Cisco IMC Smart Plugin 1.0

For HP Operations Manager - Windows

Operations Guide

Mar 12th, 2014

Table of Contents

1 Introduction

Cisco IMC Smart Plugin provides the monitoring capability for IMC nodes.

On integration of Cisco IMC Smart Plugin with the Hewlett Packard Operations Manager (HPOM), you can use the HPOM console for managing the faults on IMC (Cisco Integrated Management Controller). It enables you to view the service hierarchy of the IMC nodes being monitored.

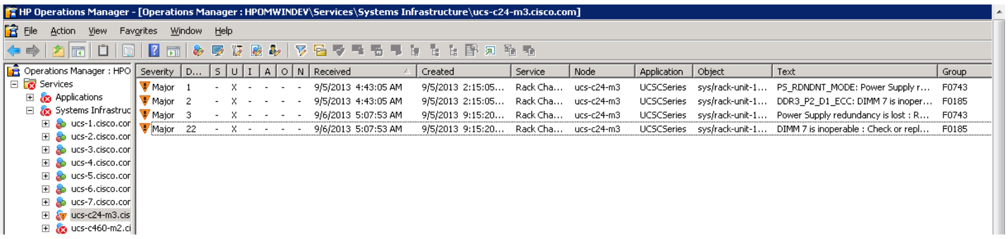
This Operations Guide describes the various operations which you can perform after installing the Cisco IMC Agent Controller on the HPOM server.

1.1 Viewing Faults in HPOM

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

To View all faults:

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



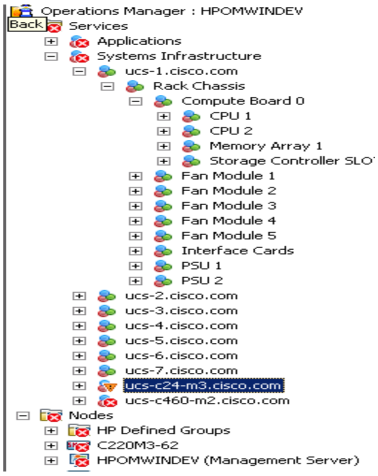
HP Operations Manager - [Operations Manager : HPOMWINDEV\Services\Systems Infrastructure\ucs-c24-m3.cisco.com]

Severity	D...	S	U	I	A	O	N	Received	Created	Service	Node	Application	Object	Text	Group
Major	1	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:15:05...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	PS_RDNDNT_MODE: Power Supply r...	F0743
Major	2	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:15:05...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	DDR3_P2_D1_ECC: DIMM 7 is inoper...	F0185
Major	3	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:15:20...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	Power Supply redundancy is lost : R...	F0743
Major	22	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:15:20...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	DIMM 7 is inoperable : Check or repl...	F0185

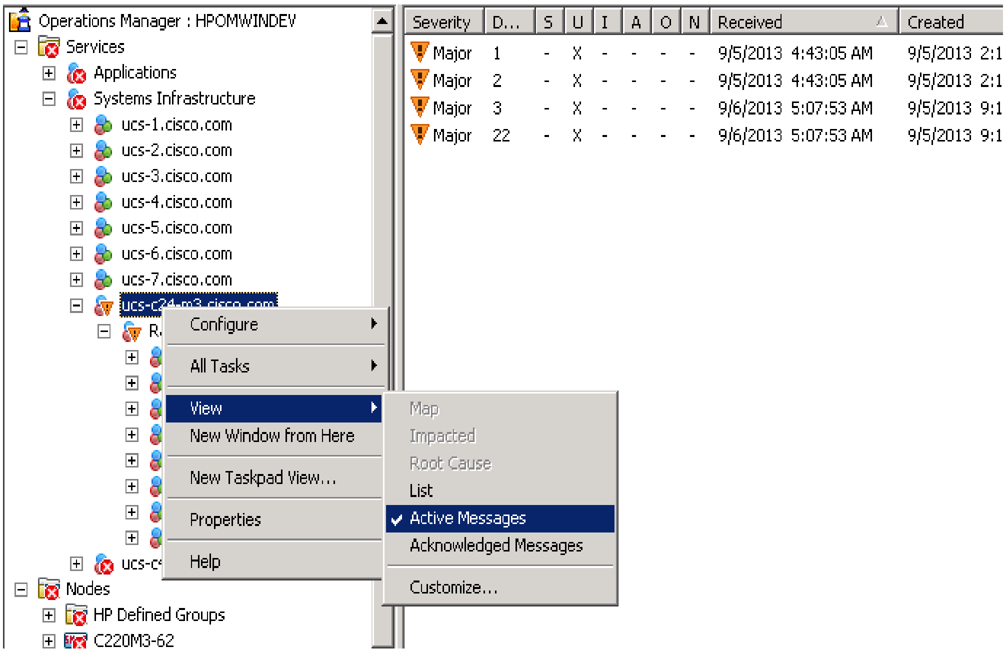
To View faults against a component:

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 > <IMC node name>**.
   All the UCS IMC components of the node appear.
2. Select the component for which the faults are to be viewed. Select **View** from the Right click menu.

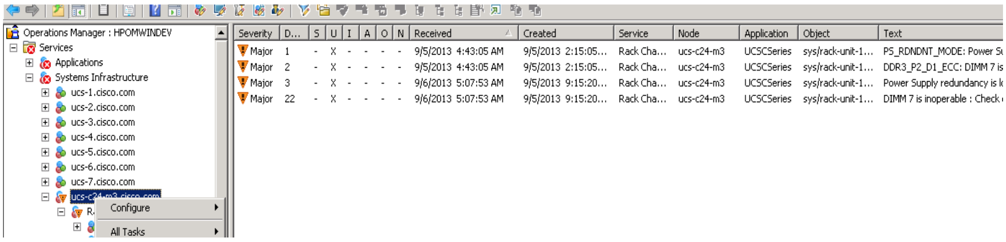


3. Select the message type to view either **Active Messages** from the **View** menu.



Severity	D...	S	U	I	A	O	N	Received	Created
Major	1	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:1
Major	2	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:1
Major	3	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:1
Major	22	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:1

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



Severity	D...	S	U	I	A	O	N	Received	Created	Service	Node	Application	Object	Text
Major	1	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:15:05...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	PS_RDNDNT_MODE: Power Su
Major	2	-	X	-	-	-	-	9/5/2013 4:43:05 AM	9/5/2013 2:15:05...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	DDR3_P2_D1_ECC: DIMM 7 is
Major	3	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:15:20...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	Power Supply redundancy is l
Major	22	-	X	-	-	-	-	9/6/2013 5:07:53 AM	9/5/2013 9:15:20...	Rack Cha...	ucs-c24-m3	UCSCSeries	sys/rack-unit-1...	DIMM 7 is inoperable : Check

To View faults of a particular type:

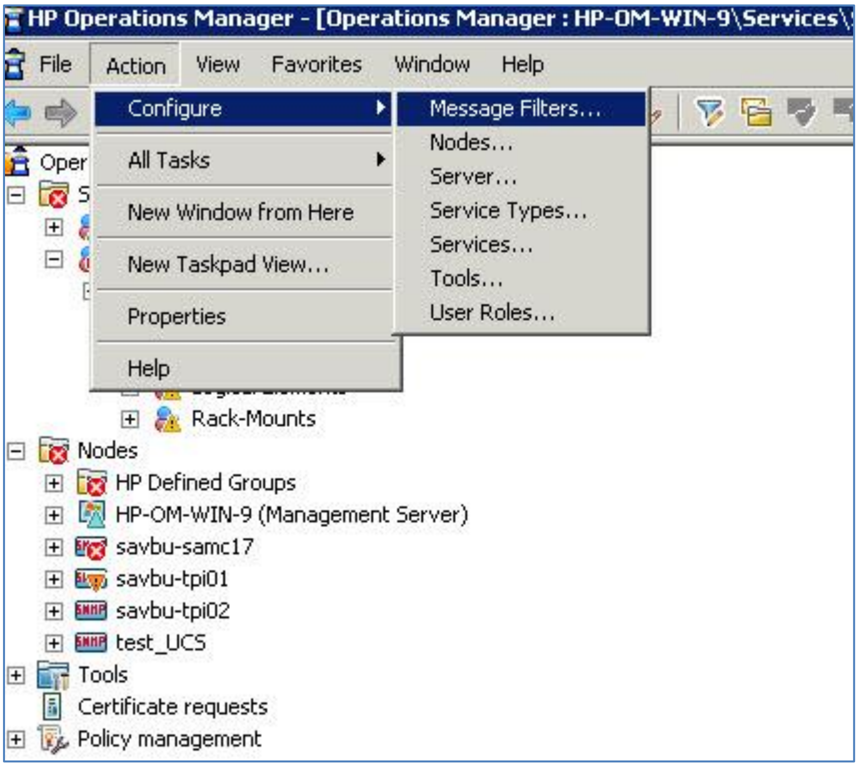
You can view faults only of a particular type out of the below options:

