Hewlett Packard
Enterprise

HPE Security Fortify Runtime Application Protection (RTAP)

Software Version: 17.3

Agent Installation Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Change Log

The following table lists changes made to this document. Revisions to this document are published only if the changes made affect product functionality.

Software Release / Document Version	Change
17.3	Added: Support for Jetty 9.3. Added: Support for JBoss 6.3.0, 6.4.0. Changed: The Fail Closed flag replaces the Fail Open flag. The Fail Closed flag stops your application from starting when it fails to connect with the Fortify Application Defender Agent.
16.8	Added: Silent installation for the .NET agent. Added: Notes on changing the default value of the .NET Fail Open Timer.
16.3	Updated: Minor update for 16.3 release; no significant content changes. HP to HPE rebranding.

Installing the Runtime Application Protection (RTAP) Agent

To begin the correct procedure to install the agent, go to one of the following sections:

"Overview of Java Agent Installation" on the next page

"Overview of .NET Agent Installation" on page 31

Installing the Java Agent

Topics covered in this section:

Getting Started with the Java Agent Installation

Topics covered in this section:

Overview of Java Agent Installation

The runtime agent protects all applications running under a supported Java Runtime Environment (JRE) on a supported application server or service.

Note: If you need to protect a particular subset of applications, you must run that subset under its own JVM.

To install the runtime agent and add it to an application server or service, follow these steps:

Step	Description	Instructions
1.	Ensure that your target application runs on supported versions of Java Runtime Environment (JRE) and the application server or service.	"About the System Requirements for Java Agents" on the next page
2.	Install the Java agent.	"Installing the Java Agent" on page 10
3.	Add the agent to an application server or service.	"Adding the Agent to an Application Server or Service Running Java" on page 12
4.	Restart the application server and view the new agent.	"Verifying the Java Agent Installation" on page 29

About the System Requirements for Java Agents

Before you begin to work with the runtime agent, check to make sure that your system meets all requirements.

General Requirements

- Users must have read and write permissions to the application server and the agents.
- HPE recommends that you run the most recent version of the runtime.

Supported JREs

The runtime agent for Java is supported on the following Java Runtime Environments (JREs) and application servers:

JREs	Major Version
IBM J9	5 (SR10 and above) 6 (SR6 and above)
Oracle HotSpot	5, 6, 7, 8
Oracle JRockit	5 and 6 (Rev 27.6 and above)

Supported Application Servers

Application Server	Version
Apache Tomcat	6.0, 7.0, 8.0,
IBM WebSphere	7.0, 8.0, 8.5, 8.5.5,
Oracle WebLogic	10.0, 10.3, 11g, 11gR1, 12c
Red Hat JBoss Enterprise Application Platform (JBoss EAP)	5.1.2, 5.2.0, 6.0.1, 6.1.0, 6.1.1, 6.2.0, 6.3.0, 6.4.0
Jetty	9.3

Note: The runtime agent for Java is supported on UNIX, Linux, and Windows.

Installing the Java Agent

Important:

- The agent must have the same permissions on the computer as the user who is responsible for starting the application server.
- HPE recommends that you install the agent in a secure directory having limited access on your computer or in a subdirectory of the application server. If you use a WebSphere server, make sure the directory path does not contain any spaces.

To install the agent:

1. Copy the agent installation file to the computer on which you are going to install the agent.

   Where `xx.x` represents the Runtime version number:
   - For UNIX or Linux, the file name is `HPE_Security_Fortify_RTAP_Runtime_Agent_Java_xx.x.tar.gz`
   - For Windows, the file name is `HPE_Security_Fortify_RTAP_Runtime_Agent_Java_xx.x_windows.zip`
2. Expand the agent installation file:
   - **UNIX or Linux**:

     Use the following command:

     ```
     tar -xzf HPE_Security_RTAP_Runtime_Agent_Java_xx.x.tar.gz

     tar -xzf HPE_Security_AppView_Runtime_Agent_Java_xx.x_Linux.tar.gz
     ```
   - **Windows:** Logged in as an administrator, expand the file using unzip software.
     By default, the extracted files are installed in a directory named:

     ```
     HPE_Security_RTAP_Runtime_Agent_Java_xx.x

     HPE_Security_AppView_Runtime_Agent_Java_xx.x_Linux
     ```

     Important: The full path to this installation directory is referred to as <*install_dir*> in these instructions.

