
Micro Focus

Fortify WebInspect Runtime Agent

Software Version: 18.4
For use with WebInspect 18.20

Installation Guide

Document Release Date: November 2018
Software Release Date: November 2018



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus 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. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Copyright Notice

© Copyright 2014 - 2018 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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.microfocus.com/support-and-services/documentation>

Contents

Preface	5
Contacting Micro Focus Fortify Customer Support	5
For More Information	5
About the Documentation Set	5
Change Log	6
Installing the WebInspect Agent	7
Installing the Java Agent	7
Getting Started with the Java Agent Installation	8
Overview of Java Agent Installation	8
About the System Requirements for Java Agents	9
General Requirements	9
Supported JREs	9
Supported Application Servers	9
Installing the Java Agent	10
Adding the Agent to an Application Server or Service Running Java	10
Adding the Agent to a Standalone Apache Tomcat Server	11
Adding the Agent to an Apache Tomcat Windows Service	12
Adding the Agent to an IBM WebSphere Server Using the Server Administrative Console	13
Adding the Agent to an IBM WebSphere Server Using wsadmin	14
Adding the Agent to a Red Hat JBoss Server	15
Adding the Agent to an Oracle WebLogic Server	19
Adding the Agent to a System Service	20
Adding the Agent to a Standalone Java Application	20
Adding the Agent to a Host Machine That Has More Than One Protected Application	21
Verifying the Java Agent Installation	22
Restarting IIS and Viewing the New .NET Agent	22
Troubleshooting Tips for the .NET Agent	23
Uninstalling a .NET Agent	23

- Installing the .NET Agent24
 - Getting Started with the .NET Agent Installation24
 - Overview of .NET Agent Installation24
 - About the System Requirements for .NET Agents25
 - General Requirements25
 - System Requirements for .NET Agents25
 - Supported .NET Frameworks25
 - Supported IIS Versions25
 - Installing the .NET Agent25
 - Silent Install26
 - Verifying the .NET Agent Installation27
 - Restarting IIS and Viewing the New .NET Agent27
 - Troubleshooting Tips for the .NET Agent27
 - Uninstalling a .NET Agent28
- Installing the Java Agent28
- Send Documentation Feedback30

Preface

Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

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

<https://softwaresupport.softwaregrp.com>

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/application-security>

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all 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 Micro Focus Product Documentation website:

<https://www.microfocus.com/support-and-services/documentation>

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
18.4	Updated: Minor version and branding updates.
18.1	Updated: Applied new template and rebranded to Micro Focus.
17.3	Added: Silent installation for the .NET agent. Added: Notes on changing the default value of the Startup Connection Timer. 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.

Installing the WebInspect 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 24](#)

Installing the Java Agent

Topics covered in this section:

Getting Started with the Java Agent Installation	8
Overview of Java Agent Installation	8
About the System Requirements for Java Agents	9
Installing the Java Agent	10
Adding the Agent to an Application Server or Service Running Java	10
Adding the Agent to a Standalone Apache Tomcat Server	11
Adding the Agent to an Apache Tomcat Windows Service	12
Adding the Agent to an IBM WebSphere Server Using the Server Administrative Console	13
Adding the Agent to an IBM WebSphere Server Using wsadmin	14
Adding the Agent to a Red Hat JBoss Server	15
Adding the Agent to an Oracle WebLogic Server	19
Adding the Agent to a System Service	20
Adding the Agent to a Standalone Java Application	20
Adding the Agent to a Host Machine That Has More Than One Protected Application	21
Verifying the Java Agent Installation	22
Restarting IIS and Viewing the New .NET Agent	22
Troubleshooting Tips for the .NET Agent	23
Uninstalling a .NET Agent	23

Getting Started with the Java Agent Installation

Topics covered in this section:

Overview of Java Agent Installation	8
About the System Requirements for Java Agents	9
Installing the Java Agent	10

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 28
3.	Add the agent to an application server or service.	"Adding the Agent to an Application Server or Service Running Java" on page 10
4.	Restart the application server and view the new agent.	"Verifying the Java Agent Installation" on page 22

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.
- Fortify 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.
- Fortify 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
`Fortify_WebInspect_Runtime_Agent_Java_xx.x_Linux.tar.gz`
- For Windows, the file name is
`Fortify_WebInspect_Runtime_Agent_Java_xx.x_windows.zip`

2. Expand the agent installation file:

- **UNIX or Linux:**

Use the following command:

```
tar -xzf Fortify_WebInspect_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:

```
Fortify_WebInspect_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 `Fortify_WebInspect_Runtime_Agent_Java_xx.x` directory is located at `C:\`, you replace `<install_dir>` with `C:\Fortify_WebInspect_Runtime_Agent_Java_xx.x` wherever these instructions refer to `<install_dir>`.

