Foglight® 5.6.7

Investigating Guest Processes
Installation and Configuration Guide
This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST’S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:
Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, Foglight, IntelliProfile, PerformaSure, Spotlight, StealthCollect, TOAD, Tag and Follow, Vintela Single Sign-on for Java, vOPS, and vFoglight are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software’s trademarks, please see http://www.quest.com/legal/trademark-information.aspx. Other trademarks and registered trademarks are property of their respective owners.

Third Party Contributions

This product contains some third party components. For a complete list, see the License Credits page in the online help.

Installation and Configuration Guide
March 2013
Cartridge Version 5.6.7
# Table of Contents

## Introduction to this Guide

- About Quest Software, Inc. .......................... 4
- Contacting Quest Software......................... 4
- Contacting Quest Support ......................... 4

## Installing and Configuring the Cartridge for Guest Process Investigation

- Installing the Cartridge for Guest Process Investigation on Foglight .................. 6
- Installing the Cartridge for Guest Process Investigation on vFoglight .............. 6
- Guest Process Investigation Collection Methods ............................................... 7
  - Windows Management Instrumentation (WMI) ............................................ 7
  - Windows Remote Management (WinRM) .................................................... 8
- Operating Systems and Collection Methods ...................................................... 11
- Installing the Foglight Agent Manager (FglAM) ............................................. 11
- Configuring Root Certificates for FglAM .......................................................... 12
- Installing the Cartridge for Guest Process Investigation Cartridge .................. 12
- Creating an Agent .............................................................................................. 13

## Index ................................................. 15
Introduction to this Guide

This *Installation and Configuration Guide* provides instructions for installing and configuring the Foglight Cartridge for Guest Process Investigation. Before you begin, refer to the *System Requirements and Platform Support Guide*.

About Quest Software, Inc.

Established in 1987, Quest Software (Nasdaq: QSFT) provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, user workspace management to Windows management. For more information, visit [www.quest.com](http://www.quest.com).

Contacting Quest Software

<table>
<thead>
<tr>
<th></th>
<th><a href="mailto:info@quest.com">info@quest.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>Quest Software, Inc.</td>
</tr>
<tr>
<td></td>
<td>World Headquarters</td>
</tr>
<tr>
<td></td>
<td>5 Polaris Way</td>
</tr>
<tr>
<td></td>
<td>Aliso Viejo, CA 92656</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
</tbody>
</table>

Refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to our Support Portal at [http://www.quest.com/support](http://www.quest.com/support).

From our Support Portal, you can do the following:
• Retrieve thousands of solutions from our Knowledge Base
• Download the latest releases and service packs
• Create, update, and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, policies, and procedures. The guide is available at: http://www.quest.com/support.
Installing and Configuring the Cartridge for Guest Process Investigation

The Cartridge for Guest Process Investigation installs on:

- Foglight (For more information, see “Installing the Cartridge for Guest Process Investigation on Foglight” on page 6.)
- vFoglight (For more information, see “Installing the Cartridge for Guest Process Investigation on vFoglight” on page 6.)

Installing the Cartridge for Guest Process Investigation on Foglight

To install and configure the Cartridge for Guest Process Investigation on Foglight:

<table>
<thead>
<tr>
<th>Note</th>
<th>Steps one and three are optional.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install and configure the Windows Remote Management (WinRM) on the remote machine. For more information, see “Downloading WinRM” on page 9.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Foglight Agent Manager (FglAM) on Foglight. For procedures to install the Foglight Agent Manager, refer to the Foglight Getting Started Guide.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the Root Certificates for the Cartridge for Guest Process Investigation. For more information, see “WinRM Configuration” on page 9.</td>
</tr>
<tr>
<td>4</td>
<td>Install the Cartridge for Guest Process Investigation on Foglight. For more information, see “Installing the Cartridge for Guest Process Investigation Cartridge” on page 12.</td>
</tr>
<tr>
<td>6</td>
<td>Create an agent. For more information, see “Creating an Agent” on page 13.</td>
</tr>
</tbody>
</table>

Installing the Cartridge for Guest Process Investigation on vFoglight

When you install vFoglight, the following actions take place:
• The Foglight Agent Manager installs.
• The Cartridge for Guest Process Investigation installs.
• The agent is created and deploys.