     For example, if the `HPE_RTAP_Runtime_Agent_Java_xx.x` directory is located at `C:\`, you replace <*install_dir*> with `C:\HPE_Security_RTAP_Runtime_Agent_Java_xx.x` wherever these instructions refer to <*install_dir*>.

3. By default, when RTAP detects an attack against a web application, RTAP displays a *Protected by HPE Security Fortify* HTML page. This default RTAP behavior presents a possible security issue because the default HTML page divulges how you are protecting your applications.

   Your secure deployment of RTAP should therefore be revised to present a generic error page rather than a page that discloses any information about your enterprise's security mechanisms.

   For information about changing the default RTAP response to attacks, including the display of the default *Protected by HPE Security Fortify* page, see the *HPE Security Fortify Runtime Application Protection Operator Guide* for a discussion of `DisplayDefaultHtml`.

Adding the Agent to an Application Server or Service Running Java

The instructions for adding an agent vary depending on the application server or service to which you are adding the agent. The following topics provide instructions for adding the agent to each supported application server or service.

In general, adding the agent to an application server involves adding an appropriate `-javaagent` argument to the server startup.

Topics covered in this section:

Adding the Agent to a Standalone Apache Tomcat Server

To configure a standalone Apache Tomcat server to start with the agent, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

UNIX or Linux

To add the agent:

1. Open <*Tomcat_home*>/bin/catalina.sh.
2. Do one of the following:
   - To add the first agent, add the following line beneath the JAVA_OPTS section and above the `Execute The Requested Command` comment:

     ```
     CATALINA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar
        $CATALINA_OPTS"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     CATALINA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar,
        <existing_agent> $CATALINA_OPTS"
     ```

Windows

To add the agent:

1. Open <*Tomcat_home*>\bin\catalina.bat.
2. Do one of the following:
   - To add the first agent, add the following line beneath the JAVA_OPTS section and above the `Execute The Requested Command` comment:

     ```
     set CATALINA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar
        %CATALINA_OPTS%"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     set CATALINA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar,
        <existing_agent> %CATALINA_OPTS%"
     ```

Adding the Agent to an Apache Tomcat Windows Service

To configure an Apache Tomcat Windows service to start with the agent, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

To add the agent:

1. Start the Apache Tomcat configuration application. For example, for Apache Tomcat 7, this is `tomcat7w.exe`.
2. Do one of the following:
   - To add the first agent, add the following line to the `Java Options` section under the `Java` tab:

     ```
     "-javaagent:<install_dir>\lib\FortifyAgent.jar"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     "-javaagent:<install_dir>\lib\FortifyAgent.jar, <existing_agent>"
     ```

Adding the Agent to a Docker Container

To add Fortify Application Defender agent to a Docker container for your application deployment, perform the steps in this topic:

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

HPE Security Fortify Application Defender Agent Installed as Part of Docker Image Creation

Including the downloaded Fortify Application Defender agent with the docker image as part of the application build gives you more control over the agent and allows you to determine vulnerabilities in advance and configure risk group settings for a production environment.

To add the agent installed as part of Application Docker image creation, when the Fortify Application Defender agent is installed in the `CATALINA_HOME` folder and that the `CATALINA_HOME` environment variable is set (example `/usr/local/tomcat`)

1. Copy the downloaded agent (`AppDefender_Agent.tar.gz`) to the folder from where you are executing docker build.
2. Add following section to the Dockerfile:

```
ENV CATALINA_HOME=/usr/local/tomcat/
COPY AppDefender.tar.gz $CATALINA_HOME
RUN tar xzf $CATALINA_HOME/AppDefender.tar.gz -C $CATALINA_HOME
ENV CATALINA_OPTS="$CATALINA_OPTS -javaagent:$CATALINA_
HOME/AppDefender/lib.latest/FortifyAgent.jar"
```

Using Docker Volume Mapping

Docker Volume Mapping allows you to download the Fortify Application Defender agent and use the Volume Mapping feature provided by Docker to start the application with the Fortify Application Defender agent. This method allows you to maintain the state of an existing agent after destroying and recreating a docker container.

