

HP WebInspect Enterprise

for the Windows[®] operating system

Software Version: 10.20

Installation Guide

Document Release Date: April 2014
Software Release Date: April 2014



Legal Notices

Copyright Notice

© Copyright 2014 Hewlett-Packard Development Company, L.P.

Restricted Rights Legend

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

Disclaimer of Warranty

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark Acknowledgements

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

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

Other Acknowledgements

This product contains the following Apache open source component: Log4Net (<http://logging.apache.org/log4net/>). This component was modified from its original form and incorporated into this software product. To learn more about the apache software license, please visit <http://www.apache.org/licenses/LICENSE-2.0>.

Documentation Updates

This guide's title page contains the following identifying information:

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

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

<http://h20230.www2.hp.com/selfsolve/manuals>

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

Support

For information or assistance regarding WebInspect Enterprise, contact customer support.

You can open a support case for WebInspect Enterprise via e-mail, online, or by telephone. These options are designed to provide easier access and improved customer satisfaction.

E-Mail (Preferred Method)

Send an e-mail to fortifytechsupport@hp.com describing your issue. Please include the product name so we can help you faster.

Online (Fortify Support Portal)

Access your account at the Fortify Support Portal at [**https://support.fortify.com**](https://support.fortify.com)

If you do not have an account, you forgot your username or password, or you need any assistance regarding your account, please contact us at fortifytechsupport@hp.com or (650) 735-2215.

Telephone

Call our automated processing service at (650) 735-2215. Please clearly provide your name, telephone number, the name of the product, and a brief description of the issue.

Installing WebInspect Enterprise 10.20

System Requirements

Before installing WebInspect Enterprise, make sure that your systems meet the requirements described in the *HP Fortify Software Security Center System Requirements* for Software Security Center version 4.10. This installation guide also refers to the *HP WebInspect Enterprise User Guide* for detailed information. Both documents are available at:

<https://download.hpsmartupdate.com/wie>

FIPS Compliance

WebInspect Enterprise version 10.20 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.

WebInspect Enterprise and the WebInspect sensors it uses must all be compliant with FIPS or they must all be non-compliant. FIPS compliance is supported only for new WebInspect Enterprise 10.20 installations, not for any upgrade from an older version of WebInspect Enterprise, nor for any migration from Assessment Management Platform (AMP).

Requirements for Migrating from AMP 9.20

Note: You can install WebInspect Enterprise 10.20 using an existing Assessment Management Platform (AMP) 9.20 database that the installation procedures convert to the WebInspect Enterprise 10.20 data schema while leaving the original AMP system unchanged. This type of installation is called an AMP migration or simply a migration.

If you migrate from AMP 9.20, you are expected to back up the AMP database. The Initialization Wizard part of installation will back up and copy the AMP database, and then modify the copy as needed to make it compatible with the WebInspect Enterprise 10.20 database schema. For this process, the server that hosts the AMP database must have available disk space at least three times the size of the current AMP database to be migrated. For example, if the AMP database to be migrated is 500 GB, then the AMP database server must have at least 1.5 TB of free space.

Depending on the size of your AMP database, migration can take a very long time. Make sure that the machines that run your database server and WebInspect Enterprise Initialization cannot reboot during the migration as a result of Windows updates.

Installing or Upgrading HP Fortify Software Security Center

HP Fortify Software Security Center (SSC) version 4.10 must be installed and running before you install WebInspect Enterprise version 10.20. See the *HP Fortify Software Security Center Installation and Configuration Guide* for information about installing or upgrading SSC to the required version.

In SSC:

- Note the SSC URL. You will need to specify it during the installation of WebInspect Enterprise.
- Create a general SSC 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 WebInspect Enterprise and this person will automatically become the first WebInspect Enterprise system administrator.
- Create an account in SSC for the WebInspect Enterprise Service, give it a recognizable user name such as wie_service, and give it the role of WebInspect Enterprise System. This service controls the sharing of project versions with WebInspect Enterprise and obtains lists of completed and running scans from WebInspect Enterprise. You will need to specify the user name and password of this account during the installation of WebInspect Enterprise.

For information about creating accounts in SSC, see the *HP Fortify Software Security Center User Guide*. The HP Fortify Software Security Center documentation set contains installation, user, and deployment guides for all HP Fortify Software Security Center 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, go to the HP Software Product Manuals site:

<http://h20230.www2.hp.com/selfsolve/manuals>

To access this web site, you must first obtain an HP Passport account.

Upgrading from WebInspect Enterprise 10.10

You can upgrade to WebInspect Enterprise 10.20 directly from WebInspect Enterprise 10.10, but not from any other versions of WebInspect Enterprise. Also, see [Installing or Upgrading HP Fortify Software Security Center](#) on page 6.

Migrating from AMP 9.20

You can migrate to WebInspect Enterprise 10.20 directly from Assessment Management Platform (AMP) 9.20, but not from any other versions of AMP.

If you perform this AMP migration:

- See [Requirements for Migrating from AMP 9.20](#) on page 5 and [Installing or Upgrading HP Fortify Software Security Center](#) on page 6.
- During the migration, the Initialization Wizard needs access to the AMP database.
- While running the Initialization Wizard, you will see additional screens related to AMP migration only, as described in this document.
- When the migration is complete:
 - AMP 9.20 can continue to operate with its original, unmodified database as before.
 - Independently, WebInspect Enterprise 10.20 operates with its database, including the migrated AMP data converted to the WebInspect Enterprise 10.20 schema.

- Scans cannot be archived in WebInspect Enterprise. Scans that are archived in AMP are copied to WebInspect Enterprise during the AMP migration, but their Status remains Archived and they can only be deleted, not viewed, in WebInspect Enterprise. If a scan is currently archived in AMP and you want to be able to view it in WebInspect Enterprise, restore it in AMP before performing the migration.
- Using a new Administrative Console shortcut named **Site Migration**, any time after the full AMP migration procedures are complete, an administrator with the required access can migrate the copied AMP sites that you select to WebInspect Enterprise project versions. Migrating an AMP site allows users to see visualizations of its unpublished scans in WebInspect Enterprise, which was not possible in AMP.

Preparing to Install WebInspect Enterprise

This section describes how to prepare to install WebInspect Enterprise by installing IIS and Microsoft .NET Framework, enabling ASP.NET v2.0 and v4.0 for ISAPI and CGI, installing SQL Server, and creating an account for a sensor user.

First, see [Installing or Upgrading HP Fortify Software Security Center](#) on page 6.

On a Microsoft Windows server:

- 1 Install IIS as follows. You must install IIS before installing Microsoft .NET Framework 4.0.
 - a Open the Windows Server Manager.
 - b Click the **Roles** option, and click **Add Roles** under Roles Summary in the Roles pane. The Add Roles Wizard opens.
 - c Click **Next**.
 - d In the **Select Server Roles** dialog, make sure the **Web Server (IIS)** option is selected (installed).
 - e Close the wizard.
 - f Under Role Services in the Roles pane, click **Add Role Services**.
 - g In the list of role services in the Select Role Services dialog, scroll as needed and, under Management Tools, select the **IIS6 Management Compatibility** option (which also selects all of its suboptions).
 - h Click **Next**.
 - i Click **Install** to install IIS.
- 2 Install Microsoft .NET Framework 4.0.
- 3 Enable ASP.NET v2.0 and v4.0 for ISAPI and CGI:
 - a In the Server Manager window, under Server Manager (<localhost>), select **Roles** → **Web Server (IIS)** → **Internet Information Services (IIS) Manager**.
 - b In the *Internet Information Services (IIS) Manager* window, select the localhost in the Connections pane.
 - c In the IIS section, double-click the **ISAPI and CGI Restrictions** icon.
 - d In the ISAPI and CGI Restrictions pane, if any Restriction value for an ASP.NET v2.0.xxxxx entry or an ASP.NET v4.0.xxxxx entry is set to **Not Allowed**, right-click that entry and select **Allow**.

If you receive an error message indicating that the feature cannot be installed because your operating system lacks IIS Management Compatibility, make sure you followed the preceding steps correctly.

- 4 Install SQL Server software if it is not already installed.
- 5 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 WebInspect Enterprise. Note the domain name, the account name, and the password.

Installing WebInspect Enterprise

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

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

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

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

- Post-installation configuration
 - Installing WebInspect as a sensor
 - Adding sensor users (if not previously done)
 - Enabling sensors and configuring sensor permissions
 - Assigning administrators and roles
 - Moving project versions from the default group
 - Configuring WebInspect Enterprise to publish scans to SSC
 - For an AMP 9.20 migration, optionally migrating sites to project versions
- Guided Scan and creating reports
- Time stamping and scheduling
- Installations lacking internet connection

Installing the WebInspect Enterprise Server Software

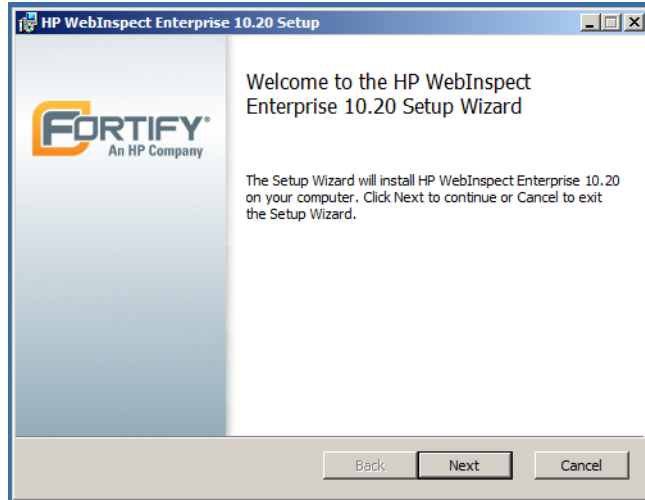
Review the section [FIPS Compliance](#) on page 5.