- generic
- equipment
- environmental
- management

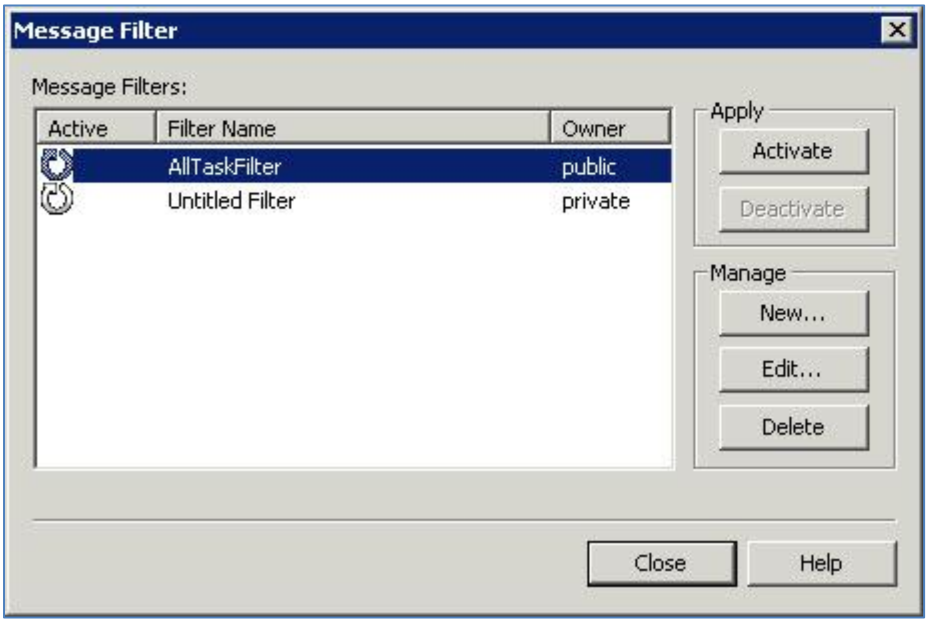
- fsm
- sysdebug
- configuration
- server
- network
- connectivity
- operational

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.

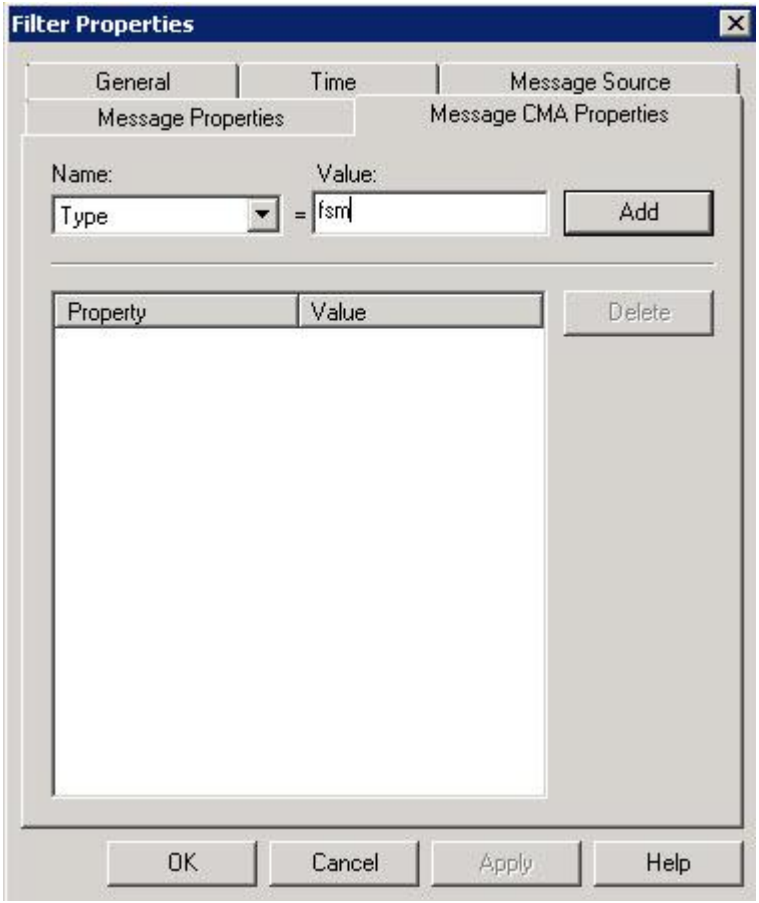


Message Filter

Message Filters:

Active	Filter Name	Owner
	AllTaskFilter	public
	Untitled Filter	private

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.

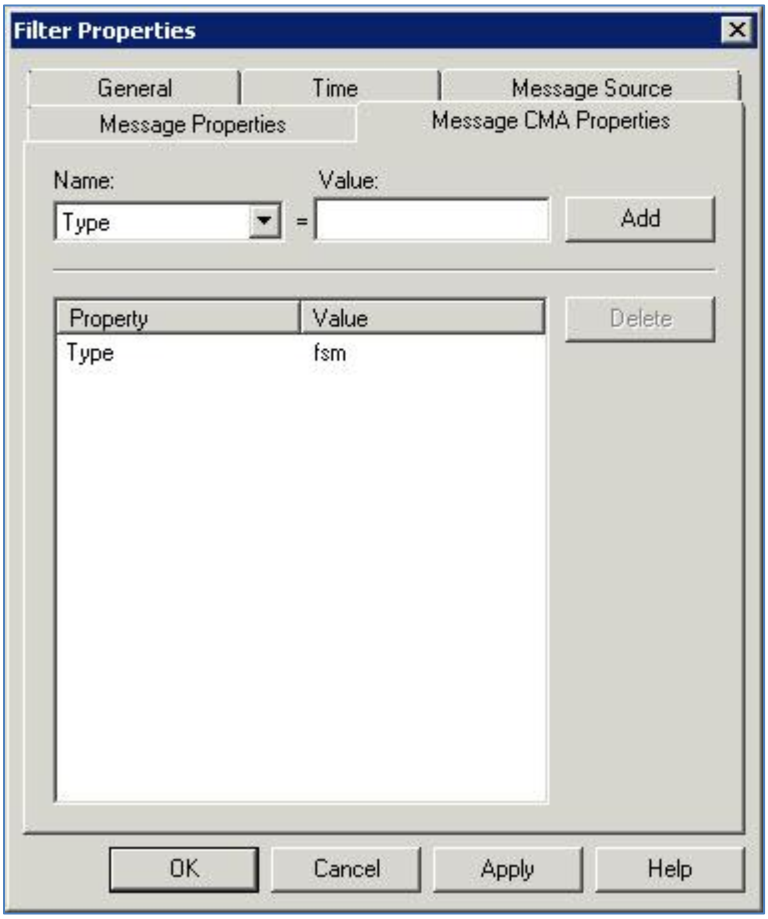


Filter Properties

Name: Type = Value: fsm

Property	Value

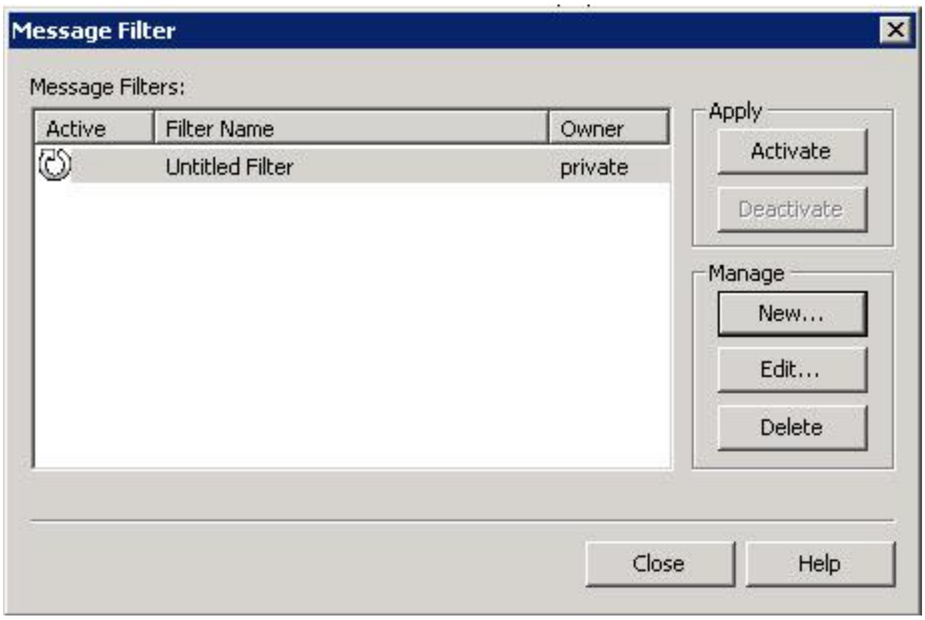
4. Click the **Add** button followed by the **OK** button.



Name: Type = Value:

Property	Value
Type	fsm

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.



Message Filters:

Active	Filter Name	Owner
	Untitled Filter	private

2 Plugin Features

This section describes various features provided with the Cisco IMC Agent Controller like add and delete IMC nodes for monitoring, start monitoring, stop monitoring, export list as .csv and provide server details.

2.1 Editing the Configuration File

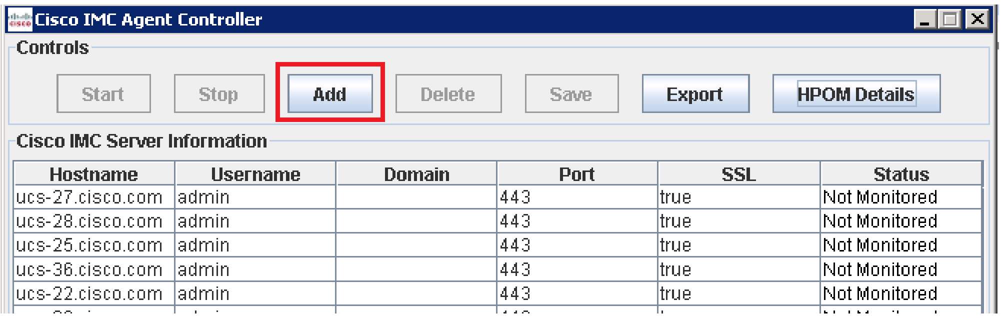
This section describes the steps for editing the configuration file to add/delete the IMC nodes or to edit an existing node.

