

# Remote Symantec Agent Diagnostics Utility

Remote Symantec Management Agent Diagnostics

Enter Computer Name or IP Address:

Add

Recent Computers

- smpwin7single 132.168.1.50

**SMP Server Details**

SMP Server:  Connected To:  IP Address:

GUID:

**SMP Configuration Request Information**

Last Requested:

Last Changed:

Next Request:

Request Interval:

**SMP Basic Inventory Information**

Last Sent:

Next Send:

Send Interval:

**Current Agent Version**

SMP Agent Version:

**Installed Agents/Plug-ins**

Agent Name	Product Version	Install Path
Altiris Application Metering Agent	7.1.7867	C:\Program Files (x86)\Altiris\Altiris ...
Altiris Base Task Handlers	7.1.15440	C:\Program Files\Altiris\Altiris Agent\...
Altiris Client Task Agent	7.1.15440	C:\Program Files\Altiris\Altiris Agent\...
Altiris Inventory Agent	7.1.7867	C:\Program Files (x86)\Altiris\Altiris ...
Altiris Software Update Agent	7.1.0.7858	C:\Program Files\Altiris\Altiris Agent\...
Inventory Rule Agent	7.1.8440.0	C:\Program Files\Altiris\Altiris Agent\...
Software Management Framework Ag...	7.1.8440.0	C:\Program Files\Altiris\Altiris Agent\...
Software Management Solution Agent	7.1.7858.0	C:\Program Files\Altiris\Altiris Agent\...

**Service Status**

Running

Right click on a computer or IP address above for action items.

Ready

Prerequisite	Description
Operating System	Any of the following: <ul style="list-style-type: none"> <li>• Windows 7 SP1</li> <li>• Windows 8</li> </ul>
PowerShell	PowerShell version 3.0. Install <a href="#">Windows Management Framework 3.0</a> to run Windows PowerShell 3.0.
.NET Framework 4.0 or 4.5	<p>Windows PowerShell 3.0 requires the full installation of Microsoft .NET Framework 4. Windows 8 includes Microsoft .NET Framework 4.5 by default, which fulfills this requirement. To install Microsoft .NET Framework 4.5 (dotNetFx45_Full_setup.exe), see <a href="#">Microsoft .NET Framework 4.5</a> on the Microsoft Download Center.</p> <p>To install the full installation of Microsoft .NET Framework 4 (dotNetFx40_Full_setup.exe), see <a href="#">Microsoft .NET Framework 4 (Web Installer)</a> on the Microsoft Download Center.</p>
Symantec Management Agent	Symantec Management Agent version 7.1

Features	Description
Retrieve Agent Details	Retrieve Symantec agent details from a remote computer. This populates the main screen.
View Logs	Retrieve remote Symantec agent log data. Choose one or more logs on remote computer.
Update Configuration	Force selected computer to update configuration request.
Send Basic Inventory	Force selected computer to send basic inventory.
View Client Policies	View the client policy XML file on the remote computer. Useful to see what policies are applied to computer.
Execute SWD	View software that could be executed remotely. It is your responsibility to make sure that software should be run.
Enable Verbose Logging	Enable verbose logging on the remote computer. Useful when troubleshooting.
Disable Verbose Logging	Disable verbose logging on the remote computer.
Set NSE Capture Folder	Configure a location on the remote computer to store outgoing NSE files.
Disable NSE Capture	Removes the location to store outgoing NSE files.
View Patch Install Log	View the patch management installation log file. Useful when you want to know if a bulletin is installed or not.
Open File System	Open C on remote computer
Remove Computer From List	Removes selected computer from list.

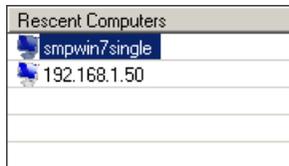
## Directions:

Launch the program from Start > All Programs > Remote Symantec Agent Diagnostics Utility



Enter Computer Name or IP  
Address:  
  
Add

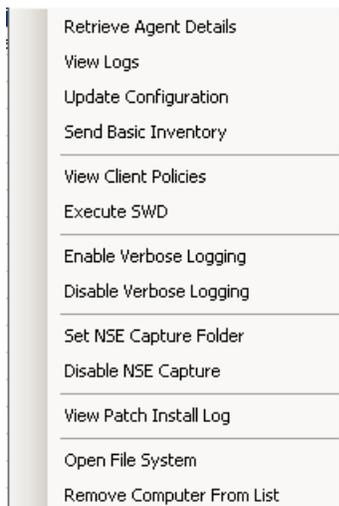
Enter computer name or IP Address and click on the Add button.



Rescent Computers

 smpwin7single
 192.168.1.50

Right click on the computer to bring up the actionable items list.



- Retrieve Agent Details
- View Logs
- Update Configuration
- Send Basic Inventory
- View Client Policies
- Execute SWD
- Enable Verbose Logging
- Disable Verbose Logging
- Set NSE Capture Folder
- Disable NSE Capture
- View Patch Install Log
- Open File System
- Remove Computer From List

## How Things Work

- When you first launch the Remote Symantec Agent Diagnostics utility, RSAD, the program will create a text file called computers.txt. This text file is used to store recently used computers.
- The following features require that the remote computer be configured for PowerShell remoting. <http://technet.microsoft.com/en-us/library/hh849694.aspx>
  - Retrieve Agent Details
  - Update Configuration
  - Send Basic Inventory
  - Execute SWD
  - Enable Verbose Logging
  - Disable Verbose Logging
  - Set NSE Capture Folder
  - Disable NSE Capture Folder

When you click on any of the above listed features, the program will check that remoting is enabled on the selected computer. If not, it will make two attempts to enable PSRemoting. The following is what will be attempted:

### Enable-PSRemoting First Attempt:

Create a scheduled task on the remote computer called EnablePSRemote. This scheduled task runs powershell.exe, passing the command "enable-psremoting -force".

- Execute scheduled task
- Delete scheduled task.
- Pause for 20 seconds.
- Verify first attempt was successful.

### Enable-PSRemoting Second Attempt:

If verification for the first attempt fails, the following five steps will be done:

1. Configure remote computer's WinRM service to listen for WinRM requests by creating one registry key on the remote computer.
  - Create registry key: "SOFTWARE\Policies\Microsoft\Windows\WinRM\Service"
  - Create two DWORD values and two String values as follows:
    - DWORD Name = "AllowAutoConfig"
    - DWORD Value = "0x1"
    - String Name = "IPv4Filter"
    - String Value = "\*"
    - String Name = "IPv6Filter"
    - String Value = "\*"
2. Change the startup type of the WinRM service to automatic.
3. Restarts the WinRM service.
4. Configure remote computer's firewall by setting one registry key.
  - Create registry key: "SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules"
    - String Name = "WINRM-HTTP-In-TCP"

- String Value =  
"v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Domain|Profile=Private|LPort=5985|App=System|Name=@FirewallAPI.dll,-30253|Desc=@FirewallAPI.dll,-30256|EmbedCtxt=@FirewallAPI.dll,-30267|"
- String Name = "WINRM-HTTP-In-TCP-PUBLIC"
- String Value =  
"v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|Profile=Public|LPort=5985|RA4=LocalSubnet|RA6=LocalSubnet|App=System|Name=@FirewallAPI.dll,-30253|Desc=@FirewallAPI.dll,-30256|EmbedCtxt=@FirewallAPI.dll,-30267|"

#### 5. Restarts Windows Firewall