Install the 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 WebInspect Enterprise server software, uninstall that version using Control Panel and then relaunch the installation file.

The *Welcome* screen of the *HP WebInspect Enterprise 10.20 Setup* wizard appears.

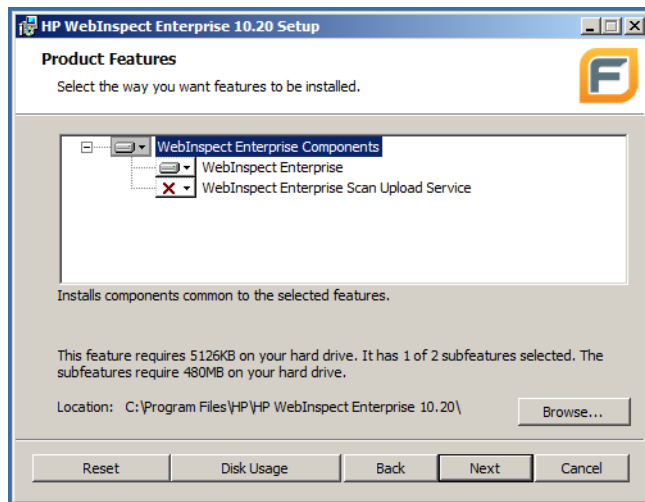


- 2 Click **Next**.

The *End-User License Agreement* dialog 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* dialog appears. (Memory requirements stated for the features might vary slightly from the values shown in the following screen capture.)



- 4 On the *Product Features* dialog:

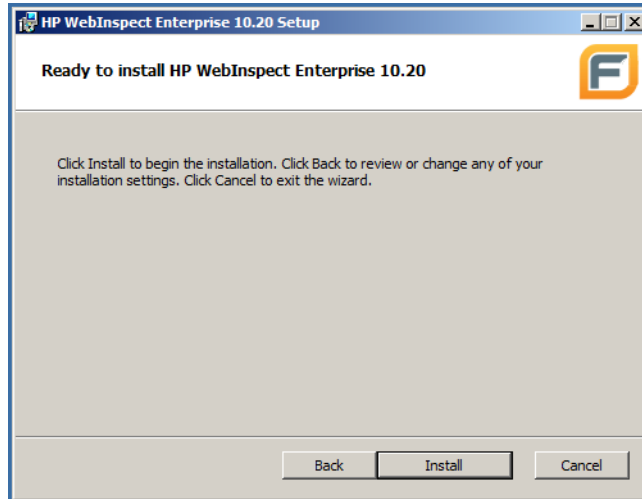
- a Select the components you want to install.

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 WebInspect Enterprise Manager. To install the 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.

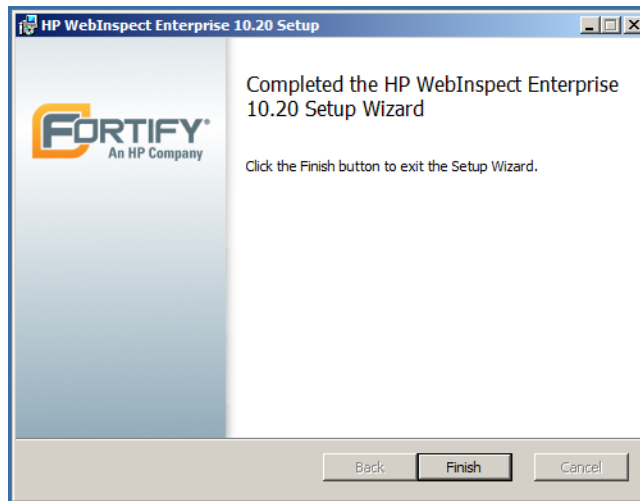
- c Click **Next**.

The *Ready to install HP WebInspect Enterprise 10.20* dialog appears.



- 5 When you are ready to install, click **Install**.

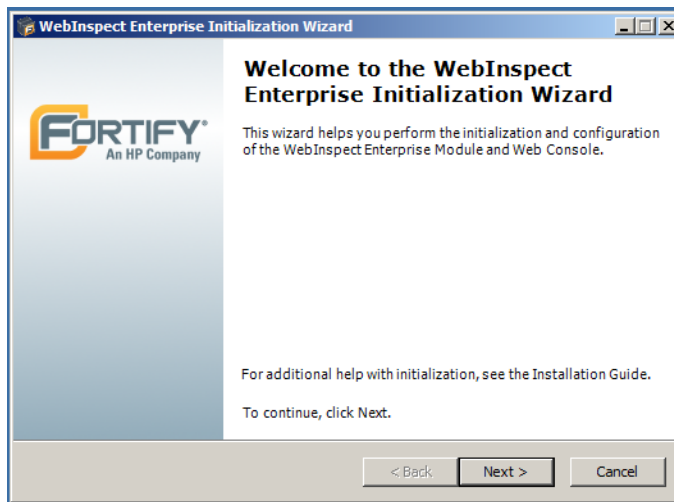
WebInspect Enterprise 10.20 software is installed on the computer and the Setup Wizard completes.



- 6 Click **Finish**.

Running the Initialization Wizard

After the Setup Wizard completes, the *Welcome* screen of the *HP WebInspect Enterprise Initialization Wizard* appears.



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

- Activating the WebInspect Enterprise license
- Creating a new WebInspect Enterprise database or updating an existing one as needed
- Creating the WebInspect Enterprise website and web service
- Connecting WebInspect Enterprise and HP Fortify Software Security Center (SSC)
- Establishing the initial WebInspect Enterprise system administrator
- For AMP migration:
 - Copying particular data from the AMP database to the WebInspect Enterprise database
 - Preparing the WebInspect Enterprise database for the optional migration of AMP sites to project versions
 - Allowing you to map legacy AMP user accounts to SSC user accounts, if desired

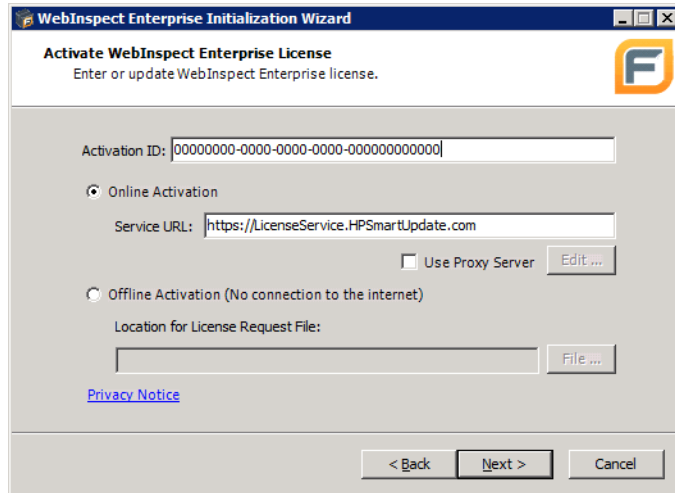
Note: After you complete these installation procedures, you will always be able to restart the Initialization Wizard if necessary, by clicking

Start → All Programs → HP → HP WebInspect Enterprise 10.20 → WebInspect Enterprise Initialize.

Run the Initialization Wizard:

- 1 Click **Next**.

The *Activate WebInspect Enterprise License* dialog appears.



- 2 Enter the Activation ID that HP sent to you.

- 3 Do one of the following:

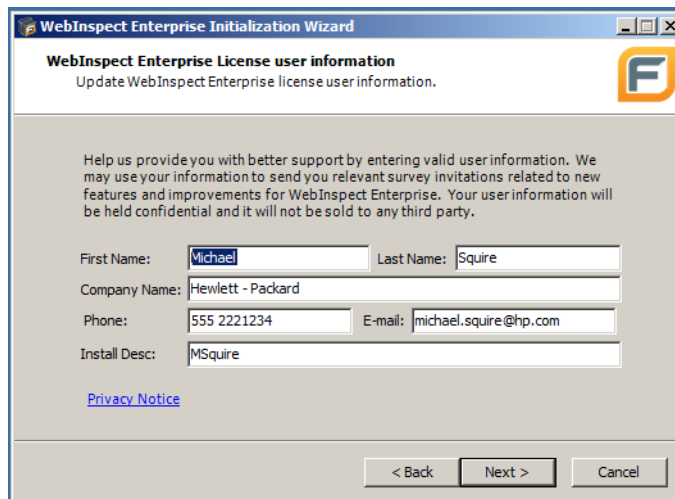
- If the computer is connected to the Internet, select **Online Activation**.

If you are using a proxy server, select **Use Proxy Server**, click **Edit**, and provide the requested information.

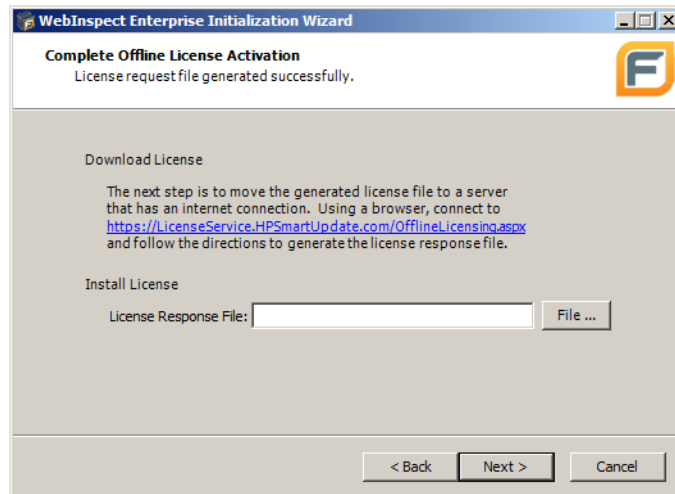
- If the computer is *not* connected to the Internet, select **Offline Activation** and then click **File** to select the location on this computer where you want the installation software to create a license *request* file named `LicenseRequest.xml`. This file will contain information about the computer that is required to obtain a license.

