opentext™

Fortify WebInspect Enterprise

Software Version: 23.2.0
Windows® operating systems

Installation and Implementation Guide

Document Release Date: December 2023
Software Release Date: December 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2009-2023 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 November 07, 2023. 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 ... 8
Contacting Fortify Customer Support ... 8
For More Information ... 8
About the Documentation Set ... 8
Fortify Product Feature Videos ... 8
Change Log ... 9

Chapter 1: Before You Begin ... 10
FIPS or Non-FIPS Compliance ... 10
Installation and Upgrade Options ... 10
Important Considerations About Decoupling ... 11
System Requirements ... 12
Installation Recommendation ... 12
Installing or Upgrading Fortify Software Security Center (Optional) ... 12
About Fortify WebInspect Enterprise SSL Certificate and Fortify Software Security Center JRE ... 13
Importing Fortify WebInspect Enterprise SSL Certificate ... 13
Upgrading from Earlier Versions ... 14
Upgrading from Fortify WebInspect Enterprise 22.2.0 ... 15
Fortify Software Security Center Upgrade Requirements (Optional) ... 15
Preparing to Install Fortify WebInspect Enterprise ... 15
Installing IIS, ASP.NET, and .NET Framework ... 16
IIS Integrated Mode ... 16
IIS Application Pool Identity ... 17
Installing SQL Server ... 17
Creating a Sensor User ... 17
Ensuring Secure HTTPS Operation ... 17
Using SAN or Wildcard Certificates and Non-Standard Ports in IIS ... 18
HTTP Binding Host Name ... 18
Using HTTPS with Guided Scan and Reports ... 19
Databases in Availability Groups ... 19
Mirrored Databases ... 19
Related Documents ... 19

All Products 20
Fortify Software Security Center 20
Fortify WebInspect 21
Fortify WebInspect Enterprise 23

Chapter 2: Installing Fortify WebInspect Enterprise 24
About the Installation 24
Installing the Fortify WebInspect Enterprise Server Software 25
About the Initialization Wizard 26
Activating the License 27
Configuring the Database 30
Configuring the Web Service 32
Setting Up Fortify WebInspect Enterprise Database Users 33
What's Next? 34
Setting Up a Fortify Software Security Center (SSC) Connection 34
Initializing Fortify WebInspect Enterprise 36
Adding Sensor Users 38
Completing Initialization 39
What's Next? 39
Installing or Upgrading a Standalone Fortify WebInspect Enterprise 40
Initializing Fortify WebInspect Enterprise 40
Adding Sensor Users 43
Completing Initialization 44
What's Next? 44
Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center 45
Initializing Fortify WebInspect Enterprise 47
Adding Sensor Users 50
Completing Initialization 51
Important Information about Upgrading WebInspect 51
What's Next? 52
Configuring Services 52
Configuring the Scan Uploader Service 52
Service Status 52
Fortify WebInspect Enterprise Configuration 53
Dropbox Configuration 53
Logging Configuration 53
Start the Service 54

Configuring the Task Service 54
Service Status 54
Database Configuration 55
Logging Configuration 55
Fortify Software Security Center Poll Interval 56
Start the Service 56
Configuring the Scheduler Service 56
Service Status 56
Fortify WebInspect Enterprise Manager 57
Logging Configuration 57
Start the Service 57
Post Configuration 58
Installing the Fortify WebInspect Enterprise Administrative Console 58
Logging on to the Administrative Console 58
Using the Administrative Console 59
Post-Installation Configuration 60
Installing Fortify WebInspect as a Sensor 60
Configuring the Sensor, Testing Credentials, and Starting the Sensor Service 65
Verifying Sensor Setup 67
Adding Sensor Users (if Not Previously Done) 68
Enabling Sensors and Configuring Sensor Permissions 68
About Assigning Administrators and Roles 69
System Level 69
Organization Level 70
Group Level 70
Moving Application Versions from the Default Group 71
Configuring Manual Publishing of Scans to Fortify Software Security Center, if Necessary 71
About the WebInspect Enterprise Desktop Application 72
Timestamps and Effect of Time Zones on Schedules 72
About the REST API 73
REST API Categories 73
Accessing the REST API 74
Using the Swagger UI 75
Getting Field-level Details 76
Installations Lacking Internet Connection 77
Downloading and Installing a CRL 78

Chapter 3: Troubleshooting the Installation 79
About Fortify WebInspect Enterprise Manager Logging 79
Changing Fortify WebInspect Enterprise Initializer Log Debug Settings 80
Changing Fortify WebInspect Enterprise Manager Log Debug Settings 80
Changing Fortify WebInspect Enterprise Scheduler Service Log Debug Settings 81
Changing Fortify WebInspect Enterprise Task Service Log Debug Settings 81
Troubleshooting and IIS 83
IIS Settings and File Permissions Used by Fortify WebInspect Enterprise 83
IIS Admin Service Must be Running 83
Restarting IIS Quick Commands 84
SQL Login 84
Account Rights and Privileges 84

Chapter 4: Implementing Fortify WebInspect Enterprise 86
Fortify WebInspect Enterprise Components 87
Component Descriptions 87
Fortify WebInspect Enterprise Manager Account Requirements 88
System Account Requirements 89
Sensor Requirement 89
Fortify WebInspect Enterprise System Administrator 89
SQL Database Account Requirements 90
Fortify WebInspect Enterprise Manager License Components 90
Customizing Data Path and Scan Publication Settings 90
Changing the Storage Folders Location 91
Disabling Automatic Publishing of Scans to Fortify Software Security Center 91
Enabling Fortify Software Security Center to Automatically Mark Vulnerabilities as Fixed 92
Changing Logging Locations 92
Encrypting the Communication Between Fortify WebInspect Enterprise and SQL Server 93
Enabling Fortify WebInspect Enterprise to Use SSL 93
Editing the Encrypted SQL Connection String Section of web.config 94
Encrypt Connection String in the TaskService.exe.config File 94
Fortify WebInspect Sensor Remote SQL Server Standard Edition Connectivity 95
Using Windows Authentication 95
Fortify WebInspect Sensor Logging 95
Fortify WebInspect Sensor Scan Logs 96

Fortify WebInspect Sensor Directory Path Customization 96
Modifying the SharedSettings.config File 96
Retaining Copies of Scan Data on the Fortify WebInspect Sensor 97
About Database Size and Growth Settings 97
General Database Settings for Fortify WebInspect Enterprise 98
Database Maintenance for Fortify WebInspect Enterprise 98
Check Database Integrity Task 99
Database Fragmentation Maintenance 100
Reorganize Index Task 100
Rebuild Index Task 101
Update Statistics Task 102

Send Documentation Feedback 103

Preface

Contacting Fortify 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 OpenText 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 Community:

https://community.microfocus.com/cyberres/fortify/w/fortify-product-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 between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
23.2.0	Updated: • Minor edits to incorporate branding changes.
22.2.0 / May 2023	Updated: • Information related to downloading a certificate revocation list (CRL). See "Installations Lacking Internet Connection" on page 77.
22.2.0	Updated: • Release version and date.
21.2.0	Updated: • Initialization content with an example of a complete Fortify Software Security Center URL. See "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34.
21.1.0	Updated: • Release version and date.

Chapter 1: Before You Begin

OpenText™ Fortify WebInspect Enterprise is available in FIPS and non-FIPS compliant versions for 64-bit operating systems. This topic provides information to help you select the appropriate installer package and to ensure that your system meets the requirements and recommendations for installing Fortify WebInspect Enterprise.

FIPS or Non-FIPS Compliance

Federal Information Processing Standards (FIPS) are standards developed by the U.S. federal government for use in computer systems to ensure that all agencies adhere to the same guidelines regarding security and communication.

Fortify WebInspect Enterprise version 23.2.0 has two installer packages with different filenames—one installation complies with FIPS cryptography requirements and the other does not. Make sure that you download and use the correct installer package, based on whether your environment uses FIPS. The user interface for the installation procedure is the same for both packages.

Fortify WebInspect Enterprise and the OpenText™ Fortify WebInspect sensors it uses must all be compliant with FIPS or they must all be non-compliant.

OpenText™ Fortify Software Security Center runs on an Apache Tomcat server, which includes a FIPS mode. When integrating Fortify WebInspect Enterprise with Fortify Software Security Center in a FIPS-compliant environment, see your Apache Tomcat documentation for instructions on configuring FIPS mode on the server.

Installation and Upgrade Options

The following table describes the installation and upgrade options for Fortify WebInspect Enterprise.

Option	Description
Integration with Fortify Software Security Center	Integration with Fortify Software Security Center provides a way to publish scans to a central repository of all static and dynamic scans. It also provides somewhat centralized accounts, although permissions are still managed separately, the ability to submit scan requests, and more extensive reporting than a standalone installation.
Standalone	For new installations, you may choose not to integrate your Fortify WebInspect Enterprise with Fortify Software Security

Option	Description
	Center. **Important!** If you install Fortify WebInspect Enterprise as standalone, you cannot integrate with Fortify Software Security Center at a later date. You must choose to integrate with Fortify Software Security Center initially.
Decouple from Fortify Software Security Center	For existing installations, you may choose to decouple your Fortify WebInspect Enterprise from Fortify Software Security Center. If you choose to decouple, the Initialization Wizard provides an option to map each existing Fortify Software Security Center account—either user account or LDAP account—to a Windows account. Only Fortify Software Security Center accounts that were configured with permissions in Fortify WebInspect Enterprise will be displayed for mapping. **Important!** Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center is permanent. Reconnecting to Fortify Software Security Center is not supported.

Important Considerations About Decoupling

Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center ends all links and communication between the two systems. Before decoupling Fortify WebInspect Enterprise from Fortify Software Security Center, you should perform maintenance in both systems to ensure that you are ready to decouple.

Consider the following:

- You will not be able to log into Fortify WebInspect Enterprise and Fortify Software Security Center using the same credentials.
  - Decoupled and standalone Fortify WebInspect Enterprise installations use Windows Authentication.

    Important! Before decoupling Fortify WebInspect Enterprise from Fortify Software Security Center, enable Windows Authentication as described in "Installing IIS, ASP.NET, and .NET Framework" on page 16.
  - When decoupling, you will have the opportunity to map Fortify Software Security Center users to Fortify Windows Users for logging into Fortify WebInspect Enterprise.

- You will not be able to publish scans to Fortify Software Security Center from Fortify WebInspect Enterprise.
- Any previous scans published to Fortify Software Security Center will remain in Fortify Software Security Center.
- You will not be able to perform or see previous Scan Requests.
- Deleted Application Versions that have not been purged will remain in Fortify WebInspect Enterprise.
- Any new Applications and Application Versions that are created in Fortify Software Security Center will not be created in Fortify WebInspect Enterprise.
- Any new Applications and Application Versions that are created in Fortify WebInspect Enterprise will not be created in Fortify Software Security Center.

System Requirements

Before installing Fortify WebInspect Enterprise, make sure that your systems meet the requirements described in the *Fortify Software System Requirements*.

Installation Recommendation

We recommend that you do not install Fortify WebInspect Enterprise on the same machine as Fortify WebInspect. Doing so may result in known issues that affect the usability of the products.

Installing or Upgrading Fortify Software Security Center (Optional)

If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, then Fortify Software Security Center version 23.2.0 must be installed and running before you install Fortify WebInspect Enterprise version 23.2.0. See the *OpenText™ Fortify Software Security Center User Guide* for information about installing or upgrading Fortify Software Security Center to the required version.

Important! Before making each upgrade of Fortify WebInspect Enterprise, you must first upgrade Fortify Software Security Center to the supported version. For more information, see "Upgrading from Earlier Versions" on page 14.

In Fortify Software Security Center:

- Note the Fortify Software Security Center URL. You will need to specify it during the installation of Fortify WebInspect Enterprise.
- Create a general Fortify Software Security Center administrator account or make note of an existing one. You will need to specify the user name and password of this account during the

installation of Fortify WebInspect Enterprise and this person will automatically become the first Fortify WebInspect Enterprise system administrator.

- Create an account in Fortify Software Security Center for the Fortify WebInspect Enterprise Service, give it a recognizable user name such as wie_service, and give it the role of Fortify WebInspect Enterprise System. This service controls the sharing of application versions with Fortify WebInspect Enterprise and obtains lists of completed and running scans from Fortify WebInspect Enterprise. You will need to specify the user name and password of this account during the installation of Fortify WebInspect Enterprise.

  Important! Do not combine the Fortify WebInspect Enterprise Service account with any other role. Also, do not modify the permission of the Fortify WebInspect Enterprise Service account in the Fortify WebInspect Enterprise Administration Console. Doing so may prevent new application versions from being created in Fortify Software Security Center or cause them to be created in the wrong Security Group.

For information about creating accounts in Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*. The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, technical notes and release notes describe new features, known issues, and last-minute updates. To obtain the latest versions of these documents, see the "Preface" on page 8.

About Fortify WebInspect Enterprise SSL Certificate and Fortify Software Security Center JRE

When Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the Fortify WebInspect Enterprise SSL certificate must be in the Fortify Software Security Center trust store. Therefore, you must import the Fortify WebInspect Enterprise SSL certificate into the Java runtime environment (JRE) certificate store in Fortify Software Security Center.

Importing Fortify WebInspect Enterprise SSL Certificate

Use the following process to import the Fortify WebInspect Enterprise SSL certificate into the JRE certificate store in Fortify Software Security Center.

Stage	Description
1	Install or upgrade Fortify Software Security Center.
2	Install or upgrade Fortify WebInspect Enterprise. For more information, see "Installing the Fortify WebInspect Enterprise Server Software" on page 25.
3	Run the Fortify WebInspect Enterprise Initialization Wizard to integrate Fortify WebInspect Enterprise with Fortify Software Security Center. For more information, see "About the Initialization Wizard" on page 26 and "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34.

Stage	Description
4	Log into the Fortify WebInspect Enterprise Web Console using a supported version of Internet Explorer or Firefox. For more information, see *Fortify Software System Requirements*. Do one of the following to export the Fortify WebInspect Enterprise SSL certificate: • If using Internet Explorer, export the CER encoded binary X.509 (*.CER) file. • If using Firefox, export the DER encoded binary X.509 (*.DER) file.
5	Copy the Fortify WebInspect Enterprise SSL certificate to the SSL Server install machine. **Example** C:\Program Files\Java\jre1.8.0_xxx\lib\security\WIESSL.cer (or *.der)
6	Use the keytool utility to import the Fortify WebInspect Enterprise SSL certificate into the Java Store: 1. Type the following at the command prompt to access the keytool utility: `C:\Program Files\Java\jre1.8.0_<xxx>\bin>keytool -import -alias wie -keystore "C:\ Program Files\Java\jre1.8.0_xxx\lib\security\cacerts" -file "C:\Program Files\Java\jre1.8.0_xxx\lib\security\WIESSL.cer" (or *.der)` 2. Enter the keystore password. **Note:** The default password is *changeit*. 3. When prompted to trust this certificate, select **yes**. The certificate is added to the keystore.
7	Restart the Tomcat server hosting Fortify Software Security Center.

Upgrading from Earlier Versions

This topic describes the options for upgrading from earlier versions of Fortify WebInspect Enterprise.

Upgrading from Fortify WebInspect Enterprise 22.2.0

You can upgrade to Fortify WebInspect Enterprise 23.2.0 directly from Fortify WebInspect Enterprise 22.2.0, but not from any other versions of Fortify WebInspect Enterprise. Also, see "Installing or Upgrading Fortify Software Security Center (Optional)" on page 12.

Important! If you previously downloaded the WebInspect Enterprise Desktop Application from Fortify WebInspect Enterprise 22.2.0, you must download and install the application again after upgrading to get the 23.2.0 version.

Fortify Software Security Center Upgrade Requirements (Optional)

If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, then before making each upgrade of Fortify WebInspect Enterprise, you must first upgrade Fortify Software Security Center to the supported version as shown in the following table.

Before upgrading to Fortify WebInspect Enterprise version	First upgrade to Fortify Software Security Center version
21.1.0	21.1.0
21.2.0	21.2.0
22.2.0	22.2.0
23.2.0	23.2.0

Note: The supported versions of .NET Framework must be installed on the Fortify WebInspect sensor before Fortify WebInspect is upgraded to version 23.2.0. For more information, see the *Fortify Software System Requirements*.

Preparing to Install Fortify WebInspect Enterprise

This section describes how to prepare for installing Fortify WebInspect Enterprise by installing and configuring the prerequisite software, creating an account for a sensor user, and ensuring secure HTTPS operation.

If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, see "Installing or Upgrading Fortify Software Security Center (Optional)" on page 12.

Installing IIS, ASP.NET, and .NET Framework

You must install and configure Internet Information Services (IIS), ASP.NET, and the Microsoft .NET Framework, if applicable. The following paragraphs provide guidance for installing and configuring these components.

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

Note: When you select role services to add, some or all of their subordinate role services might be automatically selected as well. Leave any automatic selections as is. If a message appears indicating that other particular role services must also be installed, click the button to add them and they will be automatically selected for installation.

To install IIS and add the Web Server (IIS) server role and required role services:

1. In the Server Manager, click **Manage** and then **Add Roles and Features**.

   The Add Roles and Features Wizard appears.
2. Follow the wizard to select the installation type and destination server.
3. On the Server Roles window, do the following:
   - Select the **Web Server (IIS)** check box, if it is not already selected.
   - If you are installing a standalone or decoupled Fortify WebInspect Enterprise, then expand the **Web Server > Security** role service and select the **Windows Authentication** check box.

     Important! If you do not select Windows Authentication, you will not be able to connect to the Fortify WebInspect Enterprise Manager and complete the initialization.
4. Click **Next**.
5. On the Features window under .NET Framework *<version>* Features, select **.NET Framework *<version>*** and **ASP.NET *<version>***.

   Note: The version of .NET Framework and ASP.NET available in IIS depends on the OS version you are using. For example, you may see .NET Framework 4.6 or .NET Framework 4.7.
6. Click **Next**.
7. On the Role Services window under Application Development, select **ASP.NET *<version>***.
8. Click **Install** to install IIS with the features, roles, and role services you selected.

IIS Integrated Mode

During installation or upgrade, the Fortify WebInspect Enterprise Manager Web Service (WIE server) will be set up in IIS using the IIS integrated mode for the application pool. This means that the Fortify

WebInspect Enterprise web site no longer needs to have ISAPI filters configured or ISAPI and CGI restrictions configured in IIS. Integrated mode does not use either of these elements.

IIS Application Pool Identity

Fortify WebInspect Enterprise no longer uses ASP.NET impersonation. Previously, ASP.NET impersonation was used to ensure that the account that was logged onto the server had the appropriate permissions to folders, registry keys, and encryption methods. However, Fortify WebInspect Enterprise now uses IIS7 and the application pool identity, which provides most of the required permissions.

This means that ASP.NET impersonation will not be enabled in the Authentication section of the application in IIS. The application will run with the application pool identity account, which is `IIS AppPool\WIEAppPool`. We recommend that you do not change this account in IIS.

Important! The Fortify WebInspect Enterprise server application uses the IIS application pool identity. Because the IIS application pool is not a true Windows account, Fortify WebInspect Enterprise cannot use Windows authentication for the database connection. Customers must create a SQL Server account that can be used for the database connection.

Installing SQL Server

Install a supported version of SQL Server software if it is not already installed.

We recommend that you configure the database server on a separate machine from either Fortify Software Security Center or Fortify WebInspect Enterprise.

Important! If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, the Fortify WebInspect Enterprise SQL Server database requires case-insensitive collation. This is opposite the requirement for Fortify Software Security Center databases.

Creating a Sensor User

Create a local user account or an Active Directory user account in Windows, with a recognizable name such as WIEsensor, to be used as a sensor user for Fortify WebInspect Enterprise. Note the domain name, the account name, and the password.

Ensuring Secure HTTPS Operation

We strongly recommend that you do the following to use HTTPS securely:

1. Completely disable SSLv2.
2. Enable TLS 1.1 and 1.2.

3. Disable weak ciphers, generally defined as:
   - Ciphers having key length less than 128 bits
   - NULL ciphers
   - Ciphers that use MD5
   - Ciphers that use anonymous key exchange
   - Ciphers that use RC2

Using SAN or Wildcard Certificates and Non-Standard Ports in IIS

The Fortify WebInspect Enterprise Initialization Wizard does not overwrite certificate and port bindings that you create in IIS. As a result, you can use SAN or wildcard certificates and non-standard ports when configuring the Fortify WebInspect Enterprise Manager Web Service during initialization.

To use a SAN or wildcard certificate:

- Configure the web site in IIS with the appropriate bindings. During initialization, Fortify WebInspect Enterprise will show those configured bindings and will not overwrite them.

To use a non-standard port:

- Configure the binding with the port in IIS. During initialization, Fortify WebInspect Enterprise can use this binding and port.

For more information, see "Configuring the Web Service" on page 32.

HTTP Binding Host Name

If the HTTP binding in IIS does not contain a host name, the Initialization Wizard will create the HTTP URL using the server name. This configuration causes an issue with downloading the thin client for Guided Scan, reporting, and scan imports.

To prevent this issue:

- In the Edit Site Binding dialog box in IIS, add a host name for the HTTP binding before running the Initialization Wizard.

To correct this issue, do one of the following:

- In the Edit Site Binding dialog box in IIS, add a host name for the HTTP binding and re-run the Initialization Wizard.
- Modify the URL directly in the database. If you update the URL directly in the database only, the URL will revert to the server name if you run the Initialization Wizard again. To manually modify the URL in the database:
  a. Run the following commands in the WIE database, replacing the `SettingValue` with your host name:

```
SELECT * FROM ConfigSetting WHERE SettingName = 'WIE.HttpUrl'
UPDATE ConfigSetting SET SettingValue='http://my.host.com/wie/' WHERE
SettingName = 'WIE.HttpUrl'
```

b. Restart the WIE application pool for this change to take effect.

For more information, refer to your IIS and SQL Server documentation.

Using HTTPS with Guided Scan and Reports

By default, using Guided Scan or generating reports in conjunction with a self-signed certificate requires that HTTP be enabled for Fortify WebInspect Enterprise. However, if you use a signed certificate, then you can manually modify the HTTP URL setting in the WIE database to use HTTPS.

To use HTTPS:

1. Run the following commands in the WIE database:

```
SELECT * FROM ConfigSetting WHERE SettingName = 'WIE.HttpUrl'
UPDATE ConfigSetting SET SettingValue='https://my.host.com/wie/' WHERE
SettingName = 'WIE.HttpUrl'
```

2. Restart the WIE application pool for this change to take effect.

Important! The HTTP URL setting will need to be manually modified if the Initialization Wizard is run again.

Databases in Availability Groups

If your SQL database is part of an availability group, remove it from the AlwaysOn Availability Group. After the WIE initialization is complete, rejoin the database to the availability group.

For more information, refer to your SQL Server documentation.

Mirrored Databases

If your SQL database is mirrored, set the partner option to OFF on the master database. After the WIE initialization is complete, perform a restore on the mirrored database and set the partner option to ON on the master database.

For more information, refer to your SQL Server documentation.

Related Documents

This topic describes documents that provide information about Fortify software products.

Note: You can find the Fortify Product Documentation at https://www.microfocus.com/support/documentation. Most guides are available in both PDF and HTML formats. Product help is available within the Fortify LIM product and the Fortify WebInspect products.

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Product Documentation website.

Document / File Name	Description
About Fortify Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, this document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
OpenText™ Fortify Software Security Center User Guide	This document provides Fortify Software Security Center users with detailed information about how to deploy and use

Document / File Name	Description
SSC_Guide_<*version*>.pdf	Fortify Software Security Center. It provides all of the information you need to acquire, install, configure, and use Fortify Software Security Center. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Fortify Software Security Center provides security team leads with a high-level overview of the history and current status of a project.

