

Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft Internet Security and Acceleration Server

10g Release 2 (10.2)

B28048-01

January 2006

This document provides a brief description about the Microsoft Internet Security and Acceleration Server (ISA) Plug-in, details on the ISA versions and operating system platforms the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

Microsoft Internet Security and Acceleration Server is a stateful packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that improves network security and performance.

The Microsoft Internet Security and Acceleration Server Plug-in extends Oracle Enterprise Manager Grid Control to add support for managing Microsoft ISA Server 2004. By deploying the plug-in in your Grid Control environment, you gain the following management features for Microsoft ISA:

- Monitor availability and receive Microsoft ISA Server data for the following performance areas:
 - Firewall service
 - Web proxy service
 - Firewall packet engine
- Perform trend analysis on collected performance information.
- Receive email and/or page notification concerning potential problems surrounding availability, performance, and/or configuration data.
- Gain access to rich out-of-box reports.
- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as the ISA Server.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10g Release 2 or higher Management Service
- Enterprise Manager Grid Control 10g Release 2 or higher Agent for Windows
- Any edition of Microsoft Internet Security and Acceleration Server 2004 and 2004 SP1

- Microsoft ISA running on Microsoft Windows Server 2003 (see note below)

Note: For details on which editions (such as Enterprise, Standard, and so forth) and versions of Windows operating systems that this Microsoft product is supported to run on, refer to the Microsoft website and/or documentation.

Prerequisites

The following prerequisites must be installed before you can use the Microsoft ISA Server Plug-in:

- Microsoft Internet Security and Acceleration Server 2004
- The following components of Oracle Enterprise Manager 10g Grid Control release 2 or higher:
 - Oracle Management Service with Oracle Management Repository
 - Oracle Management Agent for Windows

You can install the Agent on the same computer as ISA Server (referred to as local Agent monitoring), or you can install the Agent on a different computer from ISA Server (referred to as remote Agent monitoring).

- Ensure that the Windows Management Instrumentation Service is up and running.
- For remote Agent monitoring, a remote Agent must be properly configured. See "[Configuring a Remote Agent](#)" for the procedure.

Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the management plug-in:

1. Download the Microsoft ISA Server Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log in to Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.
9. In the Management Plug-ins page, click the icon in the **Deploy** column for the Microsoft ISA Server plug-in. The Deploy Management Plug-in wizard appears.

10. Click **Add Agents**, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you selected.
11. Click **Next**, then click **Finish**.

If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.

Adding Instances for Monitoring

After successfully deploying the plug-in, follow these steps to add the plug-in target to Grid Control for central monitoring and management:

1. From the Agent home page where the Microsoft ISA Server Plug-in was deployed, select the **Microsoft ISA Server** target type from the **Add** drop-down list, then click **Go**. The Add Microsoft ISA Server page appears.
2. Provide the following information for the properties:
 - **Name** — Unique target name across all the Grid Control targets, such as `isa_hostname`. The name represents this Microsoft ISA Server target across all user interfaces within Grid Control.
 - **Host** — Full name (inclusive of domain, such as `machineA.com`) or the IP address of the host
 - **Username** — Host user name that must be an Administrator user. Required only for remote Agent monitoring.
 - **Password** — Password for the Username. Required only for remote Agent monitoring.
 - **Agent Location** — Remote specifies that the Agent monitoring ISA targets *is not* on the same computer as the target being monitored. (See ["Configuring a Remote Agent"](#) for more information.) Local specifies that the Agent monitoring the target is on the same computer as the target being monitored. Note that remote and local are case-sensitive and should be lowercase.
3. Click **Test Connection** to make sure the parameters you entered (such as the password) are correct.
4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

Note: After you deploy and configure up the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the ISA Server target link from the Agent home page Monitored Targets table. The Microsoft ISA Server home page appears.
2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen and no errors are reported by selecting the **Reports** property page.

Configuring a Remote Agent

The steps for deploying the plug-in are the same for remote Agent monitoring and local Agent monitoring. However, if the Agent is on a remote computer from the plug-in target, certain configuration changes are required to access the Windows Management Instrumentation (WMI) data on the computer where the plug-in target resides.

In a scenario where Computer A runs the Agent, and the target is installed on Computer B, do the following to set up Computer A:

1. Go to the Windows Control Panel and select Administrative Tools, then Services.
2. Select the Oracle Enterprise Manager Agent service from the listed computer where the Agent is running.
3. Right-click the service, then select **Properties**.
4. Click the **Log On** tab. By default, this service is started with the Local System account.
5. Change the default account by selecting the **This account** radio button, and provide an account and password that exist on both computer A and computer B.

Note that the account should be a member of the Administrators group, and the account should have administrative privileges on Computer B. The password should not be left blank.

6. Click **OK**, then restart the Agent service.
7. Ensure that the Windows Management Instrumentation Service is up and running on both computers.

The Agent should now be able to collect data from the remote plug-in target computer. If the configuration above is not initiated, metric collection errors can appear for the plug-in target's metrics.

To ensure that metric collection errors do not occur within Enterprise Manager, Oracle recommends reviewing the Microsoft documentation on the WMI setup. Refer to the Microsoft documentation from the Microsoft website for additional configuration details.

Note: For a remote Agent, the platform to which the Agent is installed can be any Windows type that may not be supported for the Internet Security and Acceleration Server. For example, if the Internet Security and Acceleration Server is running on Windows 2003, you can install the remote Agent on Windows XP to monitor it.

Undeploying the Plug-in

Follow these steps to undeploy the plug-in from an Agent:

1. Log in to Enterprise Manager Grid Control as a Super Administrator.
2. Select the **Targets** tab, then the **All Targets** subtab. The All Targets page appears.
3. Select the Microsoft ISA Server Plug-in target and click **Remove**. You must do this step for all targets of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. Click the **Setup** link in the upper right corner of the All Targets page, then click the **Management Plug-ins** link on the left side of the Setup page. The Management Plug-ins page appears.
6. Click the icon in the **Undeploy** column for the Microsoft ISA Server Plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the Microsoft ISA Server Plug-in and click **OK**.

You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.

8. Select the Microsoft ISA Server Plug-in on the Management Plug-ins page and click **Delete**.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

System Monitoring Plug-in Installation Guide for Microsoft Internet Security and Acceleration Server, Release 2 (10.2)
B28048-01

Copyright © 2006 Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Alpha and Beta Draft documentation are considered to be in prerelease status. This documentation is intended for demonstration and preliminary use only. We expect that you may encounter some errors, ranging from typographical errors to data inaccuracies. This documentation is subject to change without notice, and it may not be specific to the hardware on which you are using the software. Please be advised that prerelease documentation is not warranted in any manner, for any purpose, and we will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.