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

2.1.1 Adding IMC node details

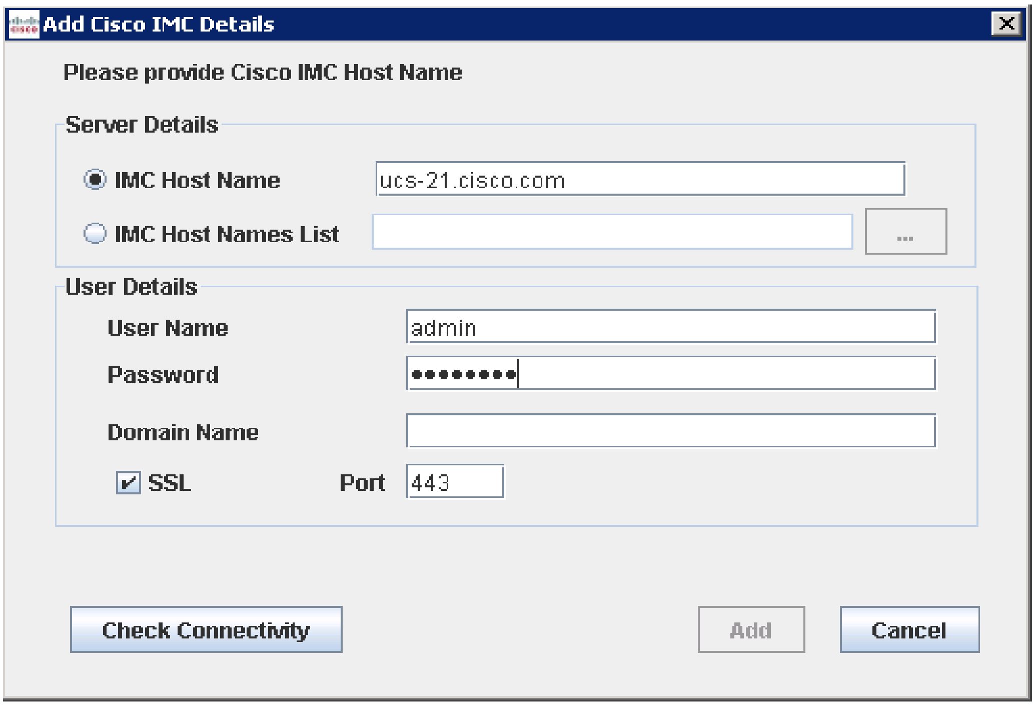
To add the details of the IMC nodes to be monitored:

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



Hostname	Username	Domain	Port	SSL	Status
ucs-27.cisco.com	admin		443	true	Not Monitored
ucs-28.cisco.com	admin		443	true	Not Monitored
ucs-25.cisco.com	admin		443	true	Not Monitored
ucs-36.cisco.com	admin		443	true	Not Monitored
ucs-22.cisco.com	admin		443	true	Not Monitored

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



Please provide Cisco IMC Host Name

● IMC Host Name: ucs-21.cisco.com

○ IMC Host Names List:

User Name: admin

Password: ●●●●●●●●

Domain Name:

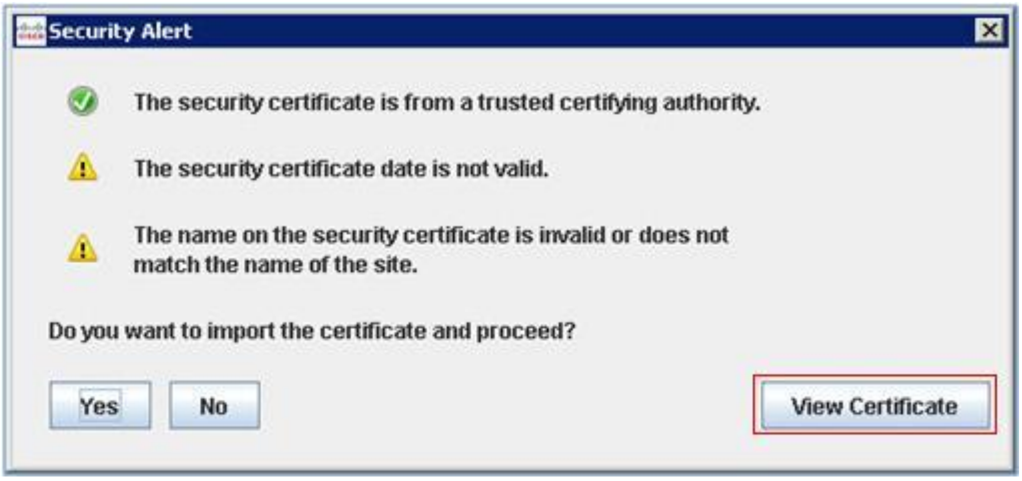
☑ SSL Port: 443

There are two modes to add a IMC node.

- Add each node individually.(IMC Host Name)
- Add a list of nodes with common user names and password. (IMC Host Names List)

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

3. To add each node individually click on the first radio button and provide all the details. Click the **Check Connectivity** button to verify the connection to the IMC and to enable Add button.
   The **Security Alert** window appears.



✓ The security certificate is from a trusted certifying authority.

⚠ The security certificate date is not valid.

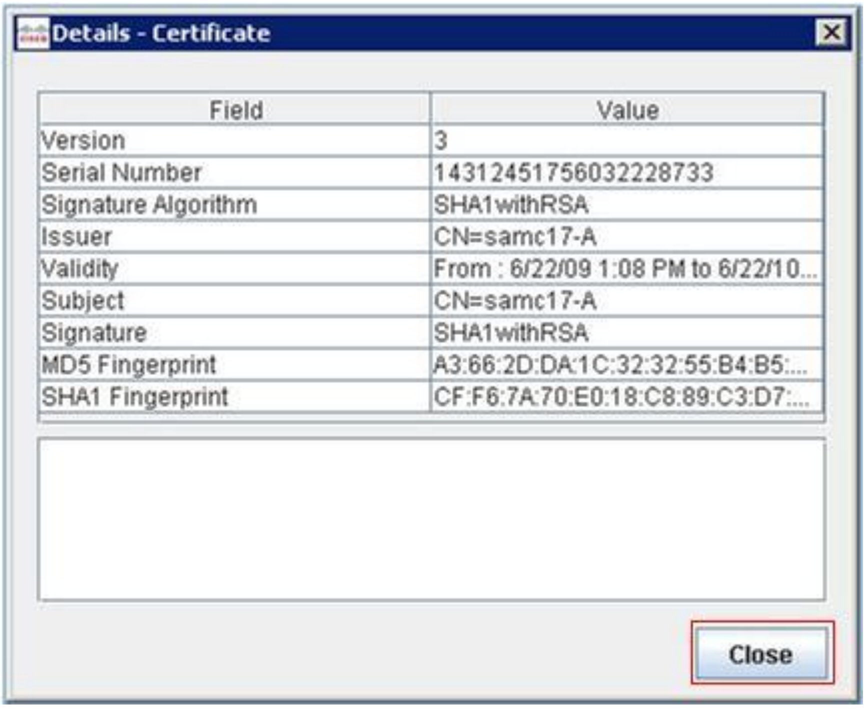
⚠ The name on the security certificate is invalid or does not match the name of the site.

Do you want to import the certificate and proceed?

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

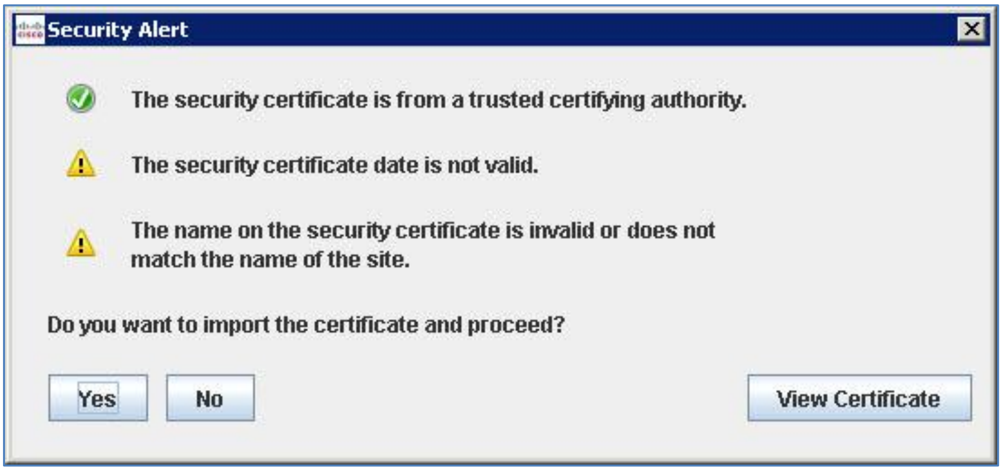
Also in case of bulk upload, All the certificates are imported by default.

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



Field	Value
Version	3
Serial Number	14312451756032228733
Signature Algorithm	SHA1withRSA
Issuer	CN=samc17-A
Validity	From : 6/22/09 1:08 PM to 6/22/10...
Subject	CN=samc17-A
Signature	SHA1withRSA
MD5 Fingerprint	A3:66:2D:DA:1C:32:32:55:B4:B5:...
SHA1 Fingerprint	CF:F6:7A:70:E0:18:C8:89:C3:D7:...