- 4 Click **Next**.

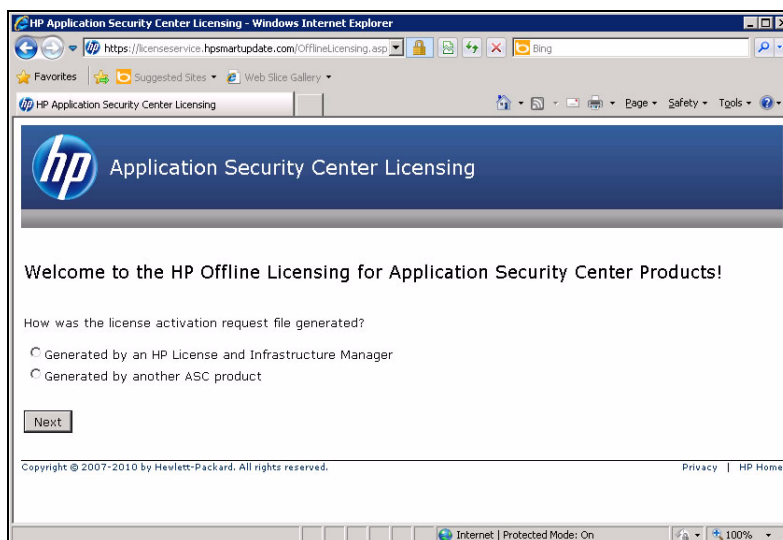
The *WebInspect Enterprise License user information* dialog displays user information as submitted to HP.



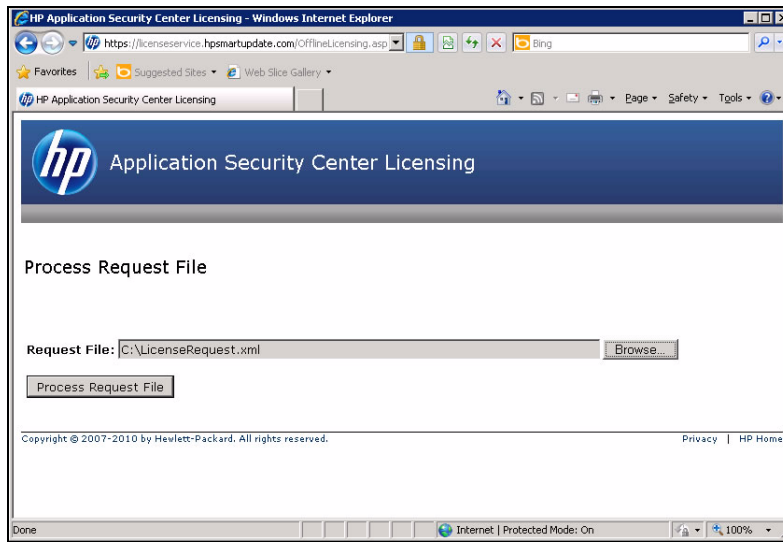
- 5 Correct the information as needed and click **Next**.
- 6 If you selected **Online Activation** in **step 3**, go to **step 8** on page 15.
- 7 If you selected **Offline Activation** in **step 3**, the *Complete Offline License Activation* dialog appears. It indicates that the license request file was generated successfully. Perform the procedure in this step to download from HP a license *response* file named `LicenseResp.xml` that you can copy to the computer, not connected to the Internet, on which you are installing 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.HPSmartupdate.com/OfflineLicensing.aspx>**.



- d Select the option that describes how the license request file was generated and click **Next**.
The *Process Request File* window appears.



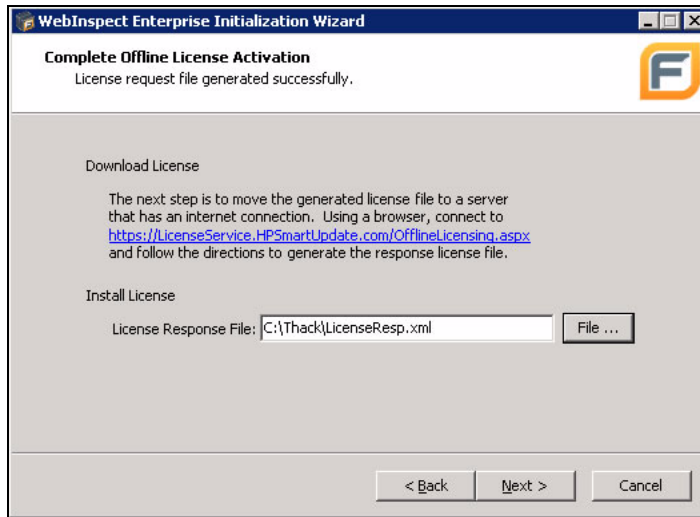
- e Click **Browse** as needed, select the `LicenseRequest.xml` file that you copied to this computer, and then click **Process Request File**.

If the request is processed successfully, the following dialog appears:



- f Click **Retrieve Response File**.
- g On the *File Download* dialog, 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 WebInspect Enterprise. Copy the `LicenseResp.xml` file from the portable device to a location on this computer.

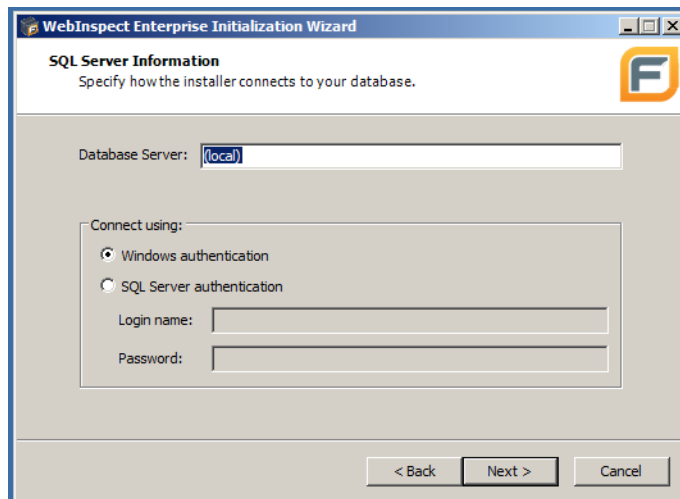
- i In the WebInspect Enterprise Initialization Wizard, specify the **License Response File** field by clicking **File** and navigating to the location of the LicenseResp.xml file you just copied from the portable device.



- j Click **Next**.

- 8 The *WebInspect Enterprise License Information* dialog displays information about the license. Review the information.
- 9 Click **Next**.

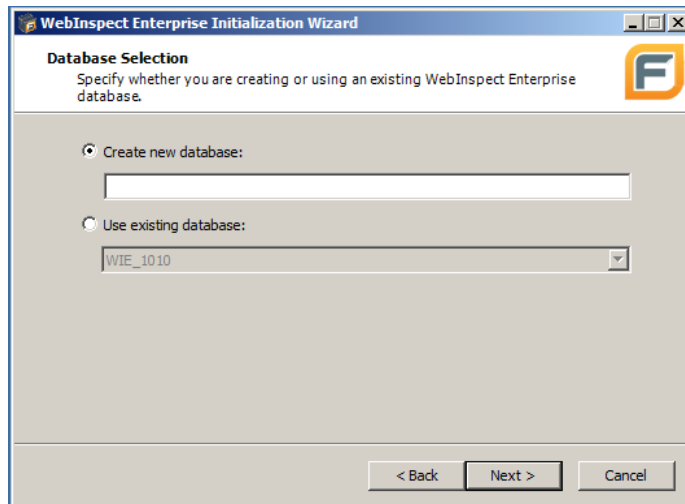
The *SQL Server Information* dialog appears.



- 10 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 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).

- 11 Click **Next**.

The *Database Selection* dialog appears.



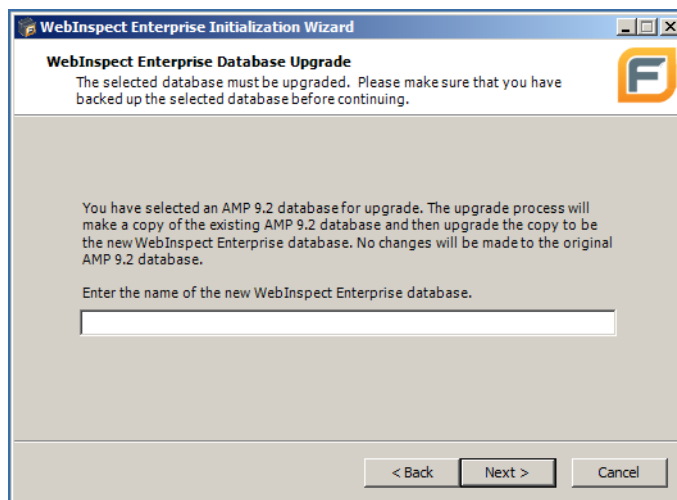
- 12 Select one of the following:

- 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 WebInspect Enterprise 10.10 database for an upgrade or an existing AMP 9.20 database for an AMP migration, select **Use existing database** and select a database from the drop-down list. You must have owner privileges for that database.