If you want to install the Cartridge for Guest Process Investigation on another Foglight Agent Manager to monitor hosts, perform the following steps:

1. Install the Foglight Agent Manager (FglAM) on the machine that will be monitoring other hosts. For procedures to install the Foglight Agent Manager, refer to the Foglight Getting Started Guide.

2. If installing on a Windows machine, configure the Root Certificates for the Cartridge for Guest Process Investigation. For more information, see “WinRM Configuration” on page 9.


4. Create an agent. For more information, see “Creating an Agent” on page 13.

Guest Process Investigation Collection Methods

The Cartridge for Guest Process Investigation provides the following methods to collect process data:

• Windows Management Instrumentation (WMI) (See page 7.)

  Note WMI is the recommend method for collection of Guest Process metrics.

• Windows Remote Management (WinRM) (See page 8.)

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) allows for management, control, and monitoring of systems in your enterprise. The Cartridge for Guest Process Investigation uses WMI to connect to virtual and physical machine hosts to collect process metrics. The following information must be taken into consideration when using the WMI with the Cartridge for Guest Process Investigation:

• You must have a local or domain administrator’s account to collect process data.

• You cannot use WMI with the Cartridge for Guest Process Investigation to collect metrics thorough a firewall. You must turn the firewall off to collect metrics or use WinRM. For more information, see “Windows Remote Management (WinRM)” on page 8.

• The WMI collection method may require that the Remote Registry service be running on the target host. Some versions of Microsoft Windows (most commonly Vista) do not enable this service by default. It is recommended that you verify this service is running and configured to start automatically.

  Note If the Remote Registry service is started after attempting collection, you must restart FglAM before the collection will be successful.
Some access restrictions on Windows Server 2008 R2 restrict access to certain areas of the registry that prohibit the Guest Process Agent from collecting data. For additional steps, see “Monitoring Windows Server 2008 R2 Host via WMI” on page 8. You can otherwise use WinRM to collect process data from these hosts.

**Monitoring Windows Server 2008 R2 Host via WMI**

The following steps provide procedures to access restrictions on Windows Server 2008 R2 that prohibit the Quest Guest Process agent from being able to collect process data.

*To collect data from Windows Server 2008 R2 via WMI:*

1. Login to the target remote host as Administrator.
2. Run the Regedit program.
3. If you are asked to allow the Regedit program to make changes to the computer, click **Yes**.
4. Navigate to the Registry item:
   
   `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

5. Right click this item and select **Permissions**.
6. Click **Advanced**.
7. Select the **Owner** tab.
8. In the “Change Owner to...” box, highlight the account you are currently logged in as.
9. Click **Ok**.
   
   The dialog closes.
10. Click **Ok**.
    
    The dialog closes.
11. Right click the registry item again and select **Permissions**.
12. Highlight the Administrator’s group.
13. Give Full Control permissions to this group by checking the **Allow** box.
14. Click **Ok**.
15. Close the Regedit program.

**Windows Remote Management (WinRM)**

*Note*  
WinRM installation is now optional. You can choose from WinRM or WMI as the collection method.

To collect process information from remote Windows installations, the Cartridge for Guest Process Investigation relies on Windows Remote Management (WinRM) to expose the process information data. While some Windows installations include WinRM, others require that you download and install it.
The Cartridge for Guest Process Investigation is compatible with two types of WinRM authentication:

- Encrypted (HTTPS) basic authentication
- Non encrypted (HTTP) basic authentication

After WinRM is installed and properly configured, ensure that process information collection is successful before moving on to the configuration of other WinRM installations.

The following sections describe the WinRM installation and configuration procedures:

- **Downloading WinRM** (For more information, see “Downloading WinRM” on page 9.)
- **WinRM Configuration** (For more information, see “WinRM Configuration” on page 9.)
- **Listening for Remote Connections** (For more information, see “Listening for Remote Connections” on page 10.)