Fortify WebInspect

The following documents provide information about Fortify WebInspect. Unless otherwise noted, these documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / File Name	Description
OpenText™ Fortify WebInspect Installation Guide WI_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect and instructions for installing Fortify WebInspect and activating the product license.
OpenText™ Fortify WebInspect User Guide WI_Guide_<*version*>.pdf	This document describes how to configure and use Fortify WebInspect to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect and OAST on Docker User Guide	This document describes how to download, configure, and use Fortify WebInspect and Fortify OAST that are

Document / File Name	Description
WI_Docker_Guide_<*version*>.pdf	available as container images on the Docker platform. The Fortify WebInspect image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as a Fortify ScanCentral DAST sensor and used in conjunction with Fortify Software Security Center. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.
OpenText™ Fortify WebInspect Agent Installation and Rulepack Guide WI_Agent_Install_<*version*>.pdf	This document describes how to install the OpenText™ Fortify WebInspect Agent and describes the detection capabilities of the Fortify WebInspect Agent Rulepack Kit. Fortify WebInspect Agent Rulepack Kit runs atop the Fortify WebInspect 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.

Fortify WebInspect Enterprise

The following documents provide information about Fortify WebInspect Enterprise. Unless otherwise noted, these documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect-enterprise.

Document / File Name	Description
OpenText™ Fortify WebInspect Enterprise Installation and Implementation Guide WIE_Install_<*version*>.pdf	This document provides an overview of Fortify WebInspect Enterprise and instructions for installing Fortify WebInspect Enterprise, integrating it with Fortify Software Security Center and Fortify WebInspect, and troubleshooting the installation. It also describes how to configure the components of the Fortify WebInspect Enterprise system, which include the Fortify WebInspect Enterprise application, database, sensors, and users.
OpenText™ Fortify WebInspect Enterprise User Guide WIE_Guide_<*version*>.pdf	This document describes how to use Fortify WebInspect Enterprise to manage a distributed network of Fortify WebInspect sensors to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify WebInspect Enterprise help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Fortify WebInspect Tools Guide WI_Tools_Guide_<*version*>.pdf	This document describes how to use the Fortify WebInspect diagnostic and penetration testing tools and configuration utilities packaged with Fortify WebInspect and Fortify WebInspect Enterprise.

Chapter 2: Installing Fortify WebInspect Enterprise

This section describes the installation process and provides detailed procedures for installing the various components that make up Fortify WebInspect Enterprise.

Important! To install Fortify WebInspect Enterprise on a server, you must be a system administrator on the server.

About the Installation

Installation of Fortify WebInspect Enterprise is driven by a series of wizards as described in the following sections. The major steps are:

- Installing the Fortify WebInspect Enterprise Server software, using the Fortify WebInspect Enterprise Setup Wizard
- Running the Fortify WebInspect Enterprise Initialization Wizard
- Configuring the Scan Uploader, Task, and Scheduler services
- Installing the Fortify WebInspect Enterprise Administrative Console, using the Fortify WebInspect Enterprise Console Setup Wizard
- Logging on to and configuring the Administrative Console

After these installation procedures, this document includes information about the following topics:

- Post-installation configuration
  - Installing Fortify WebInspect as a sensor

    Note: When you install Fortify WebInspect to be used with Fortify WebInspect Enterprise, the installed product is called a sensor. The sensor does not include a user interface, and is controlled from the Fortify WebInspect Enterprise Administrative Console.
  - Adding sensor users (if not previously done)
  - Enabling sensors and configuring sensor permissions
  - Assigning administrators and roles
  - Moving application versions from the default group
  - If you are integrating Fortify WebInspect Enterprise with Fortify Software Security Center, updating settings to allow manual publishing of scans to Fortify Software Security Center
- Guided Scan and creating reports

- Time stamping and scheduling
- Installations lacking internet connection
- Troubleshooting the installation

Note: If the installation is not successful, the prerequisites might not have been fully met. See "Troubleshooting the Installation" on page 79.

Installing the Fortify WebInspect Enterprise Server Software

Before installation, review "FIPS or Non-FIPS Compliance" on page 10.

Install the Fortify WebInspect Enterprise server software on the server by running the Setup Wizard:

1. Launch the WIE Server installation file.

   Note: If the wizard detects an earlier version of the Fortify WebInspect Enterprise server software, uninstall that version using Control Panel and then relaunch the installation file.

   The Welcome screen of the WebInspect Enterprise 23.2.0 Setup wizard appears.
2. Click **Next**.

   The End-User License Agreement window appears.
3. Review the license agreement. If you accept it, select the check box and click **Next**; otherwise click **Cancel**.

   If you accept the license agreement, the Product Features window appears.
4. On the Product Features window:
   a. Select the components you want to install.

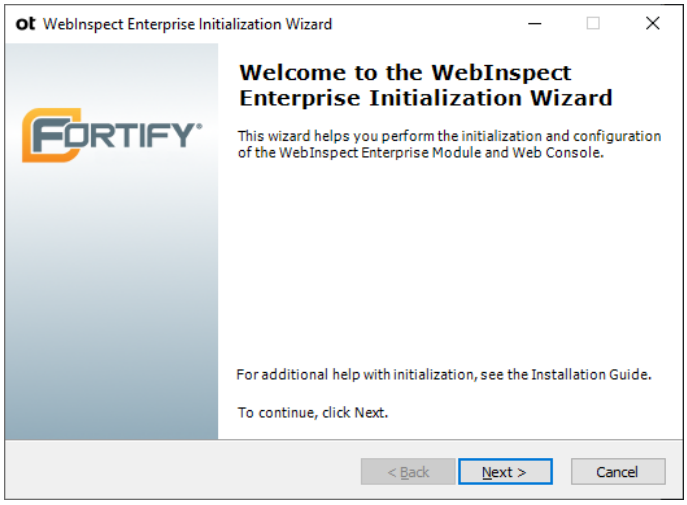
      Fortify WebInspect can scan a website and export the scan results to a location called a “dropbox.” The Scan Uploader Service accesses each dropbox periodically and, if files exist, it uploads those files to the Fortify WebInspect Enterprise Manager. To install the Fortify WebInspect Enterprise Scan Uploader Service, click the associated **x** icon, and then in the drop-down list click **Will be installed on local hard drive**.
   b. Accept the default location or click **Browse** to select the location where you want to install the software.
   c. Click **Next**.

      The Ready to install WebInspect Enterprise 23.2.0 window appears.
5. When you are ready to install, click **Install**.

   Fortify WebInspect Enterprise software is installed on the computer and the Setup Wizard completes.
6. Click **Finish**.

About the Initialization Wizard

After the Setup Wizard completes, the Welcome window of the Fortify WebInspect Enterprise Initialization Wizard appears.



The Initialization Wizard initializes the software as described in this section. Its functions include:

- Activating the Fortify WebInspect Enterprise license
- Creating a new Fortify WebInspect Enterprise database or updating an existing one as needed
- Creating the Fortify WebInspect Enterprise website and web service
- Connecting Fortify WebInspect Enterprise and Fortify Software Security Center (Optional)
- Establishing the initial Fortify WebInspect Enterprise system administrator

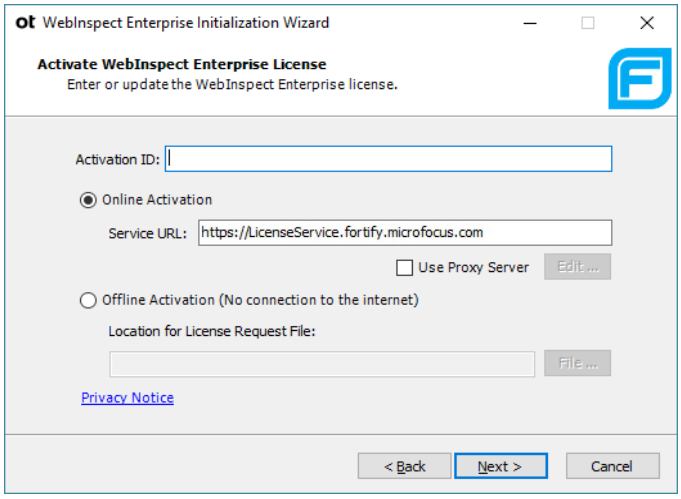
Note: After you complete these installation procedures, you will always be able to restart the Initialization Wizard if necessary, by clicking **Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Initialize**.

Activating the License

To activate the Fortify WebInspect Enterprise license:

1. Click **Next**.

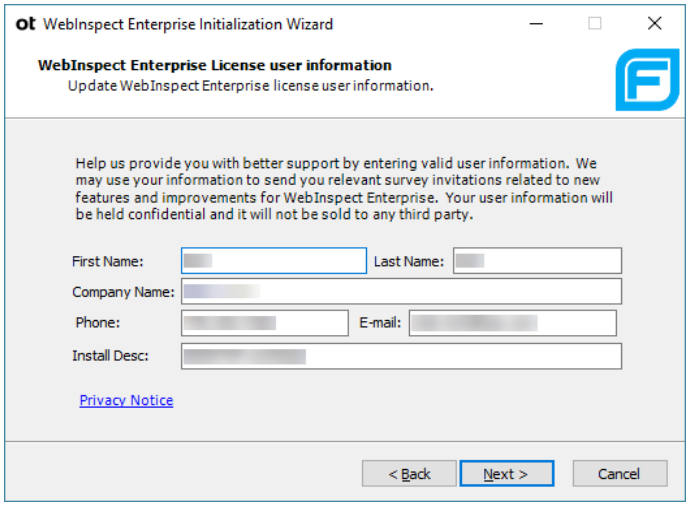
   The Activate WebInspect Enterprise License dialog box appears.



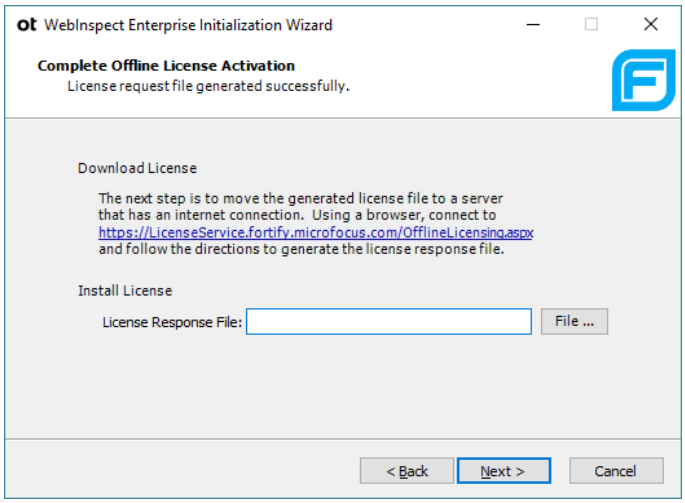
2. Enter the **Activation ID** that OpenText sent to you.
3. Do one of the following:
   - If the computer is connected to the Internet, select **Online Activation**.

     If you are using a proxy server, select **Use Proxy Server**, click **Edit**, and provide the requested information.
   - If the computer is *not* connected to the Internet, select **Offline Activation** and then click **File** to select the location on this computer where you want the installation software to create a license *request* file named **LicenseRequest.xml**. This file will contain information about the computer that is required to obtain a license.
4. Click **Next**.

The WebInspect Enterprise License user information dialog box displays user information as submitted to OpenText.



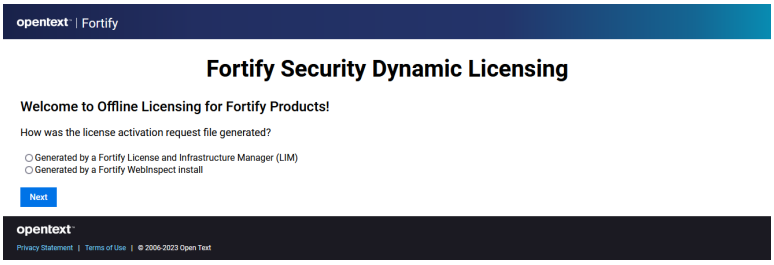
5. Correct the information as needed and click **Next**.
6. If you selected **Online Activation** in Step 3, go to Step 8.
7. If you selected **Offline Activation** in Step 3, the Complete Offline License Activation dialog box appears. It indicates that the license request file was generated successfully. Perform the procedure in this step to download from OpenText a license *response* file named **LicenseResp.xml** that you can copy to the computer, not connected to the Internet, on which you are installing Fortify WebInspect Enterprise.



   a. Copy the `LicenseRequest.xml` file you created in Step 3 to a portable device such as a flash drive.
   b. Copy the `LicenseRequest.xml` file from the portable device to a computer that is connected to the Internet.

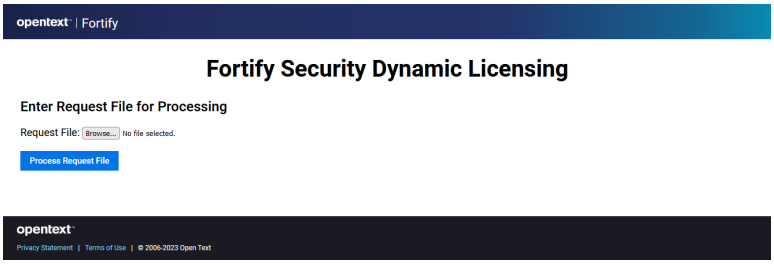
c. Open a browser and navigate to

`https://licenseservice.fortify.microfocus.com/OfflineLicensing.aspx`.



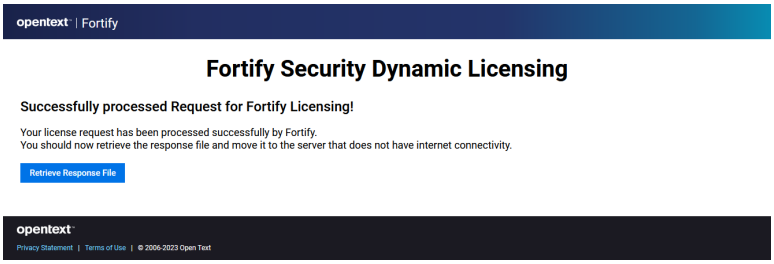
d. Select the option that describes how the license request file was generated and click **Next**.

The Enter Request File for Processing page appears.



e. Click **Browse** as needed, select the `LicenseRequest.xml` file that you copied to this computer, and then click **Process Request File**.

If the request is processed successfully, the Successfully processed Request for Fortify Licensing page appears.

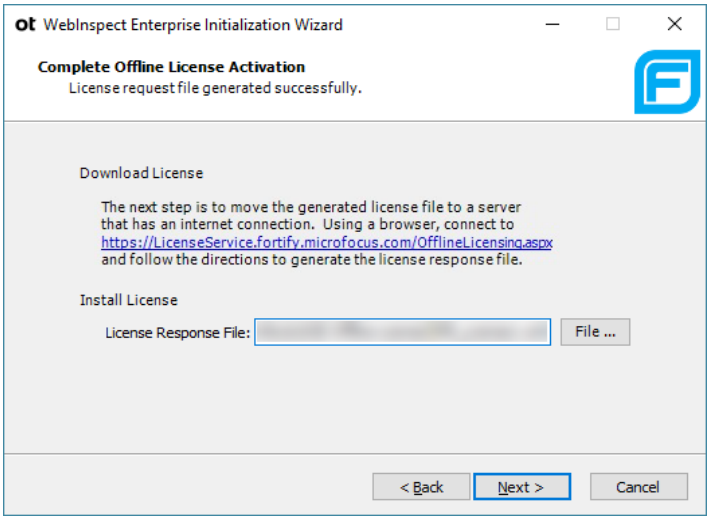


f. Click **Retrieve Response File**.

g. On the File Download dialog box, click **Save** and specify the location on the portable device where you want to download the response file `LicenseResp.xml`.

h. Return to the computer on which you are installing Fortify WebInspect Enterprise. Copy the `LicenseResp.xml` file from the portable device to a location on this computer.

i. In the Fortify WebInspect Enterprise Initialization Wizard, specify the **License Response File** field by clicking **File** and navigating to the location of the `LicenseResp.xml` file you just copied from the portable device.



j. Click **Next**.

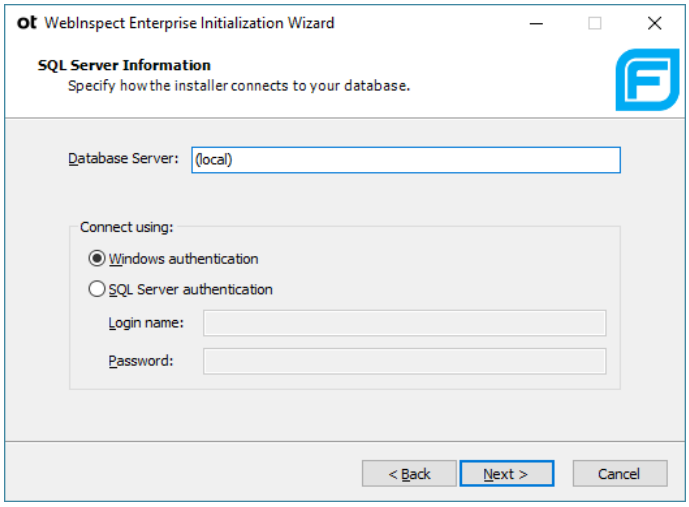
8. The WebInspect Enterprise License Information dialog box displays information about the license. Review the information.

Configuring the Database

To provide the SQL Server information and select the database:

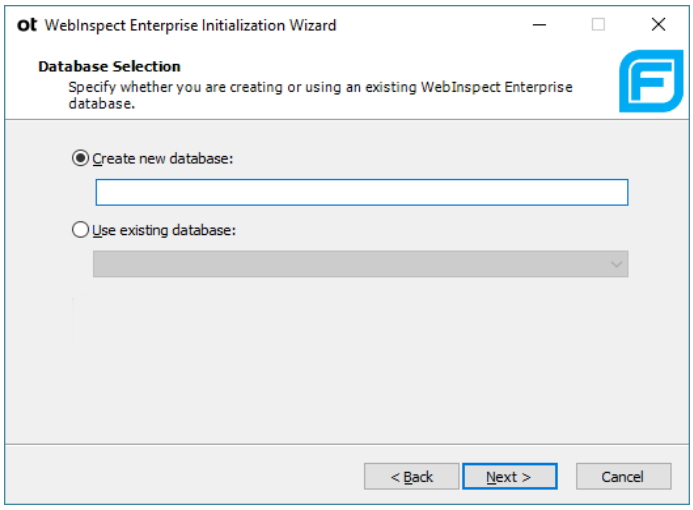
1. Click **Next**.

   The SQL Server Information window appears.



2. Enter the name of the SQL Server instance in the **Database Server** field and select the authentication that will be used. If you are installing Fortify WebInspect Enterprise for the first time, you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).
3. Click **Next.**

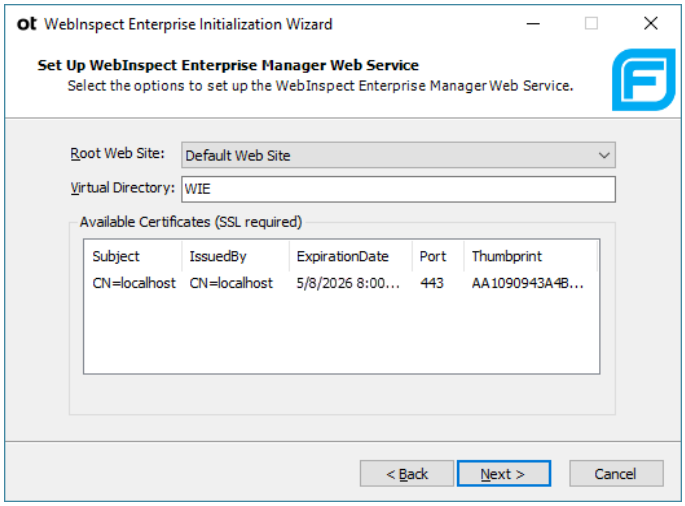
   The Database Selection window appears.



4. Do one of the following:
   - To use a new database, select **Create new database** and enter a database name. You must have privileges to create this database.
   - To use an existing Fortify WebInspect Enterprise 22.2.0 database for an upgrade, select **Use existing database** and select a database from the drop-down list. You must have owner privileges for that database.
5. Click **Next**.
6. Do one of the following:
   - If you created a new database, skip to "Configuring the Web Service" on the next page.
   - If you are using an existing database for an upgrade from Fortify WebInspect Enterprise 22.2.0, the database must be upgraded, and the Fortify WebInspect Enterprise Database Upgrade window appears, instructing you to back up that database before upgrading it. After you have backed up the database, select the **Database is backed up** check box and click **Next**.

Configuring the Web Service

After configuring the database, the Set Up WebInspect Enterprise Manager Web Service window appears.



If you have configured HTTPS bindings for the root web site in IIS, only those bindings will be listed in the Available Certificates. You will not be able to create a new binding for a web site in the Fortify WebInspect Enterprise Initialization Wizard. You can create a new binding only in IIS. The following table describes your options, based on your IIS settings.

If...	Then...
HTTPS is setup on the default web site for port 443 in IIS	Only that binding is available to select. You cannot create a new binding in the initialization wizard.
Multiple HTTPS bindings are configured in IIS	You may select the binding you want Fortify WebInspect Enterprise to use. Your selection determines the host name that is used in the URL and the port that is used. This allows Fortify WebInspect Enterprise to run on a non-standard port.
No HTTPS bindings have been created for port 443	You may select the certificate you want to use or create a new certificate.

To configure the web service:

1. Specify the root Web site and the IIS virtual directory name (`WIE` in the previous example), and select (or add and select) a certificate.

   These entries create the URLs for the following components:

   - Fortify WebInspect Enterprise URL for login to the Administrative Console:

     `http(s)://<computer name>/<Virtual Directory name>`

   - Web Console URL:

     `http(s)://<computer name>/<Virtual Directory name>/WebConsole`

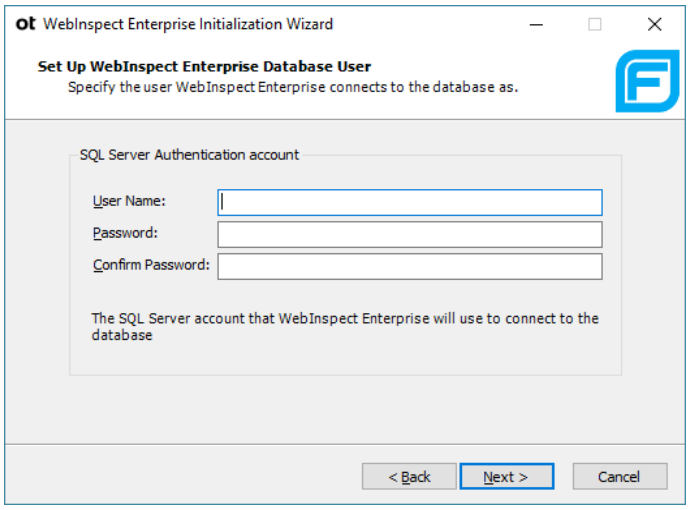
2. Click **Next**.

Note: If an HTTPS binding has been created for site A and you select site B, which does not have any HTTPS bindings configured, then a warning message appears. You must set up an HTTPS binding manually for site B or select another site.

Setting Up Fortify WebInspect Enterprise Database Users

At this point, the Initialization Wizard performs a file check to ensure that the user has read access to the machine keys directory where the Data Protection Application Programming Interface (DPAPI) keys used for decrypting the connection string are stored. If you receive an error message, ensure that the Administrator has read access to the machine keys directory.

The Set Up WebInspect Enterprise Database User window appears.