- 13 Click **Next**.

- 14 If you created a new database or you are upgrading from WebInspect Enterprise 10.10, skip to [step 16](#).

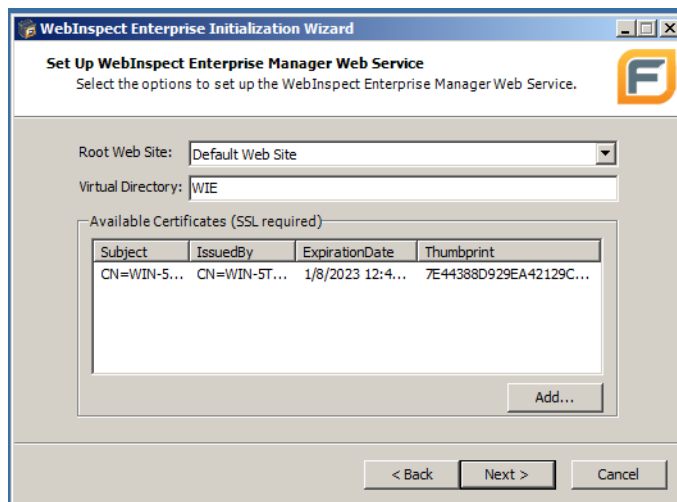
- 15 If you are using an existing database for an AMP 9.20 migration, the *WebInspect Enterprise Database Upgrade* window appears, instructing you to back up the existing database before continuing, and requiring you to specify a name for the new WebInspect Enterprise database. See [Requirements for Migrating from AMP 9.20](#) on page 5.



After you back up the existing database, specify the name of the new WebInspect Enterprise database as requested, and click **Next**.

Later, the Initialization Wizard will copy the existing database to the new WebInspect Enterprise database, and modify the copy to make it compatible with WebInspect Enterprise 10.20.

- 16 The *Set Up WebInspect Enterprise Manager Web Service* dialog appears.



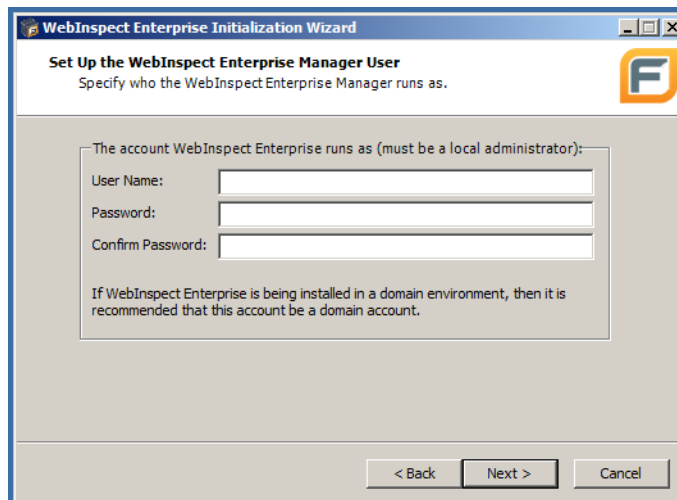
Specify the root Web site and the IIS virtual directory name (**WIE** in the example above), and select (or add and select) a certificate.

These entries create the URLs for the following components:

- 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`

- 17 Click **Next**.

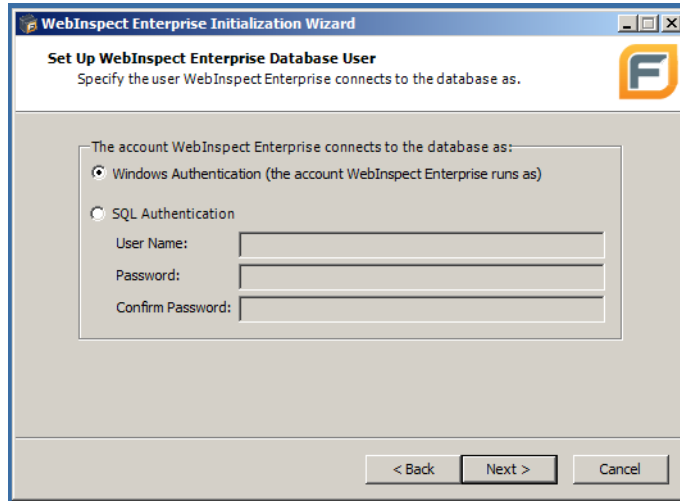
The *Set Up the WebInspect Enterprise Manager User* dialog appears.



- 18 Specify the local or domain Windows user account that will run the WebInspect Enterprise website and Web service. The **User Name** should be in the format `localhost\administrator` or `domain\administrator`. For WebInspect Enterprise to work properly, this account must be a local administrator. This account enables the WebInspect Enterprise Manager to install service packs and patches released by HP.

19 Click **Next**.

The *Set Up WebInspect Enterprise Database User* dialog appears.

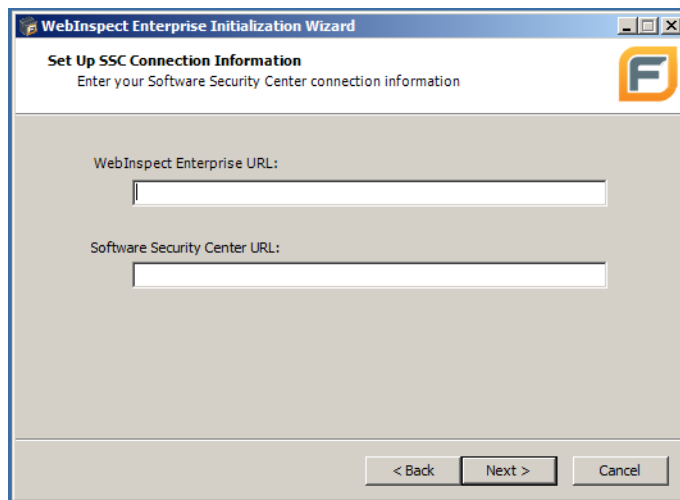


20 Specify how the WebInspect Enterprise Manager should connect to the WebInspect Enterprise database.

- **Windows Authentication** - The name and password specified in the WebInspect Enterprise Manager's user account is used to authenticate to the database. When working in a domain environment, the 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 WebInspect Enterprise Manager and the database computers.
- **SQL Authentication** - Enter the SQL Server user name and password.

21 Click **Next**.

The *Set Up SSC Connection Information* dialog appears.

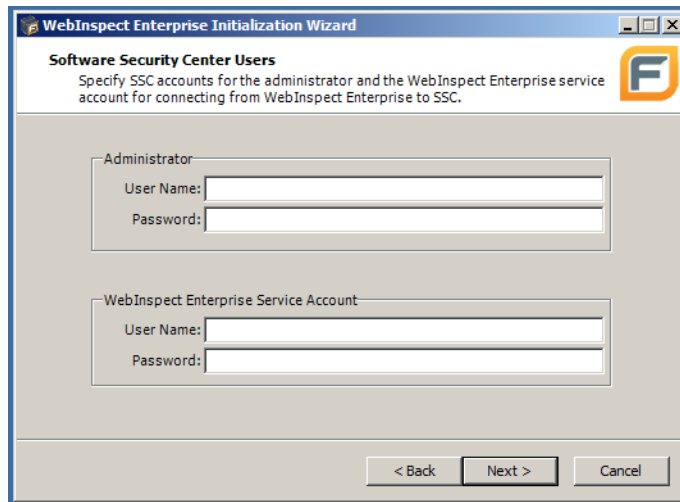


The **WebInspect Enterprise URL** field has a default value based on previous configuration. Make a note of this URL.

Specify the **Software Security Center URL**. See [Installing or Upgrading HP Fortify Software Security Center](#) on page 6.

22 Click **Next**.

The *Software Security Center Users* dialog appears.



Make sure that SSC is running and that an SSC administrator is logged on.

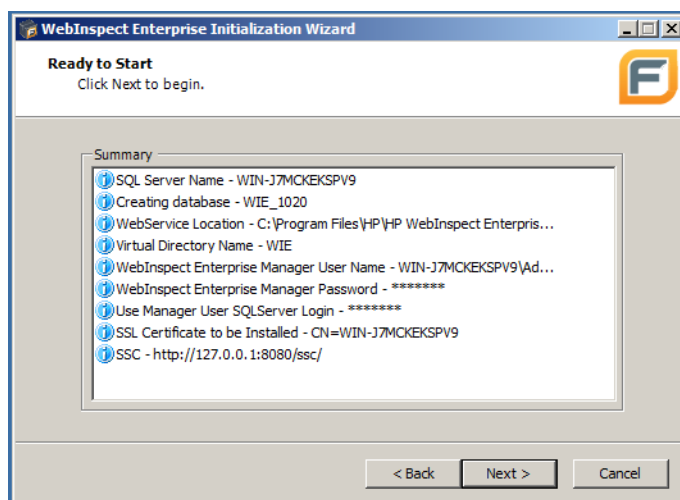
In the *Software Security Center Users* dialog, specify the SSC accounts for that administrator and for the WebInspect Enterprise Service Account. See [Installing or Upgrading HP Fortify Software Security Center](#) on page 6. The SSC administrator you specify here will automatically become the first WebInspect Enterprise system administrator.