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



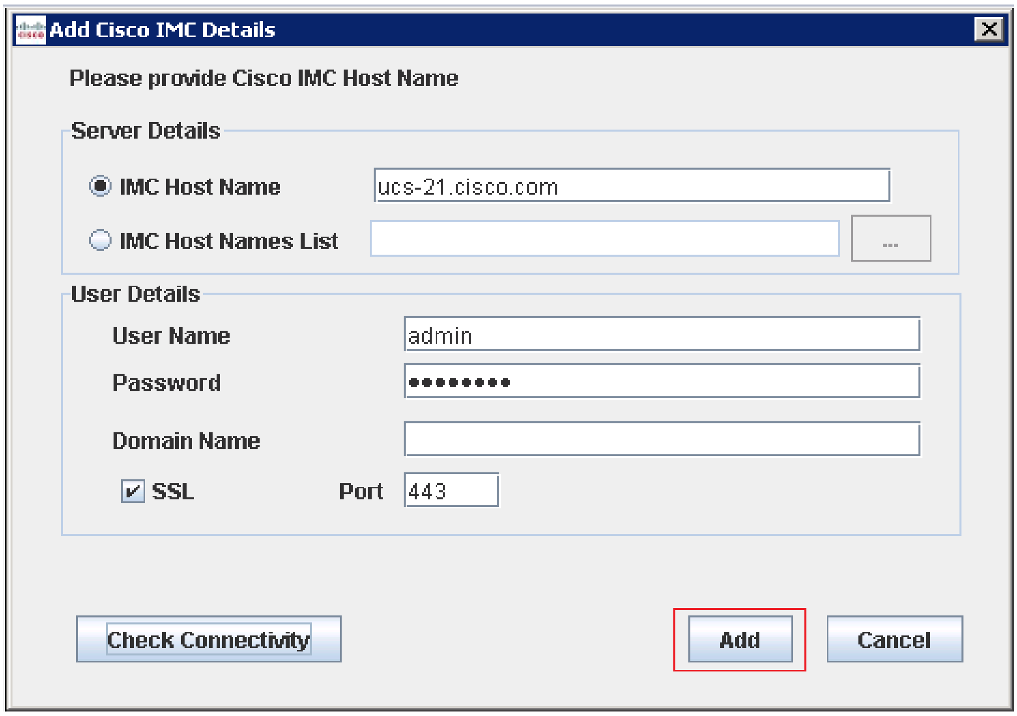
✓ The security certificate is from a trusted certifying authority.

⚠ The security certificate date is not valid.

⚠ The name on the security certificate is invalid or does not match the name of the site.

Do you want to import the certificate and proceed?

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



Add Cisco IMC Details

Please provide Cisco IMC Host Name

Server Details

● IMC Host Name: ucs-21.cisco.com

○ IMC Host Names List:

User Details

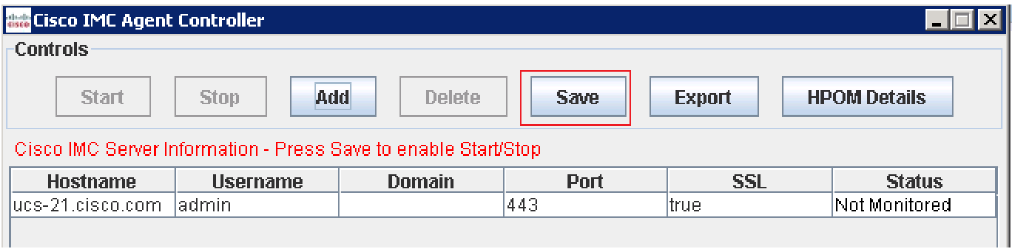
User Name: admin

Password: ●●●●●●●●●

Domain Name:

☑ SSL Port: 443

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



Cisco IMC Agent Controller

Cisco IMC Server Information - Press Save to enable Start/Stop

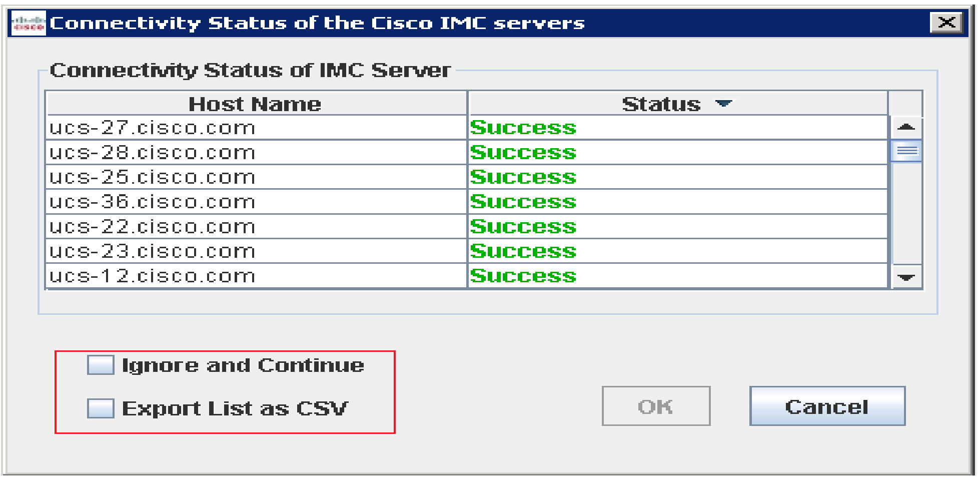
Hostname	Username	Domain	Port	SSL	Status
ucs-21.cisco.com	admin		443	true	Not Monitored

8. Bulk addition of node is possible only through a .csv file.

   The .csv file should contain list of servers in the format as shown:-

   Host Name
   FQDN1, FQDN2, FQDN3
   FQDN4
   FQDN5, FQDN6

9. When we perform a check connectivity in this case, we get the result for each host in a tabular form:-



Connectivity Status of the Cisco IMC servers

Connectivity Status of IMC Server

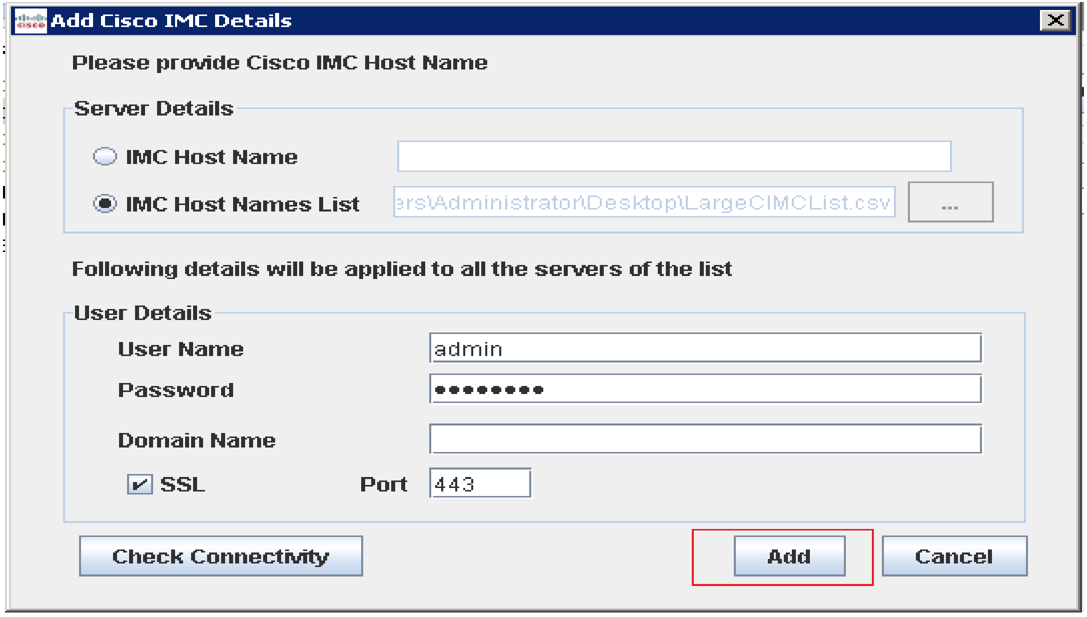
Host Name	Status
ucs-27.cisco.com	Success
ucs-28.cisco.com	Success
ucs-25.cisco.com	Success
ucs-36.cisco.com	Success
ucs-22.cisco.com	Success
ucs-23.cisco.com	Success
ucs-12.cisco.com	Success

☐ Ignore and Continue

☐ Export List as CSV

10. User has the option to either ignore the result and continue or export the result to excel and then continue.

11. Once that is done, the add button gets enabled.



Add Cisco IMC Details

Please provide Cisco IMC Host Name

Server Details

○ IMC Host Name

● IMC Host Names List ers\Administrator\Desktop\LargeCIMCList.csv

Following details will be applied to all the servers of the list

User Details

User Name: admin

Password: ●●●●●●●●●

Domain Name:

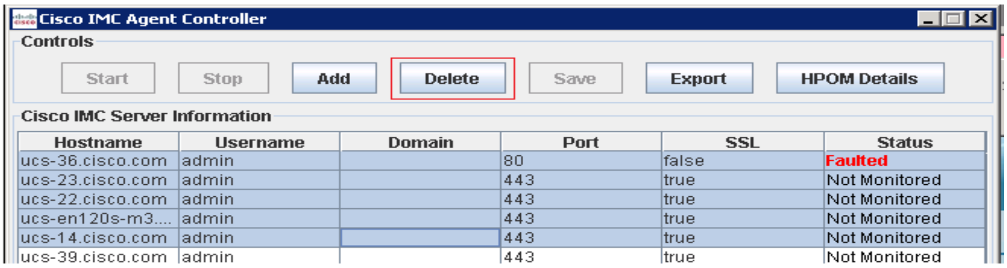
☑ SSL Port: 443

12. Click the **Save** button to save the node details in the application. (As shown in 7) The details are saved successfully.