1. Enter the **User Name** and **Password** used for SQL server authentication.
2. Click **Next**.

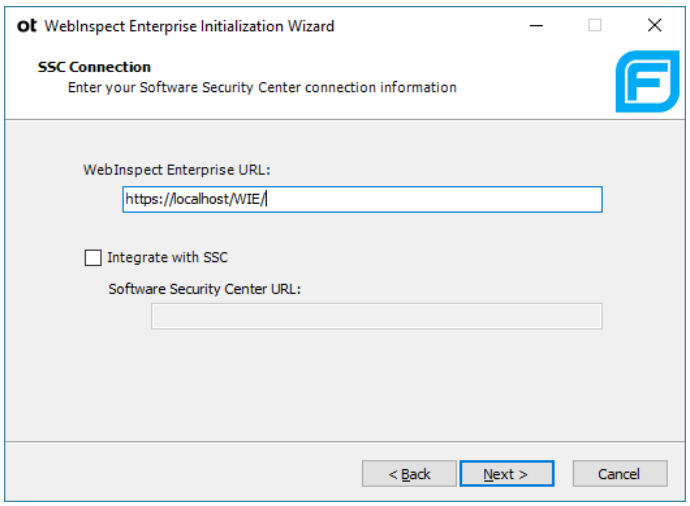
What's Next?

Continue as follows:

- To install or upgrade a Fortify WebInspect Enterprise that is integrated with Fortify Software Security Center, go to "Setting Up a Fortify Software Security Center (SSC) Connection" below.
- To install or upgrade a standalone Fortify WebInspect Enterprise, go to "Installing or Upgrading a Standalone Fortify WebInspect Enterprise" on page 40.
- To upgrade and decouple Fortify WebInspect Enterprise that is integrated with Fortify Software Security Center, go to "Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center" on page 45.

Setting Up a Fortify Software Security Center (SSC) Connection

After setting up Fortify WebInspect Enterprise Manager and database users, the SSC Connection window appears.



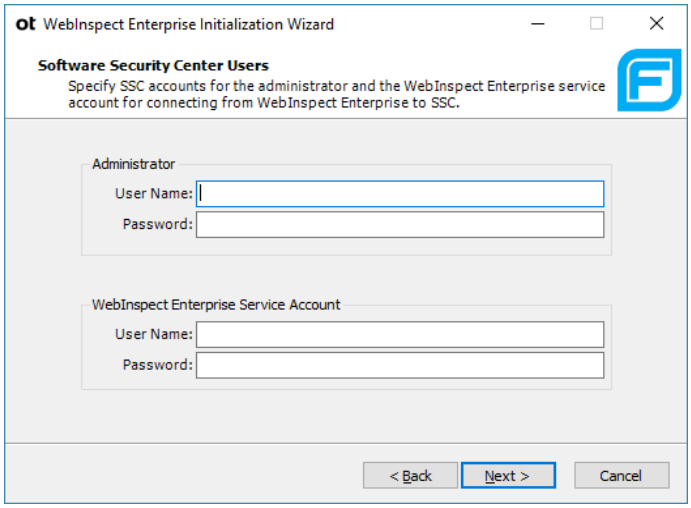
To set up a connection to Fortify Software Security Center:

1. The **WebInspect Enterprise URL** field has a default value based on previous configuration. Make a note of this URL.
2. Ensure that the **Integrate with SSC** check box is selected.
3. Specify the **Software Security Center URL**. See "Installing or Upgrading Fortify Software Security Center (Optional)" on page 12.

   Important! You must specify the complete Fortify Software Security Center URL, as shown in the following example:

   ```
   http://Mydomain.com:8080/ssc
   ```
4. Click **Next**.

The Software Security Center Users window appears.

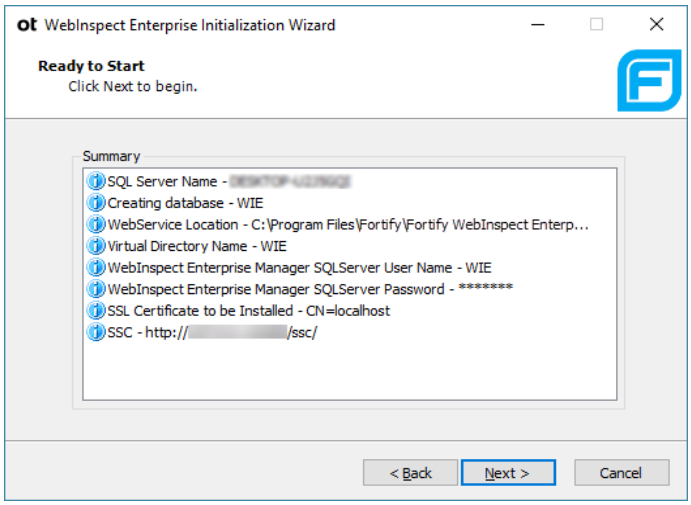


5. Before continuing, make sure that Fortify Software Security Center is running and that a Fortify Software Security Center administrator is logged on.
6. In the Software Security Center Users window, specify the Fortify Software Security Center accounts for that administrator and for the Fortify WebInspect Enterprise Service Account. See "Installing or Upgrading Fortify Software Security Center (Optional)" on page 12. The Fortify Software Security Center administrator you specify here will automatically become the first Fortify WebInspect Enterprise system administrator.
7. Click **Next**.

   The installation software verifies that Fortify WebInspect Enterprise can access the Fortify Software Security Center server and use the Fortify Software Security Center accounts you specified. If it cannot, an error message is displayed; make sure that Fortify Software Security Center is running.

Initializing Fortify WebInspect Enterprise

After configuring the connection to Fortify Software Security Center, the Ready to Start window appears.

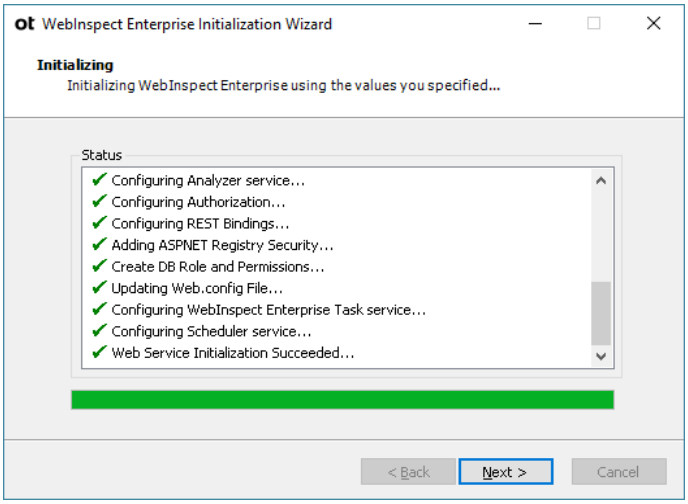


Verify your previous choices and begin initializing Fortify WebInspect Enterprise.

1. Do one of the following:
   - To change settings, click **Back**.
   - To begin initializing Fortify WebInspect Enterprise using the values you have specified, click **Next**.

     The Initialization Wizard:
     - Creates a new database if you chose to do so in "Configuring the Database" on page 30.
     - Registers Fortify WebInspect Enterprise with Fortify Software Security Center. Then Fortify Software Security Center sends all current application versions (finished and unfinished) to Fortify WebInspect Enterprise, where they get created and can be displayed.
     - Configures various system components.
     - In the displayed, cumulative Status list in the Ready to Start window, adds the next step when it begins, with a flashing blue information icon while that step is running, and changes that icon to a green check mark when that step completes successfully (except for the first step, which is Initializing Database).

When the initialization completes successfully, a window displays a list of initialization steps and the final initialization step is “Web Service Initialization Succeeded…”

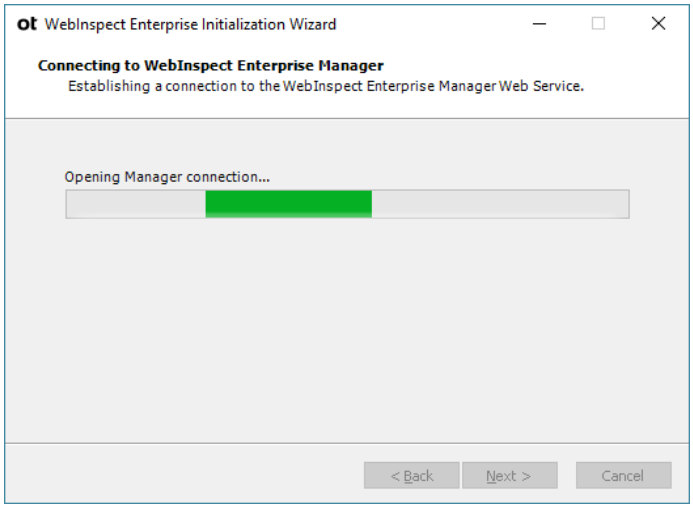


2. Click **Next**.

   The Fortify Software Security Center administrator you specified in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34 automatically becomes the first System Administrator in Fortify WebInspect Enterprise.

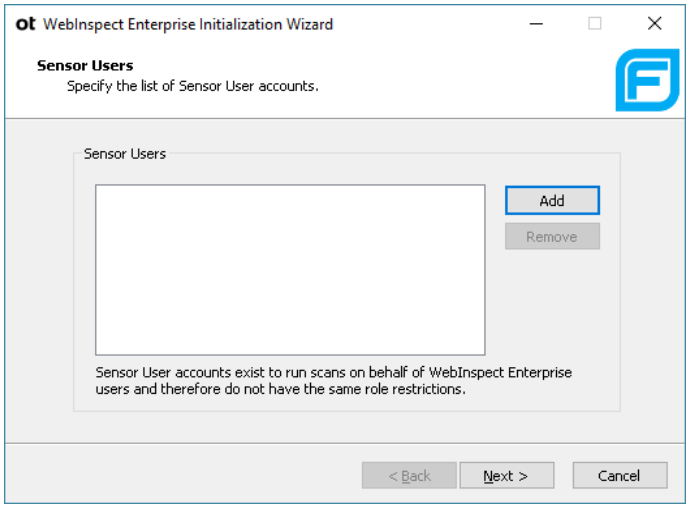
   Note: If the Fortify Software Security Center administrator’s password expires or is changed, or if a new Fortify Software Security Center administrator is chosen for interaction with Fortify WebInspect Enterprise, a Fortify WebInspect Enterprise administrator will need to rerun the Initialization Wizard (**Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Initialize**) and specify the new credentials for the Fortify Software Security Center administrator in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34. Then at this point in the initialization process, the Initialization Wizard will detect that the newly specified Fortify Software Security Center administrator exists in Fortify Software Security Center but is not a System Administrator in Fortify WebInspect Enterprise. In this case, the Wizard will display the Administrator Role Page, allowing you to add the new administrator to Fortify WebInspect Enterprise with the System Administrator role by selecting the **Add Current User to System Administrator Role** check box and clicking **Next**.

The Connecting to WebInspect Enterprise Manager screen appears until the connection is made.



Adding Sensor Users

After Fortify WebInspect Enterprise is initialized, the Sensor Users window appears.



Optionally add at least one sensor user for Fortify WebInspect Enterprise to use to run scans. Sensor users must not be general console users and they must have been previously created as Windows users as described in "Preparing to Install Fortify WebInspect Enterprise" on page 15.

You do not have to add any sensor users to Fortify WebInspect Enterprise at this point, but you will need to specify at least one sensor user before you can run any scans. Post-installation configuration procedures in this document also describe how to add sensor users.

To add a sensor user to Fortify WebInspect Enterprise now:

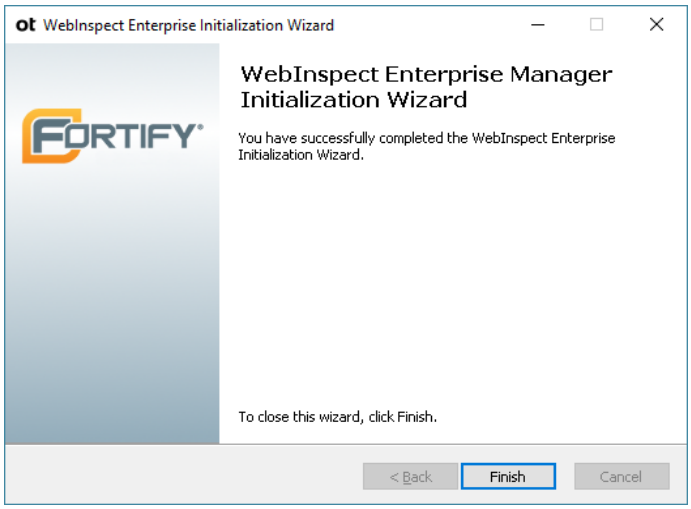
1. Click **Add**.
2. In the Select Users or Groups dialog box, type the name of an existing user to add (see "Preparing to Install Fortify WebInspect Enterprise" on page 15), in the format localhost\user or domain\user. If you specify only the user, you can click **Check Names** to help identify the localhost or domain.
3. Click **OK**.
4. Verify that the sensor user you specified has been added to the list of Sensor Users in the window.

Completing Initialization

To complete the initialization process:

1. Click **Next**.

   The Initialization Wizard completes.



2. Click **Finish**.

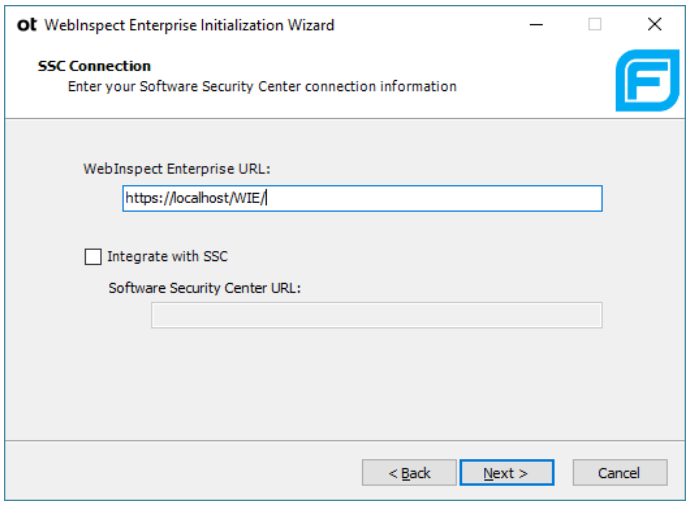
   The Initialization Wizard closes.

What's Next?

Continue with "Configuring Services" on page 52.

Installing or Upgrading a Standalone Fortify WebInspect Enterprise

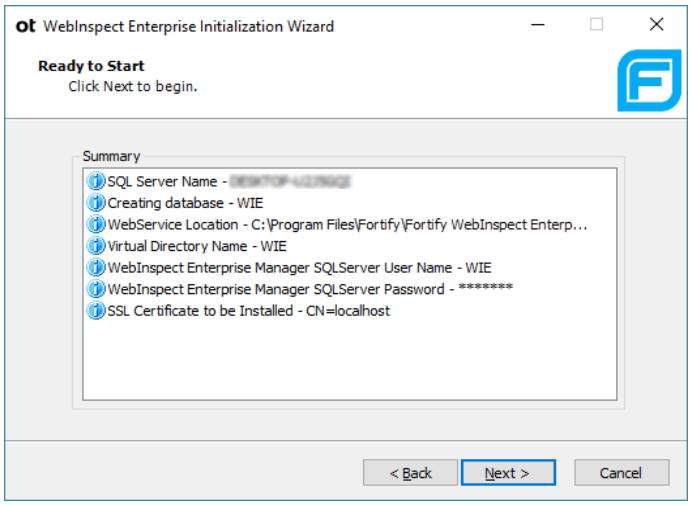
After setting up Fortify WebInspect Enterprise Manager and database users, the SSC Connection window appears. This section describes how to install Fortify WebInspect Enterprise as standalone without a connection to Fortify Software Security Center.



1. Clear the **Integrate with SSC** check box.
2. Click **Next**.

Initializing Fortify WebInspect Enterprise

After configuring a standalone Fortify WebInspect Enterprise, the Ready to Start window appears.

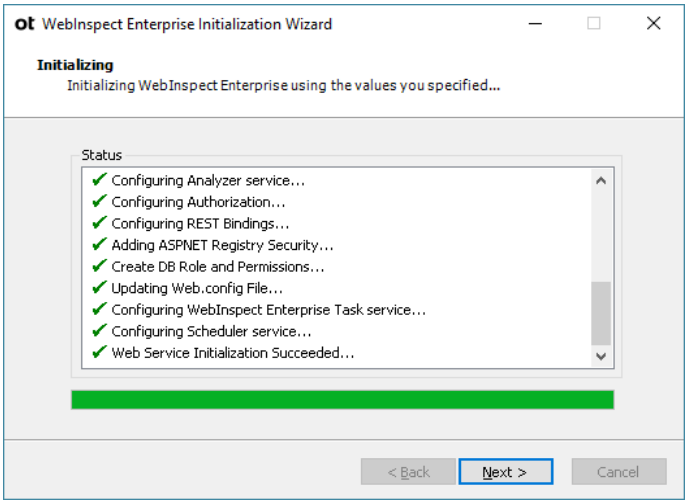


Verify your previous choices and begin initializing Fortify WebInspect Enterprise.

1. Do one of the following:
   - To change settings, click **Back**.
   - To begin initializing Fortify WebInspect Enterprise using the values you have specified, click **Next**.

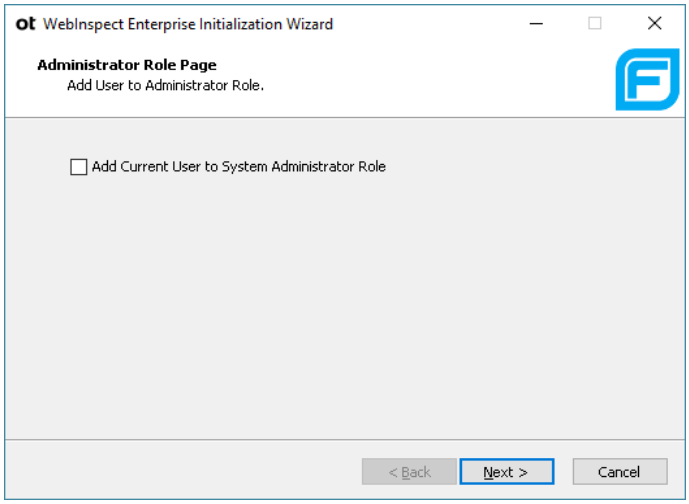
     The Initialization Wizard:
     - Creates a new database if you chose to do so in "Configuring the Database" on page 30.
     - Configures various system components.
     - In the displayed, cumulative Status list in the Ready to Start window, adds the next step when it begins, with a flashing blue information icon while that step is running, and changes that icon to a green check mark when that step completes successfully (except for the first step, which is Initializing Database).

     When the initialization completes successfully, a window displays a list of initialization steps and the final initialization step is “Web Service Initialization Succeeded…”



2. Click **Next**.

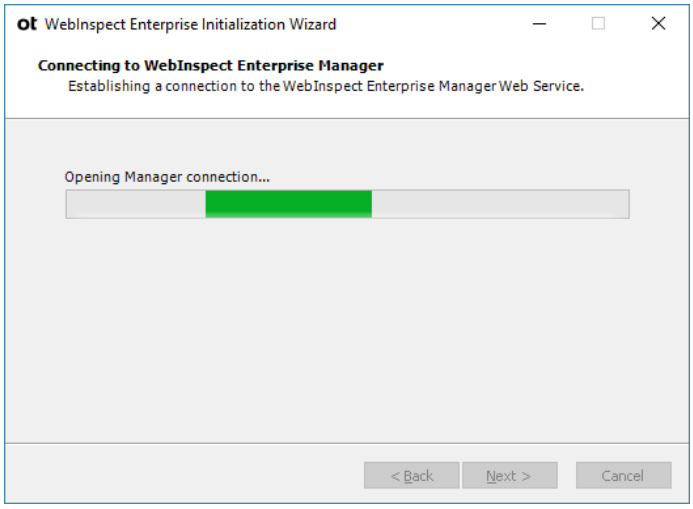
If a system administrator exists in WebInspect Enterprise, but the current user is not a system administrator, the Administrator Role Page appears.



Otherwise, the current user is added as the first WebInspect Enterprise system administrator and the procedure continues with the Connecting to WebInspect Enterprise Manager window after Step 4.

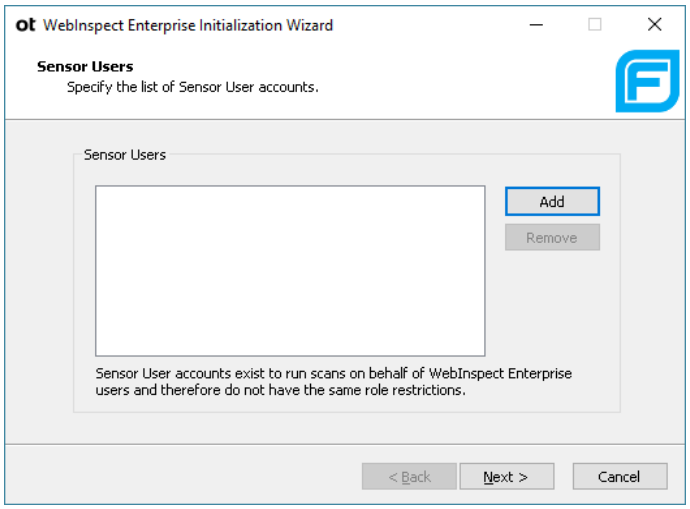
3. On the Administrator Role Page, select the **Add Current User to System Administrator Role** check box to make the current user a WebInspect Enterprise system administrator.
4. Click **Next**.

   The Connecting to WebInspect Enterprise Manager window appears until the connection is made.



Adding Sensor Users

After Fortify WebInspect Enterprise is initialized, the Sensor Users window appears.



Optionally add at least one sensor user for Fortify WebInspect Enterprise to use to run scans. Sensor users must not be general console users and they must have been previously created as Windows users as described in "Preparing to Install Fortify WebInspect Enterprise" on page 15.

You do not have to add any sensor users to Fortify WebInspect Enterprise at this point, but you will need to specify at least one sensor user before you can run any scans. Post-installation configuration procedures in this document also describe how to add sensor users.

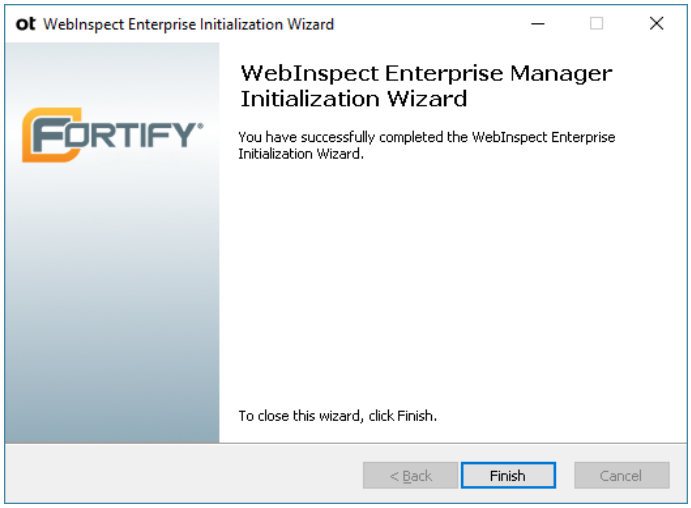
To add a sensor user to Fortify WebInspect Enterprise now:

1. Click **Add**.
2. In the Select Users or Groups dialog box, type the name of an existing user to add (see "Preparing to Install Fortify WebInspect Enterprise" on page 15), in the format localhost\user or domain\user. If you specify only the user, you can click **Check Names** to help identify the localhost or domain.
3. Click **OK**.
4. Verify that the sensor user you specified has been added to the list of Sensor Users in the window.

