Oracle Enterprise Manager

Plug-in for Oracle Secure Global Desktop Gateway User's Guide

April 2015
E52285-01

Oracle Legal Notices

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Table of Contents

Preface

The *Enterprise Manager Plug-in for Oracle Secure Global Desktop Gateway User Guide* describes how to install and use the Enterprise Manager Plug-in for Oracle Secure Global Desktop Gateway in order to monitor Oracle Secure Global Desktop Gateway (SGD Gateway) resources from within Oracle Enterprise Manager.

1 Audience

This guide is intended for administrators who are familiar with SGD and require access to the comprehensive metrics and performance data that Oracle Enterprise Manager collects for all managed Oracle systems.

2 Document Organization

The document is organized as follows:

- Chapter 1, *Introduction to the Plug-in* is an introduction to the plug-in. Supported versions and requirements are covered in this chapter.
- Chapter 2, *Installing and Configuring the Plug-in* describes how to install and deploy the plug-in. Instructions on how to how to undeploy and uninstall the plug-in are also included.
- Chapter 3, *Monitoring an SGD Gateway Target* describes the layout and content of the monitoring pages for the plug-in.
- Chapter 4, *Troubleshooting the Plug-in* includes basic troubleshooting information for the plug-in.
- Chapter 5, *Plug-in Metrics Reference* lists the metrics collected by the plug-in.

3 Related Documents

The documentation for the Oracle Secure Global Desktop product is available at:

http://www.oracle.com/technetwork/documentation/sgd-193668.html

For additional information, see the following manuals:

- *Oracle Secure Global Desktop Gateway Administration Guide*
- *Oracle Secure Global Desktop Platform Support and Release Notes*
- *Oracle Secure Global Desktop Administration Guide*

4 Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1 Introduction to the Plug-in

The Enterprise Manager Plug-in for Oracle Secure Global Desktop Gateway extends Oracle Enterprise Manager Cloud Control to add support for monitoring an Oracle Secure Global Desktop Gateway (SGD Gateway) deployment.

The SGD Gateway is a component of Oracle Secure Global Desktop (SGD). The SGD Gateway is a proxy server designed to be deployed in front of an SGD array in a demilitarized zone (DMZ).

The plug-in provides an SGD Administrator with centralized monitoring of SGD Gateway resources in a single view. The plug-in enables integration with the SGD Gateway by adding an Oracle Secure Global Desktop Gateway target type, together with monitoring pages for an SGD Gateway and related resources.

Monitoring pages show a summary of system information, user activity, and alerts. A description of the monitoring pages is provided in Chapter 3, *Monitoring an SGD Gateway Target*.

For an overview of the architecture, terminology, and components of Oracle Enterprise Manager Cloud Control, see the Oracle Enterprise Manager Cloud Control documentation.

1.1 Requirements for the Plug-in

This section describes the requirements to enable monitoring of an SGD Gateway deployment.

1.1.1 Supported Versions

The plug-in supports the following versions of Oracle Enterprise Manager Cloud Control and Oracle Secure Global Desktop Gateway:

- Oracle Enterprise Manager Cloud Control 12c Release 4 (12.1.0.4) [1]
- Oracle Secure Global Desktop Gateway version 5.2 or later

1.1.2 Prerequisites

Before you install the plug-in, verify that your environment meets these requirements:

- An Oracle Enterprise Manager installation must be running.

  For Oracle Enterprise Manager Cloud Control system requirements and installation instructions, see the Oracle Enterprise Manager Cloud Control installation documentation.

- An Oracle Management Agent (Management Agent) must be installed on each SGD Gateway host that you want to monitor.
- For each SGD Gateway, the reflection service must be enabled and configured for authorized access. The reflection service is a collection of RESTful web services used by SGD Gateway Administrators.

  See the SGD Gateway documentation for details of how to enable and configure the reflection service.

1.1.3 User Requirements

To monitor an SGD Gateway deployment with the plug-in, the following user requirements apply.

[1] Requires ARU 18654647.

On each SGD Gateway host, the Oracle Software Owner User must have an account and must be a member of the `sgdgserv` UNIX group.

- The Oracle Software Owner User (typically, `oracle`) is required to install the Oracle Management Agent on the host. For details of the requirements for this user, see the Oracle Enterprise Manager Cloud Control installation documentation.
- The `sgdgserv` group contains the SGD Gateway system account users. Adding the Oracle Software Owner User to this group enables the Oracle Software Owner User to run `gateway` commands.