Note: Docker Volume Mapping is not included in the application build process. Document it as part of your deployment, and verify that the application is started with the Fortify Application Defender agent.

1. Extract contents of agent to a folder on the required host:

```
#tar –xzf AppDefender_Agent.tar.gz
```

2. Start your container with Application Defender agent using following command:

```
#docker run -d –p 8080:8080 -e "CATALINA_OPTS = $CATALINA_OPTS -
javaagent:/opt/AppDefender/lib.latest/FortifyAgent.jar" -v
/opt/AppDefender:/opt/AppDefender tomcat:7
```

See Also

"(Optional) Configure Fail Closed" on page 27

Adding the Agent to an IBM WebSphere Server Using the Server Administrative Console

To add the agent to an IBM WebSphere server using the IBM WebSphere administrative console, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

UNIX or Linux

To add the agent:

1. On the WebSphere Application Servers page, select the server for which you want to add the agent.
2. Do one of the following:
   - To add the first agent, add the following option to the `Generic JVM Arguments` section:

     ```
     -javaagent:<install_dir>/lib./FortifyAgent.jar
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent in the `Generic JVM Arguments` section. For example:

     ```
     -javaagent:<install_dir>/lib./FortifyAgent.jar, <existing_agent>
     ```

3. If you are using WebSphere 7 or higher, you must also add the following option to the `Generic JVM Arguments` section:

   ```
   -Xshareclasses:none
   ```

Windows

To add the agent:

1. On the WebSphere Application Servers page, select the server for which you want to add the agent.
2. Do one of the following:
   - To add the first agent, add the following option to the `Generic JVM Arguments` section:

     ```
     -javaagent:<install_dir>\lib\FortifyAgent.jar
     ```

- To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent in the `Generic JVM Arguments` section. For example:

```
-javaagent:<install_dir>\lib\FortifyAgent.jar, <existing_agent>
```

3. If you are using WebSphere 7 or higher, you must also add the following option to the `Generic JVM Arguments` section:

```
-Xshareclasses:none
```

Adding the Agent to an IBM WebSphere Server Using wsadmin

To add the agent to an IBM WebSphere server using the IBM WebSphere wsadmin command-line utility:

1. In the `<WebSphere_home>/profiles/AppSrvN/bin` directory, execute the following command:

   Note: On UNIX or Linux systems, you must use a forward slash (/) when specifying the path to the `wsadmin` command-line utility. On Windows, use a backslash (\).

   UNIX or Linux

   ```
   wsadmin -conntype none -f <install_dir>/tools/
      websphereJvmSetup.jacl -fortifyHome <install_dir>
   ```

   Windows

   ```
   wsadmin.bat
   ```

2. If the application server does not have default WebSphere settings, one or more of the following options might need to be added to the `wsadmin` command:

Parameter	Description
`-cell`	Specifies the WebSphere server's cell
`-server`	Specifies the WebSphere server's name Default: `server1`
`-node`	Specifies the WebSphere server's node name

Adding the Agent to a Red Hat JBoss Server

To configure a Red Hat JBoss server to start with the agent, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

This topic contains the following sections:

JBoss 5.2.0 or Lower

Configure JBoss 5.20 or lower to start with the agent.

UNIX or Linux

To add the agent:

1. Open <*JBoss_home*>/bin/run.sh.
2. Do one of the following:
   - To add the first agent, add the following line:

     ```
     JAVA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar $JAVA_OPTS"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     JAVA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar,
        <existing_agent> $JAVA_OPTS"
     ```

Windows

To add the agent:

1. Open <*JBoss_home*>\bin\run.bat.
2. Do one of the following:
   - To add the first agent, add the following line:

     ```
     set JAVA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar %JAVA_OPTS%"
     ```

- To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

```
set JAVA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar,
   <existing_agent> %JAVA_OPTS%"
```

JBoss 6.0.1 or Higher

Configure JBoss version 6.0.1 or higher to start with the agent.