Completing Initialization

To complete the initialization process:

1. Click **Next**.
   The Initialization Wizard completes.



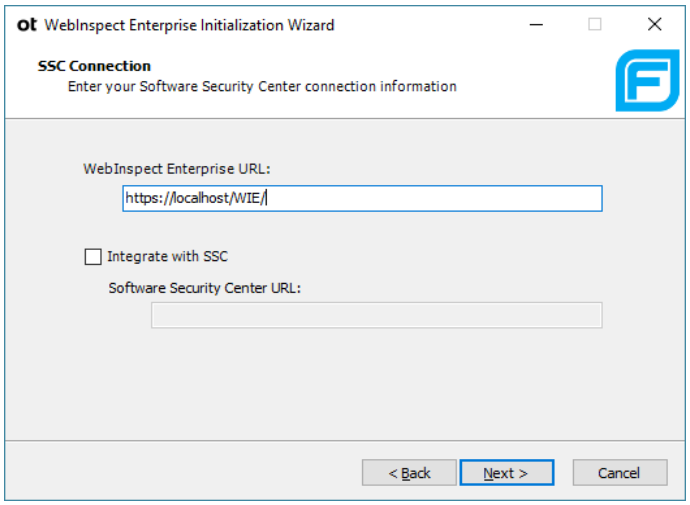
2. Click **Finish**.
   The Initialization Wizard closes.

What's Next?

Continue with "Configuring Services" on page 52.

Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center

After setting up Fortify WebInspect Enterprise Manager and database users, the SSC Connection window appears. This section describes how to decouple an existing Fortify WebInspect Enterprise installation from Fortify Software Security Center.



Important! Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center is permanent. Reconnecting to Fortify Software Security Center is not supported. You can choose to map existing Fortify Software Security Center users to Windows accounts, allowing mapped user accounts to continue using Fortify WebInspect Enterprise.

Decoupled Fortify WebInspect Enterprise installations use Windows Authentication. Before decoupling Fortify WebInspect Enterprise from Fortify Software Security Center, enable Windows Authentication as described in "Installing IIS, ASP.NET, and .NET Framework" on page 16.

To decouple an existing Fortify WebInspect Enterprise installation from Fortify Software Security Center:

1. Clear the **Integrate with SSC** check box.
2. Click **Next**.

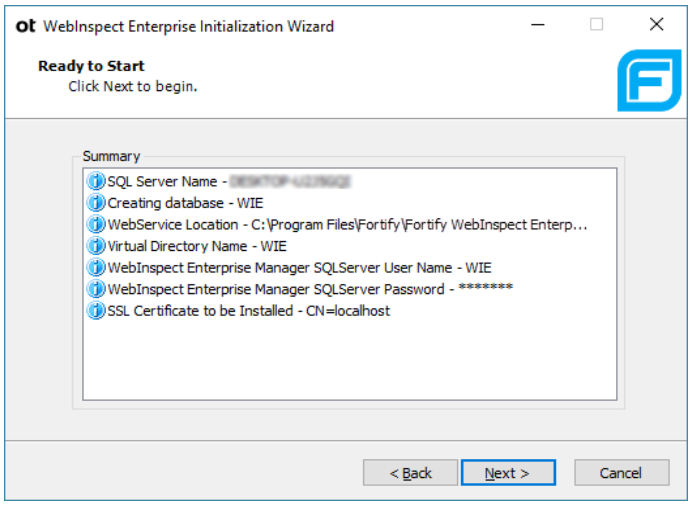
   A warning appears advising that decoupling from the SSC server will require remapping all the existing SSC user accounts to Windows accounts.
3. Click **Yes**.

After confirming your selection to decouple, the Initialization Wizard checks for the items described in the following table. If no configuration errors are detected, skip ahead to "Initializing Fortify WebInspect Enterprise" on the next page.

Item Checked	Corrective Action
The Initialization Wizard determines whether your Fortify WebInspect Enterprise server is part of your domain. If the server is not part of the domain, the following message appears: The Fortify WebInspect Enterprise server is not joined to a domain or the domain cannot be contacted. If you continue, Windows authentication for the server will be restricted to local accounts. For access to domain accounts, you can cancel the initialization, add the server to your domain (which will require a reboot), and rerun the Initialization Wizard. Press "Yes" if you would like to continue and use only local accounts.	Do one of the following: • To continue with authentication restricted to local accounts, click **Yes**. • To cancel the initialization and add the server to your domain, click **No**.
The Initialization Wizard determines whether Fortify Software Security Center is running. If it is not running, the following message appears: SSC is currently not running or cannot be accessed to deregister Fortify WebInspect Enterprise. If you decouple without deregistering, SSC will continue to run as if connected to Fortify WebInspect Enterprise. Do you wish to continue?	Do one of the following: • To continue without deregistering Fortify WebInspect Enterprise, click **Yes**. • To cancel the initialization and ensure that Fortify Software Security Center is running, click **No**.

Initializing Fortify WebInspect Enterprise

After configuring the decouple from Fortify Software Security Center, the Ready to Start window appears.

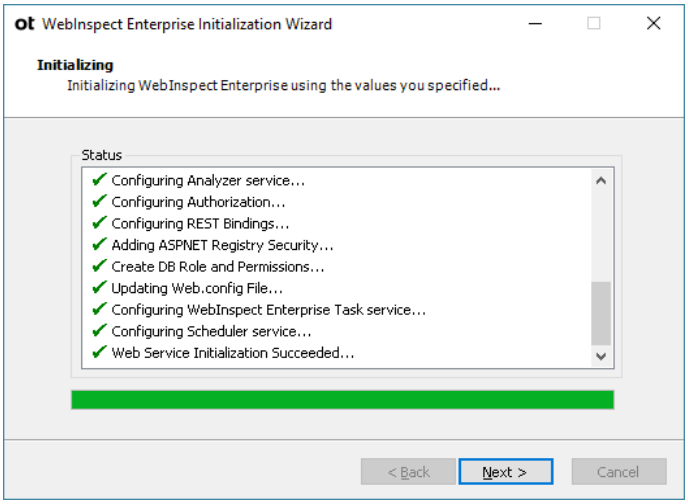


Verify your previous choices and begin initializing Fortify WebInspect Enterprise.

1. Do one of the following:
   - To change settings, click **Back**.
   - To begin initializing Fortify WebInspect Enterprise using the values you have specified, click **Next**.

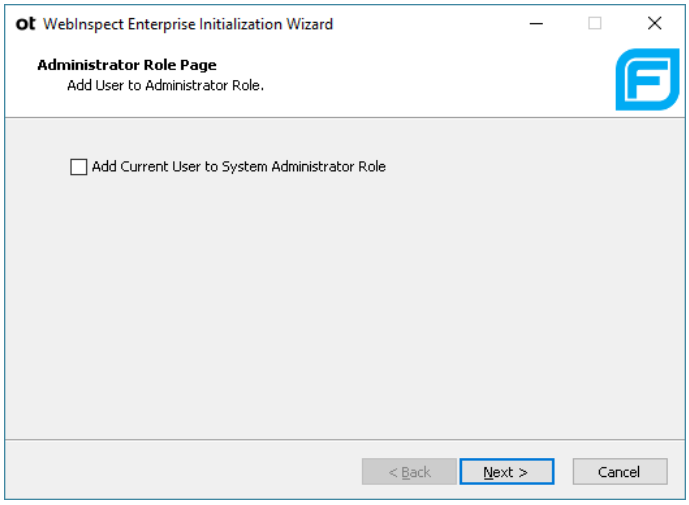
     The Initialization Wizard:
     - Creates a new database if you chose to do so in "Configuring the Database" on page 30.
     - Configures various system components.
     - In the displayed, cumulative Status list in the Ready to Start window, adds the next step when it begins, with a flashing blue information icon while that step is running, and changes that icon to a green check mark when that step completes successfully (except for the first step, which is Initializing Database).

When the initialization completes successfully, a window displays a list of initialization steps and the final initialization step is “Web Service Initialization Succeeded…”



2. Click **Next**.

   If a system administrator exists in WebInspect Enterprise, but the current user is not a system administrator, the Administrator Role Page appears.

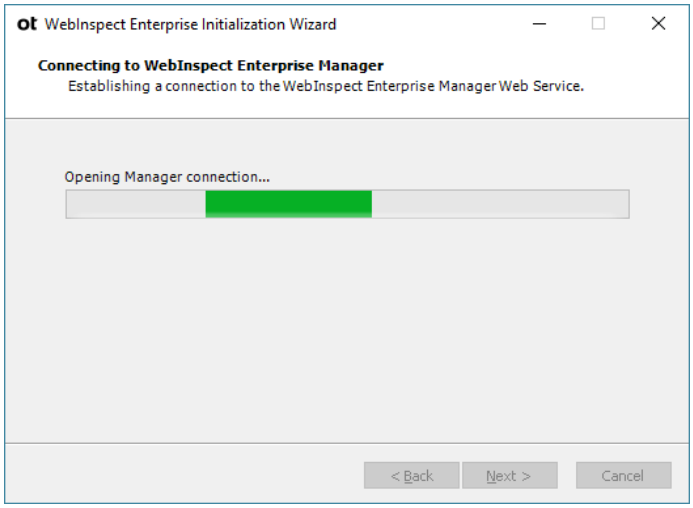


   Otherwise, the current user is added as the first Fortify WebInspect Enterprise system administrator and the procedure continues with the Decoupling from SSC window after Step 3.

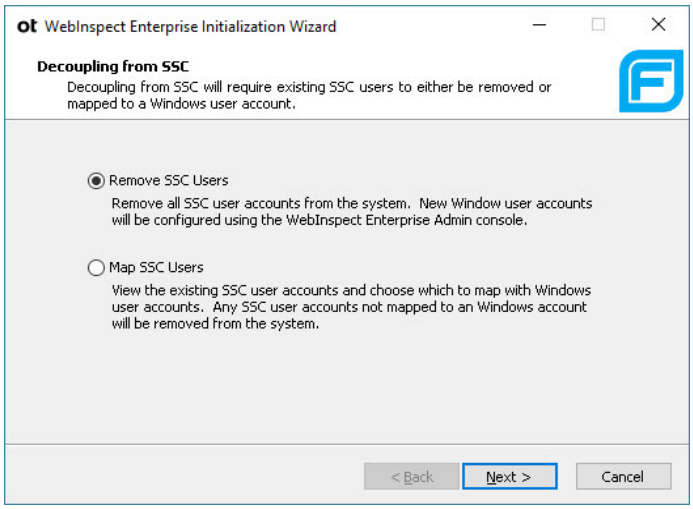
3. On the Administrator Role Page, select the **Add Current User to System Administrator Role** check box to make the current user a Fortify WebInspect Enterprise system administrator.

   Important! If you do not select this option, then the current user cannot map Fortify Software Security Center users to Windows accounts.

The Connecting to WebInspect Enterprise Manager screen appears until the connection is made.

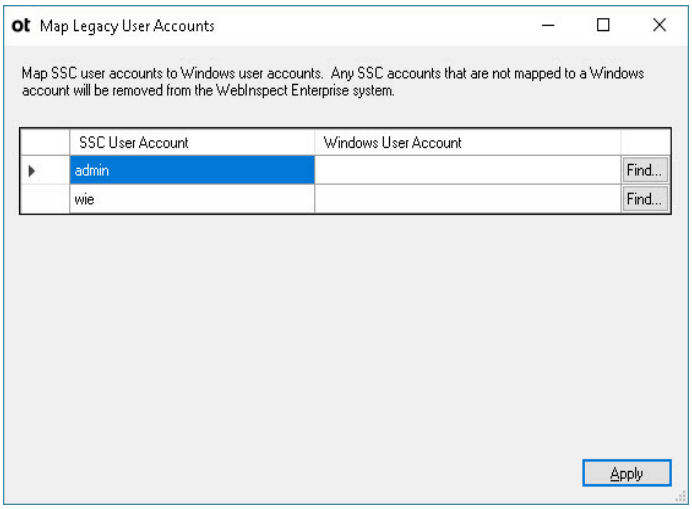


The Decoupling from SSC window appears.



4. Do one of the following:
   - To remove all Fortify Software Security Center user accounts from the system:
     i. Select **Remove SSC Users**.
     ii. Click **Next**.
   - To view the list of existing Fortify Software Security Center user accounts and choose the accounts to map to Windows user accounts:
     i. Select **Map SSC Users**.
     ii. Click **Next**.

     The Map Legacy User Accounts window appears.



iii. In the **Windows User Account** column, type the user account that you want to map to each SSC User Account.

> **Note:** You can click **Find...** to search for NT users to map.

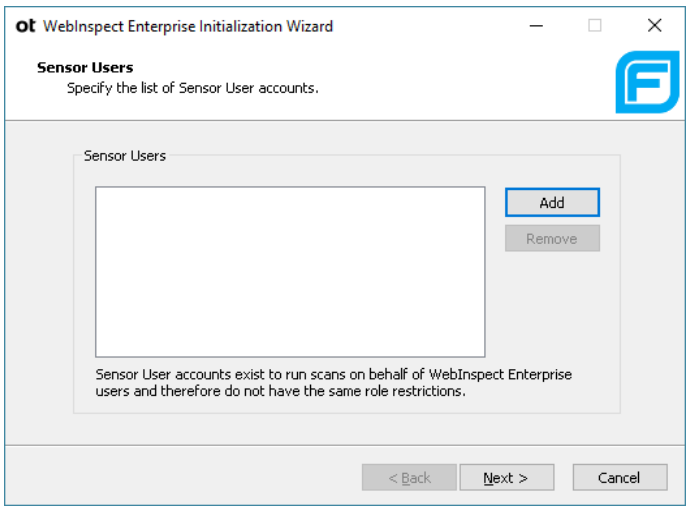
iv. Click **Apply**.

v. If you do not map all Fortify Software Security Center users, a message appears asking if you want the unmapped users to be removed from WebInspect Enterprise. Do one of the following:

- Click **Yes** to remove the unmapped users.
- Click **No** and map the remaining users.

Adding Sensor Users

After Fortify WebInspect Enterprise is initialized, the Sensor Users window appears.



Optionally add at least one sensor user for Fortify WebInspect Enterprise to use to run scans. Sensor users must not be general console users and they must have been previously created as Windows users as described in "Preparing to Install Fortify WebInspect Enterprise" on page 15.

You do not have to add any sensor users to Fortify WebInspect Enterprise at this point, but you will need to specify at least one sensor user before you can run any scans. Post-installation configuration procedures in this document also describe how to add sensor users.

To add a sensor user to Fortify WebInspect Enterprise now:

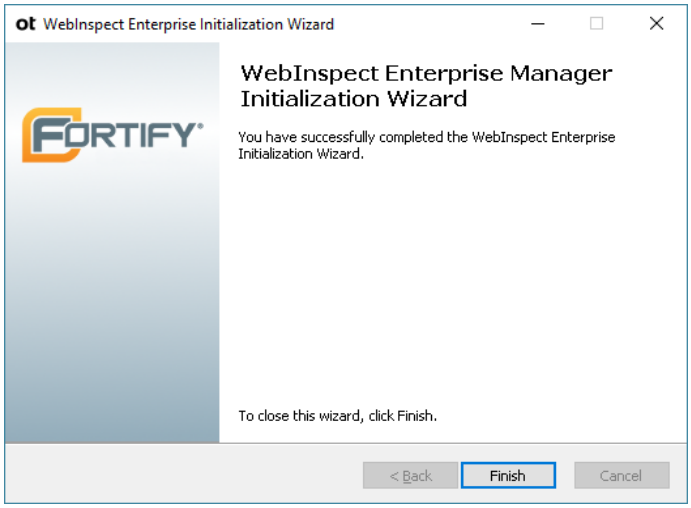
1. Click **Add**.
2. In the Select Users or Groups dialog box, type the name of an existing user to add (see "Preparing to Install Fortify WebInspect Enterprise" on page 15), in the format localhost\user or domain\user. If you specify only the user, you can click **Check Names** to help identify the localhost or domain.
3. Click **OK**.
4. Verify that the sensor user you specified has been added to the list of Sensor Users in the window.

Completing Initialization

To complete the initialization process:

1. Click **Next**.

   The Initialization Wizard completes.



2. Click **Finish**.

   The Initialization Wizard closes.

Important Information about Upgrading WebInspect

After decoupling from Fortify Software Security Center, you must upgrade Fortify WebInspect to 23.2.0 if you plan to connect it to Fortify WebInspect Enterprise. Connecting a previous version of

Fortify WebInspect, such as version 22.2.0, with a decoupled Fortify WebInspect Enterprise can cause known issues with certain functionality.

What's Next?

Continue with "Configuring Services" below.

Configuring Services

Use the Fortify WebInspect Enterprise Services Configuration Utility to configure or modify services associated with Fortify WebInspect Enterprise. Make sure the services are started even if you do not change any options.

To start the utility, click **Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Services Manager**.

After the utility starts, the following buttons appear in the left column:

- **Scan Uploader Service** - Handles the transfer of scans from Fortify WebInspect to Fortify WebInspect Enterprise.
- **Task Service** - Monitors the queue for various tasks, including Fortify Software Security Center application version updates and Fortify Software Security Center issue synchronization (if applicable).
- **Scheduler Service** - Handles the scheduling of scans, discovery scans, and smart updates.

Perform the procedures in the following sections after selecting each of these services.

Configuring the Scan Uploader Service

If the Fortify WebInspect Enterprise Scan Uploader Service was selected for installation as described in "Installing the Fortify WebInspect Enterprise Server Software" on page 25, Fortify WebInspect can scan a website and export the scan results to a location called a “dropbox.” The Scan Uploader Service accesses each dropbox periodically and, if files exist, it uploads those files to the Fortify WebInspect Enterprise Manager.

Service Status

This area of the interface displays the current status of the Scan Uploader service. You can start, stop, restart, or configure the service.

To configure the service:

1. Click **Configure** in the Service Status section.
   The Configure Service window appears.

2. Select which credentials should be used for logging on to the service:
   - **Local System account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.
   - **This account** - An account identified by the credentials you specify.
3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Fortify WebInspect Enterprise Configuration

This area of the interface displays the Fortify WebInspect Enterprise configuration.

To configure Fortify WebInspect Enterprise:

1. Click **Configure** in the WebInspect Enterprise Configuration section.

   The WebInspect Enterprise Configuration window appears.
2. Enter the URL of the Fortify WebInspect Enterprise Manager.
3. Provide the Fortify WebInspect Enterprise Manager's authentication credentials.
4. To verify that the user name and password are correct, click **Test**.
5. If the Scan Uploader service uses a proxy, select **Enable Proxy** and provide the requested information.
6. Click **OK**.

Dropbox Configuration

Fortify WebInspect can scan a website and export the scan results to a location called a “dropbox.” The purpose of the Fortify WebInspect Enterprise Uploader service is to access each dropbox periodically and, if files exist, to upload those files to the Fortify WebInspect Enterprise Manager.

To create a dropbox:

1. Click **Add** in the Dropbox Configuration section.

   The Configure Dropbox window appears.
2. Enter a dropbox name.
3. Enter the full path and name of the folder that will be used as the dropbox (or click **Browse** to select or create a folder).
4. Be sure to select or create a folder that will not be used for any other purpose.
5. Enter the application version that will be serviced by this dropbox.
6. Click **OK**.

Logging Configuration

This area of the interface displays current settings for the logging function.

To configure settings:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration widow appears.
2. The logging output is contained in `UploaderService_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location**

     The default location is `C:\ProgramData\HP\WIE\UploaderService`
   - **Enter location for log file**

     Type a path to the folder that will contain the logs, or click **Browse** to select a location.
3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.

   When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `UploaderService_trace.log`, `UploaderService_trace.log.1`, etc.
6. Click **OK**.

Start the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Configuring the Task Service

Configure the Task Service to monitor the queue for various tasks, including Fortify Software Security Center application version updates and Fortify Software Security Center issue synchronization (if applicable).

Service Status

This area of the interface displays the current status of the Task service, which handles background tasks such as Fortify Software Security Center application version updates and Fortify Software Security Center issue synchronization (if applicable). You can start, stop, restart, or configure the service.

To configure the service:

1. Click **Configure** in the Service Status section.

   The Configure Service window appears.

2. Select which credentials should be used for logging on to the service:
   - **Local System account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.
   - **This account** - An account identified by the credentials you provide.
3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Database Configuration

This area of the interface displays the database server name and database name.

To configure the database:

1. Click **Configure** in the Database Configuration section.

   The Database Configuration window appears.
2. Enter a server name.
3. Specify the account under which Fortify WebInspect Enterprise will connect to the database.
   - **Windows Authentication** - The name and password specified in the Fortify WebInspect Enterprise Manager's user account is used to authenticate to the database. When working in a domain environment, the Fortify WebInspect Enterprise Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the Fortify WebInspect Enterprise Manager and the database computers.
   - **SQL Authentication** - Enter the SQL Server user name and password.
4. Enter or select a database.
5. Click **OK**.

Logging Configuration

This area of the interface displays current settings for the logging function.

To configure settings:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration window appears.
2. The logging output is contained in `TaskService_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location**

     The default location is `C:\ProgramData\HP\WIE\TaskService`

- **Enter location for log file**

  Type a path to the folder that will contain the logs, or click **Browse** to select a location.

3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.
6. When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `TaskService_trace.log`, `TaskService_trace.log.1`, etc.
7. Click **OK**.

Fortify Software Security Center Poll Interval

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center (SSC), this area of the interface determines how often Fortify WebInspect Enterprise contacts Fortify Software Security Center for updates.

1. In the **SSC application version updates polling interval (in seconds)** field, specify how frequently Fortify WebInspect Enterprise contacts Fortify Software Security Center to check for application version name changes or deletions.
2. In the **SSC issue synchronization interval (in minutes)** field, specify how frequently Fortify WebInspect Enterprise contacts Fortify Software Security Center to check for changes to audit information, comments, attachments, and “not an issue” and “suppressed” status.
3. Click **Apply**.

Start the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Configuring the Scheduler Service

Configure the Scheduler Service to handle the scheduling of scans, discovery scans, and smart updates.

Service Status

This area of the interface displays the current status of the Scheduler service. You can start, stop, restart, or configure the service.

To configure the Scheduler service:

1. Click **Configure** in the Service Status section.

   The Configure Service window appears.

2. Select which credentials should be used for logging on to the service:
   - **Local System account** - This account is a predefined local account used by the service control manager (SCM). It has extensive privileges on the local computer, and acts as the computer on the network. A service that runs in the context of the Local System account inherits the security context of the SCM.
   - **This account** - An account identified by the credentials you specify.
3. If you select **This account**, enter an account name and password.
4. Click **OK**.

Fortify WebInspect Enterprise Manager

If the Fortify WebInspect Enterprise Manager URL is changed using IIS or another tool, change the URL here as well.

Logging Configuration

This area of the interface displays current settings for the logging function.

To configure settings:

1. Click **Configure** in the Logging Configuration section.

   The Logging Configuration window appears.
2. The logging output is contained in `Scheduler_trace.log`. To specify the location of the logs, choose one of the following:
   - **Default location**

     The default location is `C:\ProgramData\HP\WIE\Scheduler`
   - **Enter location for log file**

     Type a path to the folder that will contain the logs, or click **Browse** to select a location.
3. For the logging level, choose either **INFO** (the default) or **DEBUG** (which records more data).
4. In the **Max file size** field, specify the maximum file size of a log file (in megabytes).
5. In the **Number of backup files** field, specify the maximum number of log files that will be retained.

   When a log file reaches its maximum size, Fortify WebInspect Enterprise closes it and opens another file, repeating this process until the maximum number of log files is created. When that file is full, Fortify WebInspect Enterprise closes it, deletes the oldest file, and opens a new one.

   Files are named in sequence: `Scheduler_trace.log`, `Scheduler_trace.log.1`, etc.

