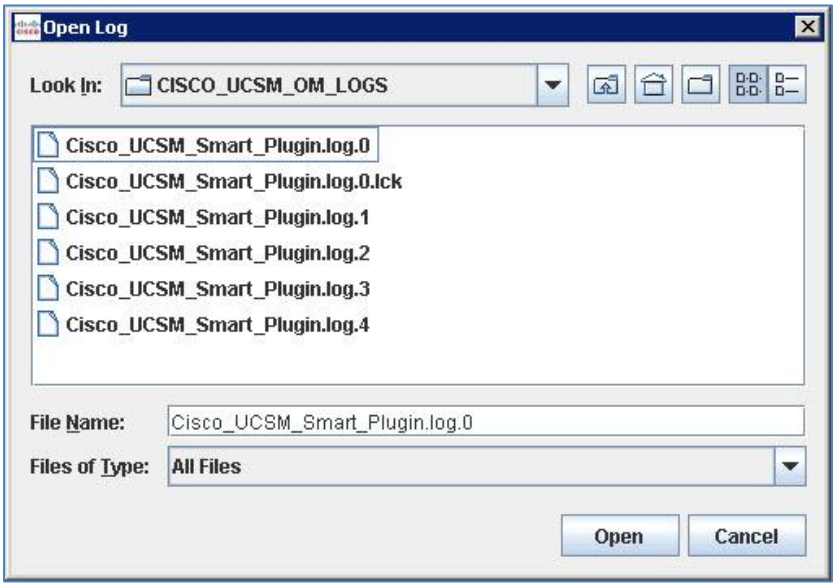
Note: When user selects both type of UCSM node rows with status as “Monitored” or “Not Monitored”/”Faulted” at the same time, both Start and Stop buttons will be disabled.

2.6 Open Log

1. Click the **Open Log** button in the **Controls** section of the Cisco UCSM Agent controller window.



2. The **Open Log** window appears.



Note: The log files are being continuously rolled after the file size reaches 5MB. At any given point of time, the latest five log files are available for users’ view. The Cisco_UCSM_Smart_Plugin.log.0 contains the current logs.

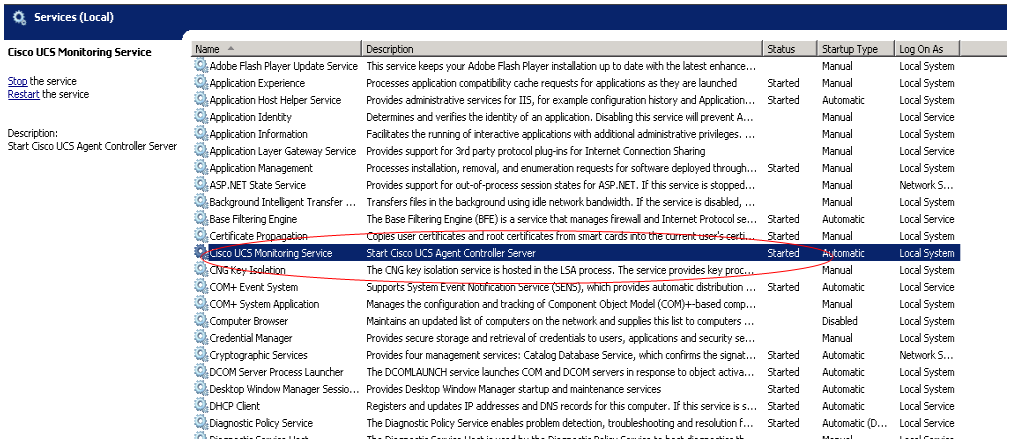
The location of the log files is :- %OvDataDir%/CISCO_UCSM_OM_LOGS.

3 Troubleshooting

This section provides information on the issues which may exist and how to bypass them.

3.1 Verifying Cisco UCSM Service is started

1. Verify if "CiscoUCSMonitorService" is started by launching the windows service manager.



2. In case of issues with starting the service refer to the service logs under :-

%SystemRoot%\System32\LogFiles\Apache.