UNIX or Linux

To add the agent:

1. Open `<JBoss_home>/bin/standalone.sh`.
2. Do one of the following:
   - To add the first agent, add the following lines:

```
JAVA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar $JAVA_OPTS"

PROCESS_CONTROLLER_JAVA_OPTS =
   "-javaagent:<install_dir>/lib./FortifyAgent.jar
   $PROCESS_CONTROLLER_JAVA_OPTS"
```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

```
JAVA_OPTS="-javaagent:<install_dir>/lib./FortifyAgent.jar,
   <existing_agent> $JAVA_OPTS"

PROCESS_CONTROLLER_JAVA_OPTS =
   "-javaagent:<install_dir>/lib./FortifyAgent.jar,
   <existing_agent> $PROCESS_CONTROLLER_JAVA_OPTS"
```

3. Add the lines described in step 2 to `<JBoss_home>/bin/domain.sh`.
4. Modify the `standalone.conf` file as follows:
   a. Append the following to the `-Djboss.modules.system.pkgs=org.jboss.byteman` JVM option:

```
,org.jboss.logmanager,com.fortify
```

b. Add the following JVM options, depending on the version of JBoss. Replace <*JBoss_home*> with the full path to the JBoss home, and replace <*jar_file_version*> with the version of the jar file for your JBoss release.

- **If the JBoss version is 6.0.1:**

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath/p:<JBoss_home>/modules/org/
   jboss/logmanager/main/
   jboss-logmanager-<jar_file_version>.jar
```

- **If the JBoss version is 6.1.0 or higher:**

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath/p:<JBoss_home>/modules/
   system/layers/base/org/jboss/logmanager/main/
   jboss-logmanager-<jar_file_version>.jar
```

For example, if you are running JBoss 6.2.0 and it is located in `/usr/bin/jboss/jboss-eap-6.2`, you add JVM options similar to the following:

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath/p:/usr/bin/jboss/jboss-eap-6.2/modules/
   system/layers/base/org/jboss/logmanager/main/
   jboss-logmanager-1.5.1.Final-redhat-1.jar
```

5. Perform the procedures of step 4 for `domain.conf`.

Windows

To add the agent:

1. Open <*JBoss_home*>`\bin\standalone.bat`.
2. Do one of the following:
   - To add the first agent, add the following lines:

```
set JAVA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar
   %JAVA_OPTS%"

set PROCESS_CONTROLLER_JAVA_OPTS =
   "-javaagent:<install_dir>\lib\FortifyAgent.jar
   %PROCESS_CONTROLLER_JAVA_OPTS%"
```

- To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

```
set JAVA_OPTS="-javaagent:<install_dir>\lib\FortifyAgent.jar,
   <existing_agent> %JAVA_OPTS%"

set PROCESS_CONTROLLER_JAVA_OPTS =
   "-javaagent:<install_dir>\lib\FortifyAgent.jar,
   <existing_agent> %PROCESS_CONTROLLER_JAVA_OPTS%"
```

3. Add the lines described in step 2 to *<JBoss_home>*`\bin\domain.bat`.
4. Modify the `standalone.conf.bat` file as follows:
   a. Append the following to the `-Djboss.modules.system.pkgs=org.jboss.byteman` JVM option:

```
,org.jboss.logmanager,com.fortify
```

   b. Add the following JVM options, depending on the version of JBoss. Replace *<JBoss_home>* with the full path to the JBoss home, and replace *<jar_file_version>* with the version of the jar file for your JBoss release.
      - **If the JBoss version is 6.0.1:**

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath\p:<JBoss_home>\modules\org\
   jboss\logmanager\main\
   jboss-logmanager-<jar_file_version>.jar
```

      - **If the JBoss version is 6.1.0 or higher:**

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath\p:<JBoss_home>\modules\
   system\layers\base\org\jboss\logmanager\main\
   jboss-logmanager-<jar_file_version>.jar
```

      For example, if you are running JBoss 6.2.0 and it is located in `C:\bin\jboss\jboss-eap-6.2`, you add JVM options similar to the following:

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager

-Xbootclasspath\p:C:\bin\jboss\jboss-eap-6.2\modules\
   system\layers\base\org\jboss\logmanager\main\
   jboss-logmanager-1.5.1.Final-redhat-1.jar
```