Start the Service

Click **Start** in the Service Status section to start the service if it is not already running.

Post Configuration

After configuring the services, close the WebInspect Enterprise Services Configuration utility.

Installing the Fortify WebInspect Enterprise Administrative Console

For system requirements and notes about the Fortify WebInspect Enterprise Administrative Console, see the *Fortify Software System Requirements*.

To install the Fortify WebInspect Enterprise Administrative Console, along with the various Fortify WebInspect Enterprise tools:

1. Launch the WIE Console installation file.

   Note: If the wizard detects an earlier version of the Administrative Console, uninstall that version using Control Panel and then relaunch the installation file.

   The Welcome screen of the WebInspect Enterprise Console Setup wizard appears.
2. Click **Next**.

   The End-User License Agreement window appears.
3. Review the license agreement. If you accept it, select the check box and click **Next**; otherwise click **Cancel**.

   If you accept the license agreement, the Destination Folder window appears.
4. Accept the default location or click **Change** to select the location where you want to install the software, and click **Next**.

   The Ready to install WebInspect Enterprise Console window appears.
5. When you are ready to install, click **Install**.

   After the Fortify WebInspect Enterprise Administrative Console files are installed, the Console Setup Wizard completes.
6. Click **Finish**.

Logging on to the Administrative Console

To log on to the Fortify WebInspect Enterprise Administrative Console, which is also known as the Fortify WebInspect Enterprise Console:

1. If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, make sure that Fortify Software Security Center is running and that a Fortify Software Security Center administrator is logged on.

2. Do one of the following:
   - Click **Start > Fortify WebInspect Enterprise 23.2.0 Console**.
   - Click **Start > Fortify > Fortify WebInspect Enterprise 23.2.0 Console > Fortify WebInspect Enterprise 23.2.0 Console**.

   The Log On to WebInspect Enterprise window appears.

   Note: This window does not appear for subsequent logins if you select the option **Automatically log on when this application starts**.
3. Using the **Log on to** list, enter or select the URL of the Fortify WebInspect Enterprise manager. In this case, the value can be `https://localhost/WIE`.
4. Enter the **Username** and **Password** for an account that has permission to access the Administrative Console.

   Note: If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, you can initially specify the Fortify Software Security Center Administrator you specified in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34.

   If Fortify WebInspect Enterprise is not integrated with Fortify Software Security Center, you can specify the user who was added to the System Administrator Role on the Administrator Role Page, as described in "Installing or Upgrading a Standalone Fortify WebInspect Enterprise" on page 40 or "Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center" on page 45.

   Thereafter, you can add other Fortify WebInspect Enterprise administrators, as described in "About Assigning Administrators and Roles" on page 69 and in the Fortify WebInspect Enterprise online Help.
5. Optionally, select the **Save password** option.
6. Optionally, select the **Automatically log on when this application starts** option.
7. To go through a proxy server to reach the Fortify WebInspect Enterprise manager:
   a. Click the **Proxy** tab.
   b. Select one of the following:
      - **Use the System proxy** (to use the proxy server information from the local machine).
      - **Use the proxy below**, and then provide the proxy server's IP address and port number.
   c. Provide a valid **Username** and **Password**.
8. Click **OK**.

   Note: If you see a message indicating that the server refused the request, you may have entered your user name and password incorrectly, or your account may not have been assigned to a role.

Using the Administrative Console

For information about using the capabilities of the Administrative Console, see its online Help.

Post-Installation Configuration

After Fortify WebInspect Enterprise installation procedures are complete, perform the configuration procedures in the following sections as needed:

- "Installing Fortify WebInspect as a Sensor" below
- "Adding Sensor Users (if Not Previously Done)" on page 68
- "Enabling Sensors and Configuring Sensor Permissions" on page 68
- "About Assigning Administrators and Roles" on page 69
- "Moving Application Versions from the Default Group" on page 71
- "Configuring Manual Publishing of Scans to Fortify Software Security Center, if Necessary" on page 71

Installing Fortify WebInspect as a Sensor

Note: For additional information about installing Fortify WebInspect, see the *OpenText™ Fortify WebInspect Installation Guide*.

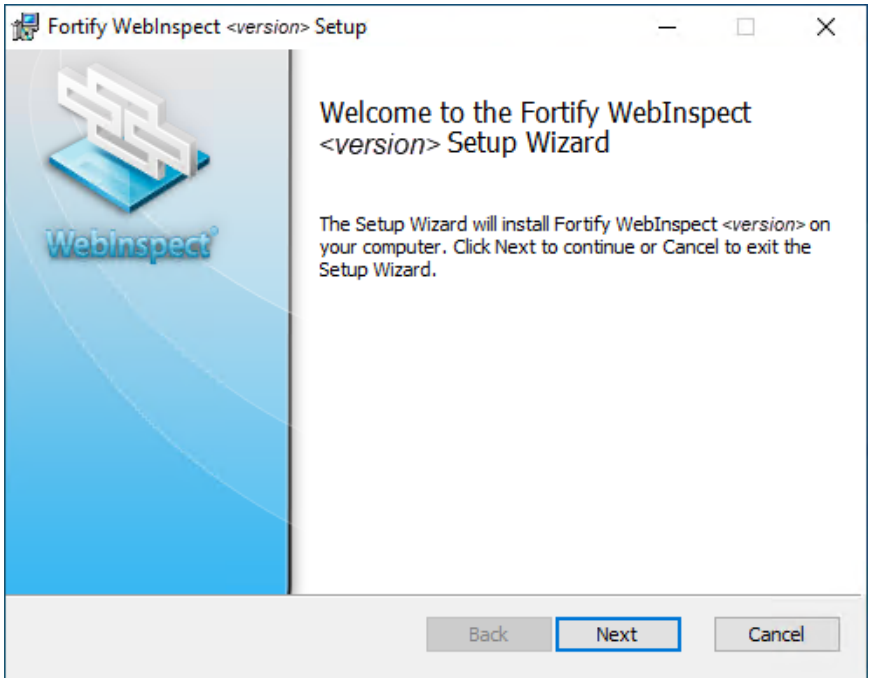
If Fortify WebInspect Enterprise is not already connected to an instance of Fortify WebInspect that is configured as a sensor, install Fortify WebInspect as a sensor.

Important! Before you begin, verify that you have installed the required software listed in the *Fortify Software System Requirements*. This includes having SQL Express installed on the same machine as the sensor if you plan to use it for the sensor database. Otherwise, you must configure the sensor to use a remote SQL Server after installation.

To install Fortify WebInspect as a sensor:

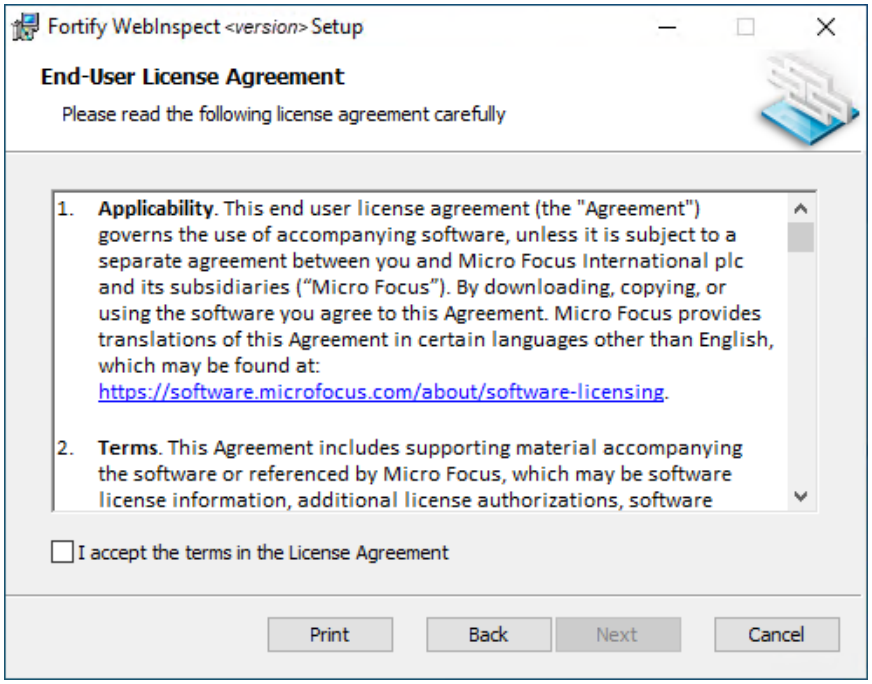
1. Launch the WebInspect 23.2.0 installation file.

   The Welcome screen of the Fortify WebInspect Setup wizard appears.



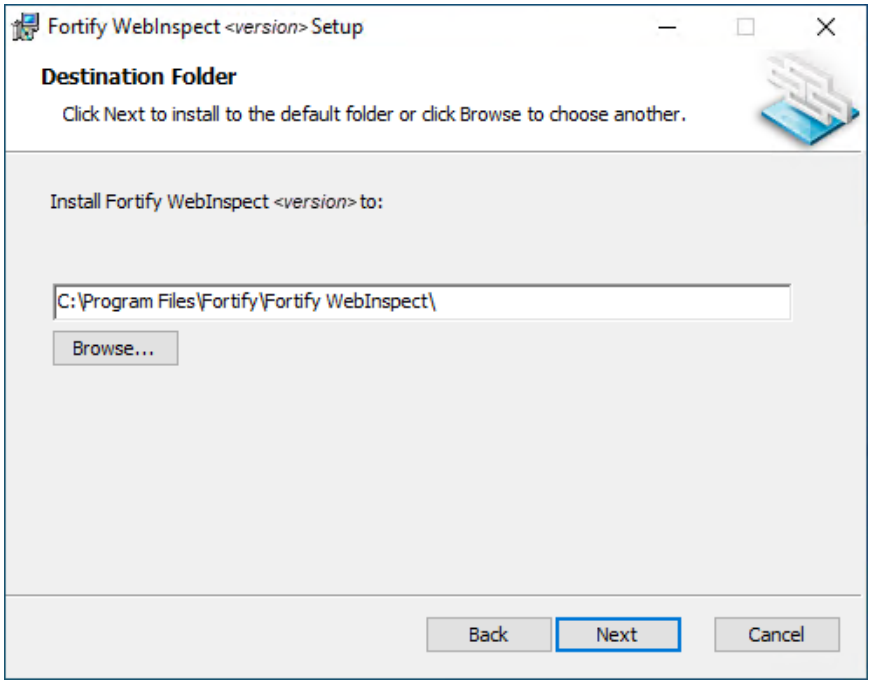
2. Click **Next**.

   The End-User License Agreement window appears.



3. Review the license agreement. If you accept it, select the check box and click **Next**; otherwise click **Cancel**.

If you accept the license agreement, the Destination Folder window appears.

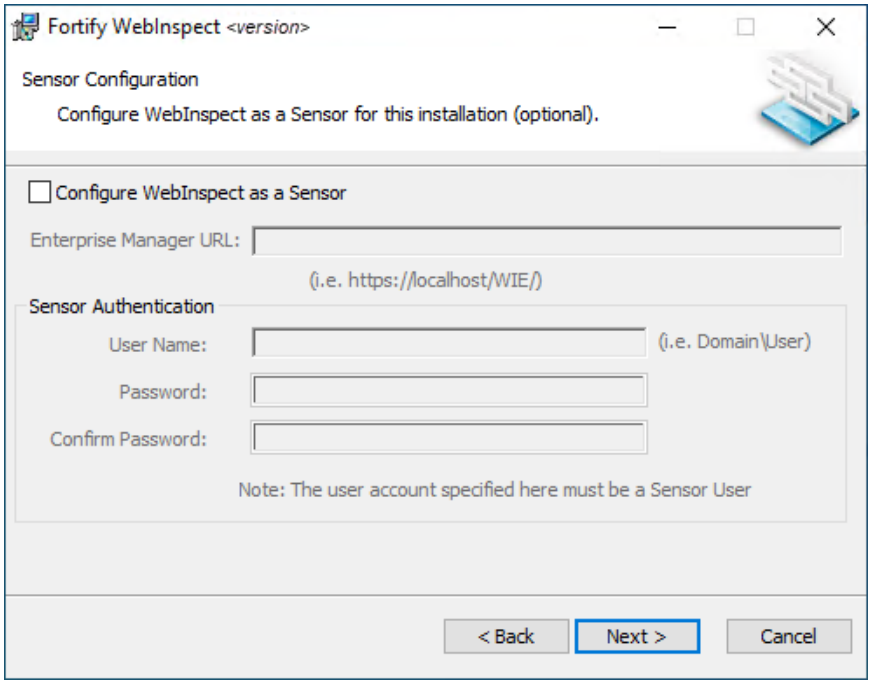


4. Accept the default location and click **Next**.

Important! When installing Fortify WebInspect as a sensor, you must use the default Destination Folder. Otherwise, SmartUpdates to the sensor will not work. The default Destination Folder is:

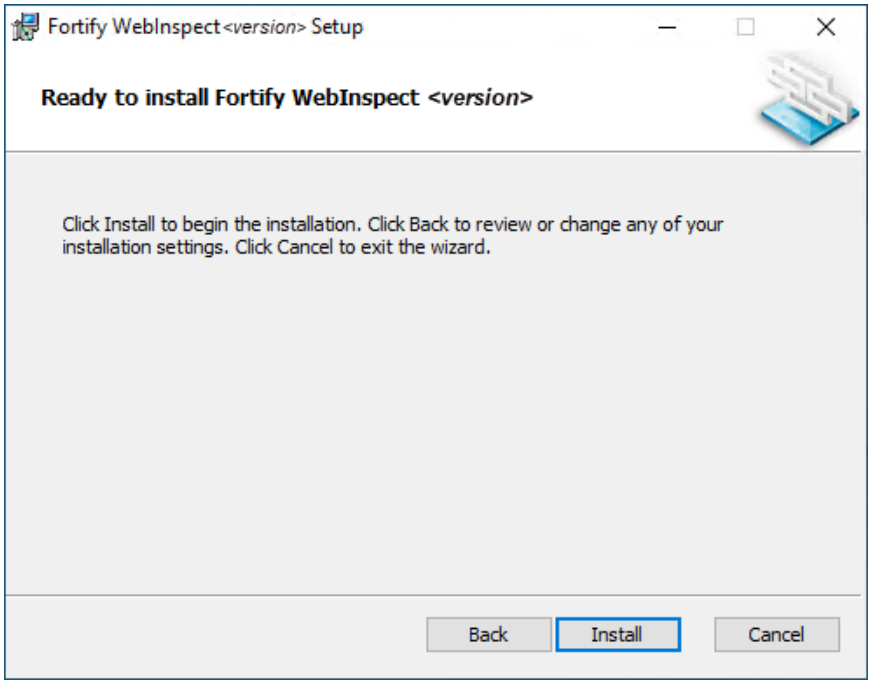
```
C:\Program Files\Fortify\Fortify WebInspect
```

The Sensor Configuration window appears.



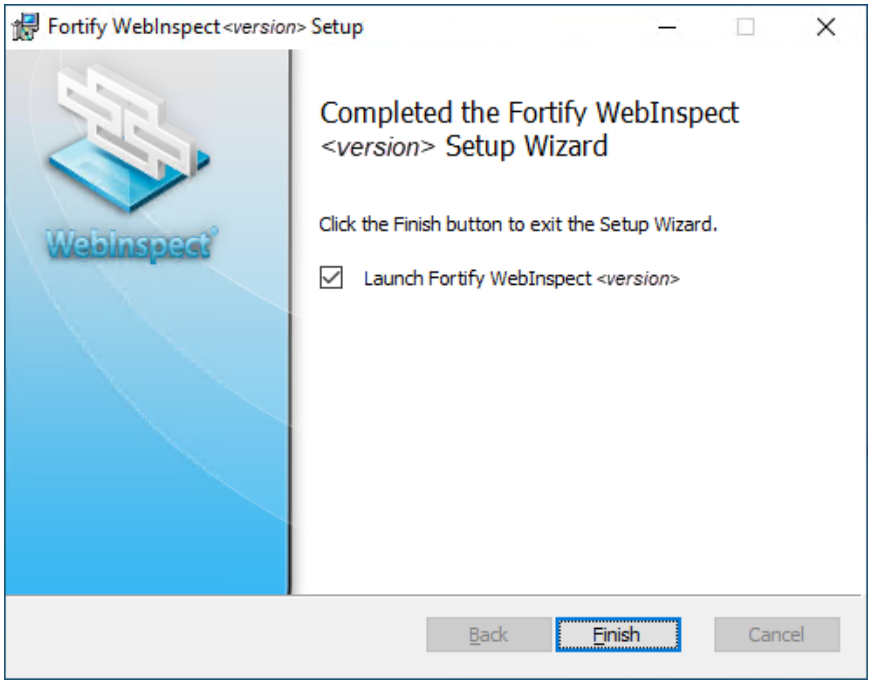
5. If you want to test the sensor User Name and Password credentials before starting the sensor service or you want to connect the sensor to a remote SQL Server, skip to Step 7 and do not configure Fortify WebInspect as a sensor at this time. In this case, you will install Fortify WebInspect, then configure Fortify WebInspect as a sensor, test the sensor credentials, and connect to a remote SQL server (if necessary).
6. Complete the fields on the **Sensor Configuration** window:
   - Select the **Configure WebInspect as a Sensor** option.
   - In the **Enterprise Manager URL** field, enter the Fortify WebInspect Enterprise URL.
   - In the **Sensor Authentication** section, enter the Windows account credentials of a sensor user for this sensor. For more information, see "Creating a Sensor User" on page 17.
7. Click **Next**.

The Ready to install Fortify WebInspect window appears.



8. When you are ready to install, click **Install**.
9. When the installation process is complete, clear the option to launch Fortify WebInspect and click **Finish**.

Note: You do not need to activate the license on the machine where the sensor is installed. Licensing for the sensor is covered by your Fortify WebInspect Enterprise license.



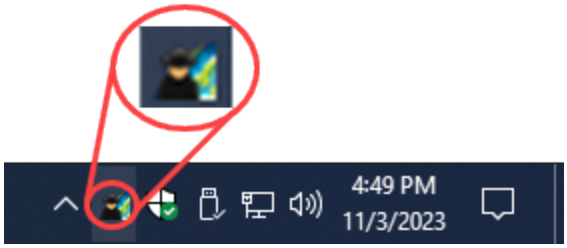
Configuring the Sensor, Testing Credentials, and Starting the Sensor Service

Important! We recommend that you perform these tasks in the following order:

1. Configure the sensor.
2. Test the sensor user name and password credentials.
3. Configure a remote SQL Server database, if needed.
4. Start the sensor service.

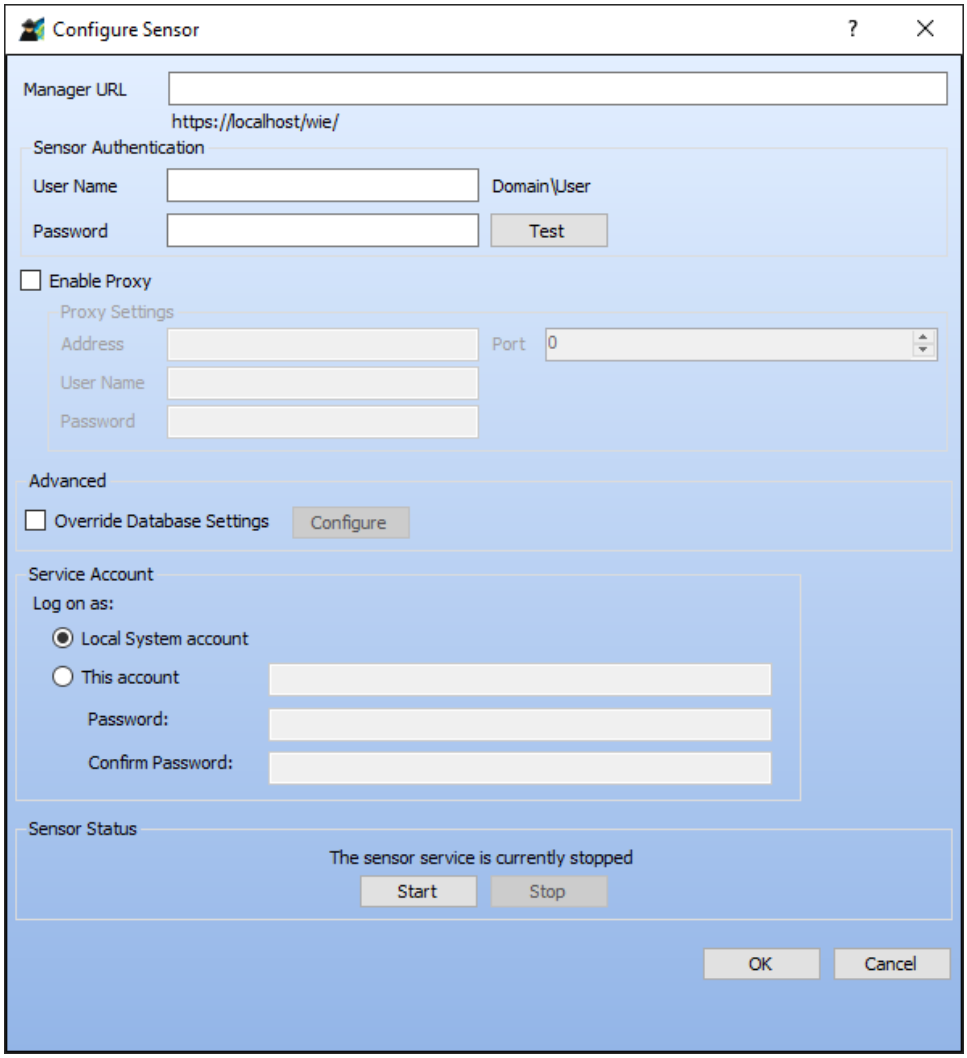
To perform these tasks:

1. On the machine where the sensor is installed, click **All Programs > Fortify > Fortify Monitor** to launch the Fortify Monitor program.
2. Click the Fortify Monitor icon in the task tray.



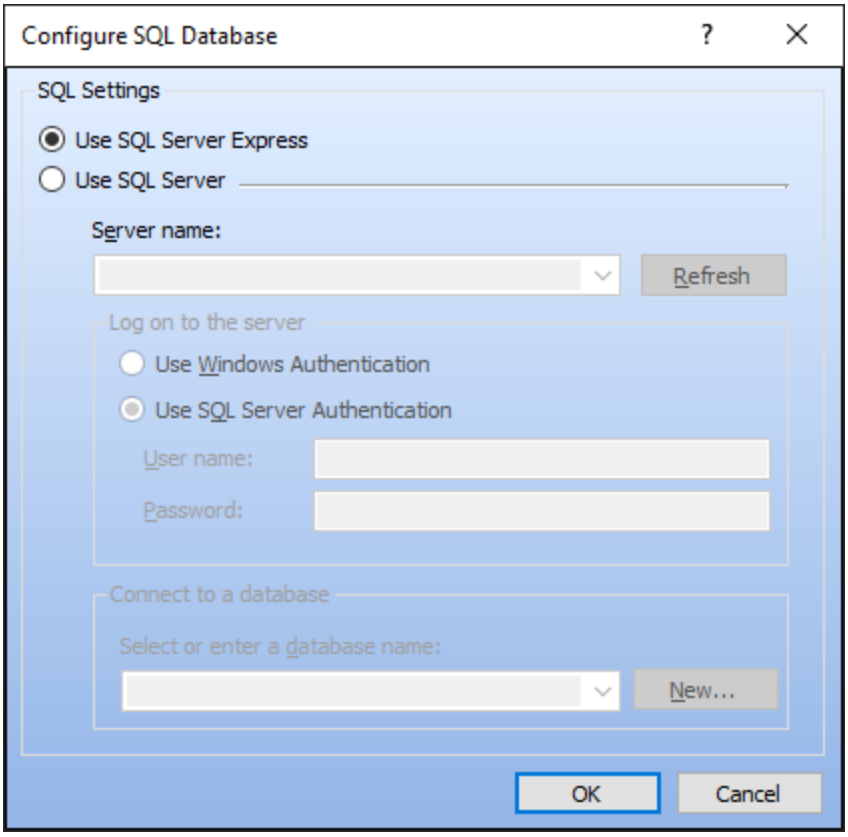
3. Click **Configure Sensor**.