3.2 Verifying Cisco UCSM Smart Plugin Installation

To verify successful installation of Cisco UCSM Smart Plugin:

1. Verify that the Cisco UCSM Agent Controller Shortcut is created on the Desktop.

2. Launch the HPOM console and verify that the policy group **CISCO_UCS_Policies** is created under **Policy Management > Policy Groups.**
3. Verify that the following policies are present in the **CISCO_UCS_Policies** (Policy Group):

- **UCS-AutoDiscovery**
- **UCS-Opcmsg**

4. If any of the above is missing, reinstall the Cisco UCSM Smart Plugin.

3.3 Plugin not starting after installation

1. After the Plugin is installed successfully, try to launch the smart plugin.
2. If it is unable to do so, then try the following steps :-

- Check if the windows user that you are logged in has the administrative privileges and is assigned to HP-OVE-ADMINS group.
- Check if ping and nslookup for your management server which is given in the plugin are working fine.

  Example:-

  C:\>ping hpomwindev.partner.com

  It should produce this result:-

  Pinging hpomwindev [10.29.143.180] with 32 bytes of data:
  Reply from 10.29.143.180: bytes=32 time<1ms TTL=128
  Reply from 10.29.143.180: bytes=32 time<1ms TTL=128
  Reply from 10.29.143.180: bytes=32 time<1ms TTL=128

  and nslookup

  C:\>nslookup Hpomwindev.partner.com

  Result should be:-

  Server: ldap.partner.com
  Address: 10.29.143.13

  Name: Hpomwindev.partner.com
  Address: 10.29.143.180
- Now run the runclient.bat utility provided by HP at the following location:- C:\Program Files\HP\HP BTO Software\support\OprWsInc\client\java.

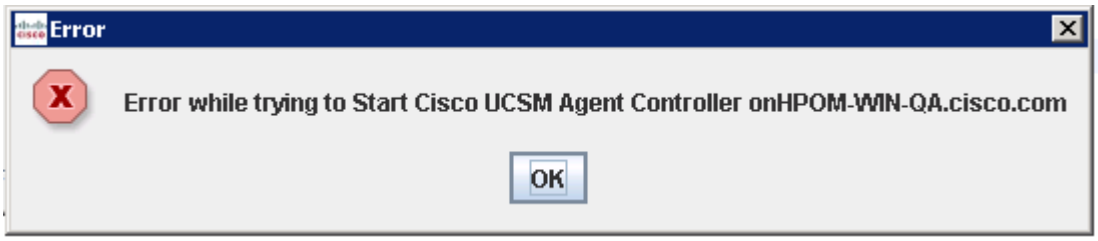
  Example :- With Administrator :-

  C:\Program Files\HP\HP BTO Software\support\OprWsInc\client\java>runclient.bat -host WINQA -port 443 -user Administrator -password mypass -ssl -action subscribe.