5. Perform the procedures of step 4 for `domain.conf.bat`.

Adding the Agent to an Oracle WebLogic Server

To configure an Oracle WebLogic server to start with the agent, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

UNIX or Linux

To add the agent:

1. Open <*WebLogic_home*>/bin/startWebLogic.sh.
2. Do one of the following:
   - To add the first agent, add the following line:

     ```
     JAVA_OPTIONS="-javaagent:<install_dir>/lib./FortifyAgent.jar $JAVA_
        OPTIONS"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     JAVA_OPTIONS="-javaagent:<install_dir>/lib./FortifyAgent.jar,
        <existing_agent> $JAVA_OPTIONS"
     ```

Windows

To add the agent:

1. Open <*WebLogic_home*>\bin\startWebLogic.cmd.
2. Do one of the following:
   - To add the first agent, add the following line:

     ```
     set JAVA_OPTIONS="-javaagent:<install_dir>\lib\FortifyAgent.jar
        %JAVA_OPTIONS%"
     ```

   - To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

     ```
     set JAVA_OPTIONS="-javaagent:<install_dir>\lib\FortifyAgent.jar,
        <existing_agent> %JAVA_OPTIONS%"
     ```

Adding the Agent to a System Service

To add runtime agent protection to a Java Virtual Machine (JVM) or application server running as a system service for UNIX, Linux, or Windows, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on page 26.

UNIX, Linux, and Windows

Incorporate the following parameter into the script that starts the JVM or application server for the system service:

Note: On Windows systems, replace the forward slashes (/) in the following paths with backslashes (\).

- To add the first agent, add the following line:

```
"-javaagent:<install_dir>/lib./FortifyAgent.jar"
```

- To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent in the `Java Options` section under the `Java` tab. For example:

```
"-javaagent:<install_dir>/lib./FortifyAgent.jar,
    <existing_agent>"
```

Adding the Agent to a Standalone Java Application

To configure a standalone Java application to start with the agent, perform the steps in this topic if you are doing one of the following:

- Adding the first agent (you are adding the agent to a system that does not already have an agent)
- Adding another agent (the system already has an agent)

If you are adding the agent to a host machine that is running more than one protected application, follow the instructions in "Adding the Agent to a Host Machine That Has More Than One Protected Application" on the next page.

UNIX, Linux, and Windows

Note: On Windows systems, replace the forward slashes (/) in the following paths with backslashes (\).

- To add the first agent, add the following parameter to the application's execution command:

  ```
  "-javaagent:<install_dir>/lib./FortifyAgent.jar"
  ```

  For example:

  ```
  java "-javaagent:<install_dir>/lib./FortifyAgent.jar
      <other_java_parameters> <application_name>"
  ```

- To add another agent, add the `-javaagent` startup option (shown in bold text below) to the beginning of the option for the existing agent. For example:

  ```
  java "-javaagent:<install_dir>/lib./FortifyAgent.jar, <existing_agent>
     <other_java_parameters> <application_name>"
  ```

Adding the Agent to a Host Machine That Has More Than One Protected Application

Note: If you are adding the agent to a system that has (or will have) only one protected application, follow the instructions for the application server or service to which you are adding the agent. See "Adding the Agent to an Application Server or Service Running Java" on page 12.

If you have more than one protected application running on the same host machine, perform the following steps to add the agent to the application server or service.

UNIX, Linux, and Windows

To add the agent:

Note: On Windows systems, replace the forward slashes (/) in the following paths with backslashes (\) .

1. For each protected application, you must create a unique agent configuration file. Do this by copying the `<install_dir>/config/rt_config.xml` file into the same directory with an application-appropriate name, such as `myapp1_config.xml`.
2. In the new file, change the `ProgramName` setting from `default` to the name of the application. For example, in `<install_dir>/config/myapp1_config.xml`, change the `ProgramName` setting from `default` to `myapp1`.
3. For each application server or service, add the new configuration file to the appropriate `-javaagent` startup option (shown in bold text below) as follows:
   - To add the first agent, add the following line:

     ```
     "-javaagent:<install_dir>/lib./FortifyAgent.jar"
     ```

     For example:

     ```
     "-javaagent:<install_dir>/lib./FortifyAgent.jar=
        <install_dir>/config/myapp1_config.xml"
     ```