If you are performing an AMP 9.20 migration, an additional field named **Default Group** appears in the Administrator section. Its drop-down list displays the current set of parent organizations and their groups. Select one group to use for saving project versions sent from SSC. In AMP, the default value for the **Default Group** field is **Default Organization : Default Project**, but someone might have changed the default value or added other values. This field is provided in case you want to use a different **Default Group** in WebInspect Enterprise than the one that has been used in AMP.

23 Click **Next**.

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

The *Ready To Start* dialog appears.



24 Verify your previous choices and begin initializing WebInspect Enterprise.

- To change settings, click **Back**.
- To begin initializing WebInspect Enterprise using the values you have specified, click **Next**.

For new installations of WebInspect Enterprise, upgrades from WebInspect Enterprise 10.10, and AMP 9.20 migrations, the Initialization Wizard:

- Creates a new database if you chose to do so in [step 12](#) on page 16.
- Registers WebInspect Enterprise with SSC. Then SSC sends all current project versions (finished and unfinished) to WebInspect Enterprise, where they get created and can be displayed.
- Configures various system components.
- In the displayed, cumulative Status list, 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).

In addition, for AMP 9.20 migrations, the Initialization Wizard does the following to allow the customer to start using WebInspect Enterprise with data from the AMP database:

- Copies (backs up) the entire existing AMP database you specified.

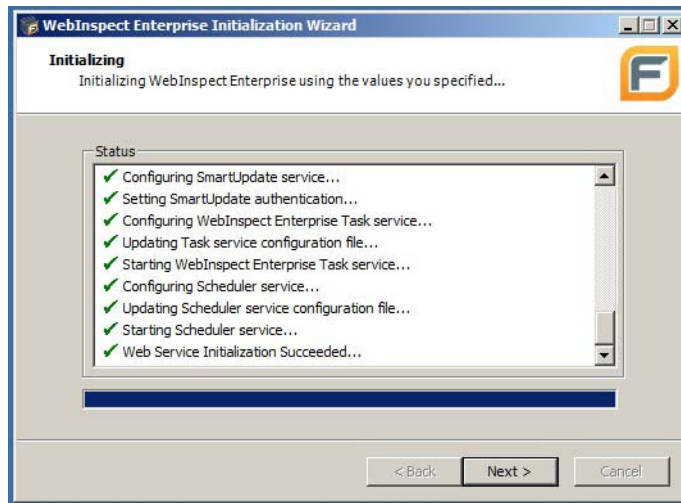
When the backup is complete, the Status list shows the location to which the database is backed up. In case the path is too long to display on one line, this location is also written to the initializer logs in C:\Program Files\HP\HP WebInspect Enterprise 10.20\Initializer\Initializer_trace.
- Applies a script to the copy, modifying the copy so it becomes compatible with the WebInspect Enterprise 10.20 database schema. Legacy AMP data that is no longer used in WebInspect Enterprise is deleted.

The Initialization Wizard establishes data in the WebInspect Enterprise database for each of the AMP sites. However, unpublished scans that were created in AMP cannot be displayed in WebInspect Enterprise until a WebInspect Enterprise system administrator performs “site migration” to assign the AMP sites to project versions, as described later.

The Initialization Wizard also copies some types of data from the AMP database to the WebInspect Enterprise database that are not associated with particular scans or AMP sites, such as blackout periods for sensors, custom policies, roles, proxy settings, configuration settings for email and SNMP alerts, and SecureBase data.

- Assigns scans that were previously published from AMP to SSC to have the same project versions in WebInspect Enterprise as they already have in SSC. When installation of WebInspect Enterprise is completed, these previously published scans can be viewed in WebInspect Enterprise as part of their project versions.

When the initialization completes successfully, the window appears similar to the one shown below. The final initialization step is “Web Service Initialization Succeeded...”

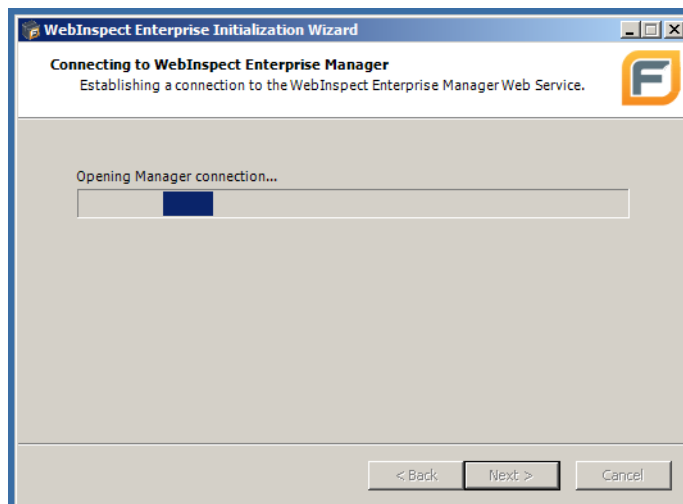


25 Click **Next**.

The SSC administrator you specified in [step 22](#) on page 19 automatically becomes the first System Administrator in WebInspect Enterprise.

Note: If that person becomes unavailable, no one knows his password, and he did not create other System Administrators in WebInspect Enterprise, it might seem that there would be no way to administer WebInspect Enterprise. However, you can rerun the Initialization Wizard (**Start** → **All Programs** → **HP** → **HP WebInspect Enterprise 10.20** → **WebInspect Enterprise Initialize**) and specify another SSC administrator in [step 22](#). Then at this point in the initialization process, the initializer would detect that your newly specified SSC administrator exists in SSC but she is not a System Administrator in WebInspect Enterprise. In this case, the initializer would display the *Administrator Role Page*, which allows you to add her to 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.

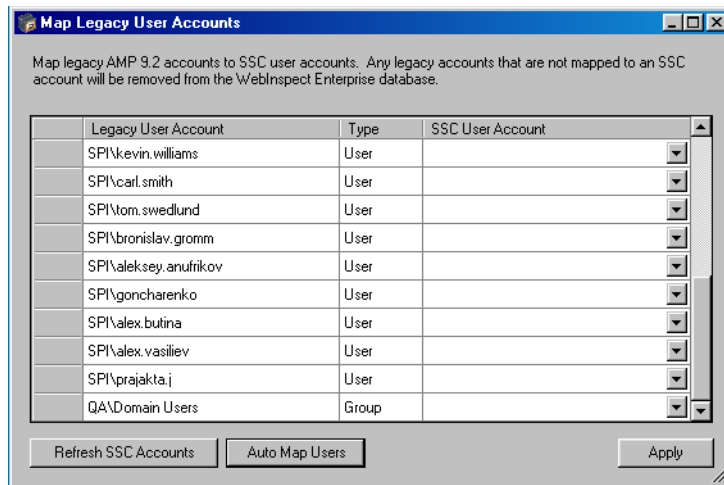


- 26 If you are *not* performing an AMP 9.20 migration, skip to [step 31](#) on page 23.
- 27 WebInspect Enterprise 10.20 and SSC use single sign-on functionality, with a common set of user accounts that are specified in SSC, whereas AMP 9.20 accounts use NTLM authentication and are no longer valid. If you are performing an AMP 9.20 migration, *and* if you specified in [step 11](#) on page 16 that you want to continue to use the existing AMP database, the *Legacy Users* dialog appears.



28 Do one of the following:

- Select **Remove Legacy Users** to remove all existing (legacy) AMP 9.20 accounts, and skip to [step 31](#).
- Select **Map Legacy Users** to map (assign) some or all of the legacy AMP 9.20 user accounts to existing SSC user accounts. If you select this option, the *Map Legacy User Accounts* dialog opens for you to make the desired mappings.



29 In the *Map Legacy User Accounts* dialog, for each account in the **Legacy User Account** column that you want to retain, select an SSC user account from the drop-down list in the **SSC User Account** column to establish the desired mapping. You can map any number of legacy accounts to the same SSC user account. Each SSC user account will inherit the roles and privileges of the legacy user accounts that are mapped to it.

If you create new accounts in SSC at this time, you can click **Refresh SSC Accounts** to add them to the drop-down lists in the **SSC User Account** column.

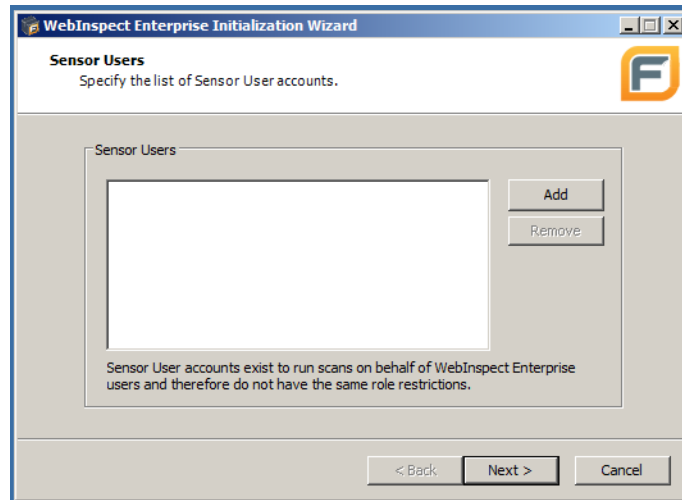
If you click **Auto Map Users**, for each row where a person's name in the **Legacy User Account** column exactly matches an existing SSC user account name, that account name automatically populates the **SSC User Account** field. After the automatic mapping finishes, you can still change any of the automatically mapped **SSC User Account** names.

Any legacy account that you do not map to an SSC account is removed. If you leave any legacy user accounts unmapped, a message is displayed to remind you that they will be removed if you continue.

- 30 After specifying the desired mapping, click **Apply**.

The legacy user accounts are mapped to SSC user accounts as you specified.