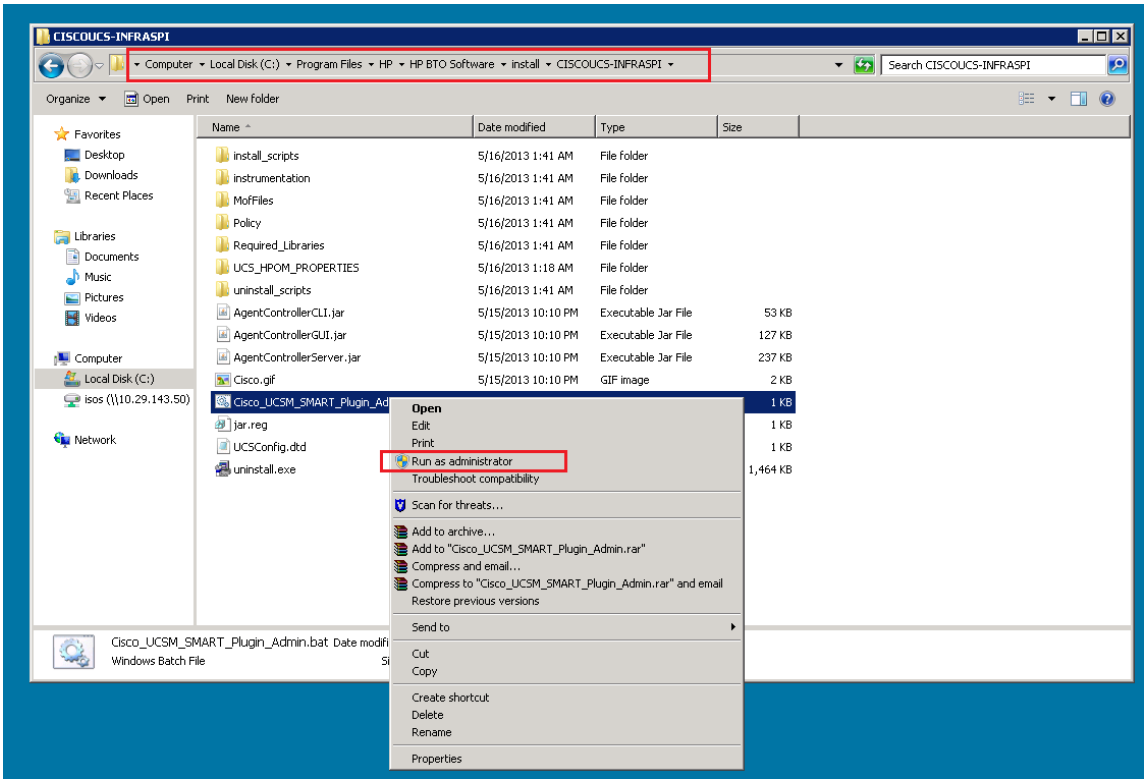
  This should give a result like this:-

  <Context>c7bdc21e-2b84-47e5-ab47-1e53975dbef5</Context>
  <Expires>2013-04-03T23:40:13.828-07:00</Expires>
- Check if your system has firewall enabled.
- Check if your windows user has the read and write permissions on the following folders :-
  1. C:\ProgramData\HP\HP BTO Software\bin\instrumentation.
  2. C:\Users\<User>\AppData\Local\Temp\1\CISCO_UCSM_LOGS.
  3. C:\Users\<User>\UCSM_TEMP.

3. After verifying these things, if you are still getting a screen like this :-

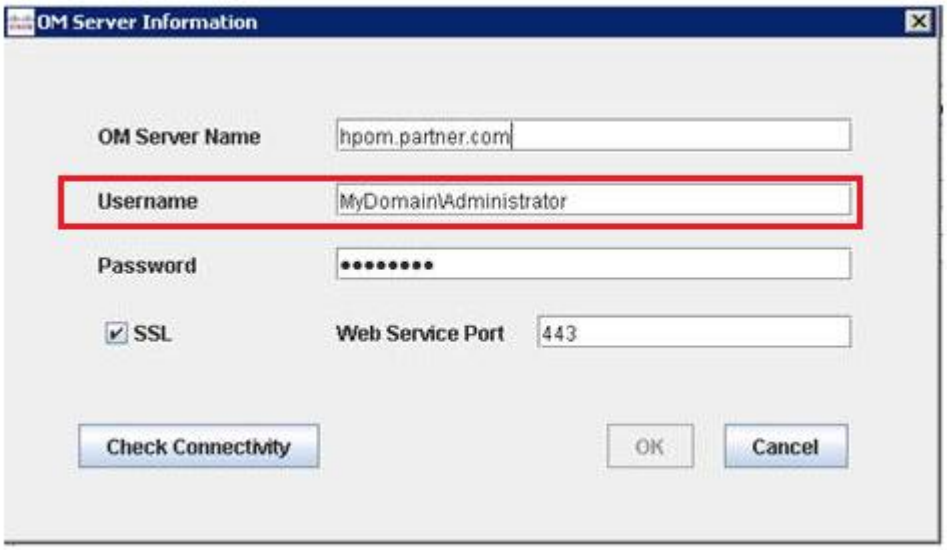


Then go to highlighted path which is the installation directory.



And run the Cisco_UCSM_SMART_Plugin_Admin.bat file as administrator.