When you add the Oracle Software Owner User to the `sgdgserv` group, ensure that you preserve any existing supplementary groups for this user.

For example, if the Oracle software owner user is `oracle`:

```
# usermod -G group1,group2,sgdgserv oracle
```

where *`group1`* and *`group2`* are the existing supplementary groups for the `oracle` user.

Chapter 2 Installing and Configuring the Plug-in

This chapter describes how to install and configure the plug-in in your Oracle Enterprise Manager environment.

Note

This chapter summarises the main steps required to install, deploy, and configure the plug-in. For more detailed instructions, see the Oracle Enterprise Manager Cloud Control documentation.

The following tasks are described in this chapter:

- Downloading and deploying the plug-in to Oracle Enterprise Manager.

  You deploy the plug-in to Oracle Enterprise Manager and to an SGD Gateway host.

  See Section 2.1, “Downloading and Deploying the Plug-in”.

- Configuring targets for monitoring an SGD Gateway host.

  See Section 2.2, “Adding Monitoring Targets”.

- Verifying the plug-in installation and deployment.

  See Section 2.3, “Verifying the Plug-in Deployment”.

- Uninstalling the plug-in.

  See Section 2.4, “Uninstalling the Plug-in”.

2.1 Downloading and Deploying the Plug-in

The plug-in is distributed through the Oracle Enterprise Manager Store.

For detailed steps on how to download and deploy the plug-in, see the Oracle Enterprise Manager Cloud Control Administrator's Guide.

The following is a summary of the required tasks for downloading and deploying the plug-in.

- Download the plug-in to the Management Repository.

  Plug-in Manager in the Enterprise Manager Cloud Control Console shows that the plug-in is available in your environment.

- Deploy the plug-in to Oracle Management Service (OMS).

  This enables the OMS to manage SGD Gateway targets.

- Deploy the plug-in to a Management Agent on an SGD Gateway host.

  This enables the Management Agent to discover and monitor SGD Gateway targets.

2.2 Adding Monitoring Targets

After the plug-in is deployed, Oracle Enterprise Manager recognizes monitoring targets of the type *Oracle Secure Global Desktop Gateway*. To monitor an SGD Gateway, you add the Gateway host as a monitoring target.

Repeat the following steps for each SGD Gateway host.

1. Log in to the Enterprise Manager Cloud Control Console.
2. In the **Setup** menu, select **Add Target**, and then select **Add Targets Manually**.
3. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**.
4. In the **Target Type** list, select Oracle Secure Global Desktop Gateway.
5. In the **Monitoring Agent** field, do one of the following:
   - Enter the fully qualified host name and port of the target. For example: `boston.example.com:3872`.
   - Click the search icon to search for an SGD Gateway host that is running the Management Agent.
6. Click **Add Manually**. The properties page for the new Oracle Secure Global Desktop Gateway target is displayed.
7. Configure the new Oracle Secure Global Desktop Gateway target.

   You must complete all of the following fields.

   - **Target Name:** A unique name to identify the monitoring target.
   - **Gateway Installation Directory:** The path to the SGD Gateway installation on the host. This is `/opt/SUNWsgdg` by default.
8. Click **OK** to save details and add the new target.

2.3 Verifying the Plug-in Deployment

After you add an SGD Gateway as a monitoring target, wait at least 15 minutes for the plug-in to start collecting data. Then use the following steps to verify that Oracle Enterprise Manager is correctly monitoring the target.

1. Log in to the Enterprise Manager Cloud Control Console.
2. From the **Targets** menu, select **All Targets**.
3. In the Refine Search pane, select **Target Type**, then **Servers, Storage and Network**, and then **Oracle Secure Global Desktop Gateway**.

   Check that the target is present and that the **Target Status** is Up.
4. Click the name of the target that you want to verify.

   The target home page is displayed.
5. From the **Oracle Secure Global Desktop Gateway** menu in the upper-left of the page, select **Monitoring**, and then select **Metric Collection Errors**.

   Check any metric collection errors listed in the table.
6. From the **Oracle Secure Global Desktop Gateway** menu, select **Monitoring**, and then select **All Metrics**.

   Click the metrics in the left-hand pane and check that data is being collected.

2.4 Uninstalling the Plug-in

The plug-in can be uninstalled from your Oracle Enterprise Manager environment.