- 31 The *Sensor Users* dialog appears.



Optionally add at least one sensor user for 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 see [step 5](#) on page 8.

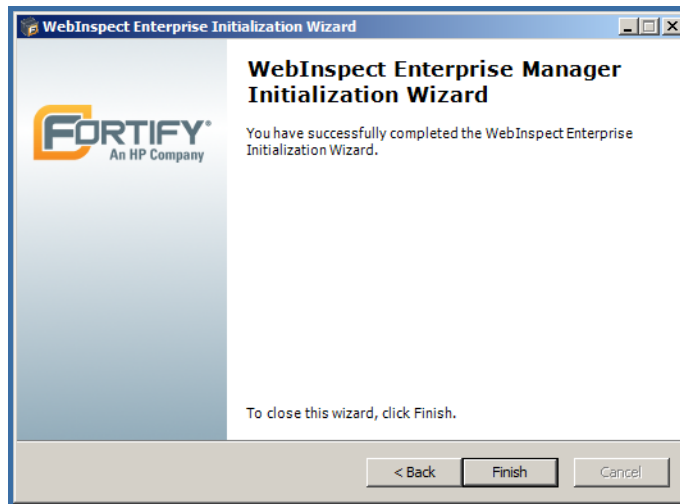
You do not have to add any sensor users to WebInspect Enterprise in this step, but you will need to specify at least one sensor user before you can run any scans. Post-installation configuration procedures in this document also describe how to add sensor users.

To add a sensor user to WebInspect Enterprise now:

- a Click **Add**.
- b In the *Select Users or Groups* dialog, type the name of an existing user to add (see [step 5](#) on page 8), 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.
- c Click **OK**.
- d Verify that the sensor user you specified has been added to the list of Sensor Users in the dialog.

32 Click **Next**.

The Initialization Wizard completes.



33 Click **Finish**.

The Initialization Wizard closes. (If you have performed an AMP migration, connection to the AMP database is no longer required.)

Configuring Services

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

To start the utility, click **Start** → **All Programs** → **HP** → **HP WebInspect Enterprise 10.20** → **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 WebInspect to WebInspect Enterprise.
- **Task Service** - Monitors the queue for various tasks, including SSC project version updates and SSC issue synchronization.
- **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 WebInspect Enterprise Scan Uploader Service was selected for installation in [step 4](#) on page 9, 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 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* dialog 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**.

WebInspect Enterprise Configuration

This area of the interface displays the WebInspect Enterprise configuration.

To configure WebInspect Enterprise:

- 1 Click **Configure** in the WebInspect Enterprise Configuration section.
The *WebInspect Enterprise Configuration* dialog appears.
- 2 Enter the URL of the WebInspect Enterprise Manager.
- 3 Provide the 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

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

To create a dropbox:

- 1 Click **Add** in the Dropbox Configuration section.
The *Configure Dropbox* dialog 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).
Be sure to select or create a folder that will not be used for any other purpose.
- 4 Enter the project version that will be serviced by this dropbox.
- 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* dialog 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**
On Windows Server 2003, the location is:
`\Documents and Settings\All Users\Application Data\HP\WIE\UploaderService`
On Windows Server 2008, the location is:
`\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, 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, 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

Service Status

This area of the interface displays the current status of the Task service, which handles background tasks such as SSC project version updates and SSC issue synchronization. You can start, stop, restart, or configure the service.

To configure the service:

- 1 Click **Configure** in the Service Status section.
The *Configure Service* dialog 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* dialog appears.
- 2 Enter a server name.
- 3 Specify the account under which WebInspect Enterprise will connect to the database.
 - **Windows Authentication** - The name and password specified in the WebInspect Enterprise Manager's user account is used to authenticate to the database. When working in a domain environment, the 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 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* dialog 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**
On Windows Server 2003, the location is:
`\Documents and Settings\All Users\Application Data\HP\WIE\TaskService`
On Windows Server 2008, the location is:
`\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.
When a log file reaches its maximum size, 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, 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.
- 6 Click **OK**.

SSC poll interval

This area of the interface determines how often WebInspect Enterprise contacts Software Security Center (SSC) for updates.

- 1 In the **SSC project version updates polling interval** field, specify (in seconds) how frequently WebInspect Enterprise contacts SSC to check for project version name changes or deletions.
- 2 In the **SSC issue synchronization interval** field, specify (in minutes) how frequently WebInspect Enterprise contacts SSC 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

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* dialog 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**.

WebInspect Enterprise Manager

If the 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* dialog 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**

On Windows Server 2003, the location is:
`\Documents and Settings\All Users\Application Data\HP\WIE\Scheduler`

On Windows Server 2008, the location is:
`\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, 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, 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.

Close the WebInspect Enterprise Services Configuration utility.

Installing the WebInspect Enterprise Administrative Console

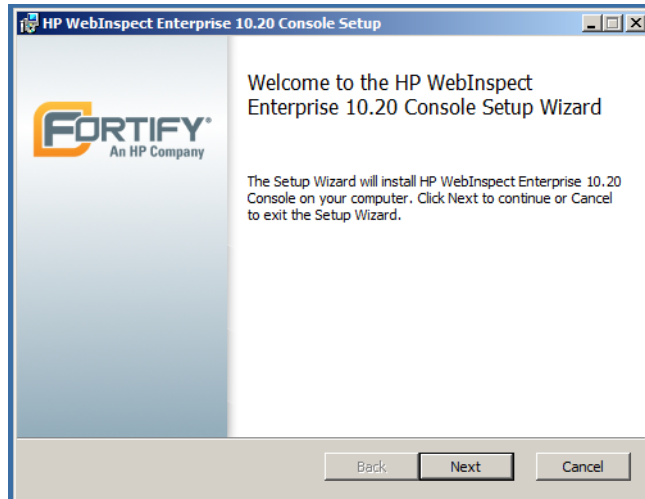
For system requirements and notes about the WebInspect Enterprise Administrative Console, see the *HP Fortify Software Security Center System Requirements* for Software Security Center version 4.10.

To install the WebInspect Enterprise Administrative Console, along with the various 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 *HP WebInspect Enterprise 10.20 Console Setup* wizard appears.

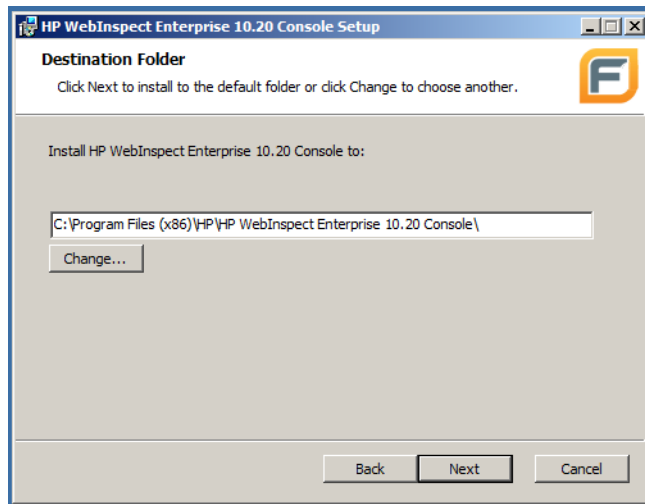


- 2 Click **Next**.

The *End-User License Agreement* dialog appears.

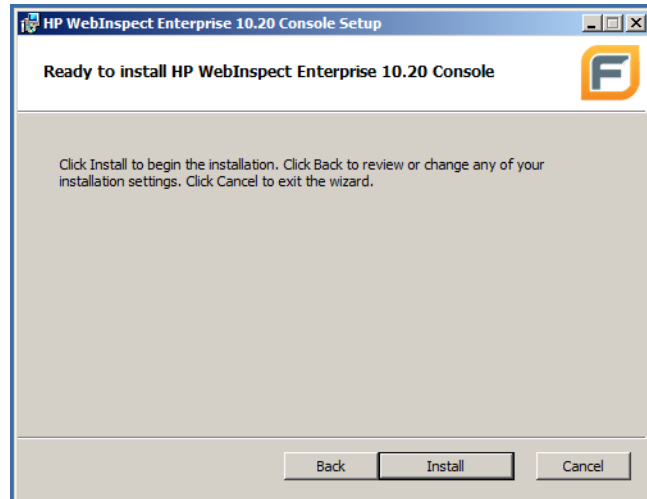
- 3 Review the license agreement. If you accept it, select the check box and click **Next**; otherwise click **Cancel**.

If you accept the license agreement, the *Destination Folder* dialog appears.



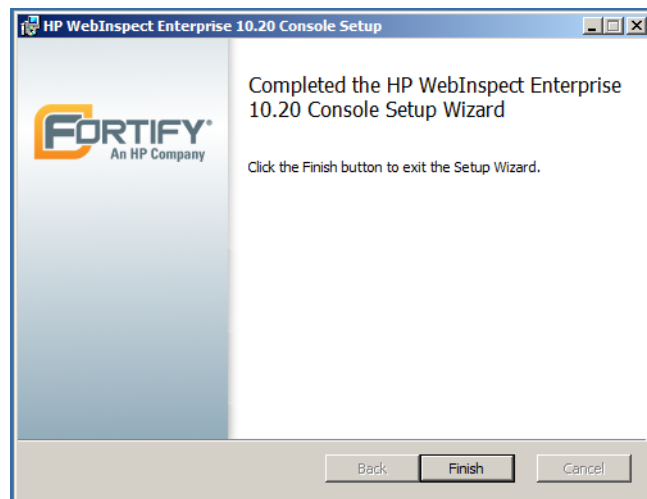
- 4 Accept the default location or click **Change** to select the location where you want to install the software, and click **Next**.