   - To add another agent, add the `-javaagent` startup option to the beginning of the option for the existing agent:

     ```
     "-javaagent:<install_dir>/lib./FortifyAgent.jar,
         <existing_agent>"
     ```

     For example, if you are adding an agent to an application server or service that does not already have an installed agent, you add the following:

     ```
     "-javaagent:<install_dir>/lib./FortifyAgent.jar=
        <install_dir>/config/myapp1_config.xml, <existing_agent>"
     ```

(Optional) Configure Fail Closed

The Fail Closed flag stops your application from starting when the Fortify Application Defender agent is not able to load or instrument the application. By default, the flag is not set ensuring that your application starts up even though your application is unprotected and unmonitored. If you want to prevent your application from starting without protection and monitoring, then it is important to set the Fail Closed flag on the application host where you are installing the Fortify Application Defender Agent.

Note: Once an application starts up without the Fortify Application Defender Agent, then it will require a restart of that application to allow the Agent to instrument the application.

To set the Fail Closed flag add the following to your application's host network environment variable:

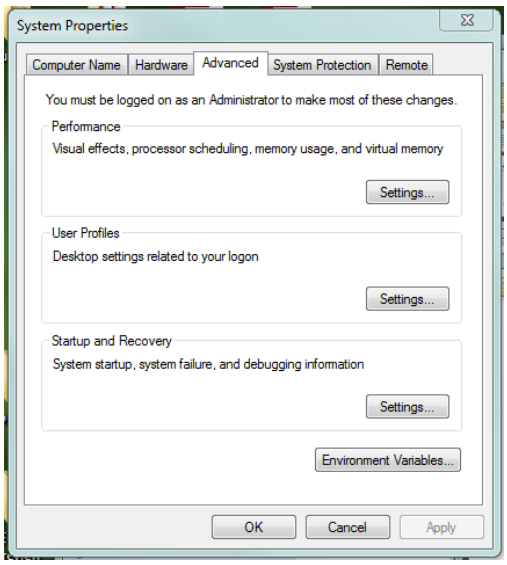
Windows:

You can set the environment variable either in the command shell which starts the application server using `set FORTIFY_DONT_CONTINUE_ON_STARTUP_ERROR=1` or by configuring it in the Environment Variables system dialog box.

Note: The way you access the Environment Variables system dialog box varies based on the version of Windows you are using.

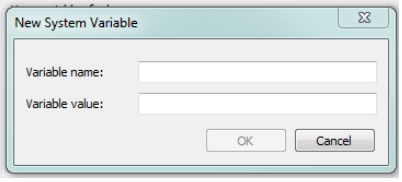
To set the Fail Closed Flag in a Windows 7 system dialog box:

1. Select the **Advanced tab** in the System Properties.



2. Click **Environment Variables**.

3. Click **New...** in the System variables section. The New System Variable window appears.



   a. Type **FORTIFY_DONT_CONTINUE_ON_STARTUP_ERROR** in the Variable Name field.
   b. Type **1** in the Variable value field.
4. Click **OK** to save the new variable and close the New System Variable window.
5. Click **OK** to save the setting and close the Environment Variables window.
6. Click **OK** to save the setting and close the System Properties window.
7. Restart the IIS.

Linux

```
export FORTIFY_DONT_CONTINUE_ON_STARTUP_ERROR=1
```

Changing the Default Startup Connection Timer

By default, a newly installed agent attempts to establish a connection to the server for five (5) minutes before giving up and allowing the application to start. If you want to change the length of time the agent waits,

Update the `rt_config.xml` in your `<agent install>/config` directory by creating or modifying the following entry:

```
<Setting name="MaxWaitForInitialConfiguration">timeout in
seconds</Setting>
```

Verifying the Java Agent Installation

Topics covered in this section:

Restarting the Application Server and Viewing the New Java Agent

To restart the application server and view the new agent:

1. Restart the application server.
2. Do one of the following:
   - If RTAP is operating in Federated Mode, that is, if it is connected to Software Security Center (Fortify SSC):
     i. Log on to Fortify SSC.
     ii. Select the **Runtime** tab, then select the **Applications** tab.
     iii. Select the name of the application in the left pane.
     iv. Click the **Hosts** link in the right pane.
     v. In the table of hosts, verify that the agent is present and in Active status.
   - If RTAP is operating in Stand-Alone Mode:
     i. Open the `<install_dir>/log/system.log` file (UNIX or Linux) or the `<install_dir>\log\system.log` file (Windows).
     ii. Verify that the file exists, contains no errors, and includes "Fortify Runtime setup complete."
3. If the new agent is not operating as described above, see "Troubleshooting Tips for the Java Agent" below.

