**How to check Symantec Management Agent logs on client computer, within SMP Console using Real Time System Management solution**

***Case:***

Very often we need to perform quickly analyze of logs on client computer to determine root cause of some failures, etc and sometimes RDC session is required to get client logs.

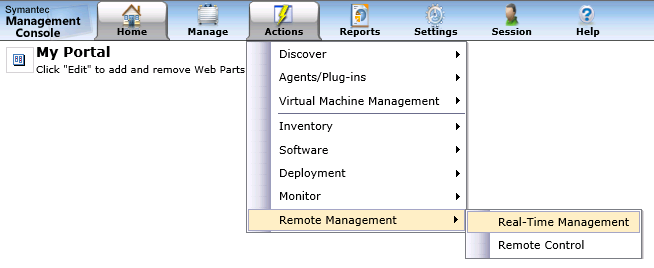
***Solution:***

ITMS/CMS/SMS 7.5 and 7.5 SP1 has "Real Time System Management" solution which provides such functionality, when customer is able to check SMA logs of client computer within SMP Console.

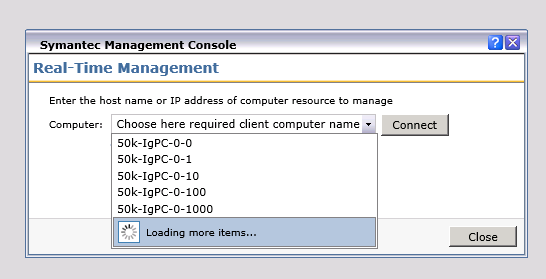
***How to do this?***

Let' see below

**1.** Open SMP Console and go to Actions menu where you can open RTSM connection window



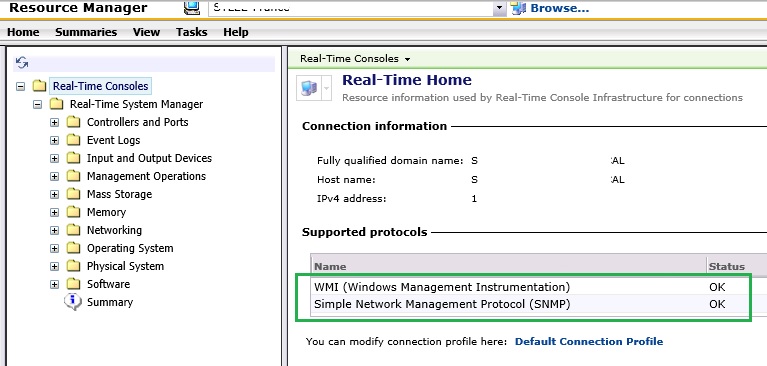
**2.** Here you can manually type hostname or IPv4 address of your client computer, or browse from list of all available computers and choose required one.



**Note:**

You can manually type there hostname or IPv4 address of non-existing client computer in NS Server "Symantec\_CMDB" and try to connect. On attempt to establish connection to non-existing PC, it will perform discovering of it and will create a record of this new discovered resource.

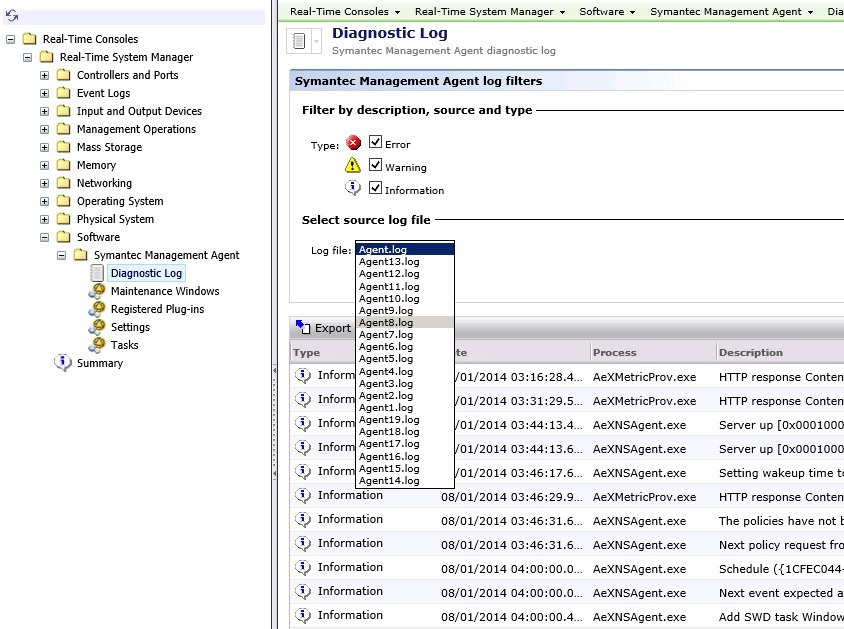
**3**. After successful connection to client computer via Real Time System Management, you will see a Tree View node with all available data. In my case my credentials are correct for successful authentication with client PC and connection status is "OK".