4. If you are a domain user then provide your domain information as domain\username



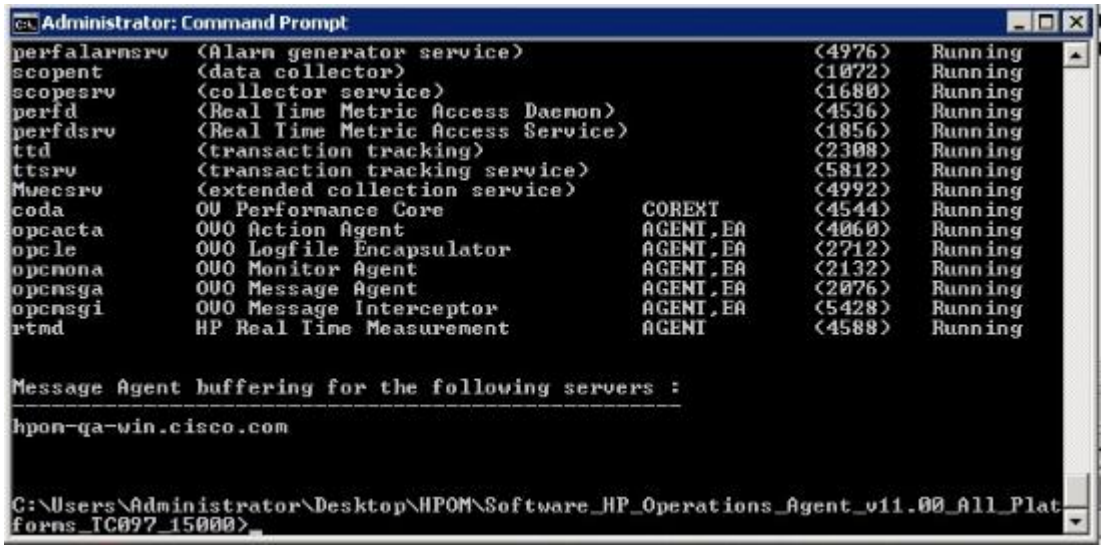
3.4 Faults not populating in HPOM due to improper install

1. Verify a proper installation of the Cisco UCSM Smart Plugin. To read more on installation refer, **Cisco UCSM Smart Plugin Install Guide_Win.pdf**.
2. Verify that the HPOM services are in the running state. Check this by running command "`ovc -status`" on command prompt.
3. Check if UCSM node details have been provided correctly.
4. Check the monitoring status.
5. Restart the monitoring through Cisco UCSM Agent Controller. Click Stop and then click Start.
6. If none of the above described resolves the issue, restart the HPOM Console.

3.5 Faults not populating in HPOM due to agent buffering

HPOM Agent (opcagt) keeps on buffering messages continuously for longer run due to which faults generated are not populated. Check if the agent is buffering the

1. Confirm if the agent is buffering the messages by running command "`opcagt -status`" on command prompt.



If the agent is buffering the messages then as a workaround, perform the following steps after which the faults should start appearing in HPOM.

1. Stop Monitoring and close the Smart Plugin GUI and server process completely.
2. Kill ovc services by running command "`ovc -kill`" on command prompt.
3. Kill opcagt services by running command "`opcagt -kill`" on command prompt.
4. Clear the directory %OvShareDir%\tmp\OpC (Clear only the files and do not delete the directories.)
5. Clear the directory %OvDataDir%\tmp\OpC (Clear only the files and do not delete the directories.)
6. Now start the ovc services by running command "`ovc -start`" on command prompt.
7. Now start the opcagt services by running command "`opcagt -start`" on command prompt.