Troubleshooting Tips for the Java Agent

A new agent does not appear

If, after restarting the application server, the new agent does not appear as described in "Restarting the Application Server and Viewing the New Java Agent" above, check the agent's log file for errors as follows:

1. In the log file

   `<install_dir>/log/system.log` for UNIX or Linux
   or
   `<install_dir>\log\system.log` for Windows

look for a message similar to the following:

```
[<PID> <TIMESTAMP> INFO] HPE Security Fortify Runtime setup complete
```

2. Ensure that the timestamp on the message corresponds to the time that the application server was started. Also ensure that there are no messages in the log with the prefix `ERROR` or `FATAL`.

The log file does not exist or application server startup messages are not present

If the log file does not exist or if messages that correspond to the application server startup time are not present, it indicates that the agent is not running. Take the following steps to identify the issue:

1. Make sure the startup arguments that you modified earlier are correct.
2. Check the `stderr` output from the application server or service for any fatal configuration errors.

Uninstalling a Java Agent

To uninstall a runtime agent for Java and remove the agent from your system:

1. To deactivate Runtime, undo any startup script changes that you made.
2. Delete <*install_dir*>.

Installing the .NET Agent

Topics covered in this section:

Getting Started with the .NET Agent Installation

Topics covered in this section:

Overview of .NET Agent Installation

The runtime agent protects all applications running under a supported .NET Framework on a supported version of IIS.

Note: If you need to protect a particular subset of applications, you must configure that subset as an application pool and protect that application pool.

Note: If you are upgrading a previous installation of a .NET agent, you must install the new agent without uninstalling the old agent, to preserve your protection settings.

To install the runtime agent and add it to IIS, follow these steps:

Step	Description	Instructions
1.	Ensure that your target application runs on supported versions of .NET Framework and IIS.	"About the System Requirements for .NET Agents" below
2.	Run the agent installer.	"Installing the .NET Agent" below
3.	Restart IIS and view the new agent.	"Verifying the .NET Agent Installation" on page 34

About the System Requirements for .NET Agents

Before you begin to work with the runtime agent, check to make sure that your system meets all requirements.

General Requirements

- Users must have read and write permissions to the application server and the agents.
- HPE recommends that you run the most recent version of the runtime.

System Requirements for .NET Agents

Supported .NET Frameworks

- The runtime agent supports .NET Framework versions 2.0, 3.0, 3.5, 4.0, 4.5, and 4.5.1.

Supported IIS Versions

The runtime agent for .NET is supported on Microsoft Internet Information Services (IIS) versions 6.0, 7.0, 7.5, 8, and 8.5.

Note: The runtime agent for .NET is supported on Windows only.

Installing the .NET Agent

Important:

- The agent must have the same permissions on the computer as the user who is responsible for starting IIS.
- HPE recommends that you install the agent in a secure directory having limited access on your computer.

To install the agent:

1. Copy the agent installation file to the computer on which you are going to install the agent, if the file was downloaded to a different computer.

   Where `xx.x` represents the Runtime version number:
   - For 64-bit Windows, the file name is `HPE_Security_RTAP_Runtime_Agent_Dotnet_xx.x.windows_x64.exe`
   - For 32-bit Windows, the file name is `HPE_Security_RTAP_Runtime_Agent_Dotnet_xx.x_windows_x86.exe`
2. Run the installer from the directory where the extracted files are stored.

   By default, the installer places the files in the following directory:

   `C:\Program Files\HPE_Security\RTAP_RuntimeAgt_Dotnet_xx.x`
   but you can use a different location. These instructions assume that you use the default location.

   Important: The full path to this installation directory is referred to as `<install_dir>` in these instructions.