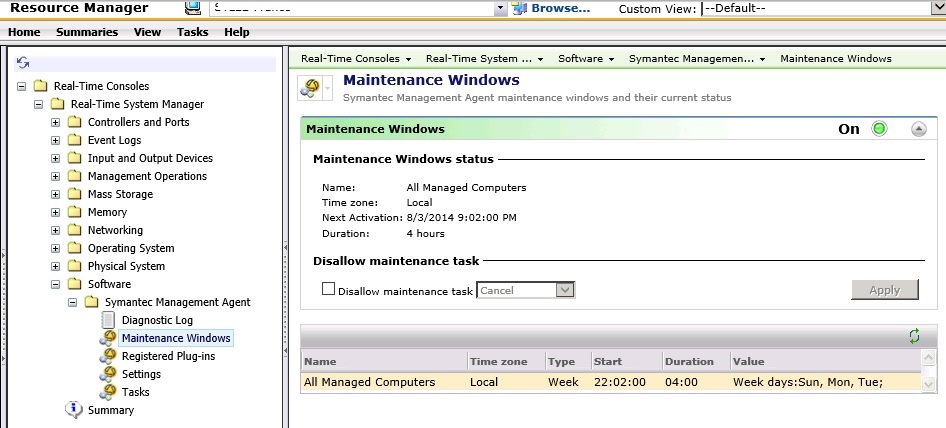
**I will provide other details about "Connection Profiles" and credentials in the end of this doc.**

**4.** Expand "**Software**" folder and there will all about "**Symantec Management Agent**" of client PC.

As you can see, you can choose there what exact SMA log to choose and see content. Also you filter it to see only Error, Warning or Informational severity of logs.



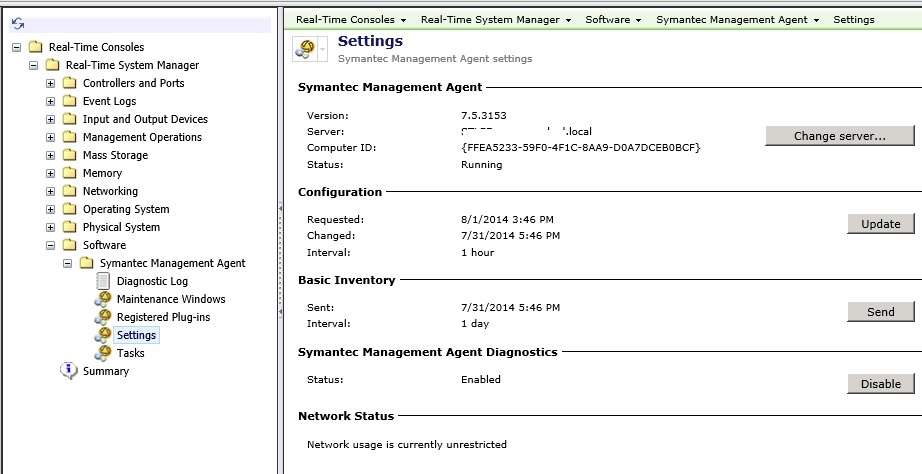
**5.** You can check what "Maintenance Window" policies has this managed endpoint and what schedule is



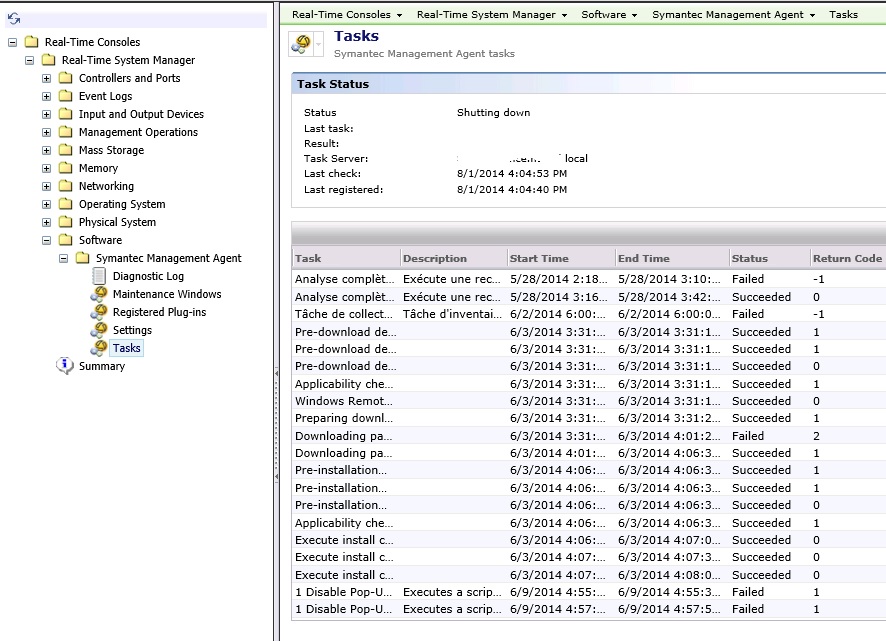
**6.** What solution and platform plug-ins are installed on managed endpoint