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	11
Adding the Agent to an Apache Tomcat Windows Service	12
Adding the Agent to an IBM WebSphere Server Using the Server Administrative Console	13
Adding the Agent to an IBM WebSphere Server Using wsadmin	14
Adding the Agent to a Red Hat JBoss Server	15
Adding the Agent to an Oracle WebLogic Server	19
Adding the Agent to a System Service	20
Adding the Agent to a Standalone Java Application	20
Adding the Agent to a Host Machine That Has More Than One Protected Application	21

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 21.

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 21](#).

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 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 21](#).

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 21](#).

This topic contains the following sections:

- ["JBoss 5.2.0 or Lower" below](#)
- ["JBoss 6.0.1 or Higher" on the next page](#)

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 21.](#)

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 the next page.](#)

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 10](#).

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>"
```

Verifying the Java Agent Installation

Topics covered in this section:

Restarting IIS and Viewing the New .NET Agent	22
Troubleshooting Tips for the .NET Agent	23
Uninstalling a .NET Agent	23

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:

```
<install_dir>\WebInspect_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:

```
<install_dir>\WebInspect_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. After the server has started, make sure the new agent appears:
 - a. Start WebInspect.
 - b. Start a scan.
 - c. In the Scan Dashboard page, verify that in the **Scan** section in the right pane, the **Agent** field is displayed as **Detected**.
 - d. If the new agent is not operating as described above, see ["Troubleshooting Tips for the .NET Agent" on page 27](#).

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 page 27](#), check the agent's log file for errors as follows:

1. In the log file

```
<install_dir>\WebInspect_RuntimeAgt_Dotnet_xx.x\  
log\system.log
```

look for a message similar to the following:

```
[<PID> <TIMESTAMP> INFO] Micro Focus 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:

```
<install_dir>\WebInspect_RuntimeAgt_Dotnet_xx.x\  
tools\IISControl.exe unregister restart
```

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

Installing the .NET Agent

Topics covered in this section:

Getting Started with the .NET Agent Installation	24
Overview of .NET Agent Installation	24
About the System Requirements for .NET Agents	25
System Requirements for .NET Agents	25
Installing the .NET Agent	25
Silent Install	26
Verifying the .NET Agent Installation	27
Restarting IIS and Viewing the New .NET Agent	27
Troubleshooting Tips for the .NET Agent	27
Uninstalling a .NET Agent	28

Getting Started with the .NET Agent Installation

Topics covered in this section:

Overview of .NET Agent Installation	24
About the System Requirements for .NET Agents	25
System Requirements for .NET Agents	25
Installing the .NET Agent	25
Silent Install	26

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 27

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.
- Fortify 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.
- Fortify 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
Fortify_WebInspect_Runtime_Agent_Dotnet_xx.x.windows_x64.exe
- For 32-bit Windows, the file name is
Fortify_WebInspect_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:

`<install_dir>\WebInspect_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 `WebInspect_RuntimeAgt_Dotnet_xx.x` directory is located at `C:\`, you replace `<install_dir>` with `C:\WebInspect_RuntimeAgt_Dotnet_xx.x` wherever these instructions refer to `<install_dir>`.

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	27
Troubleshooting Tips for the .NET Agent	27
Uninstalling a .NET Agent	28

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:

```
<install_dir>\WebInspect_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:

```
<install_dir>\WebInspect_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. After the server has started, make sure the new agent appears:
 - a. Start WebInspect.
 - b. Start a scan.
 - c. In the Scan Dashboard page, verify that in the **Scan** section in the right pane, the **Agent** field is displayed as **Detected**.
 - d. If the new agent is not operating as described above, see "[Troubleshooting Tips for the .NET Agent](#)" below.

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](#)" above, check the agent's log file for errors as follows:

1. In the log file

```
<install_dir>\WebInspect_RuntimeAgt_Dotnet_xx.x\  
log\system.log
```

look for a message similar to the following:

```
[<PID> <TIMESTAMP> INFO] Micro Focus 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:

```
<install_dir>\WebInspect_RuntimeAgt_Dotnet_xx.x\  
tools\IISControl.exe unregister restart
```
2. Select **Control Panel > Programs and Features**.
3. Right-click **Fortify WebInspect Runtime Agent Dotnet xx.x** where **xx.x** represents the version number, and perform the uninstall.

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.
- Fortify 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
Fortify_WebInspect_Runtime_Agent_Java_xx.x_Linux.tar.gz
- For Windows, the file name is
Fortify_WebInspect_Runtime_Agent_Java_xx.x_windows.zip

2. Expand the agent installation file:

- **UNIX or Linux:**

Use the following command:

```
tar -xzf Fortify_WebInspect_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:

```
Fortify_WebInspect_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 Fortify_WebInspect_Runtime_Agent_Java_xx.x directory is located at C:\, you replace *<install_dir>* with C:\Fortify_WebInspect_Runtime_Agent_Java_xx.x wherever these instructions refer to *<install_dir>*.

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 Installation Guide (Fortify WebInspect Runtime Agent 18.4)

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 FortifyTechpubs@microfocus.com.

We appreciate your feedback!