To upgrade the plug-in, simply deploy the new version as shown in Section 2.1, “Downloading and Deploying the Plug-in”. Uninstallation is not required before an upgrade.

For detailed steps on uninstalling the plug-in, see the Managing Plug-Ins chapter in the Oracle Enterprise Manager documentation.

Uninstalling the plug-in consists of the following steps:

- (Optional) Unconfigure all SGD Gateway targets.

  It is best to unconfigure targets, to halt data monitoring.

- Undeploy the plug-in.

  When you undeploy the plug-in, Oracle Enterprise Manager can no longer monitor an SGD Gateway target.

- (Optional) Remove the plug-in from the Management Repository.

Chapter 3 Monitoring an SGD Gateway Target

When you configure an SGD Gateway host as a target, the target name is shown in the All Targets page, a list of all targets that are monitored by Oracle Enterprise Manager.

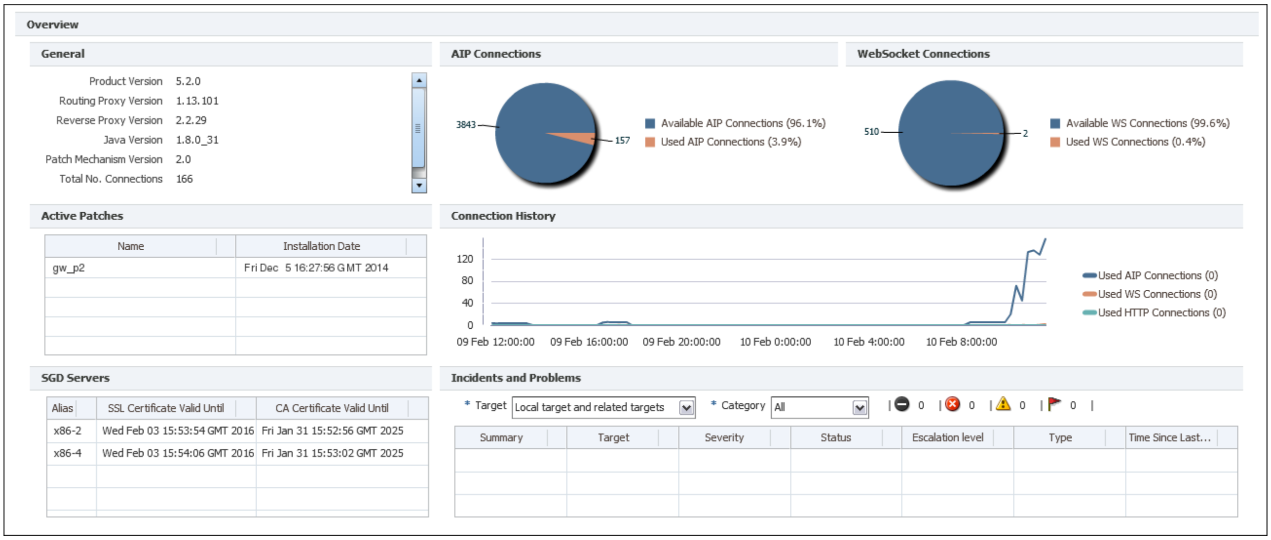
To display the monitoring page for an SGD Gateway, select from the available *Oracle Secure Global Desktop Gateway* targets on the All Targets page.

This chapter describes the data and metrics shown on the monitoring page for an SGD Gateway target. See Section 3.1, “The SGD Gateway Monitoring Page”.

3.1 The SGD Gateway Monitoring Page

The SGD Gateway monitoring page shows information on software versions, connections, and incidents for an SGD Gateway target. See Figure 3.1, “Oracle Secure Global Desktop Gateway Monitoring Page”.

Figure 3.1 Oracle Secure Global Desktop Gateway Monitoring Page



Overview

General

Product Version 5.2.0
Routing Proxy Version 1.13.101
Reverse Proxy Version 2.2.29
Java Version 1.8.0_31
Patch Mechanism Version 2.0
Total No. Connections 166

AIP Connections

3843
157
Available AIP Connections (96.1%)
Used AIP Connections (3.9%)

WebSocket Connections

Active Patches

Name	Installation Date
gw_p2	Fri Dec 5 16:27:56 GMT 2014

Connection History

SGD Servers

Alias	SSL Certificate Valid Until	CA Certificate Valid Until
x86-2	Wed Feb 03 15:53:54 GMT 2016	Fri Jan 31 15:52:56 GMT 2025
x86-4	Wed Feb 03 15:54:06 GMT 2016	Fri Jan 31 15:53:02 GMT 2025

Incidents and Problems

* Target Local target and related targets * Category All

⊖ 0 | ⊗ 0 | ⚠ 0 | 🚩 0 |

Summary	Target	Severity	Status	Escalation level	Type	Time Since Last...