2.1.2 Deleting an existing IMC Node

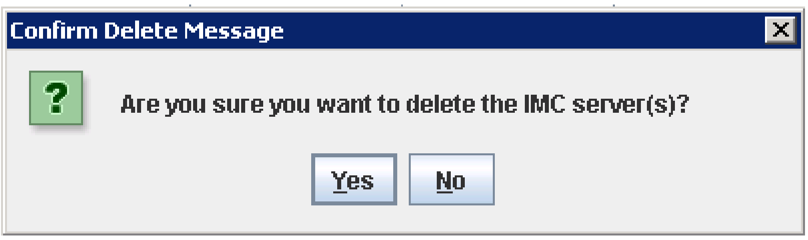
To delete the IMC nodes from the configuration file:

1. On the **Cisco IMC Agent Controller** window, select the IMC 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.



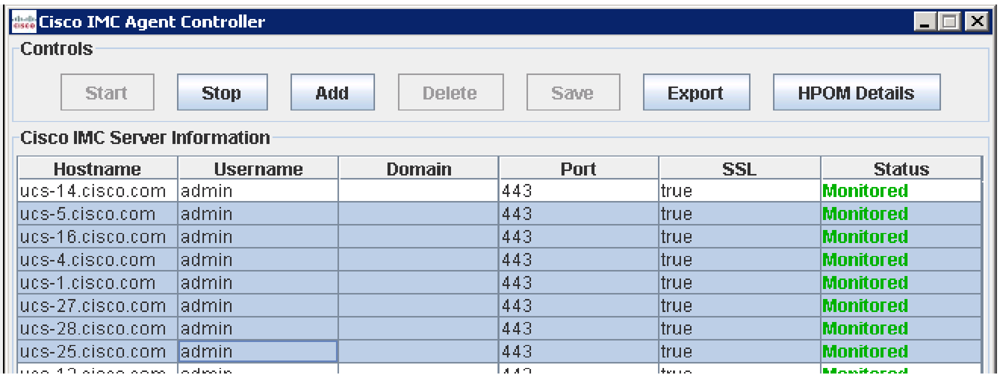
Hostname	Username	Domain	Port	SSL	Status
ucs-36.cisco.com	admin		80	false	Faulted
ucs-23.cisco.com	admin		443	true	Not Monitored
ucs-22.cisco.com	admin		443	true	Not Monitored
ucs-en120s-m3....	admin		443	true	Not Monitored
ucs-14.cisco.com	admin		443	true	Not Monitored
ucs-39.cisco.com	admin		443	true	Not Monitored

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



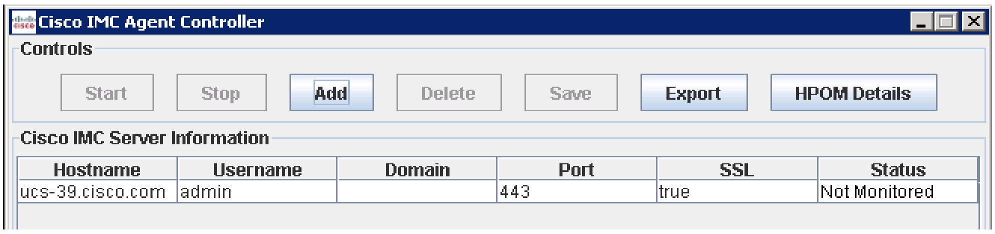
Are you sure you want to delete the IMC server(s)?

3. Deletion is not allowed while monitoring is started on a node.



Hostname	Username	Domain	Port	SSL	Status
ucs-14.cisco.com	admin		443	true	Monitored
ucs-5.cisco.com	admin		443	true	Monitored
ucs-16.cisco.com	admin		443	true	Monitored
ucs-4.cisco.com	admin		443	true	Monitored
ucs-1.cisco.com	admin		443	true	Monitored
ucs-27.cisco.com	admin		443	true	Monitored
ucs-28.cisco.com	admin		443	true	Monitored
ucs-25.cisco.com	admin		443	true	Monitored

4. Click the **Yes** button.
   The **Save** button is enabled. Click the **Save** button.
   The IMC Node Information table is updated with the remaining IMC nodes
5. The **Cisco IMC Agent Controller** window appears.



Hostname	Username	Domain	Port	SSL	Status
ucs-39.cisco.com	admin		443	true	Not Monitored

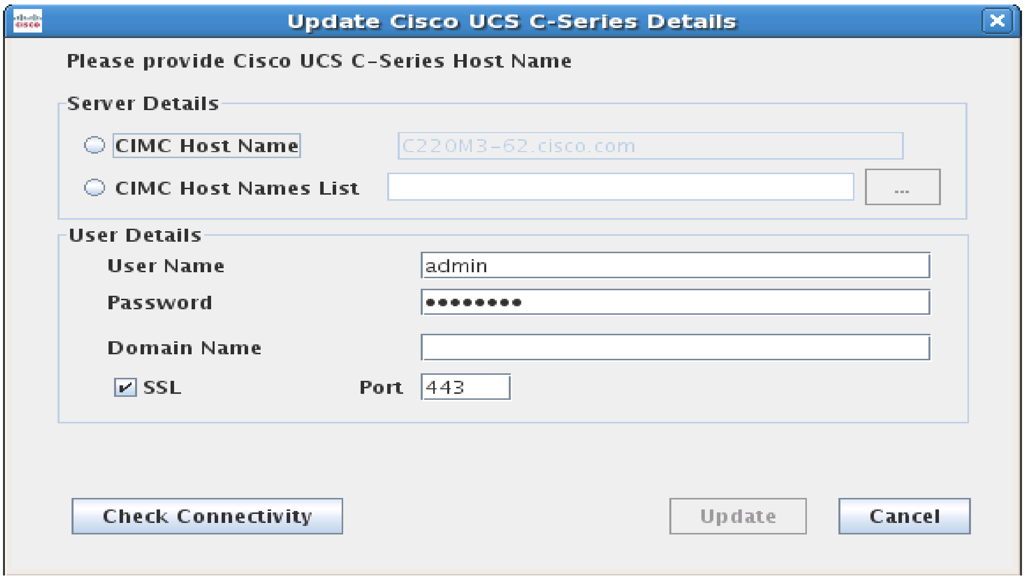
Note: Add/delete of IMC node is not allowed while monitoring is started on a server.

2.1.3 Updating an existing IMC Node

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

To update an existing IMC Node:

1. Double click on Username/Domain/Port/SSL column of the appropriate row.
   The **Update IMC Details** window appears.



Update Cisco UCS C-Series Details

Please provide Cisco UCS C-Series Host Name

Server Details

○ CIMC Host Name: C220M3-62.cisco.com

○ CIMC Host Names List:

User Details

User Name: admin

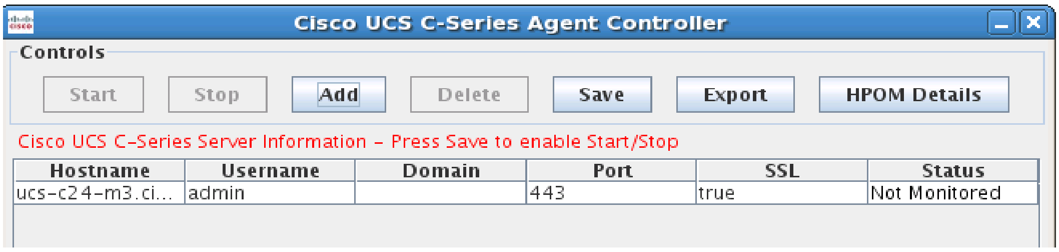
Password: ••••••••

Domain Name:

☑ SSL Port: 443

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

3. Click the **Update** button.
   The changes are reflected in the IMC Node Information table.



Cisco UCS C-Series Agent Controller

Cisco UCS C-Series Server Information – Press Save to enable Start/Stop

Hostname	Username	Domain	Port	SSL	Status
ucs-c24-m3.ci...	admin		443	true	Not Monitored

4. 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 IMC Node Information table:

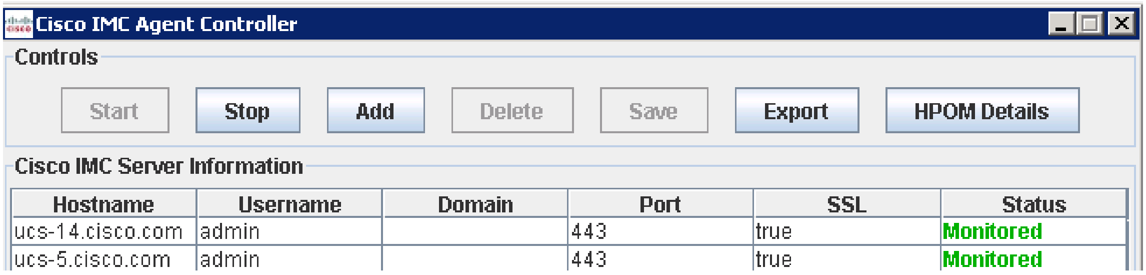
1. A new IMC node is added in table.
2. One or more IMC nodes are deleted from table.
3. A IMC node in “Not Monitored” or “Faulted” state is edited.