   For example, if the `RTAP_Runtime_Agt_Dotnet_xx.x` directory is located at `C:\`, you replace `<install_dir>` with `C:\RTAP_Runtime_Agt_Dotnet_xx.x` wherever these instructions refer to `<install_dir>`.
3. By default, when RTAP detects an attack against a web application, RTAP displays a *Protected by HPE Security Fortify* HTML page. This default RTAP behavior presents a possible security issue because the default HTML page divulges how you are protecting your applications.

   Your secure deployment of RTAP should therefore be revised to present a generic error page rather than a page that discloses any information about your enterprise's security mechanisms.

   For information about changing the default RTAP response to attacks, including the display of the default *Protected by HPE Security Fortify* page, see the *HPE Fortify Runtime Application Protection Operator Guide* for a discussion of `DisplayDefaultHtml`.

Silent Install

You can streamline the .NET installation process with a silent installation. To install the .NET agent from the command line:

- Run the installation `.exe` file from the command line with the option `--mode unattended`.
  or
- Run the installation `.exe` file from the command line with the option `--help` to access a list of options.

Verifying the .NET Agent Installation

Topics covered in this section:

Restarting IIS and Viewing the New .NET Agent

To restart IIS and view the new agent:

1. As an administrative user, execute the following command to activate Runtime:

   ```
   C:\Program Files\HPE_Security\RTAP_RuntimeAgt_Dotnet_xx.x\
   tools\IISControl.exe register restart
   ```

   Note: If you need to protect a particular subset of applications on the server, configure that subset as an application pool and add `-a <application pool name>` to the command. For example:

   ```
   C:\Program Files\HPE_Security\RTAP_RuntimeAgt_Dotnet_xx.x\
   tools\IISControl.exe -a MyAppPool register restart
   ```

2. .NET requires that you open your application from a browser. When you do so, IIS starts both the application and Runtime.
3. Do one of the following:
   - If RTAP is operating in Federated Mode, that is, if it is connected to Fortify Software Security Center (Fortify SSC):
     i. Log on to Fortify SSC.
     ii. Select the **Runtime** tab, then select the **Applications** tab.
     iii. Select the name of the application in the left pane.
     iv. Click the **Hosts** link in the right pane.
     v. In the table of hosts, verify that the agent is present and in Active status.
   - If RTAP is operating in Stand-Alone Mode:
     i. Open the `<install_dir>\log\system.log` file.
     ii. Verify that the file exists, contains no errors, and includes "HPE Security Fortify Runtime setup complete."
4. If the new agent is not operating as described above, see "Troubleshooting Tips for the .NET Agent" on the next page.

Troubleshooting Tips for the .NET Agent

A new agent does not appear

If, after restarting IIS, the new agent does not appear as described in "Restarting IIS and Viewing the New .NET Agent" on the previous page, check the agent's log file for errors as follows:

1. In the log file

   `C:\Program Files\HPE_Security\RTAP_RuntimeAgt_Dotnet_xx.x\log\system.log`
   look for a message similar to the following:

   ```
   [<PID> <TIMESTAMP> INFO] HPE Security Fortify Runtime setup complete
   ```

2. Ensure that the timestamp on the message corresponds to the time that IIS was started. Also ensure that there are no messages in the log with the prefix `ERROR` or `FATAL`.

The log file does not exist or IIS startup messages are not present

If the log file does not exist or if messages that correspond to the IIS startup time are not present, it indicates that the agent is not running. In this case, see whether an error has been reported in the Windows system event log.

Uninstalling a .NET Agent

To deactivate a .NET runtime agent and remove the agent from your system:

1. As an administrative user, execute the following command:

   ```
   C:\Program Files\HPE_Security\RTAP_RuntimeAgt_Dotnet_xx.x\tools\IISControl.exe unregister restart
   ```

2. Select **Control Panel > Programs and Features.**
3. Right-click **HPE Security Runtime Application Protection Agent Dotnet xx.x** where **xx.x** represents the version number, and perform the uninstall.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Agent Installation Guide (HPE Security Fortify Runtime Application Protection (RTAP) 17.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to HPFortifyTechpubs@hpe.com.

We appreciate your feedback!