3.6 Faults not getting acknowledged in HPOM

1. Verify a proper installation of the Cisco UCSM Smart Plugin. To read more on installation refer, **Cisco UCSM Smart Plugin Install Guide_Win.pdf**.
2. Verify that **UCS-Opcmsg** policy is deployed on the UCS nodes in HPOM as described in Section 2.3.2 (Deploying the policies) of **Cisco UCSM Smart Plugin Install Guide_Windows.pdf**
3. Verify that you have the required permissions to acknowledge faults on UCSM. Acknowledgement of faults from HPOM to UCSM will fail, in case you have "read-only" permissions on the UCS.
4. Verify that the HPOM services are in the running state. Check this by running command "`ovc -status`" on command prompt.
5. One of the known issues is that the duplicates faults of HPOM do not get acknowledged when acknowledged from UCS.
6. Check the monitoring status.
7. If none of the above described resolves the issue, restart the monitoring by clicking Stop and then Start on the Cisco UCSM Agent Controller for the UCSM node.

3.7 Service Hierarchy not appearing in the HPOM

1. Ensure that the UCSM node details have been provided correctly using Edit Config button on Cisco UCSM Agent Controller. It may take up to 30 minutes for the service hierarchy to get populated in the HPOM.
2. If the hierarchy still doesn't populate , restart the "ovc" services following the below steps:
   - Uninstall the **UCS-AutoDiscovery** policy
   - Execute **ovc -stop** on the command prompt
   - Execute **ovc -start** on the command prompt.
   - Deploy the **UCS-AutoDiscovery** policy

3.8 Application not monitoring after rebooting the system

The agent's buffer files have got corrupted, which could be due to an ungraceful exit of Agent on this machine. Executing the following steps should resolve this issue:

1. Open a command prompt with Administrator privileges and execute **ovc -kill**.
2. Manually delete all the files in **%OvDataDir%\tmp\OpC**.
   (Default HPOM Data Directory is "C:\ProgramData\HP\HP BTO Software")
3. Execute **ovc -start** on the command prompt.

3.9 Old messages in HPOM does not get acknowledged after a while

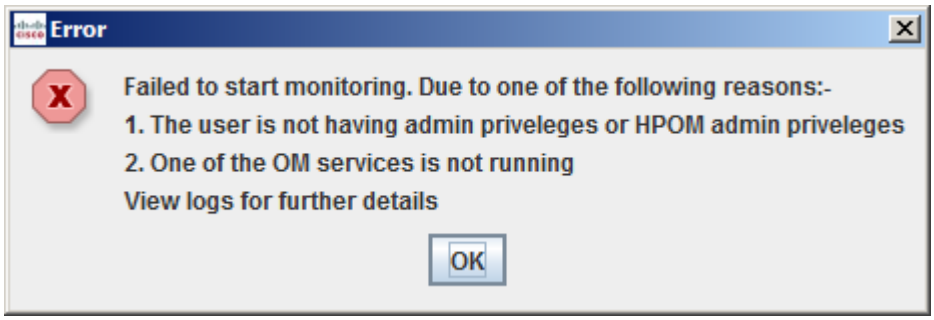
On acknowledging the existing active messages from UCSM, the messages get acknowledged on UCSM but the same sets of messages are not acknowledged in HPOM.

These messages are still visible in HPOM active messages list. This may occur on the second or third day after monitoring has been started. As a workaround following steps can be followed

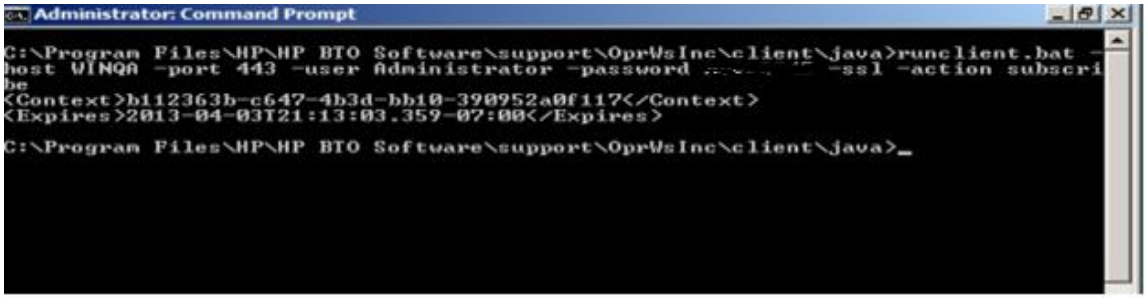
1. Stop Monitoring and close the Smart Plugin GUI and server process completely.
2. Delete all the faults from HPOM GUI using the following commands.
   a. Change the directory by running "cd %OvInstallDir%\support" on the command prompt.
   b. Now delete all the existing messages in the HPOM by running "ovowmsgutil -del -exp *" on the command prompt.
3. Now open the Smart Plugin GUI and start monitoring. Acknowledge the faults now & it should work fine.