The Configure Sensor window appears.



4. Complete the fields as follows:
   a. In the **Manager URL** field, enter the Fortify WebInspect Enterprise URL.
   b. In the **Sensor Authentication** section, enter the Windows account credentials of a sensor user for this sensor. For more information, see "Creating a Sensor User" on page 17.
   c. To test the credentials, click **Test**.
   d. If you need to configure a remote SQL Server, in the Advanced section click the **Override Database Settings** option, and then click **Configure**.

The Configure SQL Database window appears.



i. Select **Use SQL Server**.
ii. Select the server from the **Server name** drop-down list.
iii. In the Log on to the server section, configure authentication for the database.
iv. Click **OK**.

e. Back on the Configure Sensor window, complete the Service Account section as needed.
f. In the Sensor Status section, click **Start** to start the sensor service if it is stopped.

5. Click **OK**.

Continue with "Verifying Sensor Setup" below.

Verifying Sensor Setup

The Sensors shortcut in the Fortify WebInspect Enterprise Administrative Console should now list the sensor you just started. To verify the sensor setup:

1. In the Administrative Console, click **Sensors** in the left pane.
   The Sensors shortcut is selected.
2. Verify that the sensor is listed in the **Sensors** shortcut.

This completes the installation and configuration of Fortify WebInspect as a sensor. Go to "Adding Sensor Users (if Not Previously Done)" on the next page or "Enabling Sensors and Configuring Sensor Permissions" on the next page.

Adding Sensor Users (if Not Previously Done)

You must add at least one user that will be a sensor user on the Fortify WebInspect Enterprise server. At least one sensor user should have been created as a Windows user as instructed in "Creating a Sensor User" on page 17. If a sensor user was already added to Fortify WebInspect Enterprise during installation, proceed to "Enabling Sensors and Configuring Sensor Permissions" below.

Important! Sensor users must *not* be general console users.

To add a sensor user to Fortify WebInspect Enterprise:

1. Start the Administrative Console if you have not already done so. Click **Start > Fortify WebInspect Enterprise 23.2.0 Console** and log on.
2. Select **Administration** in the left pane and then select the **Sensor Users** shortcut.
3. Click **Add** in the Sensor Users form in the right pane.
4. In the Select Users or Groups window, type the name of an existing user to add (see "Creating a Sensor User" on page 17), in the format of localhost\user or domain\user. If you specify only the user, you can click **Check Names** to help identify the localhost or domain.
5. Click **OK**.
6. Verify that the sensor user you specified has been added to the list of Sensor Users in the dialog box.

Enabling Sensors and Configuring Sensor Permissions

Sensors cannot be used to run scans until you enable them and configure their permissions as follows:

1. In the Fortify WebInspect Enterprise Administrative Console, select **Sensors** in the left pane and verify that the localhost or domain of the sensor user you specified in Adding Sensor Users (as described in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34, "Installing or Upgrading a Standalone Fortify WebInspect Enterprise" on page 40, or "Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center" on page 45) or in "Adding Sensor Users (if Not Previously Done)" above has been added to the list of Sensors in the right pane.
2. Select the sensor in the list, click **Action**, and if the **Enable** option is available, click it.
3. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut.
4. Change organization permissions as follows:
   a. In the Security Group Hierarchy of the Roles and Permissions form in the right pane, select **Default Organization**.
   b. In the Organization Permissions section, select the **Resources** tab.
   c. In the Organization Resources section, in the **Object Type** drop-down list, select **Sensors**.
   d. Select one or more sensors in the **Available** column and click **>** to move the sensors you selected to the **Allowed** column, or click **>>** to move all the **Available** sensors to the **Allowed** column.

5. Change group permissions as follows:
   a. In the Security Group Hierarchy of the Roles and Permissions form, select **Default Group**.

      Note: The Default Group is the lowest level in the hierarchy. For a Fortify WebInspect Enterprise upgrade, the customer might have previously renamed this level from its default value of **Default Group**.)

   b. In the Group Permissions section, select the **Resources** tab.
   c. In the Group Resources section, in the **Object Type** drop-down list, select **Sensors**.
   d. Select one or more sensors in the **Available** column and click **>** to move the sensors you selected to the **Allowed** column, or click **>>** to move all the **Available** sensors to the **Allowed** column.

About Assigning Administrators and Roles

A role is a named collection of permissions that administrators specify. The Roles and Permissions form enables you to assign administrators for three hierarchical security levels—Fortify WebInspect Enterprise System, organization, and group. Each level has at least one administrator.

Administrators at each level can define roles, assign users to roles, and configure other security-related parameters. By assigning other users to roles, administrators can give them access to the Fortify WebInspect Enterprise system while limiting the functions they are allowed to perform, considering security. A user can be a member of more than one role.

Each security level has categories of activities, and some of the categories are used in several levels. The set of activities in each category varies among categories. You can set the permission for an entire category or for its individual activities to Allowed, Unassigned, or Denied.

The roles for each security level (system, organization, and group) contain a different set of permission categories such a Policies, Blackouts, and Application Versions. Each category contains multiple permissions, such as Can Create, Can View, Can Update, Can Delete, etc.

System Level

Fortify WebInspect Enterprise system administrators have all permissions. Legacy system administrators from a Fortify WebInspect Enterprise upgrade could also be Fortify WebInspect Enterprise system administrators. No one else can log on to Fortify WebInspect Enterprise until a Fortify WebInspect Enterprise system administrator assigns other users to roles.

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the Fortify Software Security Center administrator you specified in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34 is the initial Fortify WebInspect Enterprise system administrator.

If Fortify WebInspect Enterprise is not integrated with Fortify Software Security Center and there was not an existing Fortify WebInspect Enterprise system administrator, the user who ran the initializer was automatically added as the initial Fortify WebInspect Enterprise system administrator.

A system administrator can:

- Add other users as system administrators
- Create, rename, and delete organizations
- Create roles that allow access to certain Fortify WebInspect Enterprise Administrative Console features and assign users to those roles (thereby limiting the functions a specific user may perform)

Organization Level

The system administrator who creates an organization automatically becomes an administrator for that organization.

An organization administrator can:

- Assign other users as organization administrators
- Determine which objects are available to that organization (for example, select which of the available scanning policies may be used by applications within an organization)
- Set the maximum priority level that can be assigned to scans conducted by this organization
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the Fortify WebInspect Enterprise Web Console
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one organization to another
- Create, rename, and delete applications

You are not required to configure multiple organizations. If you prefer, you may associate all applications with a single organization.

Group Level

The organization administrator who creates a group automatically becomes an administrator for that group.

A group administrator can:

- Assign other users as group administrators
- Determine which objects are available to that group (for example, select which of the scanning policies made available to the organization may be used by this group)
- Set the maximum priority level that can be assigned to scans conducted by this group (within the limits established for the organization's maximum priority level)
- Specify which URLs or IP addresses may be scanned by this group
- Create and assign users to roles, thereby limiting their ability to perform various functions or access certain features of the Fortify WebInspect Enterprise Web Console
- Copy objects (such as blackouts, policies, e-mail alerts, etc.) or move them from one group to another

After completing the procedures in this document, your first configuration priority should be to create the organization and group hierarchy, define hierarchical roles, assign users to those roles, and perform the other functions available from the **Administration** group, **Roles and Permissions** shortcut.

For detailed information about the hierarchy and roles, see the online Help.

Moving Application Versions from the Default Group

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center and an application version is created in Fortify Software Security Center, it is also created automatically in Fortify WebInspect Enterprise. The new application version is added to the Default Group in the Default Organization in Fortify WebInspect Enterprise. To view the application versions:

1. Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut.
2. In the Security Group Hierarchy of the Roles and Permissions form, select **Default Group**.

   Note: This is the lowest level in the hierarchy. For a Fortify WebInspect Enterprise upgrade, the customer might have previously renamed this level from its default value of **Default Group**.
3. In the Group Permissions section, select the **Move/Copy Objects** tab.
4. In the User Created Group Objects section, in the **Object Type** drop-down list, select **Application Versions**.
5. Click **Retrieve**.

   All the application versions are displayed.

If you want a different group to have access to a particular application version in Fortify WebInspect Enterprise, select the check box for the application version in the list of Object Results and click **Move**. In the Move Objects window, specify the **Target Organization** and **Security Group** and click **Move**.

Repeat this procedure as needed on an ongoing basis.

Configuring Manual Publishing of Scans to Fortify Software Security Center, if Necessary

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, new scans initiated from Fortify WebInspect Enterprise or Fortify Software Security Center are automatically published to Fortify Software Security Center. Other scans, such as scans that are manually imported into Fortify WebInspect Enterprise or uploaded to Fortify WebInspect Enterprise, can only be published manually.

If the Fortify WebInspect Enterprise URL or the Fortify Software Security Center URL settings that you initially specified in "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34 have been changed (or are ever changed in the future), then to manually publish scans to Fortify Software Security Center, the settings must be correspondingly updated in the Administrative Console. See the Administrative Console Help topic for configuring settings for Fortify Software Security Center.

That Help topic, as well as "Disabling Automatic Publishing of Scans to Fortify Software Security Center" on page 91, describe how to *disable* the automatic publishing of scans to Fortify Software Security Center if you need to do so.

About the WebInspect Enterprise Desktop Application

The WebInspect Enterprise Desktop Application enables you to perform the following tasks:

- Use Guided Scan for Web sites and mobile devices
- View scan results and the Traffic Monitor
- Import a scan
- Generate reports

Before you can perform these tasks, you must download and install the application. For more information, see the Fortify WebInspect Enterprise Web Console help or the *Fortify WebInspect Enterprise User Guide*.

Important! If you previously downloaded the WebInspect Enterprise Desktop Application from Fortify WebInspect Enterprise 22.2.0, you must download and install the application again after upgrading to get the 23.2.0 version.

Timestamps and Effect of Time Zones on Schedules

For some installations, the Fortify WebInspect Enterprise Manager, the Administrative Console, and/or the Web Console reside in different time zones. To accommodate this, the Fortify WebInspect Enterprise Manager uses Coordinated Universal Time (also known as Greenwich Mean Time or Zulu time) for all time storage and manipulation. When a time is to be displayed on the Administrative Console or the Web Console, the Fortify WebInspect Enterprise Manager converts the time to conform to the time zone in which the console resides. Alert emails, however, are timestamped according to the time zone in which the Fortify WebInspect Enterprise Manager resides.

Universal Time does not honor Daylight Saving Time. Therefore, scheduled scan times will change by one hour after the transition between Daylight Saving Time and standard time. For example, suppose you schedule a scan to occur daily at 4 p.m. and you are in the Eastern time zone of the United States during the Daylight Saving Time period. The Fortify WebInspect Enterprise Manager records the settings and will begin the scan each day at 8 p.m. Universal Time (which is the equivalent of 4 p.m. Eastern daylight time). However, when the transition to standard time occurs, your scheduled scan will begin at 3 p.m. local time instead of 4 p.m. Even though you set your clocks back one hour, the Universal Time does not change.

About the REST API

As part of the installation, a REST API service is installed. The Fortify WebInspect Enterprise REST API is fully described and documented using the industry-standard Swagger RESTful API Documentation Specification version 2.0 (now known as OpenAPI Specification). The Swagger documentation provides detailed schema, parameter information, and sample code to simplify consumption of the REST API. It also provides functionality for testing the endpoints before using them in production.

REST API Categories

The REST API endpoints and methods are organized into categories, as described in the following table.

Note: Some endpoints have been refined since their initial release. These refinements have been made in new endpoints so that the changes do not break any existing customer implementations. The new endpoints have been added to categories appended with the number 2, such as ScanSchedule2. The updated endpoints also have "v2" in the api endpoint path, such as `POST/api/v2/scanTemplates`.

Category	Description
Authentication	Work with an authentication token to be cached and used at the start of an API session.
Blackout	Work with blackouts for scans, including updating and deleting existing blackouts in the database and saving a new blackout.
Configuration	Retrieve values for settings currently in use in Fortify WebInspect, Fortify WebInspect Enterprise, and Fortify Software Security Center or in the object being created, such as a new scan schedule.
Macro	Work with macros for scans, including updating and deleting existing macros in the database and saving a new macro.
Organization	Retrieve organization information for all existing organizations or a specific organization by ID or name.
Permission	Retrieve permissions for the user. You cannot edit permissions using the API.
Policies	Retrieve one or more policies. You cannot edit policies using the API.
Project	Retrieve application information for all existing applications or a specific

Category	Description
	application by ID or name. You cannot edit application information using the API.
ProjectVersion	Work with application versions, including updating and deleting existing application versions in the database and saving a new application version.
Scan	Work with scans, including updating and deleting existing scans in the database and saving a new scan.
ScanRequest	Work with scan requests, including updating an existing scan request in the database and downloading scan request attachments.
ScanSchedule	Work with scan schedules, including updating and deleting existing scan schedules in the database and saving a new scan schedule.
ScanTemplate	Work with scan templates, including updating and deleting existing scan templates in the database and saving a new scan template.
SecurityGroup	Retrieve security group information for all existing security groups or a specific security group by ID or name.
Sensor	Retrieve a sensor by ID, or a list of all sensors or sensors for a security group.
Status	Determine the status of the API endpoint.
TempFile	Work with a temporary file, including adding file content and saving a file temporarily for use in a scan or scan template.
Token	Retrieve an authentication token.
User	Work with Fortify WebInspect Enterprise users, including retrieving and deleting lists of users or individual users by ID.

Accessing the REST API

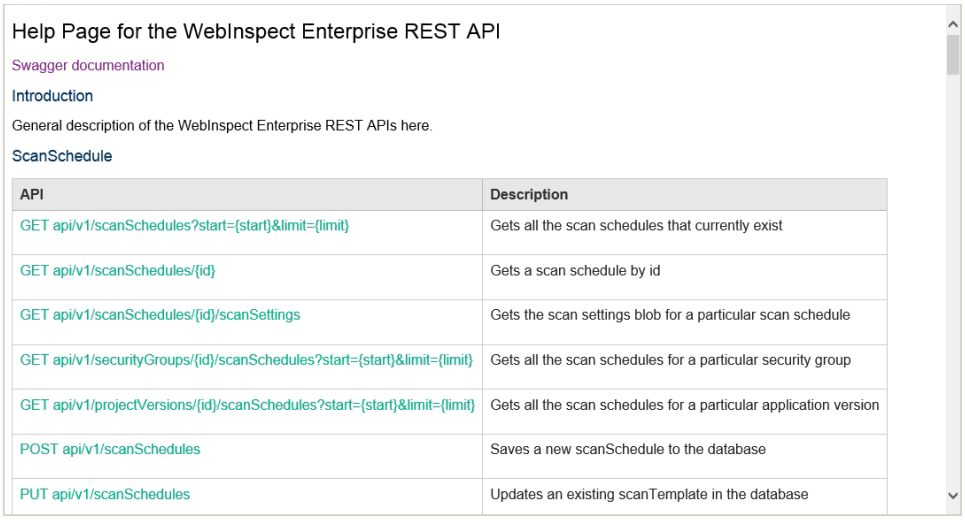
To access the Fortify WebInspect Enterprise REST API and its documentation:

1. In a browser window, navigate to `https://<computer name>/<Virtual Directory name>/REST`.

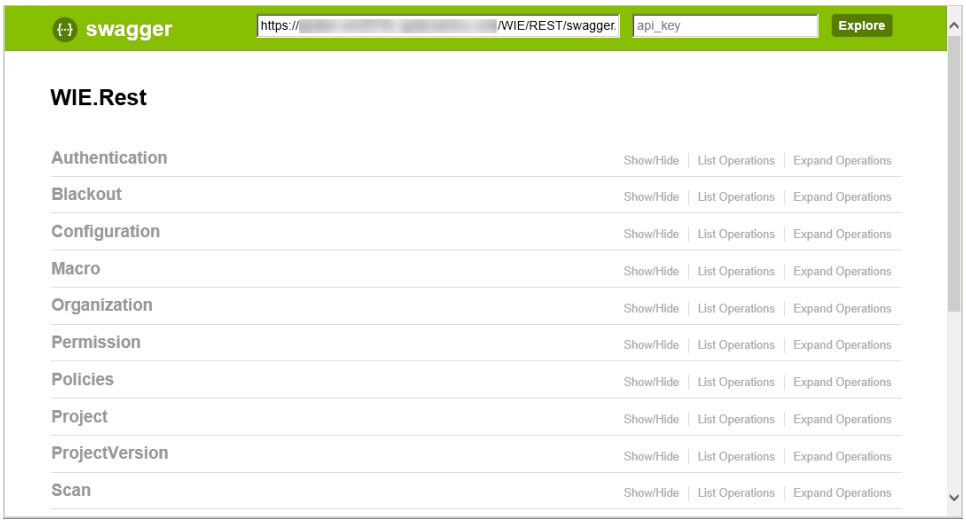
   Example:

   ```
   https://localhost/WIE/REST
   ```

The list of REST API methods appears, organized by category.



2. Do one of the following:
   - To view the specifics for a REST API method, click the method name.
     The detail page for the method appears.
   - To access the Swagger documentation and Swagger UI, click **Swagger documentation**.
     The Swagger UI page appears.



Using the Swagger UI

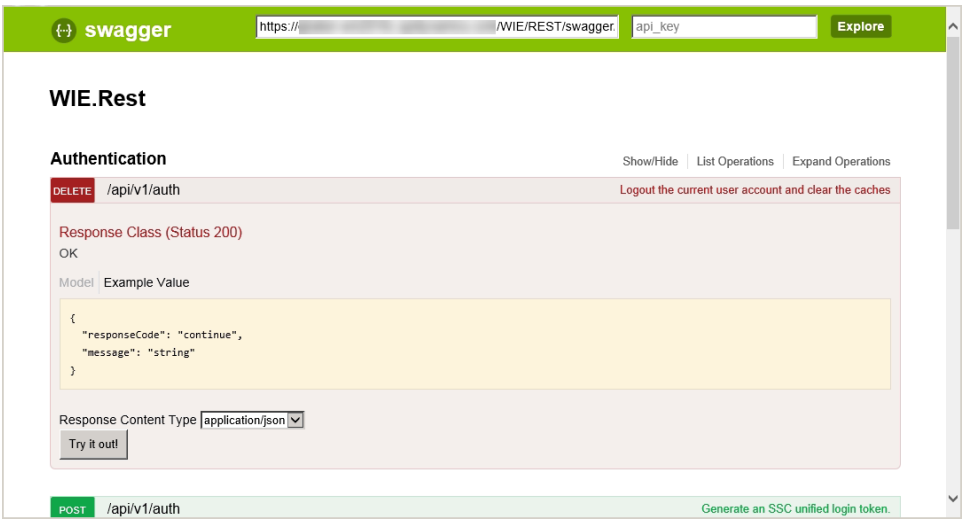
You must be authorized to work with scans, application versions, etc. Therefore, when testing REST API endpoints in Swagger, you must first make an Authentication POST and get a 200 response status code. Otherwise, all subsequent endpoint tests will fail.

For standalone WebInspect Enterprise installations, the username field requires Windows authentication. The user name must be formatted as `Domain\\firstname.lastname`. You must use the double backslashes (`\\`) because a single backslash (`\`) will not work.

To use the Swagger UI:

1. On the Swagger UI page, click an endpoint category.
2. Click the endpoint method to use.

   The page displays detailed schema, parameter information, sample code, and functionality for testing the endpoint.

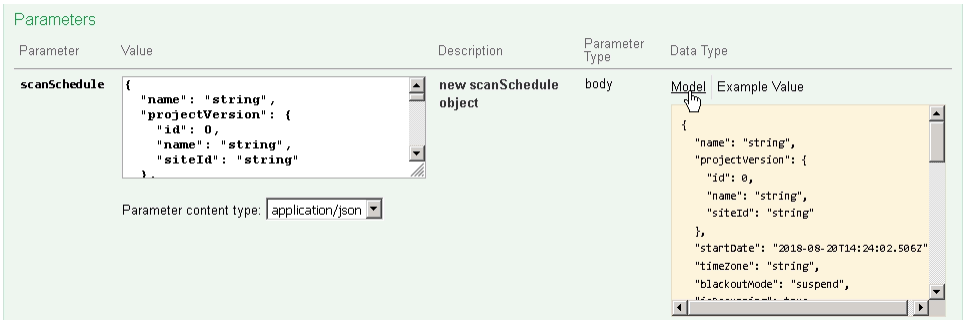


Getting Field-level Details

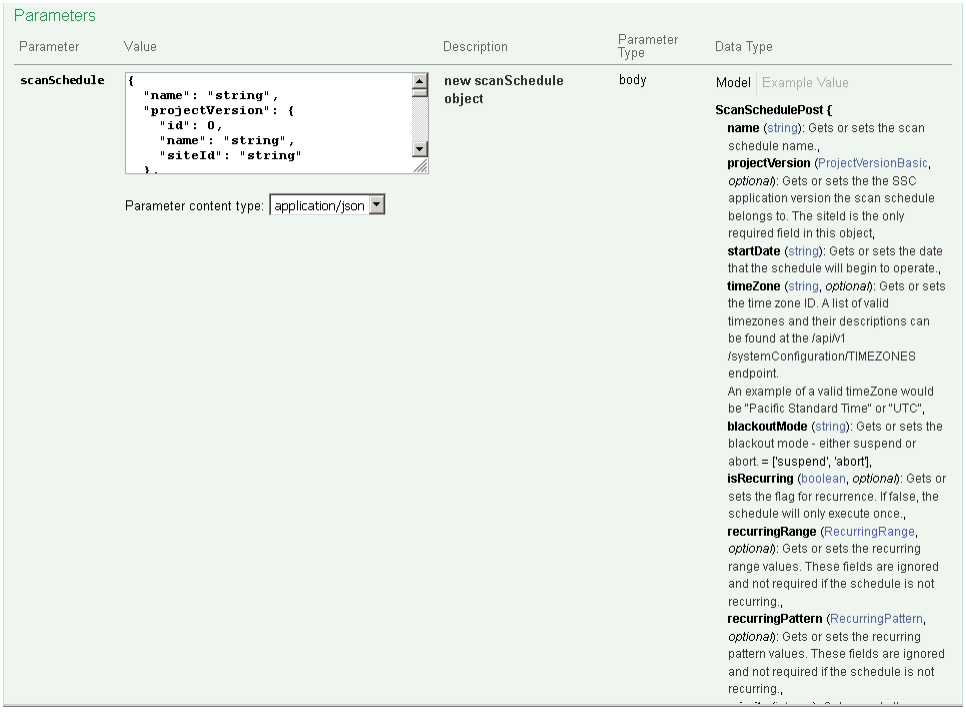
Some API endpoints have numerous fields that you can configure. These fields are documented in detail in the Swagger UI.

To view the field-level details:

- In the **Parameters** section of the endpoint, click **Model** under the **Data Type** heading.



Additional details for all the endpoint fields appear.



Installations Lacking Internet Connection

All OpenText security products contain digital certificates of authority. When a product starts, the operating system attempts to connect to the Internet and download a certificate revocation list (CRL) from the certificate's issuing authority (Sectigo) to determine if the product's certificate has been revoked. If the product cannot establish an Internet connection, it waits until the request times out, which substantially lengthens the product's start-up time. This inability to verify the certificate also causes other problems, including:

- Services fail to start.
- Multiple instances of `scriptserver.exe` are spawned.
- Scans fail to complete.