The SGD Gateway monitoring page includes a series of panels, as described in Table 3.1, “Panels on the SGD Gateway Monitoring Page”.

Table 3.1 Panels on the SGD Gateway Monitoring Page

Panel	Description
General	A table that shows software version information and a summary of connection statistics for the Gateway.
AIP Connections	A pie chart that shows the number of AIP connections for the Gateway. The percentage of used connections, compared to the maximum number of available connections, is shown.
Websocket Connections	A pie chart that shows the number of websocket connections for the Gateway. The percentage of used connections, compared to the maximum number of available connections, is shown.

Panel	Description
Active Patches	A table that shows details of the SGD software patches installed on the Gateway.
Connection History	A line chart that shows the number of AIP, HTTP, and websocket connections over the previous 24 hours.
SGD Servers	A table that shows details of the SGD server security certificates stored in the SGD Gateway keystore.
Incidents and Problems	The Incidents and Problems table shows system messages relating to events, incidents, and problems for the Gateway. For more information about managing incidents in Oracle Enterprise Manager, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Chapter 4 Troubleshooting the Plug-in

This chapter provides basic information and links to additional resources to assist you in troubleshooting issues with the plug-in and tuning the performance of the plug-in.

4.1 Plug-in Log Files

When you are troubleshooting issues with the plug-in, the following logs may contain useful information.

- **Oracle Enterprise Manager Cloud Control logs.** Logging is available for the Oracle Management Service (OMS) and Management Agents.

  For more details about Oracle Enterprise Manager logging, see the Locating and Configuring Enterprise Manager Log Files chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- **SGD Gateway logs.** See the *Oracle Secure Global Desktop Gateway Administration Guide* for information about SGD Gateway logging.

4.2 Plug-in Installation and Deployment Issues

The following topics describe how to troubleshoot issues when installing and deploying the plug-in.

4.2.1 Oracle Enterprise Manager Installation Issues

If you encounter problems during installation of the plug-in, verify that all prerequisites are met. See Section 1.1, “Requirements for the Plug-in”.

For information on installing Oracle Enterprise Manager, refer to the Oracle Enterprise Manager Cloud Control documentation.

4.2.2 Plug-in Deployment Issues

The following troubleshooting tips may apply when you are having issues with deploying the plug-in:

- If you encounter problems when adding an SGD Gateway target, verify the settings for communication between the Management Agent and the Gateway host. See Section 2.2, “Adding Monitoring Targets”.

- If a target is shown as down in the Enterprise Manager Cloud Control Console, try the following:

  - Check the status of the SGD Gateway on the target host.

    Run the `gateway status` command on the SGD Gateway host.

    For more information about troubleshooting SGD Gateway issues, see the *Oracle Secure Global Desktop Gateway Administration Guide*.

  - Verify that the plug-in is working correctly and that metrics are being collected.

    Display the All Metrics page for the target and click on a metric in the left-hand pane.

    An error message is shown if there is an issue with metrics data collection.

4.3 Configuring Metrics Collection

The following topics describe how to configure and tune metrics collection for the plug-in.

4.3.1 Changing Metrics Collection Intervals

All metrics collection intervals are configurable. To set a different collection schedule for a target, do the following:

- Display the Metric and Collection Settings page for the target.

  In the target menu, select **Monitoring**, then select **Metric and Collection Settings**.

- Change the collection interval for one or more metrics.

  In the **Collection Schedule** column, click a collection interval to change the setting.

4.3.2 Changing Event Thresholds

Many metrics collected by the plug-in have predefined thresholds and incident messages. When a threshold is crossed, an incident is reported by means of an alert message in the Incidents and Problems table for the target.

To change an event threshold for a target, do the following:

- Display the Metric and Collection Settings page for the target.

  In the target menu, select **Monitoring**, then select **Metric and Collection Settings**.

- Change the thresholds for an event.

  Edit the settings in the **Warning Threshold** or **Critical Threshold** columns.