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

2.2 IMC Node Monitoring Status

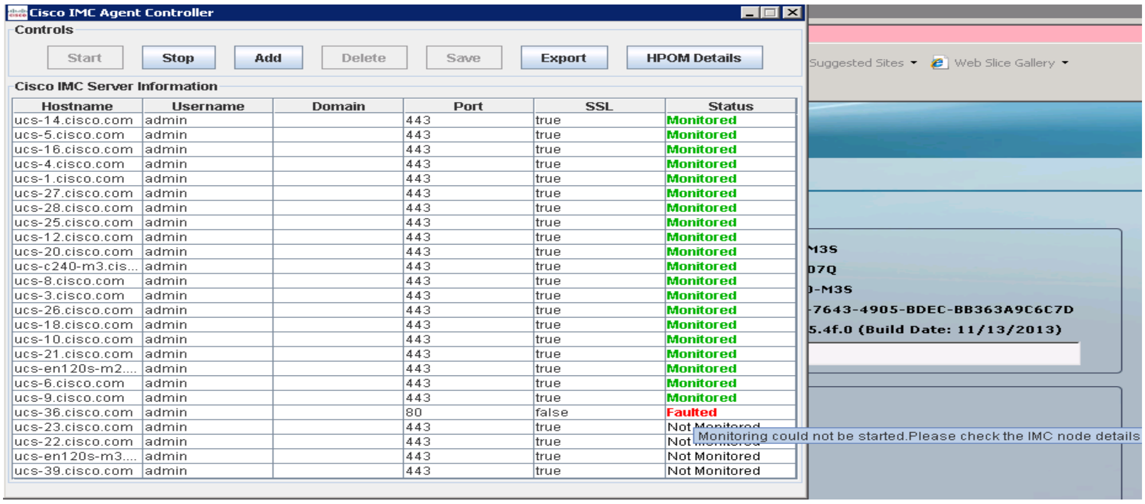
You can check the status of the IMC nodes being monitored in Status column of IMC Node Information table. The IMC nodes for which monitoring are active are shown with status as Monitored in green color. If the monitoring has been stopped for some IMC nodes due to some error condition or when you try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

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



Hostname	Username	Domain	Port	SSL	Status
ucs-14.cisco.com	admin		443	true	Monitored
ucs-5.cisco.com	admin		443	true	Monitored

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


Cisco IMC Agent Controller
Controls
Start
Stop
Add
Delete
Save
Export
HPOM Details
Cisco IMC Server Information
Suggested Sites
Web Slice Gallery
M3S
07Q
)-M3S
-7643-4905-BDEC-BB363A9C6C7D
5.4f.0 (Build Date: 11/13/2013)

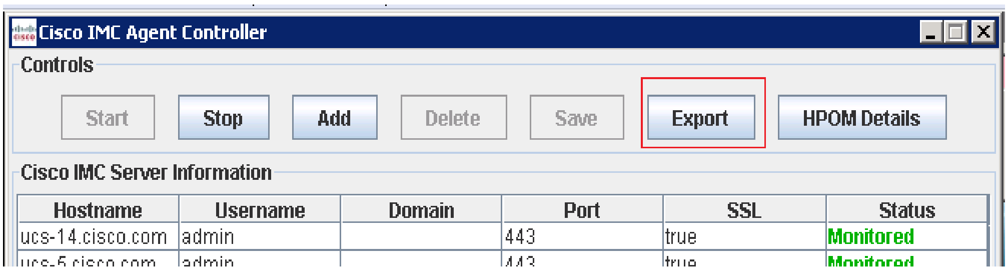
Hostname	Username	Domain	Port	SSL	Status
ucs-14.cisco.com	admin		443	true	Monitored
ucs-5.cisco.com	admin		443	true	Monitored
ucs-16.cisco.com	admin		443	true	Monitored
ucs-4.cisco.com	admin		443	true	Monitored
ucs-1.cisco.com	admin		443	true	Monitored
ucs-27.cisco.com	admin		443	true	Monitored
ucs-28.cisco.com	admin		443	true	Monitored
ucs-25.cisco.com	admin		443	true	Monitored
ucs-12.cisco.com	admin		443	true	Monitored
ucs-20.cisco.com	admin		443	true	Monitored
ucs-c240-m3.cis...	admin		443	true	Monitored
ucs-8.cisco.com	admin		443	true	Monitored
ucs-3.cisco.com	admin		443	true	Monitored
ucs-26.cisco.com	admin		443	true	Monitored
ucs-18.cisco.com	admin		443	true	Monitored
ucs-10.cisco.com	admin		443	true	Monitored
ucs-21.cisco.com	admin		443	true	Monitored
ucs-en120s-m2....	admin		443	true	Monitored
ucs-6.cisco.com	admin		443	true	Monitored
ucs-9.cisco.com	admin		443	true	Monitored
ucs-36.cisco.com	admin		80	false	Faulted
ucs-23.cisco.com	admin		443	true	Not Monitored
ucs-22.cisco.com	admin		443	true	Not Monitored
ucs-en120s-m3....	admin		443	true	Not Monitored
ucs-39.cisco.com	admin		443	true	Not Monitored

Monitoring could not be started.Please check the IMC node details

2.3 Exporting IMC Node Configuration File

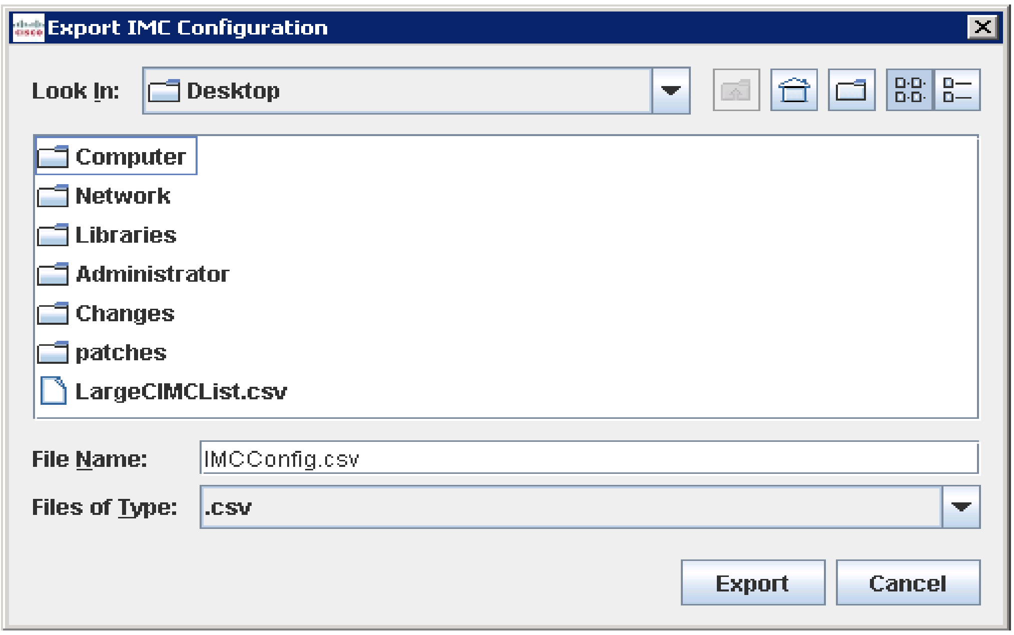
To export a IMC Node Configuration File:

1. On the Cisco IMC Agent Controller window, click the **Export** button.



Hostname	Username	Domain	Port	SSL	Status
ucs-14.cisco.com	admin		443	true	Monitored
ucs-5.cisco.com	admin		443	true	Monitored

2. A **Export IMC Configuration** dialog box appears.
Select a location where (.csv) file is to be exported and Click the **Export** button.

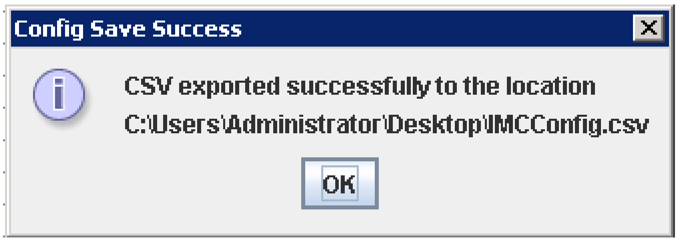


Look In: Desktop

File Name: IMCConfig.csv

Files of Type: .csv

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

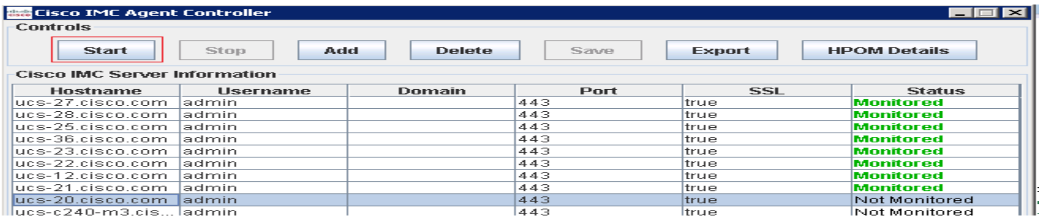


CSV exported successfully to the location
C:\Users\Administrator\Desktop\IMCConfig.csv