To avoid the complications caused by a lack of Internet access, consider the following solutions:

- (Recommended) Manually download the required CRL and install it. See "Downloading and Installing a CRL" on the next page.
- Use Microsoft Windows Server Active Directory to store and publish a CRL.
- Disable CRL checking for the server.
- Change the default CRL timeout period for the Microsoft Cryptography API (CAPI).
- Disable all certificate revocation list (CRL) checking under **Internet Options** in the **Control Panel**. Refer to your Windows documentation for more information.

Downloading and Installing a CRL

The recommended solution for lack of Internet access is to manually download the CRL, and then install it to the local computer certificate store.

To download the CRL:

1. Open a browser.
2. Go to one of the following URLs:
   - http://crl3.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crl
   - http://crl4.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crl
3. Download and save the file.

   Note: Because the CRL is valid only for a limited time, you must retrieve a new CRL periodically.

To install the CRL:

Log on to the computer as a member of the local administrators group, and install the CRL to the local computer certificate store. Refer to your Windows documentation for more information.

Tip: You might need to select **Certificate Revocation List (*.crl)** as the file type when browsing your directories to locate the CRL file to install.

Chapter 3: Troubleshooting the Installation

The most common errors encountered when installing Fortify WebInspect Enterprise are shown as either a connection message error at the final phase of the Fortify WebInspect Enterprise Initialization wizard, or when the first connection attempt is made with a console. Most of these error messages are general in nature. Consulting the logs for either Fortify WebInspect Enterprise Initialize or Fortify WebInspect Enterprise Manager should give some indication as to the nature of the error. The suggestions below are the most common quick methods for resolving the issues.

For additional detailed information about server and database configuration for Fortify WebInspect Enterprise, see "Implementing Fortify WebInspect Enterprise" on page 86.

About Fortify WebInspect Enterprise Manager Logging

Use the Fortify WebInspect Enterprise logs to troubleshoot any errors that occur during the initialization process or when trying to use Fortify WebInspect Enterprise after installation. Increasing the verbosity of the logging is recommended in the event you need to send logs to Support for review.

The logs used for troubleshooting Fortify WebInspect Enterprise installations are:

- Fortify WebInspect Enterprise Initializer Log(s)
- Fortify WebInspect Enterprise Manager Log(s)
- Fortify WebInspect Enterprise Scheduler Service Log(s)
- Fortify WebInspect Enterprise Task Service Log(s)

These logs have a default 2MB size limitation and will keep a rolling set of five log files. Turning on DEBUG logging is recommended for troubleshooting, but it is best to reset logging to the default level of INFO after troubleshooting is complete.

Note: The Program Files directory paths used in these procedures assume that the default configuration was used during installation. These paths may vary if the default configuration was not used.

Changing Fortify WebInspect Enterprise Initializer Log Debug Settings

If initialization failed and you want to increase the logging level for Fortify WebInspect Enterprise Initializer:

1. Edit the `WIE-Initialize.exe.logging.config` file in the following directory:

   `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\Initializer`
2. Change the logging level from `"INFO"` to `"DEBUG"` in the following section:

```
<root>
        <level value="INFO"/>
        <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the `Initializer_trace.log` file in the following directory:

`C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\Initializer\`

If additional files are created, they will be named `Initializer_trace.log.1`, `Initializer_trace.log.2`, etc.

Changing Fortify WebInspect Enterprise Manager Log Debug Settings

Assuming Initialization succeeded, to increase the logging level for the Fortify WebInspect Enterprise Manager:

1. Edit the `Web.logging.config` file in the following directory:

   `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\ManagerWS\`
2. Change the logging level from `"INFO"` to `"DEBUG"` in the following section:

```
<root>
        <level value="INFO"/>
        <appender-ref ref="ASPNetOut"/>
        <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the `ManagerWS_trace.log` file in the following directory:

`C:\ProgramData\HP\WIE\Manager\`

If additional files are created, they will be named `ManagerWS_trace.log.1`, `ManagerWS_trace.log.2`, etc.

Changing Fortify WebInspect Enterprise Scheduler Service Log Debug Settings

You can change the logging level for the Fortify WebInspect Enterprise Scheduler Service using the Services Manager interface (**Start > WebInspect Enterprise Services Manager** or **Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Services Manager**). For more information, see "Configuring the Scheduler Service" on page 56.

If the Service Manager is unavailable or does not work, then to increase the logging level for the Fortify WebInspect Enterprise Scheduler Service:

1. Edit the `AmpScheduler.exe.logging.config` file in the following directory:

   `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\Scheduler`
2. Change the logging level from `"INFO"` to `"DEBUG"` in the following section:

```
<root>
        <level value="INFO"/>
        <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the `Scheduler_trace.log` file in the following directory:

`C:\ProgramData\HP\WIE\Scheduler`

If additional files are created, they will be named `Scheduler_trace.log.1`, `Scheduler_trace.log.2`, etc.

Changing Fortify WebInspect Enterprise Task Service Log Debug Settings

You can change the logging level for the Fortify WebInspect Enterprise Task Service using the Services Manager interface (**Start > WebInspect Enterprise Services Manager** or **Start > All Programs > Fortify > Fortify WebInspect Enterprise 23.2.0 > WebInspect Enterprise Services Manager**). For more information, see "Configuring the Task Service" on page 54.

If the Service Manager is unavailable or does not work, then to increase the logging level for the Fortify WebInspect Enterprise Task Service:

1. Edit the `AmpTaskService.exe.logging.config` file in the following directory:

   `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\Task Service`

2. Change the logging level from "INFO" to "DEBUG" in the following section:

```
<root>
        <level value="INFO"/>
        <appender-ref ref="RollingFile"/>
</root>
```

3. Save the file.

The logging output is located in the TaskService_trace.log file in the following directory:

C:\ProgramData\HP\WIE\TaskService

If additional files are created, they will be named TaskService_trace.log.1, TaskService_trace.log.2, etc.

Troubleshooting and IIS

This topic provides Fortify WebInspect Enterprise troubleshooting information related to IIS.

IIS Settings and File Permissions Used by Fortify WebInspect Enterprise

The folders in the following table are in the *<IIS Virtual Directory>*\WIE directory, which is the following physical directory by default:

```
C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\ManagerWS
```

Folder	IIS Authentication	Notes	File Permissions
\	Integrated		User is Network Service with 'read' access. WIE Service User must be a local administrator.
\App_GlobalResources	Integrated		
\App_Themes	Integrated		
\bin	Integrated		
\ClientBin	Integrated		
\GuidedSetup	Anonymous		
\Login	Anonymous	Getting a 401 status on this page means Anonymous auth has been disabled.	
\SmartUpdateService	Anonymous	Getting a 401 status when logging in to Smart Update means Anonymous auth has been disabled.	
\WebConsole	Integrated		

IIS Admin Service Must be Running

If you cannot connect to Fortify WebInspect Enterprise using the console after installation, in **Windows Administrative Tools > Services**, verify that the Internet Information Services (IIS) Admin

Service is running.

Restarting IIS Quick Commands

You must restart IIS during the troubleshooting steps to apply changes. Usually it is best to restart IIS whenever you make changes to the user rights for service accounts or user accounts related to the installation. The easiest method for restarting IIS is to use the following commands from the command prompt. The **iisreset** command will stop and start all the web sites and application pools running on the server. The additional options are self-explanatory.

- `iisreset`
- `iisreset /stop`
- `iisreset /start`

SQL Login

If the installation or initialization of the database is not successful, you must set up an SQL login. Then an SQL database user in the Fortify WebInspect Enterprise database must be assigned to the role “amp_server” and associated with that login. Fortify WebInspect Enterprise Initialize can then be run to specify the SQL login for connecting to the database.

Account Rights and Privileges

Make sure the user logged into the machine during installation is a member of the local administrators group.

Make sure the Fortify WebInspect Enterprise Manager User is a member of the local administrators group.

If the Windows installation has been locked down, then the Fortify WebInspect Enterprise Web Service may not have sufficient rights to run. A quick test is to have the Fortify WebInspect Enterprise App Pool run as the Local System account.

To set the application pool to run as another user:

1. Open the Internet Information Services (IIS) Manager.
2. In the Internet Information Services (IIS) Manager window, expand the localhost in the Connections pane.
3. Click **Application Pools**.
4. In the list of application pools, select the WIEAppPool application pool.
5. In the Actions pane on the right, under the Edit Application Pool heading, click **Advanced Settings**.
6. In the Advanced Settings window, under the Process Model heading, click **Identity**.

7. Click the browse button to the right of the **Identity** value.
8. Change the value of the **Built-in account** field to **LocalSystem**.
9. Click **OK**.
10. Click **OK** on the Advanced Settings window.

If changing the application pool to run as the Local System account corrects the problem, start checking the permission details for the application pool user to enable appropriate permissions.

The application pool user (web service user) should have Read, Write, Read and Execute, and List Folder Contents privileges for the following directory:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
```

The application pool user (web service user) should have Read, Read and Execute, and List Folder Contents privileges for the following directories:

- `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\`
- `C:\ProgramData\Microsoft\Crypto\RSA`

Note: The Program Files directory path used in this topic assumes that the default configuration was used during installation. This path may vary if the default configuration was not used.

These are some of the more common directory permissions to research. It may be necessary to use a tool such as Procmon from Microsoft (originally produced by SysInternals) to show real-time file and registry access problems.

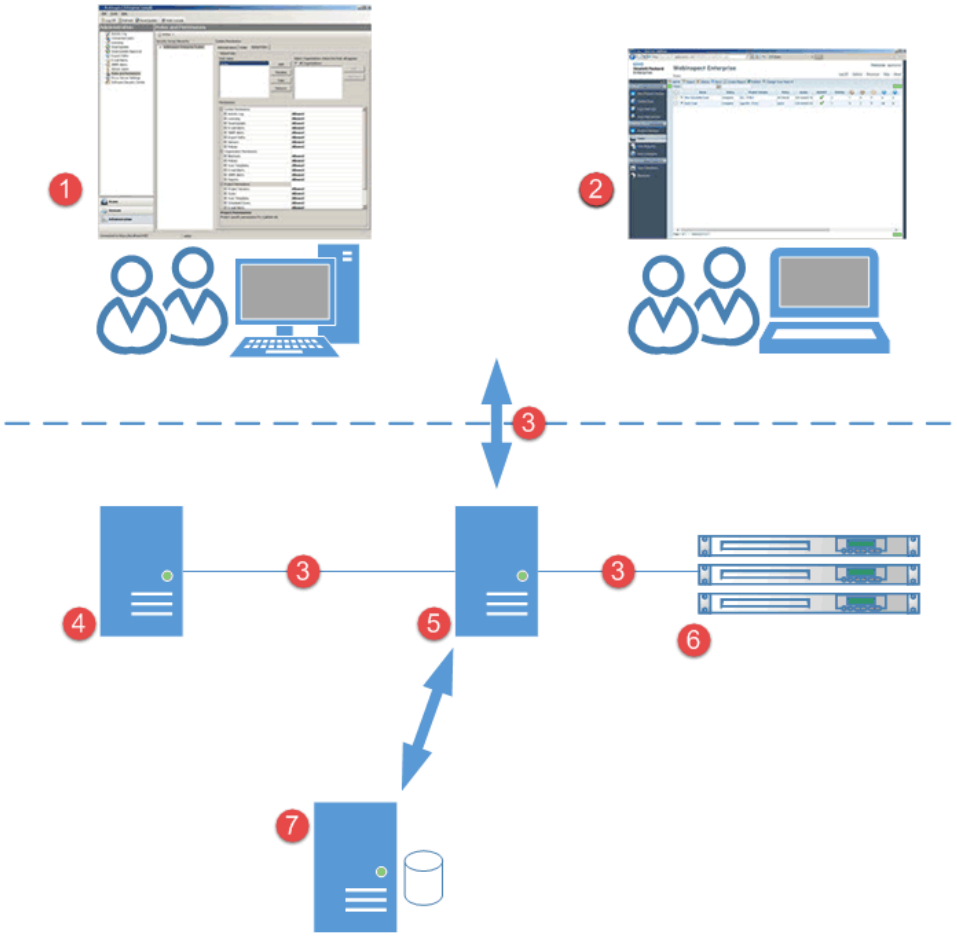
Chapter 4: Implementing Fortify WebInspect Enterprise

This chapter provides an overview of the various Fortify WebInspect Enterprise components as well as information about the following:

- Account requirements (see "Fortify WebInspect Enterprise Manager Account Requirements" on page 88)
- Licensing (see "Fortify WebInspect Enterprise Manager License Components" on page 90)
- Customizing data paths (see "Customizing Data Path and Scan Publication Settings" on page 90)
- Enabling and configuring encryption (see "Encrypting the Communication Between Fortify WebInspect Enterprise and SQL Server" on page 93)
- Configuring sensors (see "Fortify WebInspect Sensor Remote SQL Server Standard Edition Connectivity" on page 95, "Fortify WebInspect Sensor Logging" on page 95, and "Fortify WebInspect Sensor Directory Path Customization" on page 96)
- Customizing database settings (see "About Database Size and Growth Settings" on page 97, "General Database Settings for Fortify WebInspect Enterprise" on page 98, and "Database Maintenance for Fortify WebInspect Enterprise" on page 98)

Fortify WebInspect Enterprise Components

The following illustration depicts the main components of the Fortify WebInspect Enterprise system. These include the Fortify WebInspect Enterprise application, database, sensors, and users. These constitute the basis of the Fortify WebInspect Enterprise system for scheduled and remote scanning. For information about the system requirements for the components, see the *Fortify Software System Requirements*.



Component Descriptions

The following table provides descriptions of the Fortify WebInspect Enterprise user interfaces and architecture.

Item	Component	Description
1	Windows Console User Interface	This console is a thin-client application that provides administrative functionality, policy editing, and the toolkit.

Item	Component	Description
2	Web Console User Interface	This console is a browser-based application that provides user functionality. It does not provide administrative functionality, policy editing, or the toolkit.
3	HTTP or HTTPS	The Fortify WebInspect Enterprise components use these communication protocols.
4	Fortify Software Security Center (optional)	Integration with Fortify Software Security Center provides a way to publish scans to a central repository of all static and dynamic scans. It provides somewhat centralized accounts, although permissions are still managed separately, the ability to submit scan requests, and more extensive reporting than a standalone installation.
5	Fortify WebInspect Enterprise Manager	This is a Microsoft Windows server with an IIS application platform. It is a Web service whose main functions are user authentication and authorization, data repository, and remote scan scheduling.
6	Sensors	These Fortify WebInspect sensors are installed on Microsoft Windows or Windows Server operating systems. Sensors have no GUI and execute remote scans that are configured at the Web Console. You use the Web Console to control all scan configurations, results, reports, and updates.
7	Microsoft SQL Server	This Microsoft Windows server has a SQL database that stores all users, permissions, and administrative settings. The database also stores all scan data and reporting.

Fortify WebInspect Enterprise Manager Account Requirements

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, then you configure Fortify WebInspect Enterprise users (both individuals and groups) as Fortify Software Security Center users and assign roles in Fortify WebInspect Enterprise.

Fortify WebInspect Enterprise interacts with two administrator accounts in Fortify Software Security Center. One of them is a general Fortify Software Security Center administrator. The other is the Fortify WebInspect Enterprise Service, which is used to share application versions and scans between

Fortify Software Security Center and Fortify WebInspect Enterprise, and which must be given the role in Fortify Software Security Center of Fortify WebInspect Enterprise System.

For installations without Fortify Software Security Center integration, you can assign Windows accounts to roles in the Fortify WebInspect Enterprise Administrative Console.

System Account Requirements

Fortify WebInspect Enterprise requires two system accounts:

- WebInspect Enterprise Manager User - Domain user account with local administrator rights on the Fortify WebInspect Enterprise Manager
- WebInspect Enterprise Sensor User - Domain user account. No other privileges are required.

Sensor Requirement

In general, configuring Fortify WebInspect as a sensor is optional during Fortify WebInspect installation, but Fortify WebInspect Enterprise requires you to configure at least one connected instance of Fortify WebInspect as a sensor. The configuration process is described in "Installing Fortify WebInspect as a Sensor" on page 60.

The sensor is Fortify WebInspect, and in general it is referred to as a *Fortify WebInspect sensor* or, when it runs on behalf of Fortify WebInspect Enterprise, as a *Fortify WebInspect Enterprise sensor*—the terms are interchangeable (and there is only one “WebInspect Sensor” Windows service).

Fortify WebInspect Enterprise System Administrator

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, the Fortify Software Security Center administrator specified on the Set Up SSC Connection Information window automatically becomes the first Fortify WebInspect Enterprise system administrator. For more information, see "Setting Up a Fortify Software Security Center (SSC) Connection" on page 34.

For installations without Fortify Software Security Center integration, the user who was added to the System Administrator Role on the Administrator Role Page is the first Fortify WebInspect Enterprise system administrator. For more information, see "Installing or Upgrading a Standalone Fortify WebInspect Enterprise" on page 40 or "Upgrading and Decoupling Fortify WebInspect Enterprise from Fortify Software Security Center" on page 45.

If the first Fortify WebInspect Enterprise system administrator later becomes unavailable, no one knows the administrator password, and the administrator has not created other system administrators, you can rerun the Fortify WebInspect Enterprise Initializer and specify a different Fortify WebInspect Enterprise system administrator. This feature is also useful when moving the Fortify WebInspect Enterprise application to another computer.

SQL Database Account Requirements

If you are installing Fortify WebInspect Enterprise for the first time, you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).

Fortify WebInspect Enterprise Initialize is used for database creation and Fortify WebInspect Enterprise Manager configuration changes such as changing the user account used to access the database.

Fortify WebInspect Enterprise Manager License Components

The Fortify WebInspect Enterprise license contains the license information for each component of the Fortify WebInspect Enterprise environment.

Sensors (Fixed) - The “WebInspect Sensor” Windows service installed by the Fortify WebInspect installation connects to Fortify WebInspect Enterprise for the purpose of performing remotely scheduled or requested scans. It receives instructions exclusively from the configurable connection to a Fortify WebInspect Enterprise Manager.

The license information for sensors and users is located in the Fortify WebInspect Enterprise Console under **Administration > Licensing**.

Customizing Data Path and Scan Publication Settings

By default, the Fortify WebInspect Enterprise Manager uses the All Users profile path for the SmartUpdate download, sensor upload, and logging repository. Some installations may have limited space on the boot partition, and will require the redirection of these files and folders.

Additionally, scans are automatically published to Fortify Software Security Center, but fixed vulnerabilities must be manually marked as fixed in Fortify Software Security Center.

To customize these default settings, you must update the web.config file or the Web.logging.config file or both. This topic describes how to edit these files.

Note: The Program Files directory paths used in these procedures assume that the default configuration was used during installation. These paths may vary if the default configuration was not used.

Changing the Storage Folders Location

You can modify the web.config file to change the data paths:

1. Open the following file:

   ```
   C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\ManagerWS\
   web.config
   ```

2. Add the following lines inside the `<appSettings>` element in the `web.config file`:

   ```
   <add key="Manager.TempPath" value="D:\WIEData\temp" />
   <add key="Manager.BaseDataPath" value="D:\WIEData" />
   ```

   Note: Instead of using the `Manager.BaseDataPath` key, you could add the following five lines to provide greater granularity.

   ```
   <add key="Manager.ScanUploadsPath" value="D:\WIEData\ScanUploads" />
   <add key="Manager.ScanImportPath" value="D:\WIEData\ScanImports" />
   <add key="Manager.SensorUploadsPath" value="D:\WIEData\
   SensorUploads" />
   <add key="SmartUpdate.ProductsFilePath" value="D:\WIEData\
   SmartUpdatePatches" />
   <add key="Manager.PimCachePath" value="D:\WIEData\PimCache" />
   ```

   If you do not want to change all of the paths, then you can comment out the appropriate lines.

Disabling Automatic Publishing of Scans to Fortify Software Security Center

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, by default new scans are automatically published to Fortify Software Security Center. You can edit the web.config file to disable automatic publishing of scans to Fortify Software Security Center as follows:

1. Open the following file:

   ```
   C:\Program Files\Fortify\Fortify WebInspect Enterprise
   23.2.0\ManagerWS\web.config
   ```

2. Change the value in

   ```
   <add key="AutoPublishScans" value="true" />
   ```

   from `true` to `false`.

3. Save and close the file.

Enabling Fortify Software Security Center to Automatically Mark Vulnerabilities as Fixed

If Fortify WebInspect Enterprise is integrated with Fortify Software Security Center, a scan published to Fortify Software Security Center may not contain vulnerabilities that were already detected and published for that application. By default, any previously published vulnerabilities not found in the latest scan must be manually marked as fixed in Fortify Software Security Center. You can edit the web.config file to enable Fortify Software Security Center to automatically mark as fixed any vulnerabilities that are not found in the latest scan. To enable this feature:

1. Open the following file:

   `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\ManagerWS\web.config`
2. Change the value in

   `<add key="AutoResolveVulns" value="false" />`

   from `false` to `true`.
3. Save and close the file.

Changing Logging Locations

The log files are controlled by the `Web.logging.config` file. The configuration specifies an "appender" that is used to write the log entries to a file, and each appender has properties such as the log file path.

The default appender configuration uses the following settings:

```
<appender name="RollingFile"
type="SPI.Diagnostics.Logging.Appender.AppDataRollingFileAppender">
  <file value="HP\WIE\Manager\ManagerWS_trace.log/">
  <appDataLocation value="AllUsers"/>
…
</appender>
```

This defines a log file where the path is relative to the `\ProgramData\` directory. This works because the appender type is set to `AppDataRollingFileAppender`. If you want to change the configuration to use an absolute path for the log file, you must change the appender type to `RollingFileAppender` and replace the relative path with the absolute path. The `appDataLocation` setting will no longer be needed, so you can comment it out or delete it. The updated config section should look similar to the following:

```
<appender name="RollingFile"
type="SPI.Diagnostics.Logging.Appender.RollingFileAppender">
  <file value="D:\WIEData\logs\ManagerWS_trace.log/">
…
</appender>
```

This same change can be made to the Fortify WebInspect Enterprise Scheduler Service and the Fortify WebInspect Enterprise Task Service logging configuration files.

- For the Fortify WebInspect Enterprise Scheduler Service, edit the `AmpScheduler.exe.logging.config` file in the directory `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\Scheduler`
- For the Fortify WebInspect Enterprise Task Service, edit the `AmpTaskService.exe.logging.config` file in the directory `C:\Program Files\Fortify\Fortify WebInspect Enterprise 23.2.0\TaskService`

Encrypting the Communication Between Fortify WebInspect Enterprise and SQL Server

Some customers may require the communication between the Fortify WebInspect Enterprise Web Service and the SQL Server to be encrypted. Standard Microsoft instructions for enabling SSL communication between these two components are available on the internet. The instructions are focused on configuring the Fortify WebInspect Enterprise web service to use the enabled SSL encryption after the Windows configuration is complete.

The steps below detail how to configure Fortify WebInspect Enterprise to use SSL encryption *after* configuring a certificate on the SQL Server machine *and* configuring the Fortify WebInspect Enterprise manager (SQL Client) to use the encryption. Details on setting up this configuration can be found at https://learn.microsoft.com/sql/database-engine/configure-windows/configure-sql-server-encryption.

Enabling Fortify WebInspect Enterprise to Use SSL

The instructions below detail how to modify the `web.config` file to use encrypted communication (SSL) after you have configured encryption on both the SQL Server machine *and* the Fortify WebInspect Enterprise manager (SQL Client).