4.3.3 Viewing Real-Time Metrics Data

The data displayed on the monitoring page for a target is retrieved from the Management Repository. This is not real-time information.

To see the real-time metrics data, as it is collected by the Monitoring Agent, view the All Metrics page for the target.

Chapter 5 Plug-in Metrics Reference

This section contains a list of metrics collected by the plug-in. Examples of typical metrics are included.

Plug-in metrics data can be processed by reporting tools such as Oracle Business Intelligence Publisher.

The following types of metrics are collected by the plug-in:

- **Performance metrics.** Examples of performance metrics include connections and performance summary data.

  Performance metrics are typically collected at short intervals, such as every 15 minutes.

  See Section 5.1, “Performance Metrics”.

- **Configuration metrics.** Examples of configuration metrics include Gateway patch and component software versions.

  Performance metrics are typically collected at long intervals, such as every 24 hours.

  See Section 5.2, “Configuration Metrics”.

5.1 Performance Metrics

The following performance metrics are collected by the plug-in.

Response

Column	**Type**	**Description**	**Example**
Status	NUMBER	Whether the Gateway is up or down	1

Summary

Column	**Type**	**Description**	**Example**
ID	STRING (KEY)	Unique ID for the Gateway summary	*number*
TotalConnections	NUMBER	Total number of current connections	*number*
UsedHTTPConnections	NUMBER	Number of current HTTP connections for the Gateway	*number*
UsedTCCConnections	NUMBER	Number of current AIP connections for the Gateway	*number*
UsedWSConnections	NUMBER	Number of current websocket connections for the Gateway	*number*
AvailableHTTPConnections	NUMBER	Maximum number of available HTTP connections for the Gateway	*number*
AvailableTCCConnections	NUMBER	Maximum number of available AIP connections for the Gateway	*number*
AvailableWSConnections	NUMBER	Maximum number of available websocket connections for the Gateway	*number*

Column	Type	Description	Example
IncomingSecurityLevel	STRING	Security level for data received by the Gateway	SSL
UsedHTTPConnectionsPercentage	NUMBER	Percentage of used HTTP connections, compared to the maximum number of available HTTP connections	*number*
UsedTCCConnectionsPercentage	NUMBER	Percentage of used AIP connections, compared to the maximum number of available AIP connections	*number*
UsedWSConnectionsPercentage	NUMBER	Percentage of used websocket connections, compared to the maximum number of available websocket connections	*number*

5.2 Configuration Metrics

To process configuration metrics data, use the `OGDG` plug-in tag with the table name. For example, to process version metrics use the following string:

```
OGDG_VERSIONS
```

The following configuration metrics are collected by the plug-in.

ACTIVE_PATCHES

Column	Type	Description	Example
PATCH_NAME	STRING (KEY)	Name of installed SGD Gateway software patch	Patch_50p1
INSTALL_DATE	STRING	Date and time when patch was installed	Tue Jan 21 16:18:08 GMT 2014

SGD_SERVERS

Column	Type	Description	Example
ALIAS	STRING (KEY)	Alias used when storing certificates in the Gateway keystore	sgd-newyork
CA_CERT_SERIAL	STRING	Serial number of the SGD server CA certificate	*serial-no*
CA_CERT_VALID_FROM	STRING	Validity start date for the SGD server CA certificate	Tue Jan 21 16:18:08 GMT 2014
CA_CERT_VALID_UNTIL	STRING	Expiry date for the SGD server CA certificate	Sat Jan 18 16:18:08 GMT 2024
SSL_CERT_SERIAL	STRING	Serial number for the SGD server SSL certificate	*serial-no*
SSL_CERT_VALID_FROM	STRING	Validity start date for the SGD server SSL certificate	Tue Jan 21 16:18:08 GMT 2014
SSL_CERT_VALID_UNTIL	STRING	Expiry date for the SGD server SSL certificate	Sat Jan 18 16:18:08 GMT 2024

VERSIONS

Column	Type	Description	Example
SGDG_VERSION	STRING	SGD Gateway version	5.20.901
JAVA_VERSION	STRING	Java technology version	1.8.0
ROUTING_VERSION	STRING	Routing proxy component version for the SGD Gateway	2.2.27
REVERSE_VERSION	STRING	Reverse proxy component version for the SGD Gateway	1.13.101
PATCH_MECH_VERSION	STRING	SGD patch mechanism version	1.3