Enabling Windows Management Instrumentation Guide

Symantec

Enabling Windows Management Instrumentation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec and the Symantec Logo, ActiveAdmin, BindView, bv-Control, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Enable Windows Management Instrumentation

This document includes the following topics:

Enable remote access to Windows Management Instrumentation (WMI)

WMI gets installed with all modern operating systems of Microsoft (Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 20081).

This document describes the procedure to enable remote access to WMI. The following steps should take only a minute or two of your time.

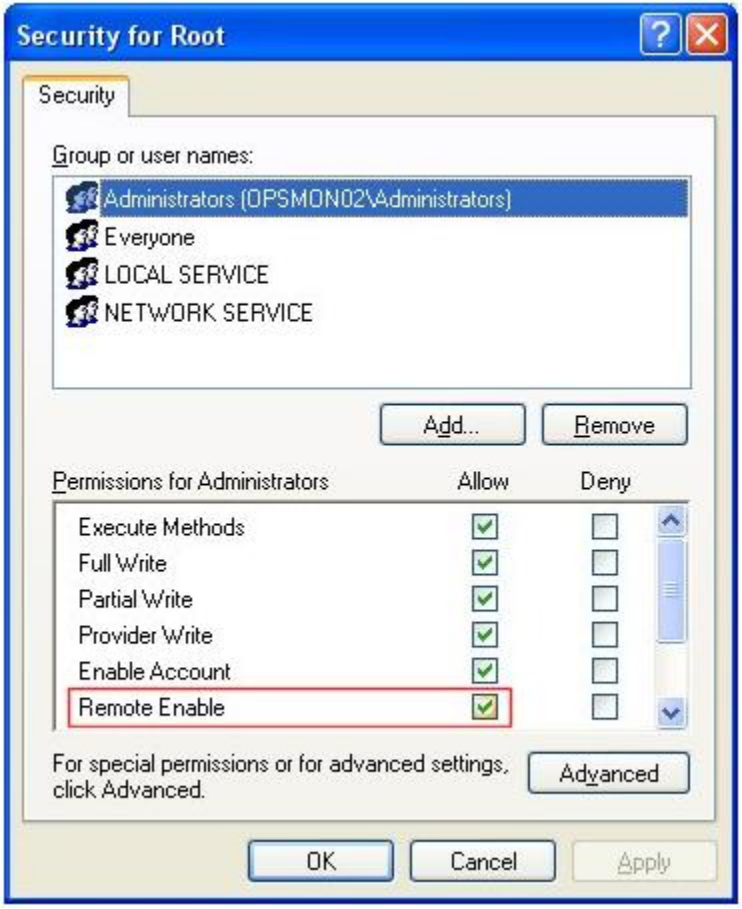
1 Enable remote WMI requests

Usually, you need to change this setting to get WMI working. (Steps 2 and 3 are typically not needed, but you may need them in some circumstances)

- On the target server, go to **Administrative Tools** -> **Computer Management**.
- Expand **Services and Applications**
- Right click **WMI Control** and select **Properties**.

- Select the **Security** tab.
- Click **Security**.

- Add the monitoring user (if needed), and make sure you check **Remote Enable** for the user/group that is requesting WMI data.



At this point you can go back and check if this fixes the problem. It might take a couple of minutes to re-generate the reports.

2 Allow WMI through Windows firewall

All users (including non-administrators) are able to query/read WMI data on the local computer.

For reading WMI data on a remote server, you must onnect your management computer (where monitoring software is installed) to the server you are monitoring (the target server). If the target server is running Windows Firewall (Internet Connection Firewall) that is shipped with Windows XP and Windows 2003, then you must make sure it accepts remote WMI requests. Add the WMI service in the exception list.

3 Enable DCOM calls on the remote machine

If the account you are using to monitor the target server is NOT an administrator on the target server, you need to enable the non-administrator to interact with DCOM by following simple steps listed on the Microsoft website.You can perform the following tasks:

- To grant DCOM remote launch and activation permissions for a user or group
- To grant DCOM remote access permissions

Further Investigation

If the above steps are do not help, Symantec recommends to install the WMI Administrative Tools from Microsoft website. This includes a WMI browser that lets you connect to a remote machine and browse through the WMI information. This helps to isolate any connectivity/rights issues in a more direct and simple environment. Once the WMI browser can access a remote machine, our products should be able to as well.

Download the WMI administrative tools from the Microsoft website.

http://www.microsoft.com/downloads/details.aspx?FamilyId=6430F853-1120-48DB-8CC5-F2ABDC3ED314&displaylang=en

User Account Control (UAC)

The reports we receive from the field let us know that UAC needs to be disabled for remote WMI queries to work. With UAC running, an administrator account actually has two security tokens, a normal user token, and an administrator token (which is only activated when you pass the UAC prompt). Unfortunately, remote

requests that come in over the network get the normal user token for the administrator, and since there is no way to handle a UAC prompt remotely, the token cannot be elevated to the true-administrator security token.