After configuring the encryption on SQL Server and configuring the Fortify WebInspect Enterprise manager to use the encryption, you additionally need to modify the `web.config` file for the Fortify WebInspect Enterprise web service to utilize the encryption. The connection string is encrypted by default, which requires the steps below to decrypt the string, perform the necessary modifications, and then re-encrypt the string in the `web.config` file. Also, if you rerun Fortify WebInspect Enterprise Initialize, then you will need to redo this process, or keep a backup copy of the encrypted connection string.

Editing the Encrypted SQL Connection String Section of web.config

To modify the `web.config` file to use encrypted communication (SSL) after you have configured both machines to use encryption:

1. Run the following command from a .NET command prompt to decrypt the `connectionStrings` section of the Fortify WebInspect Enterprise `web.config` file:

   ```
   aspnet_regiis -pd "connectionStrings" -app "/WIE"
   ```

   The `-pd` switch specifies the configuration section to decrypt. This is the XML element name of the configuration section.

   The `-app` switch specifies your Web application's virtual path. If it is a nested application, you must specify the nested path from the root directory; for example, `/test/WIE`.

   If the command is successful, you will see the following output:

   ```
   Decrypting configuration section...
   Succeeded!
   ```
2. Add the following connection string properties to the unencrypted connection string:

   ```
   encrypt=true;trustServerCertificate=true
   ```
3. Run the following command from a .NET command prompt to encrypt the `connectionStrings` section:

   ```
   aspnet_regiis -pe "connectionStrings" -app "/WIE"
   ```

   The `-pe` switch specifies the configuration section to encrypt. This is the XML element name of the configuration section.

   The `-app` switch specifies your Web application's virtual path. If it is a nested application, you must specify the nested path from the root directory; for example, `/test/WIE`.

   If the command is successful, you will see the following output:

   ```
   Encrypting configuration section...
   Succeeded!
   ```

Encrypt Connection String in the TaskService.exe.config File

After completing modifications to the `web.config` file, to configure the connection string in the `TaskService.exe` file:

1. Stop the Fortify WebInspect Enterprise Task Service. At a command line, enter:

   ```
   net stop "WebInspect Enterprise 23.2.0 Task Service"
   ```
2. Locate the connectionStrings element in the `web.config` file. See below. Copy the data inside the `<CipherValue>…</CipherValue>` section and paste the data in the exact same section in the `AmpTaskService.exe.config` file.

   ```
   <connectionStrings
   configProtectionProvider="DataProtectionConfigurationProvider">
     <EncryptedData>
       <CipherData>
   ```

```
      <CipherValue>M5KyPhzm+=</CipherValue>
      </CipherData>
    </EncryptedData>
  </connectionStrings>
```

3. Restart the Fortify WebInspect Enterprise Task Service. At a command line, enter:

```
net start "WebInspect Enterprise 23.2.0 Task Service"
```

Fortify WebInspect Sensor Remote SQL Server Standard Edition Connectivity

When configuring the Fortify WebInspect sensor to write to a remote SQL Server Standard Edition instead of a local SQL Server Express Edition, observe the following considerations:

- The database for the sensor must be created using the sensor configuration. The user logged into the sensor machine must have at least temporary rights to create a database on the SQL Server.
- The Fortify WebInspect sensor service on the sensor machine must use an account that can access the remote SQL database. This account needs read/write access to the SQL database created for the sensor. By default, this service runs as the local system, which will not have access to a remote database if you choose Windows Authentication when configuring the database connection information.

Using Windows Authentication

To use Windows Authentication, you must change how the service logs on, as follows:

1. Right-click the Fortify Monitor icon in the task tray and select **Configure Sensor**.
2. On the Configure Sensor window, in the Service Account section, select the option to Log on as **This account**.
3. Enter a user name in the box next to **This account**.
4. Enter the account's password in the **Password** and **Confirm Password** boxes.
5. Click **Start**.

The user performing this action must have rights to create a database on this SQL server (or instance) or an equivalent SQL Server authentication account.

Fortify WebInspect Sensor Logging

The Fortify WebInspect sensor log is in the following location:

```
C:\ProgramData\HP\HP WebInspect\Amp\logs
```

Note: The logs directory path may differ if Fortify WebInspect is configured for FIPS compliance.

The file is named `AMPSensorWI_trace.log`. If additional files are created, they will be named `AMPSensorWI_trace.log.1`, `AMPSensorWI_trace.log.2`, etc. The name can be changed in the `AmpSensorWI.exe.logging.config` file located at:

`C:\Program Files\Fortify\Fortify WebInspect`

Fortify WebInspect Sensor Scan Logs

Information regarding the scans performed by the Fortify WebInspect sensor can be found in the same `HP\HP WebInspect` directory as described previously for your operating system, but in the `EnterpriseServer\logs` subdirectory (rather than the `Amp\logs` subdirectory), and with the scan GUID as the further subdirectory name for each particular scan.

Fortify WebInspect Sensor Directory Path Customization

By default, the Fortify WebInspect sensor uses the All Users profile path as the update download and sensor scan upload repository. Some installations may have small boot partitions that require the redirection of these repository folders. Changes need to be made to the `SharedSettings.config` file in the Fortify WebInspect folder to redirect the Fortify WebInspect Enterprise data path. This will modify all of the paths for the Fortify WebInspect sensor, including both scan logs and scan data (if set to keep a local copy).

Keep in mind that this does not modify the locations for Fortify WebInspect data files. The Fortify WebInspect path settings are configured using the Fortify WebInspect interface.

Modifying the SharedSettings.config File

To edit the `SharedSettings.config` file:

1. Stop the WebInspect Sensor service, as follows:
   a. Right-click the Fortify Monitor.
   b. Select **Configure Sensor**.
   c. Click **Stop**.
2. Edit the `SharedSettings.config` file in the following directory:
   `C:\ProgramData\HP\HP WebInspect`
3. Change the "`AmpDirectory`" value to point to the new location as shown below:

```
<setting name="AmpDirectory" serializeAs="String">
  <value>D:\Put_new_path_here</value>
</setting>
```

4. Save the file.
5. Restart the WebInspect Sensor service, as follows:

a. Right-click the Fortify Monitor.
b. Select **Configure Sensor**.
c. Click **Start**.

Retaining Copies of Scan Data on the Fortify WebInspect Sensor

By default, the Fortify WebInspect sensor deletes all locally stored scan data after the data has been uploaded to Fortify WebInspect Enterprise. If customers want to keep a copy of the scan data on the sensor, use the following procedure.

1. Stop the WebInspect Sensor service, as follows:
   a. Right-click the Fortify Monitor.
   b. Select **Configure Sensor**.
   c. Click **Stop**.
2. Create a file named `AmpSensorWI.user.config` in the following directory:
   `C:\Program Files\Fortify\Fortify WebInspect`
   The file should contain the following:

```
<?xml version="1.0" encoding="utf-8"?>
<appSettings>

  <add key="KeepAllScanFiles" value="true"/>
  or
  <add key="KeepFailedScanFiles" value="true"/>
  [Note: To keep scans with a status of "failed."]

</appSettings>
```

3. Save the file.
4. Restart the WebInspect Sensor service, as follows:
   a. Right-click the Fortify Monitor.
   b. Select **Configure Sensor**.
   c. Click **Start**.

Scans run by the Fortify WebInspect sensor will store a local copy on the sensor machine, as well as uploading the data to the Fortify WebInspect Enterprise database.

About Database Size and Growth Settings

The initial size for the database for installation purposes can be as small as 1GB. This is not large enough for any scan data. The recommended minimum of 20GB will provide for the installation and the initial scanning objectives. This amount of space will not be enough to keep one year's worth of scan data for most organizations.

As each application scan will vary in size and scope, an average size scan is different for each customer. The best way to establish database size and growth requirements is to monitor the database size and compare it with scan activity. The best practice is to start with the minimum 20GB size requirement and note the unused space in the database after installation. As scans are performed, keeping a weekly data set comparing the number of scans with database growth will provide the best metric for average scan size at the customer site. Comparisons of the data set showing weekly, monthly, or quarterly metrics will provide the DBA with guidelines for proper size and growth settings.

General Database Settings for Fortify WebInspect Enterprise

Some considerations for the Fortify WebInspect Enterprise database are listed below:

- Database files and transaction log files should be stored on different disks or partitions for better performance.
- The size of the database file should be set to the largest amount available on the system. Setting this value low and then allowing the database option to auto-grow the file will decrease performance once the size limit is reached. Some DBAs suggest turning off the auto-grow option and monitoring the file size, increasing the size of the database as it becomes larger. The logic is that once a database is full, and it starts to auto-grow, it will most likely do so during periods when the database is being used, which will cause system performance to degrade.
- If the database is performing poorly, turning off the auto-update statistics option may increase performance, as it may be running continuously on databases that are incurring large amounts of activity. If you turn off this option, you should run the Update Statistics Maintenance Task.

Database Maintenance for Fortify WebInspect Enterprise

The descriptions included in this document cover only the most important maintenance tasks associated with database performance issues and are intended for customers that do not have a DBA on staff.

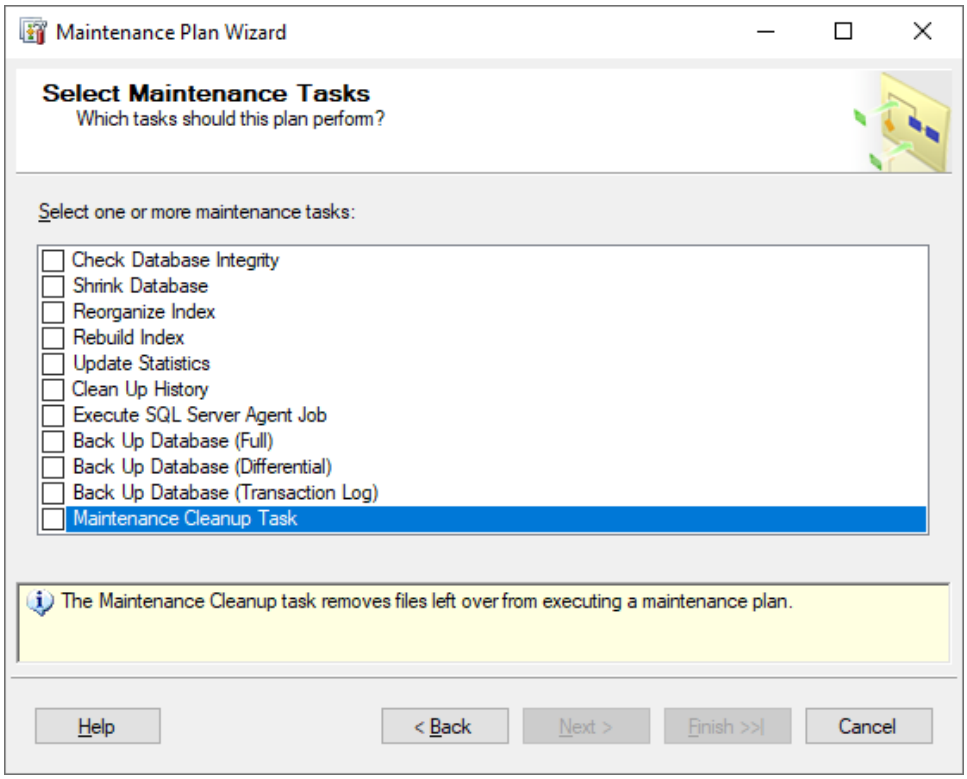
Note: With tasks that have multiple options, the recommended setting for the Fortify WebInspect Enterprise database is noted by the Fortify WebInspect Enterprise Recommended Options.

In SQL Server Management Studio, the Maintenance Plan Wizard guides you through a series of steps that request several bits of information for a complete plan that are saved as an SQL Server Integration Services package. This plan is executed by the SQL Server Agent Service. This service must be running for the Maintenance Plan to initiate.

The steps are listed in a logical order of progression for the tasks to be performed. Each option important for the Fortify WebInspect Enterprise database is listed followed by the general description

of the selected maintenance task. Keep in mind that these are general suggestions for customers that do not have a DBA resource on staff.

To access the Maintenance Plan Wizard, in SQL Server Management Studio, expand **Management**, right-click **Maintenance Plans**, and select **Maintenance Plan Wizard**. Multiple maintenance plans can be created and run on different schedules. We generally recommend running separate maintenance plans for the system databases (master, model, msdb) and user databases (the Fortify WebInspect Enterprise database).



Fortify WebInspect Enterprise Recommended Options

The maintenance plan should be scheduled to run during a non-peak time. It can be run daily, weekly, or monthly at the customer's discretion. Each should be configured to write the results to a common log directory and should be reviewed frequently to monitor the health of the database.

Check Database Integrity Task

The Check Database Integrity task checks the allocation and structural integrity of all the objects in the specified database. The task can check a single database or multiple databases, and you can choose whether to also check the database indexes.

Note: You can repair errors with the DBCC CHECKDB Transact-SQL command. Using a repair option with this command requires the database to be in single-user mode, which will take the database and Fortify WebInspect Enterprise application offline.

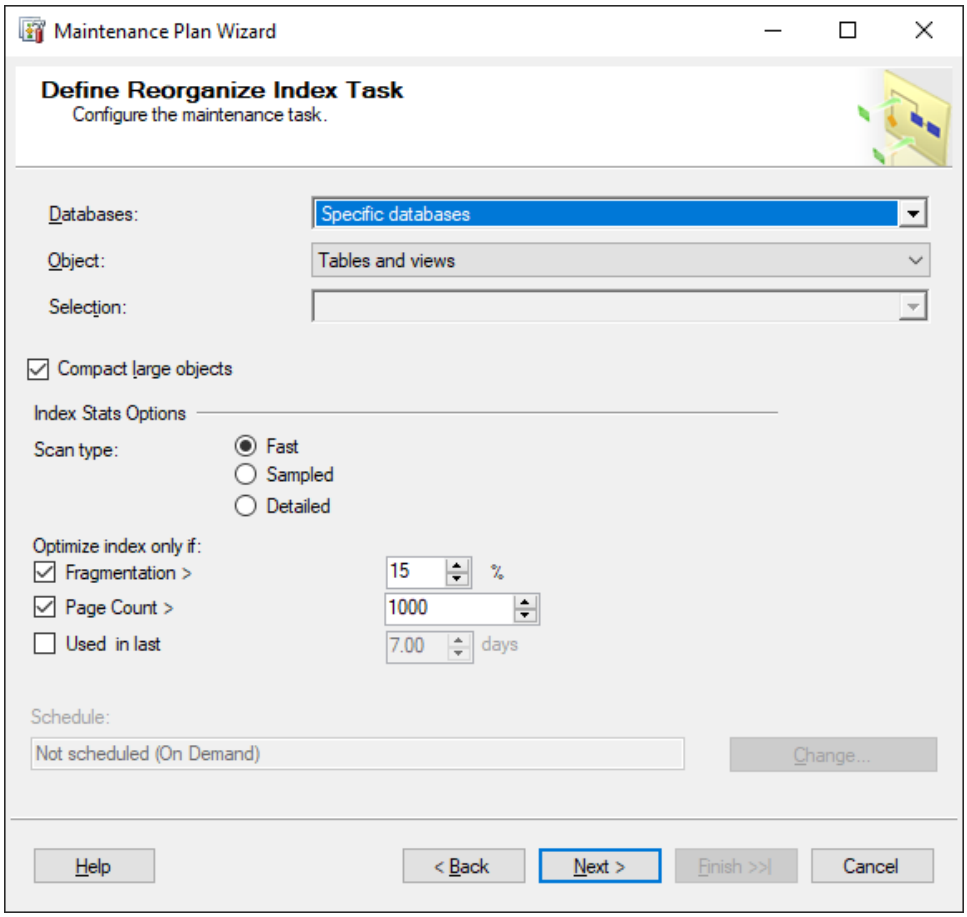
Database Fragmentation Maintenance

The Reorganize Index, Rebuild Index, and Update Statistics maintenance tasks come under the subject of fragmentation.

The SQL Server Database Engine automatically maintains indexes whenever insert, update, or delete operations are made to the underlying data. Over time, these modifications can cause the information in the index to become scattered in the database (fragmented). Fragmentation exists when indexes have pages in which the logical ordering, based on the key value, does not match the physical ordering inside the data file. Heavily fragmented indexes can degrade query performance and cause the application to respond slowly.

Reorganize Index Task

The Reorganize Index task reorganizes indexes in SQL Server database tables and views. Use the Define Reorganize Index Task window to move index pages into a more efficient search order. Having the pages in order improves index-scanning performance.

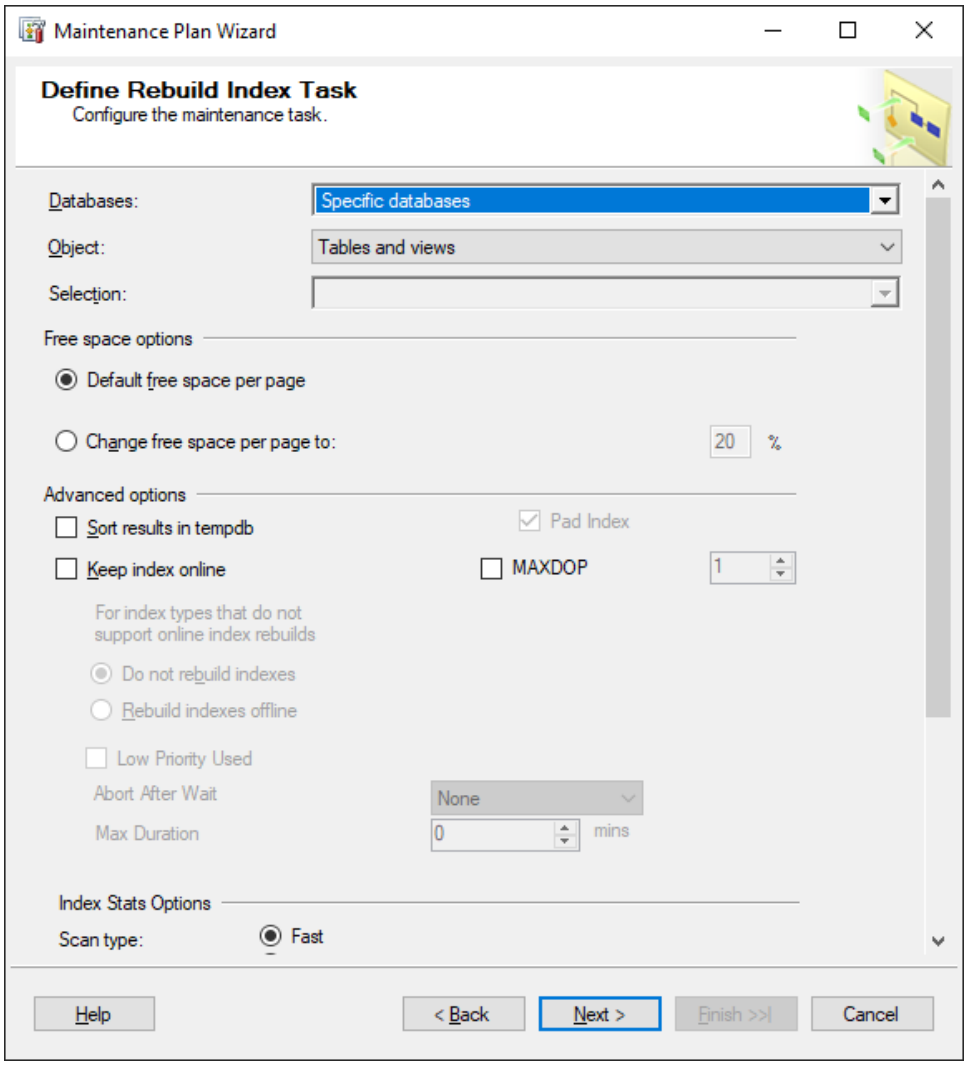


Fortify WebInspect Enterprise Recommended Options

Select the **Tables and views** object and the **Compact large objects** check box.

Rebuild Index Task

The Rebuild Index task rebuilds indexes in SQL Server database tables and views. Rebuilding an index drops the index and creates a new one. In doing this, fragmentation is removed, disk space is reclaimed by compacting the pages using the specified or existing fill factor setting, and the index rows are reordered in contiguous pages (allocating new pages as needed). This can improve disk performance by reducing the number of page reads required to obtain the requested data.

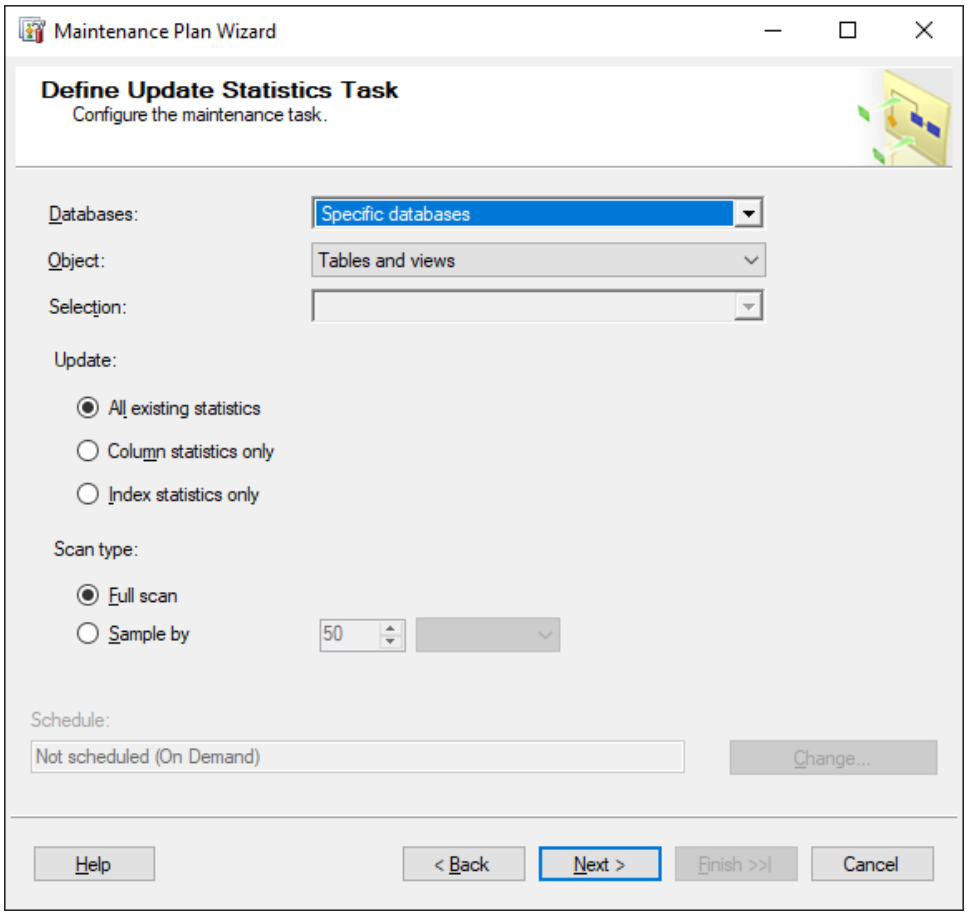


Fortify WebInspect Enterprise Recommended Options

Select the **Tables and views** object and the **Reorganize pages with the default amount of free space** option.

Update Statistics Task

The Update Statistics task updates information about the distribution of key values for one or more statistics groups (collections) in the specified table or indexed view. SQL Server allows for statistical information to be created regarding the distribution of values in a column. The query optimizer uses this statistical information to determine the optimal query plan by estimating the cost of using an index to evaluate the query.



Fortify WebInspect Enterprise Recommended Options

Select the **Tables and views** object, the **All existing statistics** option, and the **Full scan** option.

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 Implementation Guide (Fortify WebInspect Enterprise 23.2.0)

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!