The *Ready to install HP WebInspect Enterprise 10.20 Console* dialog appears.



When you are ready to install, click **Install**.

After the WebInspect Enterprise Administrative Console files are installed, the Console Setup Wizard completes.



- 5 Click **Finish**.

Logging on to the Administrative Console and Configuring Its Refresh Rate

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

- 1 Click **Start** → **HP WebInspect Enterprise 10.20 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**.

- 2 Using the **Log on to** list, enter or select the URL of the WebInspect Enterprise manager. In this case, the value can be literally `https://localhost/WIE/`.

- 3 Enter the **Username** and **Password** for an account that has permission to access the Administrative Console. Initially, you can specify the SSC Administrator you specified in [step 22](#) on page 19. Thereafter, you can add other WebInspect Enterprise administrators, as described in [Assigning Administrators and Roles](#) on page 38 and in the *HP WebInspect Enterprise User Guide*, which (now that the software is installed) you can access by clicking **Start** → **All Programs** → **HP** → **HP WebInspect Enterprise Console 10.20** → **WebInspect Enterprise User Guide**.
- 4 Select the option **Save password** as desired.
- 5 Select the option **Automatically log on when this application starts** as desired.
- 6 To go through a proxy server to reach the WebInspect Enterprise manager:
 - a Click the **Proxy** tab.
 - b Select one of the following:
 - **Use the Internet Explorer proxy** (to use the proxy server specified in Tools → Internet Options → Connections → LAN Settings).
 - **Use the proxy below**, and then provide the proxy server's IP address and port number.
 - c Provide a valid **Username** and **Password**.
- 7 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.

Configuring the Administrative Console Refresh Rate

To specify a refresh rate for the WebInspect Enterprise Administrative Console:

- 1 From the **Tools** menu, select **Options**.
The *WebInspect Enterprise Options* window opens.
- 2 To refresh the Administrative Console information periodically, select the **Automatically refresh display every** check box and specify how often (in seconds) the display should be updated.
- 3 Click **OK**.

Post-Installation Configuration

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

- Installing WebInspect as a sensor
- Adding sensor users (if not previously done)
- Enabling sensors and configuring sensor permissions
- Assigning administrators and roles
- Moving project versions from the default group
- Configuring WebInspect Enterprise to publish scans to SSC
- For an AMP 9.20 migration, optionally migrating AMP sites to project versions

Installing WebInspect as a Sensor

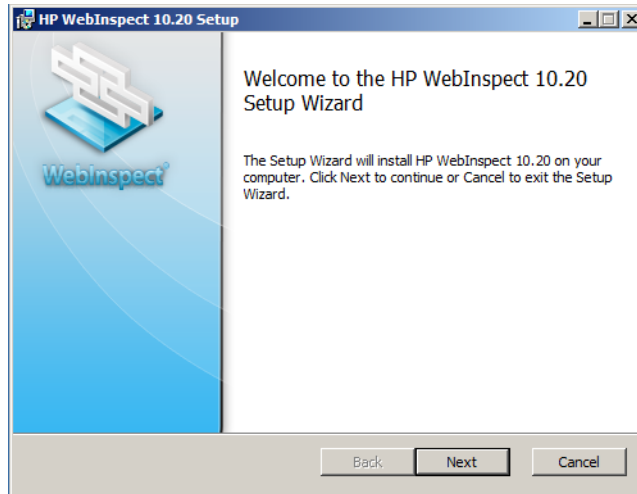
Note: For additional information about installing WebInspect, see the *WebInspect User Guide*.

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

- 1 Launch the WebInspect 10.20 installation file.

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

The *Welcome* screen of the *HP WebInspect 10.20 Setup* wizard appears.



- 2 Click **Next**.

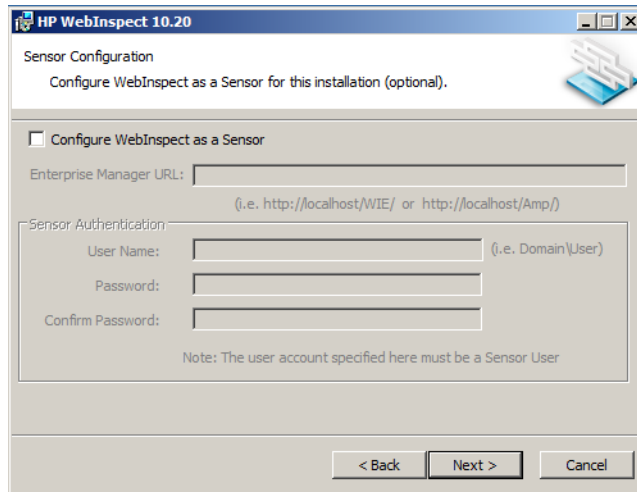
The *End-User License Agreement* dialog appears.

- 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* dialog appears.

- 4 Accept the default location or click **Browse** to select the location where you want to install the software, and click **Next**.

The *Sensor Configuration* window appears.

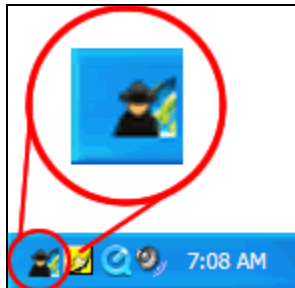


- 5 If you want to test the sensor username and password credentials before starting the sensor service and/or you want to connect the sensor to a remote SQL Server, skip to [step 7](#) and do *not* configure WebInspect as a sensor at this time. In this case, you will *install* WebInspect, then test the sensor credentials and/or connect to a remote SQL server, and then *configure* WebInspect as a sensor.
- 6 Complete the fields on the *Sensor Configuration* window:
 - a Select the **Configure WebInspect as a Sensor** option.
 - b In the **Enterprise Manager URL** field, enter the WebInspect Enterprise URL (as previously specified in [step 21](#) on page 18).
 - c In the **Sensor Authentication** section, enter the Windows account credentials of a sensor user for this sensor. See [step 5](#) on page 8.
- 7 Click **Next**.

The *Ready to install HP WebInspect 10.20* dialog appears.
- 8 When you are ready to install, click **Install**.
- 9 When the installation process is complete, select the option to launch WebInspect and click **Finish**.
- 10 The first time you launch WebInspect, its License Wizard opens. Follow the instructions. For more information, see the *WebInspect User Guide*.
- 11 If you chose not to configure WebInspect as a sensor and skipped [step 6](#), go to [Test Sensor Credentials and/or Specify a Remote SQL Server, If Necessary](#) on page 35.
- 12 Now the **Sensors** shortcut in the WebInspect Enterprise Administrative Console should list the sensor you just started (although it is not enabled yet).

If the sensor is not listed:

- a Click **Start** → **All Programs** → **HP** → **HP WebInspect** → **HP Fortify Monitor** to launch the HP Fortify Monitor program.
- b Click the HP Fortify icon in the task tray.



- c Click **Start Sensor**.
 - d Verify that the sensor is listed in the **Sensors** shortcut in the Administrative Console.
- 13 This completes the installation and configuration of WebInspect as a sensor. Go to [Adding Sensor Users \(If Not Previously Done\)](#) on page 37 or [Enabling Sensors and Configuring Sensor Permissions](#) on page 37, which are procedures that are performed in WebInspect Enterprise.

Test Sensor Credentials and/or Specify a Remote SQL Server, If Necessary

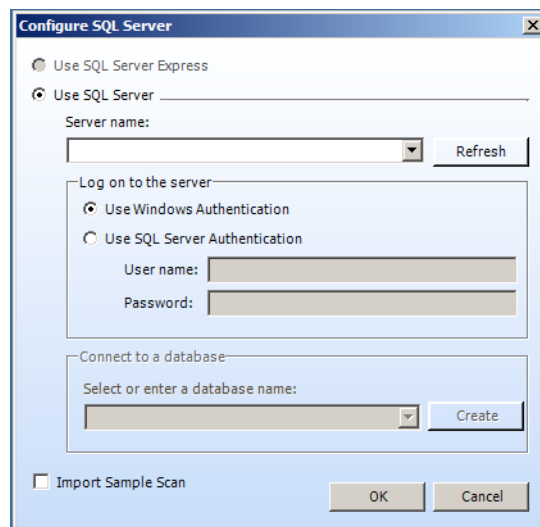
If you chose not to configure WebInspect as a sensor in [step 5](#) on page 34, you can now:

- Optionally test the sensor username and password credentials before starting the service.
- Optionally specify sensor connection to a remote SQL Server.
- Complete the configuration of WebInspect as a sensor.

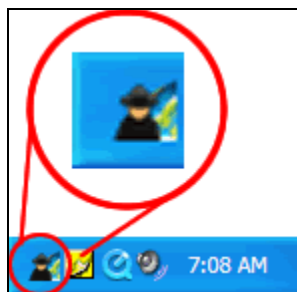
To perform these tasks:

- 1 When you launch WebInspect, if SQL Server Express is not installed, you are prompted to either run WebInspect now and enter remote SQL Server credentials, or close WebInspect and manually install SQL Server Express.

If you choose the option to run WebInspect and enter remote SQL Server credentials, the *Configure SQL Server* dialog appears. Complete this dialog and click **OK**.



- 2 On the WebInspect Start Page, click **Manage Scans** and then click **Connections**. Verify that SQL Server Express is being used as the database.
- 3 After WebInspect launches, click **Start** → **All Programs** → **HP** → **HP WebInspect** → **HP Fortify Monitor** to launch the HP Fortify Monitor program.
- 4 Click the HP Fortify icon in the task tray.