2.4 Start Monitoring

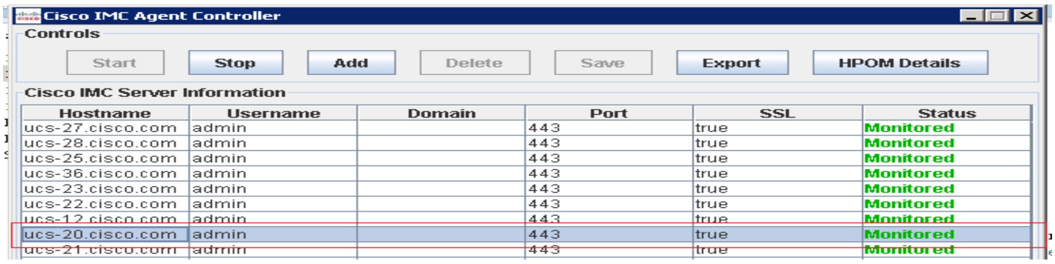
To start monitoring for multiple Cisco IMC nodes in IMC Node Information table:

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



Hostname	Username	Domain	Port	SSL	Status
ucs-27.cisco.com	admin		443	true	Monitored
ucs-28.cisco.com	admin		443	true	Monitored
ucs-25.cisco.com	admin		443	true	Monitored
ucs-36.cisco.com	admin		443	true	Monitored
ucs-23.cisco.com	admin		443	true	Monitored
ucs-22.cisco.com	admin		443	true	Monitored
ucs-12.cisco.com	admin		443	true	Monitored
ucs-21.cisco.com	admin		443	true	Monitored
ucs-20.cisco.com	admin		443	true	Not Monitored
ucs-c240-m3.cis...	admin		443	true	Not Monitored

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

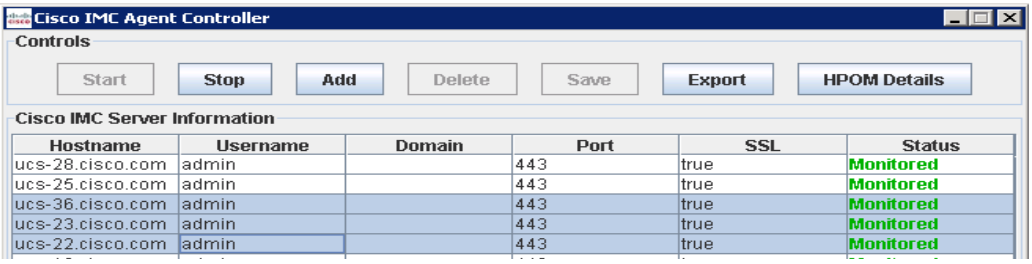


Hostname	Username	Domain	Port	SSL	Status
ucs-27.cisco.com	admin		443	true	Monitored
ucs-28.cisco.com	admin		443	true	Monitored
ucs-25.cisco.com	admin		443	true	Monitored
ucs-36.cisco.com	admin		443	true	Monitored
ucs-23.cisco.com	admin		443	true	Monitored
ucs-22.cisco.com	admin		443	true	Monitored
ucs-12.cisco.com	admin		443	true	Monitored
ucs-20.cisco.com	admin		443	true	Monitored
ucs-21.cisco.com	admin		443	true	Monitored

2.5 Stop Monitoring

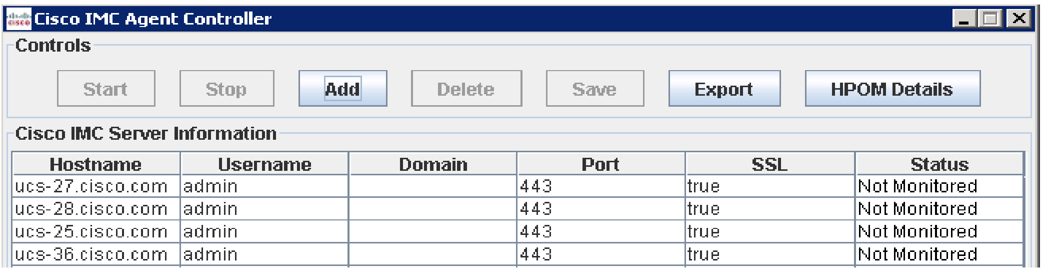
To stop monitoring for multiple Cisco IMC nodes in IMC Node Information table:

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



Hostname	Username	Domain	Port	SSL	Status
ucs-28.cisco.com	admin		443	true	Monitored
ucs-25.cisco.com	admin		443	true	Monitored
ucs-36.cisco.com	admin		443	true	Monitored
ucs-23.cisco.com	admin		443	true	Monitored
ucs-22.cisco.com	admin		443	true	Monitored

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



Hostname	Username	Domain	Port	SSL	Status
ucs-27.cisco.com	admin		443	true	Not Monitored
ucs-28.cisco.com	admin		443	true	Not Monitored
ucs-25.cisco.com	admin		443	true	Not Monitored
ucs-36.cisco.com	admin		443	true	Not Monitored

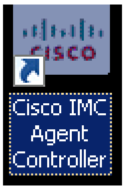
3 Troubleshooting

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

3.1 Verifying Cisco IMC Smart Plugin Installation

To verify successful installation of Cisco IMC Smart Plugin:

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



2. Launch the HPOM console and verify that the policy group **CISCO IMC Policies** is created under **Policy Management > Policy Groups.**
3. Verify that the following policies are present in the **CISCO IMC Policies** (Policy Group):
   - **IMC-AutoDiscovery**
   - **IMC-Opcmsg**
4. If any of the above is missing, reinstall the Cisco IMC Smart Plugin.

3.2 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.

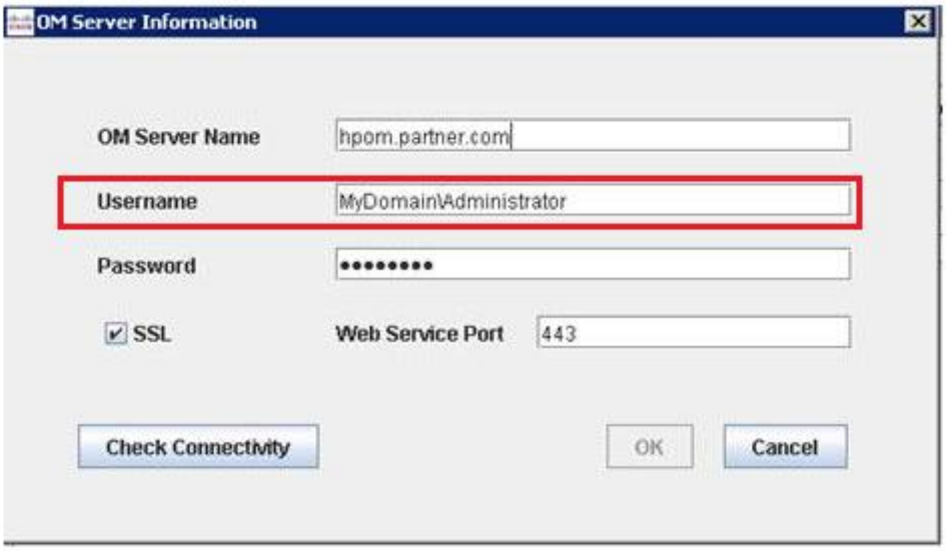
  Example :- With Administrator :-

  ```
  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_IMC_LOGS.
  3. C:\Users\<User>\IMC_TEMP.

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



OM Server Name: hpom.partner.com

Username: MyDomain\Administrator

Password: ••••••••

☑ SSL

Web Service Port: 443

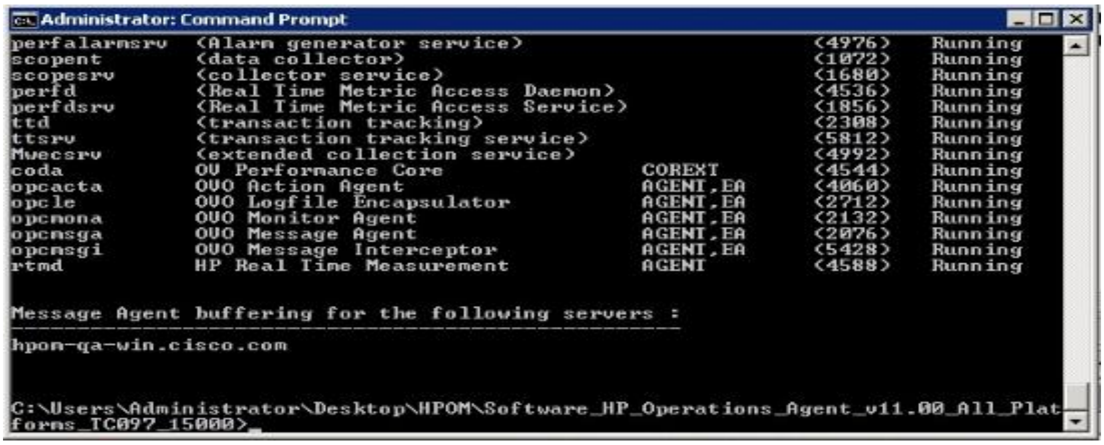
3.3 Faults not populating in HPOM due to improper install

1. Verify a proper installation of the Cisco IMC Smart Plugin. To read more on installation refer, **Cisco IMC 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 IMC node details have been provided correctly.
4. Check the monitoring status.
5. Restart the monitoring through Cisco IMC Agent Controller. Click Stop and then click Start.
6. If none of the above described resolves the issue, restart the HPOM Console.

3.4 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.



Administrator: Command Prompt