### Downloading WinRM

**Note**
The Guest Process cartridge does not work with the version of WinRM that is available through optional Windows components on Windows Server 2003 R2. The following link allows you to download the recommended update for WS-Management, which contains the latest version of WinRM that is compatible with the Guest Process Cartridge.


WinRM installations can be viewed for:

- Windows Server 2003 (x86 and 64-bit systems)
- Windows XP (x86 and 64-bit systems)

### WinRM Configuration

During WinRM configuration, it is recommended to reference the WinRM help for more specific configuration instructions. Type “`winrm`” at the command prompt to access help.

**Note**
If an "Access is denied" error occurs when running WinRM command line commands, you may need to run the command line prompt tool using "Run as administrator" or temporarily disable the User Account Control (UAC). Visit the following link for instructions on disabling UAC: [http://technet.microsoft.com/en-us/library/cc709691(VS.10).aspx](http://technet.microsoft.com/en-us/library/cc709691(VS.10).aspx).

**Note**
After configuration is complete, ensure that the Windows Remote Management service is started.

### WinRM Remote Access Account Restrictions

Listening for Remote Connections

WinRM on the monitored Windows machine must be configured to listen for incoming connections from remote parties. First however, you must decide if you want the Guest Process Investigation agent to connect to WinRM via HTTP or HTTPS.

**Note**  
After configuration is complete, confirm the HTTP/HTTPS port value by typing the command "winrm enumerate winrm/config/listener". Most Windows versions use port 80/443, however, some versions are known to use other port values such as 5985/5986.

Connection via HTTP

Using an HTTP connection is by far the easiest of the two when it comes to configuration and setup. The best option for creating a listener is to use the command "winrm quickconfig". This command creates an HTTP listener on port 80 with a URL path of “wsman”. These are the default values, but you can change them later, if necessary. Furthermore, using this command, WinRM will add an exception to the Windows Firewall. This is a necessary step if the firewall is enabled. If you experience problems with the quickconfig command or wish to have more control of the listener setup, the following shows an example of another approach:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
```

The following example shows another method to create a listener:

```
"winrm create winrm/config/listener?Address=*+Transport=HTTP"
```

After the listener has been created, run the following command to allow unencrypted communication with WinRM:

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

Connection via HTTPS

This authentication scheme establishes an encrypted HTTPS session with WinRM. This authentication requires that WinRM be configured with an HTTPS listener and that an appropriate certificate that identifies the machine WinRM is running on. In addition to this WinRM configuration, the server that is running the Foglight Agent Manager (or servers that are not vFoglight) must be configured to trust the WinRM Server’s Certificate. You must configure the Foglight Agent Manager to trust third party certificates.

**Note**  
The Foglight Agent Manager can be installed on servers that are not vFoglight servers. It is the FglAM server that needs to be configured, not the vFoglight/Foglight server.

The following is an example for configuring WinRM with an HTTPS listener and certificate:

```
* winrm create winrm/config/listener?Address=*+Transport=HTTPS @{CertificateThumbprint="PASTE_CERTIFICATE_THUMBPRINT_HERE"}
```

Allowing Basic Authentication

This is the last step required for WinRM configuration. WinRM must be configured to allow basic authentication via the following command so that the Guest Process Investigation agent is able to access WinRM:

```
winrm set winrm/config/service
```
"winrm set winrm/config/service/auth @{Basic="true"}"

Operating Systems and Collection Methods

The following table lists the operating systems and collection methods supported by this release of the Guest Process Cartridge.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows Management Instrumentation (WMI)</th>
<th>Windows Remote Management (WinRM) (^1)</th>
<th>Secure Shell (SSH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2000 R2</td>
<td>(^2) X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Windows Vista</td>
<td>(^3) X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Oracle Solaris 10</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

1 The WinRM collection method requires some configuration. See Windows Remote Management (WinRM) for procedures on installation and configuration.

2 Collecting process data from Windows Server 2008 R2 via WMI requires additional steps. See Monitoring Windows Server 2008 R2 Host via WMI for procedures.

3 Some versions of Vista require that you enable the Remote Registry Service before collecting data via WMI.

Installing the Foglight Agent Manager (FglAM)

For the Cartridge for Guest Process Investigation, the Foglight Agent Manager only needs to be installed on the Foglight server. It does not need to be installed on each individual host where you want to monitor process information. The Foglight Agent Manager also provides a number of support services such as installation, upgrade, and the ability to configure agents.

Guest Process Investigation monitors machines remotely. You do not need to install FglAM on all machines you want monitored. One installation of FglAM per Foglight Server is enough, unless another installation is needed to offset the collection load onto other machines.

For procedures to install the Foglight Agent Manager, refer to the Foglight Getting Started Guide.
Configuring Root Certificates for FglAM

If any process information collection is to be done with a WinRM server through encrypted HTTPS communication, a new Certificate Authority must be added to the Java Runtime Environment (JRE) used by the Foglight Agent Manager. The JRE includes a command line tool called “keytool” which can be used to add the new Certificate Authority.

An example command line to import a new root certificate would be:

```
JAVA_HOME/jre/bin/keytool -import -file new_cacert.pks -alias 'somename' -keystore 'jks'
```

The initial password of the “cacerts” keystore file is “changeit”. System administrators should change this password and the default access permissions of this file when installing the SDK. The file is located at:

```
"FGLAM_HOME/jre/JRE_VERSION/jre/lib/security/cacerts"
```

| Note | The certificate file to be imported should be the public certificate for the Certificate Authority that signed the server's SSL certificate, not the SSL certificate itself. |

Installing the Cartridge for Guest Process Investigation Cartridge

Installation is the first step in adding a cartridge to the Foglight Management Server. A cartridge file has the extension .car. Installing the .car file causes the Management Server to be aware of all cartridges in the .car file.

A cartridge must also be enabled before it is added to the Foglight Management Server. You can cause a cartridge to be enabled upon installation, or you can enable it after installation. See the Foglight Administration and Configuration Guide for instructions on enabling and disabling cartridges after installation.

To install a cartridge:

1. On the navigation panel, under Dashboards, click Administration > Cartridges > Cartridge Inventory.
2. In the Install Cartridge area, type the path to the .car file for the cartridge you want to install.
   - Type the path in the File on Local Machine field if you want to upload a .car file from your local machine to the Management Server.
   - Type the path in the File on Server field if you want to install a .car file that is in a local directory on the machine hosting the Management Server.
   - Alternatively, you can click Browse to navigate to a .car file on your local machine using a file chooser. Click OK in the file chooser when you have selected the .car file you want to install.
3. The check box Enable on install is selected by default.
   - If you would like the cartridge to be enabled when it is installed, leave this check box selected.
• If you would like to enable the cartridge after installation, clear this check box.

4 Click Install Cartridge.

If the cartridge installs successfully, the message “Cartridge has been installed successfully” appears.

5 Click OK.

If Enable on install was not selected (step 3), a caution symbol appears in the row for that cartridge in the table in the Cartridge Inventory. For more information about cartridge installation and configuration see the Foglight Administration and Configuration Guide.

Creating an Agent

After installing the Cartridge for Guest Process Investigation, you may need to create an additional agent to handle heavier host loads.

To create an agent:

1. On the navigation panel, under Dashboards, click Administration > Agents > Agent Status. The Agent Status dashboard displays.
2. Click Create Agent.
   The Create Agent pane displays.
3. From the Host drop-down, select the required host.
4. Click GuestProcessAgent.
5. In Instance Name, enter the required name.
6. Click Create.
   The Create Agent Results pane displays. A green check mark displays when the agent is created.
7 Click **OK**.
Index

A
authentication
   encrypted basic authentication via HTTPS  10

C
Cartridge for Guest Process Investigation
   installing the car  12
   collection methods  11
   configuring root certificates for FgLAM  12

G
Guest Process Investigation collection methods
   Windows Management Instrumentation (WMI)  7
   Windows Remote Management (WinRM)  8

I
installation steps
   configuring root certificates  12
   installing FgLAM  11
   installing on vFoglight  6

O
operating systems and collection methods  11
operating systems support  11

S
Server 2008 R2 Host and WMI
   monitoring  8
   steps required to install Guest Process  6
   support  4

T
technical support  4

W
Windows Server 2008 R2