- 5 Click **Configure Sensor**.

The *Configure Sensor* dialog appears.

The screenshot shows the 'Configure Sensor' dialog box. The 'Manager URL' field contains 'https://localhost/wie/'. The 'Sensor Authentication' section has 'User Name' and 'Password' fields, a 'Domain\User' label, and a 'Test' button. The 'Enable Proxy' section has a checkbox and a 'Proxy Settings' sub-section with 'Address', 'Port' (dropdown), 'User Name', and 'Password' fields. The 'Advanced' section has a checkbox 'Override Database Settings' and a 'Configure' button. The 'Service Account' section has 'Log on as:' radio buttons for 'Local System account' (selected) and 'This account', and 'Password:' and 'Confirm Password:' fields. The 'Sensor Status' section shows 'The sensor service is currently stopped' and 'Start' and 'Stop' buttons. At the bottom right are 'OK' and 'Cancel' buttons.

- 6 Complete the fields:
 - a In the **Manager URL** field, enter the WebInspect Enterprise URL (as previously specified in [step 21](#) on page 18).
 - b In the **Sensor Authentication** section, enter the Windows account credentials of a sensor user for this sensor. See [step 5](#) on page 8.
 - 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, click **Configure**, and configure the remote SQL Server.
 - e Complete the Service Account section as needed.
 - f In the Sensor Status section, click **Start** to start the sensor service if it is stopped.
- Now the **Sensors** shortcut in the WebInspect Enterprise Administrative Console should list the sensor you just started (although it is not enabled yet).
- g Click **OK**.

This completes the configuration of WebInspect as a sensor. Proceed to the following sections, which are performed in WebInspect Enterprise.

Adding Sensor Users (If Not Previously Done)

You must add at least one user that will be a sensor user on the WebInspect Enterprise server. At least one sensor user should have been created as a Windows user in [step 5](#) on page 8. If a sensor user was already added to WebInspect Enterprise during installation [step 31](#) on page 23, proceed to [Enabling Sensors and Configuring Sensor Permissions](#). Sensor users must *not* be general console users.

To add a sensor user to WebInspect Enterprise:

- 1 Start the Administrative Console if you have not already done so. Click **Start** → **HP WebInspect Enterprise 10.20 Console** and log on.
- 2 Select **Administration** in the left pane and then select the **Sensor Users** shortcut above.
- 3 Click **Add** in the Sensor Users form in the right pane.
- 4 In the *Select Users or Groups* dialog, type the name of an existing user to add (see [step 5](#) on page 8), 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.
- 5 Click **OK**.
- 6 Verify that the sensor user you specified has been added to the list of Sensor Users in the dialog.

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 WebInspect Enterprise Administrative Console, select **Sensors** in the left pane and verify that the localhost or domain of the sensor user you specified in [step 31](#) on page 23 or in [Adding Sensor Users \(If Not Previously Done\)](#) on page 37 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 above.
- 4 Change organization permissions:
 - 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:
 - a In the Security Group Hierarchy of the Roles and Permissions form, select **Default Group**. (This is the lowest level in the hierarchy. For a WebInspect Enterprise upgrade or an AMP migration, the customer might have previously renamed this level from its default value of **Default Group** in WebInspect Enterprise or **Default Project** in AMP.)
 - 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.

Assigning Administrators and Roles

A role is a named collection of permissions that administrators specify. The Roles and Permissions form allows you to assign administrators for three hierarchical security levels—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 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 as Policies, Blackouts, and Project Versions. Each category contains multiple permissions, such as Can Create, Can View, Can Update, Can Delete, etc.

System Level

WebInspect Enterprise system administrators have all permissions. The SSC administrator you specified in [step 22](#) on page 19 is the initial WebInspect Enterprise system administrator. Legacy system administrators from a WebInspect Enterprise upgrade or an AMP migration could also be WebInspect Enterprise system administrators. No one else can log on to WebInspect Enterprise until a WebInspect Enterprise system administrator assigns other users to roles.

A system administrator can:

- Add other users as system administrators.
- Create, rename, and delete organizations.
- Create roles that allow access to certain 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 projects 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 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 projects.

You are not required to configure multiple organizations. If you prefer, you may associate all projects 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 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 *HP WebInspect Enterprise User Guide*.

Moving Project Versions from the Default Group

When a project version is created in SSC, it is also created automatically in WebInspect Enterprise, where it is added to the Default Group in the Default Organization. To view the project versions:

- 1 Select **Administration** in the left pane and then select the **Roles and Permissions** shortcut above.
- 2 In the Security Group Hierarchy of the Roles and Permissions form, select **Default Group**. (This is the lowest level in the hierarchy. For an AMP migration, the customer might have previously renamed this level from its default value of **Default Group** in WebInspect Enterprise or **Default Project** in AMP.)
- 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 **Project Versions**.
- 5 Click **Retrieve**.

All the project versions are displayed.

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

Repeat this procedure as needed on an ongoing basis.

Configuring WebInspect Enterprise to Publish Scans to SSC

If the SSC URL or WebInspect Enterprise URL settings that you specified in [step 21](#) on page 18 have changed, then to publish scans to SSC, you must update the settings in the Administrative Console as described in the *HP WebInspect Enterprise User Guide*.

For an AMP 9.20 Migration, Optionally Migrating Sites to Project Versions

To review what the Initialization Wizard did in regard to the AMP 9.20 migration, see [step 24](#) on page 20.

AMP site migration to WebInspect Enterprise project versions is optional and can be performed at any time after WebInspect Enterprise installation, using the **Site Migration** shortcut under the **Administration** group in the Administrative Console. WebInspect Enterprise does not require anyone to migrate any sites at any particular time. This design allows users to start running WebInspect Enterprise as soon as you complete these installation procedures, regardless of the migration status of any AMP sites.

To perform site migration, the logged-in user must be *both* a WebInspect Enterprise system administrator such as the one specified in [step 22](#) on page 19 *and* a group administrator for the AMP site to be migrated. The **Site Migration** shortcut is displayed only to users who meet both requirements.

For details about site migration, in the *WebInspect Enterprise User Guide* see the information about the **Site Migration** shortcut in the **Administration** group of the Administrative Console, or from the **Site Migration** shortcut in the Administrative Console itself, press **F1** to open the associated Help topic.

Guided Scan and Creating Reports

Guided Scan is the preferred method for performing a scan because it directs users through the best steps to configure a scan that is tailored to a particular application.

The first time a user launches a Guided Scan or creates a report from WebInspect Enterprise or Software Security Center (SSC), the WebInspect Enterprise Thin Client application, including its own Help system, is automatically downloaded and installed on the user's computer. Then the function the user selected opens.

Users who want to run Guided Scans or create reports while using Mozilla Firefox must download and install the Firefox add-on for the .NET Framework Assistant. To obtain it, they can click **Add-ons** on the *Mozilla Firefox Start Page* in the Firefox browser and search .NET.

For detailed information about Guided Scan and creating reports, see the *HP WebInspect Enterprise User Guide* or the Help system for the Thin Client.

Time Stamping and Scheduling

For some installations, the WebInspect Enterprise Manager and the Administrative Console and/or the Web Console reside in different time zones. To accommodate this, the 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 WebInspect Enterprise Manager converts the time to conform to the time zone in which the console resides. Alert emails, however, are time-stamped according to the zone in which the 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 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 did not change.

Installations Lacking Internet Connection

All HP 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 from the certificate's issuing authority (VeriSign) 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.
- Use Microsoft Windows Server Active Directory to store and publish a certificate revocation list (CRL).
- Disable CRL checking for the server.
- Change the default CRL timeout period for the Microsoft Cryptography API (CAPI).
- Disable the "Check for publisher's certificate revocation" option in Internet Explorer settings. To do so, click the Internet Explorer **Tools** menu and select **Internet Options**, click the **Advanced** tab, scroll to the Security section, clear the check box next to "Check for publisher's certificate revocation," then close and restart Internet Explorer.

The recommended solution 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 <http://crl.verisign.com/pca3.crl>.
- 3 When prompted, "Do you want to open or save this file," click **Save**.
- 4 On the *Save As* dialog box, select a location and click **Save**.
- 5 Go to <http://csc3-2004-crl.verisign.com/CSC3-2004.crl>.
- 6 Repeat [step 3](#) and [step 4](#).

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

To install a CRL to the local computer certificate store:

- 1 Log on to the computer as a member of the local administrators group.
- 2 Open the Certificates snap-in for the Computer account:
 - a Click **Start**, click **Run**, type `mmc`, and then click **OK**.
 - b On the **File** menu, click **Add/Remove Snap-in**.
The *Add/Remove Snap-in* dialog box appears.
 - c On the **Standalone** tab, click **Add**.
The *Add Standalone Snap-in* dialog box appears.
 - d In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**.
 - e Select **Computer account**, and then click **Next**.

- f Click **Local computer**, and then click **Finish**.
- g Click **Close**, and then click **OK**.
- 3 Under the Console root, expand **Certificates**.
- 4 Right-click **Intermediate Certification Authorities**, click **All Tasks**, and then click **Import**.
The Certificate Import Wizard opens.
- 5 Click **Next**.
- 6 Click **Browse**.
- 7 On the *Open* dialog box, select **Certificate revocation list (*.crl)** from the **Files of type** list.
- 8 Locate and select `pca3.crl` and click **Open**.
- 9 Click **Next** and follow instructions in the wizard to complete the installation.
- 10 Go to [step 4](#) and repeat the process to import `CSC3-2004.crl`.