```
perfalarmsrv   (Alarm generator service)                           (4976)   Running
scopent        (data collector)                                    (1072)   Running
scopesrv       (collector service)                                 (1680)   Running
perfd          (Real Time Metric Access Daemon)                    (4536)   Running
perfdsrv       (Real Time Metric Access Service)                   (1856)   Running
ttd            (transaction tracking)                              (2308)   Running
ttsrv          (transaction tracking service)                      (5812)   Running
Mwecsrv        (extended collection service)                       (4992)   Running
coda           OV Performance Core                 COREXT          (4544)   Running
opcacta        OVO Action Agent                    AGENT,EA        (4060)   Running
opcle          OVO Logfile Encapsulator            AGENT,EA        (2712)   Running
opcmona        OVO Monitor Agent                   AGENT,EA        (2132)   Running
opcmsga        OVO Message Agent                   AGENT,EA        (2076)   Running
opcmsgi        OVO Message Interceptor             AGENT,EA        (5428)   Running
rtmd           HP Real Time Measurement            AGENT           (4588)   Running

Message Agent buffering for the following servers :
-------------------------------------------------------
hpom-qa-win.cisco.com


C:\Users\Administrator\Desktop\HPOM\Software_HP_Operations_Agent_v11.00_All_Plat
forms_TC097_15000>_
```

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.

3.5 Service Hierarchy not appearing in the HPOM

1. Ensure that the IMC node details have been provided correctly using Edit Config button on Cisco IMC 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 **IMC-AutoDiscovery** policy
    - Execute **`ovc -stop`** on the command prompt
    - Execute **`ovc -start`** on the command prompt.
    - Deploy the **`IMC-AutoDiscovery`** policy

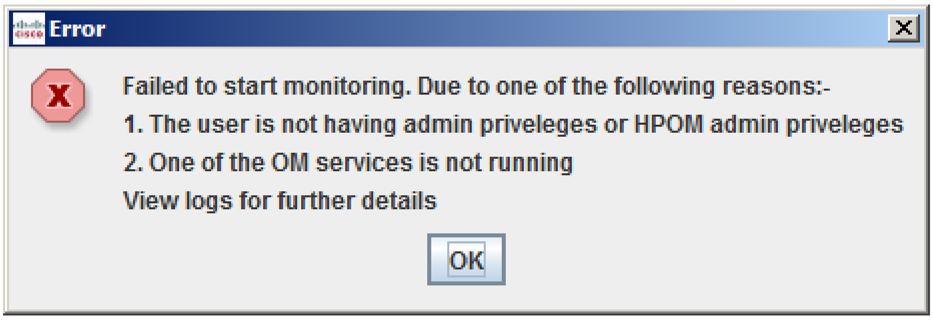
3.6 Application not monitoring after rebooting the system

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.

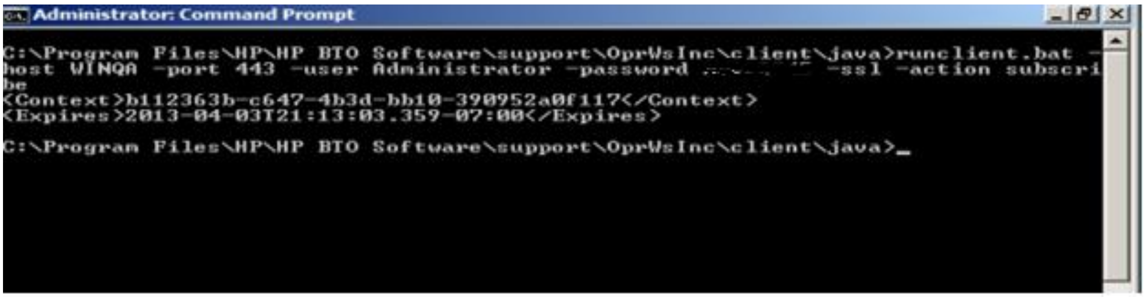
3.7 Subscription fails

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



Failed to start monitoring. Due to one of the following reasons:-
1. The user is not having admin priveleges or HPOM admin priveleges
2. One of the OM services is not running
View logs for further details

Then try and run the following script on CLI:-



```
C:\Program Files\HP\HP BTO Software\support\OprWsInc\client\java>runclient.bat -
host WINQA -port 443 -user Administrator -password [redacted] -ssl -action subscri
be
<Context>b112363b-c647-4b3d-bb10-390952a0f117</Context>
<Expires>2013-04-03T21:13:03.359-07:00</Expires>

C:\Program Files\HP\HP BTO Software\support\OprWsInc\client\java>_
```

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 Related Documentation

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

5 Appendix

5.1 Mapping of Faults from IMC to HPOM

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

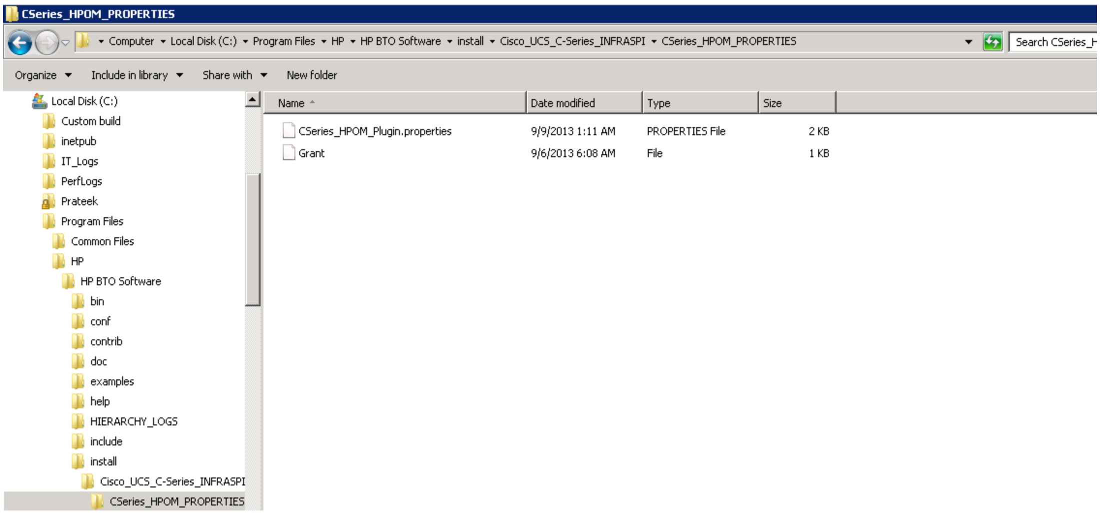
Fault Category in IMC	Fault Category in HPOM
Cleared	Normal
Critical	Critical
Info	Normal
Major	Major
Minor	Minor
Warning	Warning

5.2 Properties File

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

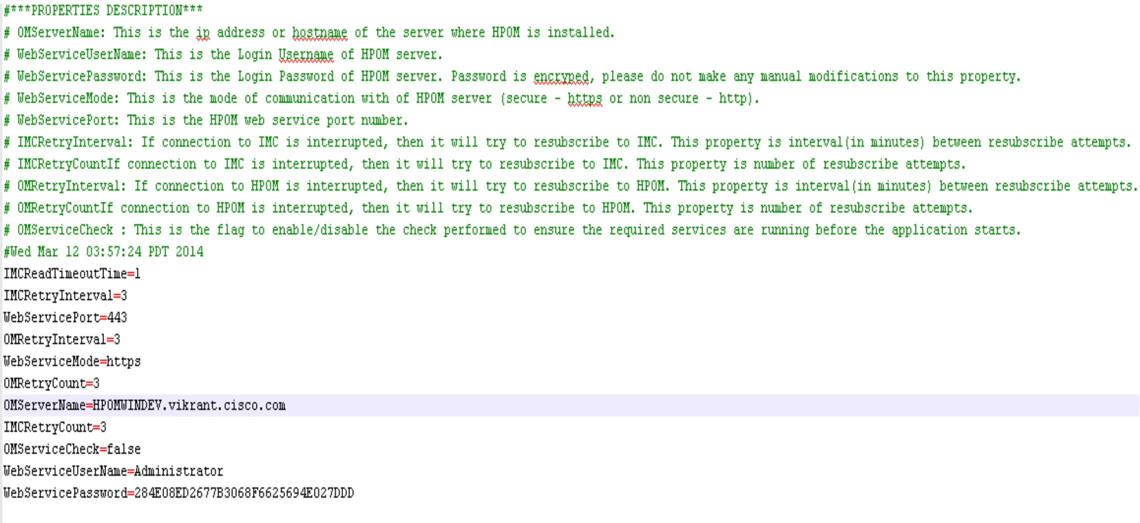
Location of properties file:
“%OvInstallDir%\install\Cisco_IMC_INFRASPI\IMC_HPOM_PROPERTIES”

File Name: **IMC_HPOM_Plugin.properties** (open with Notepad)



Name	Date modified	Type	Size
CSeries_HPOM_Plugin.properties	9/9/2013 1:11 AM	PROPERTIES File	2 KB
Grant	9/6/2013 6:08 AM	File	1 KB

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.
# IMCRetryInterval: If connection to IMC is interrupted, then it will try to resubscribe to IMC. This property is interval(in minutes) between resubscribe attempts.
# IMCRetryCountIf connection to IMC is interrupted, then it will try to resubscribe to IMC. 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.
#Wed Mar 12 03:57:24 PDT 2014
IMCReadTimeoutTime=1
IMCRetryInterval=3
WebServicePort=443
OMRetryInterval=3
WebServiceMode=https
OMRetryCount=3
OMServerName=HPOMWINDEV.vikrant.cisco.com
IMCRetryCount=3
OMServiceCheck=false
WebServiceUserName=Administrator
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 nonsecure - 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.
- **IMCRetryInterval:** If connection to IMC gets interrupted, the application tries to resubscribe to IMC. This property defines the time interval between re-subscribe attempts.
- **IMCRetryCount:** If connection to IMC is interrupted, the application tries to resubscribe to IMC. 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.