3.10 Subscription fails

On Start of the Plugin, If the plugin fails to monitor one particular UCS, and it displays this:-



Then try and run the following script on CLI:-



If this command is not working then the subscription fails because the user which is neither system admin nor HPOM admin cannot start HPOM.

In this case the user may need to contact HP for further support.

4 Cisco Support

For any queries/issues, add a discussion to the Cisco Developed Integrations sub-space on Cisco UCS Communities.

Give the following details for quicker resolution of the issues.

- HPOM Version and OS Details
- Number of UCS Domains monitored.
- Version of UCSM

5 Related Documentation

In addition to this guide, you can also refer to the **Cisco UCSM Smart Plugin Install Guide_Windows.pdf** to know more about the installation procedure to be followed on Windows system.

6 Appendix

6.1 Mapping of Faults from UCSM to HPOM

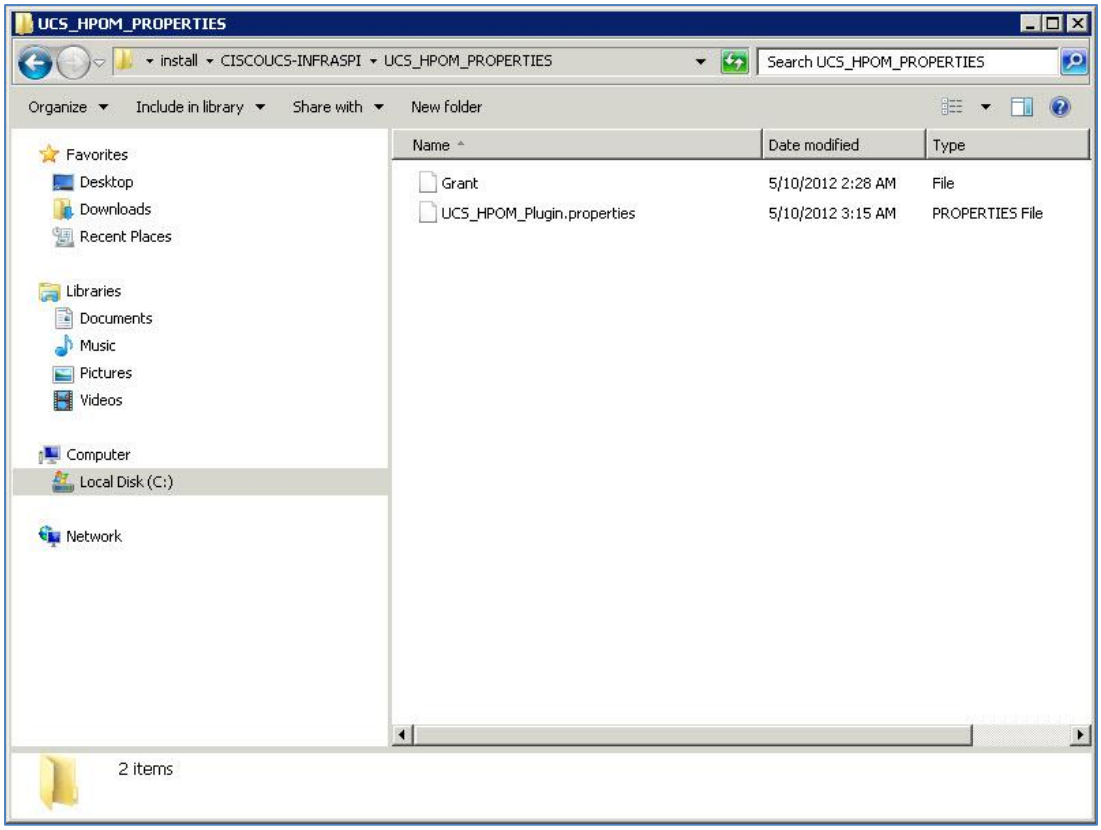
The severity levels of the faults received from UCSM are mapped to the severity levels in HPOM according to the following table:

Fault Category in UCSM	Fault Category in HPOM
Cleared	Normal
Critical	Critical
Info	Normal
Major	Major
Minor	Minor
Warning	Warning

6.2 Properties File

The Cisco UCSM Agent Controller maintains a properties file which contains the user configurable parameters. If needed, the user can modify these values.

