opentext™

OpenText™ Fortify WebInspect Agent

Software Version: 24.2.0
For use with Fortify WebInspect 24.2.0

Installation and Rulepack Guide

Document Release Date: May 2024
Software Release Date: May 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2014 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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

This document was produced on May 20, 2024. 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/documentation

Contents

Preface

Contacting Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/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 Product Documentation website:

https://www.microfocus.com/support/documentation

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText Fortify Community:

https://community.microfocus.com/cyberres/fortify/w/announcements

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

https://www.youtube.com/c/FortifyUnplugged

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
24.2.0	Updated: Release information
23.2.0	Combined the Fortify WebInspect Agent Installation Guide and the Fortify WebInspect Agent Rulepack Kit Guide into Fortify WebInspect Agent Installation and Rulepack Guide
23.1.0	Updated: Legal page and Release information
22.2.0	Updated: Release information

Installing the WebInspect Agent

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

"Overview of Java Agent Installation" below

"Overview of .NET Agent Installation" on page 22

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.	See the **Fortify WebInspect Agent Requirements** section in the *OpenText Fortify System Requirements* document for this release.
2.	Install the Java agent.	"Installing the Java Agent" on the next page
3.	Add the agent to an application server or	"Adding the Agent to an Application

Step	Description	Instructions
	service.	Server or Service Running Java" on page 9
4.	Restart the application server and view the new agent.	"Verifying the Java Agent Installation" on page 20

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

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 19.

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 19.

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 19.

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 using WebSphere 7 or higher, 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, 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 19.

This topic contains the following sections:

JBoss 5.2.0 or Earlier

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 Later

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 19.

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 9.

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:

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" on the next page, 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] OpenText 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.

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. 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 Java Agent" on the previous page.

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.	See the **Fortify WebInspect Agent Requirements** section in the *OpenText Fortify System Requirements* document for this release.
2.	Run the agent installer.	"Installing the .NET Agent" on the next page
3.	Restart IIS and view the new agent.	"Verifying the .NET Agent Installation" on page 24

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

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" on the next page, 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] OpenText 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.

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 the previous page.

Using the WebInspect Agent Rulepack Kit

This chapter describes the detection capabilities of the Fortify WebInspect Agent Rulepack Kit. The WebInspect Agent Rulepack Kit runs atop Fortify's Runtime Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify WebInspect Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

There are four major types of rules in the Fortify WebInspect Agent Rulepack Kit, the details of these rules will be discussed in the following sections.

1. Vulnerability Rules
2. Attack Surface Rules
3. Trace Rules
4. Platform Rules

Output from vulnerability rules will be logged to Runtime Agent event log (if configured) in standard Fortify WebInspect Agent event log format. However, attack surface and trace rules will only be sent to Fortify WebInspect and will not be logged in event log. Platform rules do not generate any events.

Vulnerability Rules

Vulnerability rules improve Fortify WebInspect Agent scanning by:

1. Reporting security vulnerabilities that Fortify WebInspect does not typically find. For example, Fortify WebInspect might not be able to find certain types of Blind SQL Injection while WebInspect Agent intercepts all SQL database operations, will be able to detect it.
2. Reporting code level details to Fortify WebInspect. For example, in the case of a Cross-site Scripting attack, WebInspect Agent can report the user source file name, line number and any other related stack traces which are very useful to developers when fixing the vulnerability reported.

WebInspect Agent sends the attack string being used in each request to WebInspect Agent in a custom HTTP header. Most vulnerability rules detect vulnerabilities by comparing the security sensitive parameter or argument with the Fortify WebInspect provided attack vector. For example, for SQL Injection rules, the monitor will check if the SQL query string contains the attack vector, which may be "`' or 1=1 --`".

Both Java and .NET Fortify WebInspect Agent Rulepack Kits can detect the following vulnerabilities:

- Arbitrary File Upload
- Command Injection
- Credit Card Number Disclosed
- Cross-Site Scripting
- Dangerous File Inclusion: Local

- Dangerous File Inclusion: Remote
- Denial of Service: Parse Double
- Insecure Randomness
- Leftover Debug Code
- Mass Assignment: Insecure Binder Configuration
- Open Redirect
- Privacy Violation: Credit Card Number
- Privacy Violation: Social Security Number
- SQL Injection
- Social Security Number Disclosed
- Value Shadowing
- XML External Entity Injection
- XML Entity Expansion Injection

Additionally, the Java Fortify WebInspect Agent Rulepack Kit can detect the following vulnerabilities:

- ClassLoader Manipulation: Struts
- Header Manipulation: IMAP
- Header Manipulation: SMTP
- Mail Command Injection: IMAP
- Mail Command Injection: POP3
- Mail Command Injection: SMTP
- Transport Layer Protection: Insecure Mail Transmission

Attack Surface Rules

Attack Surface Rules is used to report the list of the available web pages and URLs to [[[Undefined variable WI_Agent_Vars.WI_LongName]]]. Fortify WebInspect can then use this information to find hidden pages or pages that the crawler failed to find.

Supported attack surfaces are:

Java	**.NET**
Tomcat/WebSphere JAX-RS	IIS WCF

Trace Rules

Trace rules report various events to Fortify WebInspect Agent to help Fortify WebInspect have a better insight into the application being tested. For example, a File_IO trace may notify Fortify WebInspect Agent that the application is reading a particular file. Fortify WebInspect may then use the information to determine if the file operation is expected and/or if a “Path Manipulation” test should be conducted afterwards.

Both Java and .NET Fortify WebInspect Agent Rulepack Kits can detect the following traces:

Trace Type	Operations
Database	execute, close
Attack Suggestion	N/A
Session	start, stop
File IO	open, read, write, close
Authentication	logon, logoff
Authorization	successful, failure
Unused Parameter	N/A
Network	stream
HTTP/URL Connection	init
OAuth	client_version, server_version, token, store_token, store_access_token, request
Validation Failure	struts, spring, webcontrols
autobind	trace_spring_modelattribute, trace_spring_modelmap, trace
email	smtp_send, email_secure, smtp_command, imap_command, pop3_command

Platform Rules

Platform rules do not detect any vulnerabilities or events but modify the application or platform to be more suitable for vulnerability scanning.

The list of all supported platform rules is as follows:

Rule	Java	.NET
Enable DEBUG in web.config*	N/A	YES
Disable CAPTCHA	ReCaptcha SimpleCaptcha jCaptcha Are You A Human? NuCaptcha	ReCaptcha BotDetect NuCaptcha
Unlimited password retries	N/A	Standard MembershipProvider
Prevent accidentally changing password	N/A	Standard MembershipProvider

* DEBUG is required in order to retrieve line numbers in a stack trace.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on Installation and Rulepack Guide (Fortify WebInspect Agent 24.2.0)

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 fortifydocteam@opentext.com.

We appreciate your feedback!