**7.** You will have ability to redirect this managed endpoint to another NS Server. Quickly initiate refresh policy action or send basic inventory and also enable or disable diagnostics menu.



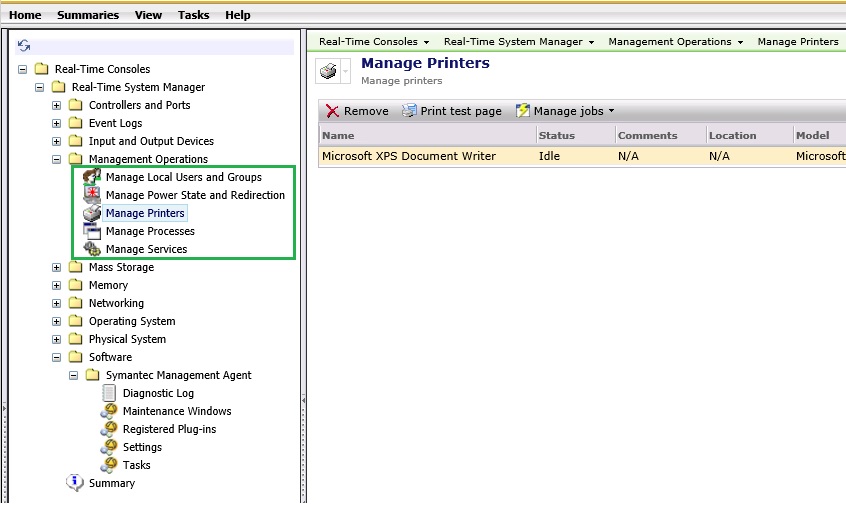
**8.** Ability to see all history list of executed tasks on client PC and their status code.



**Additional information:**

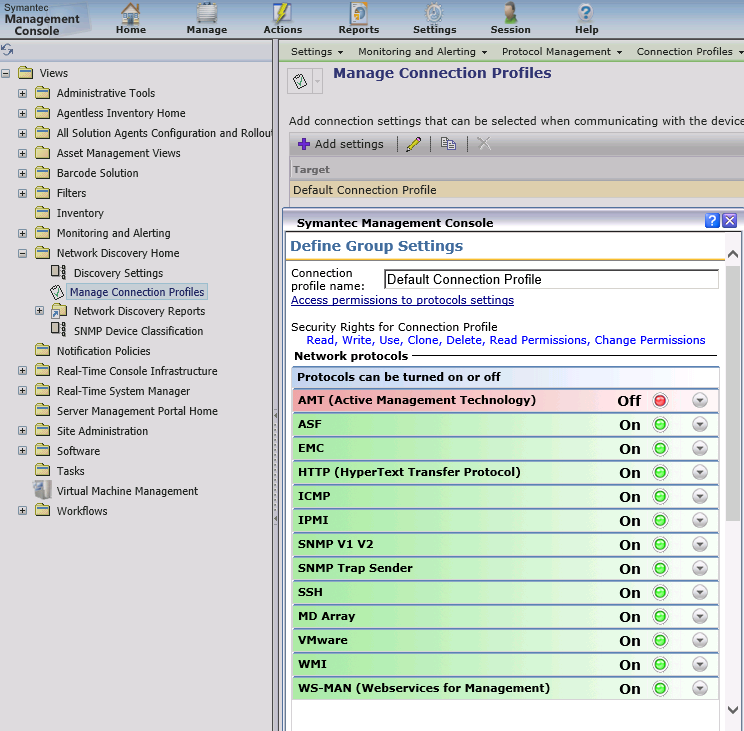
Using this RTSM console with successful connection to client PC via WMI protocol, you also able to:

* perform "Power Management" such as shut down or restart client PC
* Start/Stop/Restart Services on client PC
* Start or terminate processes on client PC
* Reset password for users or rename them on client PC

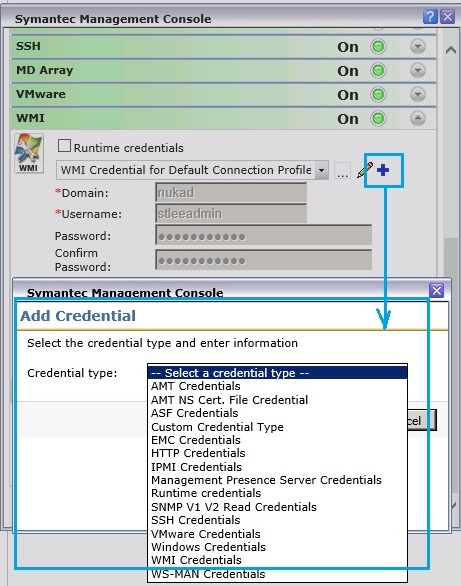


About Credentials and Connection Profile for RTSM connections:

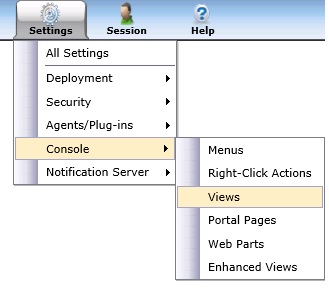
* "**Default Connection Profile**" - this is a set of all available pluggable protocols

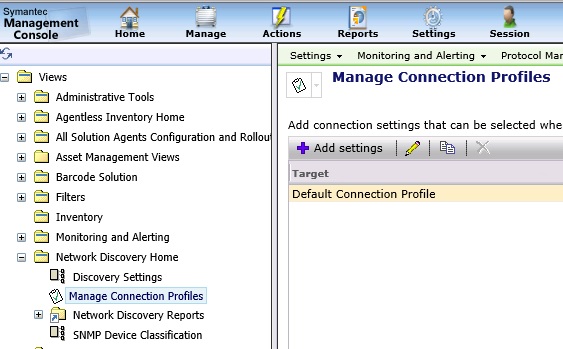


* "**Credential Manager**" - this is a set of credentials for separate protocol type.



You can find "**Default Connection Profile**" main page on SMP Console:

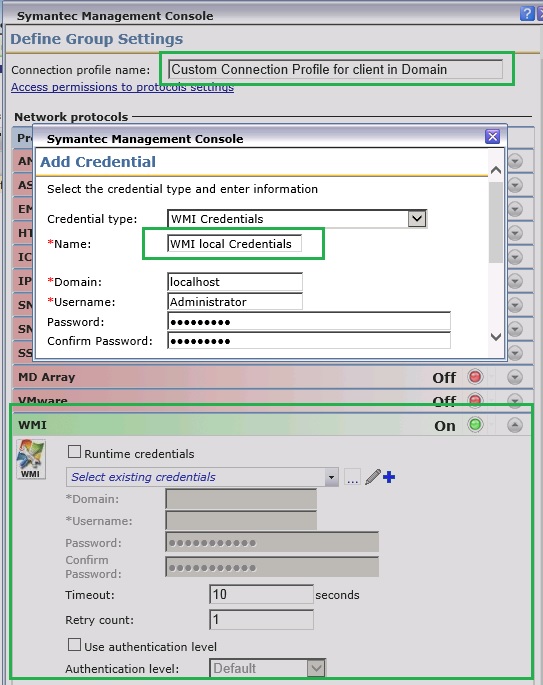




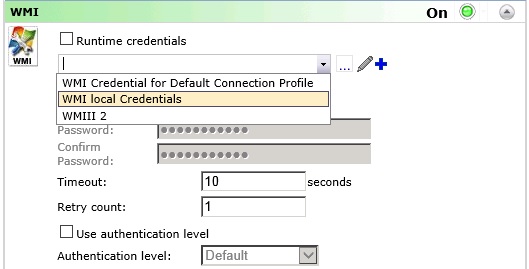
You can create custom separate "**Default Connection Profile**" and specify there required credentials for WMI protocol to make possible establish connection to client computer.



Set appropriate Name for this new Connection Profile to determine what credentials will be there for WMI protocol (Local credentials or Domain credentials)



After that you can choose these WMI credentials for your WMI protocol in Custom Profile



Save Changes

Now if you will connect to client PC via Real Time System Management, there will be an option to choose which Connection profile to use, in case if current Connection Profile contains incorrect credentials for WMI protocol.