Location of properties file: "%OvInstallDir%\install\CISCOUCS-INFRASPI\UCS_HPOM_PROPERTIES"
File Name: **UCS_HPOM_Plugin.properties** (open with Notepad)



The file looks like:

```
#***PROPERTIES DESCRIPTION***
# OMServerName: This is the ip address or hostname of the server where HPOM is installed.
# WebServiceUserName: This is the Login Username of HPOM server.
# WebServicePassword: This is the Login Password of HPOM server. Password is encryped, please do not make any manual modifications to this property.
# WebServiceMode: This is the mode of communication with of HPOM server (secure - https or non secure - http).
# WebServicePort: This is the HPOM web service port number.
# FaultAckDelay: This is delay between two consecutive acknowledgement calls in HPOM Faults. The value is in milliseconds. Increase the value if acknowledgements are getting missed while loading faults (first time) from UCSM.
# UcsRetryInterval: If connection to UCS is interrupted, then it will try to resubscribe to UCS. This property is interval(in minutes) between resubscribe attempts.
# UcsRetryCountIf connection to UCS is interrupted, then it will try to resubscribe to UCS. This property is number of resubscribe attempts.
# OMRetryInterval: If connection to HPOM is interrupted, then it will try to resubscribe to HPOM. This property is interval(in minutes) between resubscribe attempts.
# OMRetryCountIf connection to HPOM is interrupted, then it will try to resubscribe to HPOM. This property is number of resubscribe attempts.
# OMServiceCheck : This is the flag to enable/disable the check performed to ensure the required services are running before the application starts.
# ServerAliveInterval : This is the time interval for polling to check that the server is alive.
#Thu May 10 03:15:42 PDT 2012
UcsRetryCount=3
WebServicePort=443
OMRetryInterval=3
WebServiceMode=https
UcsRetryInterval=3
OMRetryCount=3
OMServerName=10.29.143.41
FaultAckDelay=300
WebServiceUserName=Administrator
OMServiceCheck=false
WebServicePassword=284E08ED2677B3068F6625694E027DDD
```

Following are the parameters covered in the properties and their description:

- **OMServerName:** This is the IP address or hostname of the server where HPOM is installed.

- **WebServiceMode:** This is the mode of communication with of HPOM server (secure - https or non secure - http).
- **WebServicePort:** This is the HPOM web service port number.
- **WebServiceUserName:** This is the username of HPOM server login.
- **WebServicePassword:** This is the password of HPOM server Login. Password is encrypted; please do not make any manual modifications to this property.
- **WebServicePort:** This is the HPOM web service port number.
- **FaultAckDelay:** This is delay between two consecutive acknowledgement calls of HPOM Faults. The value is in milliseconds. Increase the value if acknowledgements are getting missed while loading faults (first time) from UCSM.
- **UcsRetryInterval:** If connection to UCS gets interrupted, the application tries to resubscribe to UCS. This property defines the time interval between re-subscribe attempts. Default
- **UcsRetryCount:** If connection to UCS is interrupted, the application tries to resubscribe to UCS. This property defines the number of re-subscribe attempts.
- **OMRetryInterval:** If connection to HPOM is interrupted, then it will try to re-subscribe to HPOM. This property defines the time interval between re-subscribe attempts.
- **OMRetryCount:** If connection to HPOM is interrupted, then it will try to re-subscribe to HPOM. This property defines the number of re-subscribe attempts.
- **OMServiceCheck:** This is the flag to enable/disable the check performed to ensure the required HPOM services are running before the application starts.