

Fortify Audit Assistant on Premises

Software Version: 23.2.0

Installation and Administration User Guide

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2016 - 2023 Open Text or one of its affiliates.

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 October 14, 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 4
 - Contacting Fortify Customer Support 4
 - For More Information 4
 - About the Documentation Set 4
 - Fortify Product Feature Videos 4
- Chapter 1: Welcome to Fortify Audit Assistant 5
 - About the Generation 2 Prediction Model 5
 - Intended Audience 5
 - System Requirements 5
 - Hardware Requirements 5
 - Software Requirements 6
 - Software Versions to Lose Support in the Next Release 6
 - Additional Requirements 7
 - Supported Browsers 7
 - Kubernetes Cluster 7
 - Related Documents 8
 - All Products 8
 - Fortify Software Security Center 9
- Chapter 2: Preparing for Fortify Audit Assistant Deployment 10
- Chapter 3: Fortify Audit Assistant Installation 11
 - Installing Fortify Audit Assistant 11
- Chapter 4: Adding Tenants 13
- Chapter 5: Switching Tenants 14
- Chapter 6: Managing User Accounts 15
 - Creating User Accounts 15
 - Editing User Accounts 15
 - Deleting User Accounts 16
 - Accessing Online Help 16
- Send Documentation Feedback 17

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>

Chapter 1: Welcome to Fortify Audit Assistant

OpenText™ Fortify Audit Assistant (Fortify Audit Assistant) helps you to predict which of the issues returned from OpenText Fortify Static Code Analyzer (Fortify Static Code Analyzer) represent true vulnerabilities and which do not. To make its determinations, Fortify Audit Assistant needs audit data to establish a baseline for its audits. You can use **Fortify data**, which is a data set derived from the historical audits of static analysis scans performed by Fortify expert auditors in the Fortify on Demand managed service. If you would like the model to include data from your own auditors, you can choose to use **Fortify and local tenant data**. In this case, Fortify Audit Assistant on Premises will incorporate results tagged by your own audits with the **Fortify data**.

About the Generation 2 Prediction Model

The 23.2.0 release of Fortify Audit Assistant on Premises includes generation 2 (G2) of Audit Assistant's AI-powered prediction model. The new model replaces the original, generation 1 (G1) model, available in the previous release. While the G1 model is still available for those who have yet to update, Fortify recommends the use of the new, more powerful, G2 model. When updating your version of Fortify Software Security Center to 23.2.0, you will be required to use the G2 model.

Intended Audience

This content is written for users who are responsible for deploying and maintaining an instance of Fortify Audit Assistant on Premises. It provides the information needed to acquire, install, and configure the product, and to set up one or more tenants.

The information presented here is intended for users who are at least moderately knowledgeable about enterprise application development and skilled in enterprise system administration. It is written for system and instance administrators.

For information about how to use Fortify Audit Assistant after installation, see the Fortify Audit Assistant online help and the Fortify Audit Assistant on Premises configuration and usage sections in the *OpenText™ Fortify Software Security Center User Guide*.

System Requirements

This section describes the system requirements for any OpenText Fortify Audit Assistant on premises deployment.

Hardware Requirements

Following are the hardware requirements for installing and using Fortify Audit Assistant on premises.

PostgreSQL database server: 8 CPU cores, 32 GB RAM, 500 GB hard drive

Software Requirements

Product	Supported Versions
PostgreSQL Note: This requires manual installation. Fortify recommends that you install and manage the database on a Linux system.	11.x
Kubernetes cluster	1.26.x, 1.27.x, 1.28.x
Reverse proxy with SSL offloading to provide for secure HTTPS access. (You can use a load balancer, Kubernetes Ingress, HAProxy, NGINX, and so on.)	
Outgoing SMTP server (for sending emails from Fortify Audit Assistant)	
Helm Command-line client	3.11, 3.12
Kubectl	Any version that is compatible with the Kubernetes cluster. Recommended for troubleshooting.
Docker (client and server) Note: Required only for the transfer of Fortify Audit Assistant images to a private registry.	20 and later versions

Important! Fortify Audit Assistant must not be accessible over HTTP. It must be accessible over HTTPS only.

Software Versions to Lose Support in the Next Release

The following software versions are scheduled for deprecation in the Fortify Audit Assistant on Premises release.

- Kubernetes (cluster and kubectl) versions 1.26.x and 1.27.x
- Helm (either client-only or both client and a Helm Tiller service provisioned in the Kubernetes cluster) version 3.11.x

Additional Requirements

At a minimum, you must prepare the following information, which you will later use to configure the YAML file:

- Docker Hub account with access to Fortify Audit Assistant images

Note: After you purchase Fortify Audit Assistant for on premises installation, Fortify sends an email address to which you send your Docker account name. After you send your Docker account information to Fortify, Fortify sends an email response to confirm that your Docker account name was added to Fortify Docker and that you have access to the Fortify repository. If you have access problems, please contact MFI-FortifyDocker@opentext.com with your Docker account information.

- `kubeconfig` file for the Kubernetes cluster
 - DNS name for Fortify Audit Assistant web application (address used to access the Fortify Audit Assistant service)
 - PostgreSQL database connection information:
 - Database server host name
 - Database name for Fortify Audit Assistant data
- Important!** The database must be configured to use the UTF-8 character set.
- Username for an account that has permission to manage the Fortify Audit Assistant schema and data
 - Password for the username
 - Email configuration:
 - Outgoing SMTP server address / port (credentials, if required)
 - Email address to be used to send emails from the Fortify Audit Assistant service
 - Email address to use for the initial administrator account in the Fortify Audit Assistant service
 - License (XML file) for the Fortify Audit Assistant service

Supported Browsers

Fortify Audit Assistant supports the browser versions listed in the following table.

Browser	Supported Versions
Microsoft Edge	114 or later
Google Chrome	115 or later
Mozilla Firefox	115 or later
Safari	14 or later

Fortify Audit Assistant also supports mobile browser screen resolutions.

Kubernetes Cluster

Fortify Audit Assistant installation requires a Kubernetes cluster (based on a supported Kubernetes version) that uses a container runtime that is compatible with Linux x86-64 OCI (Open Container Initiative)

container images. The following table lists the hardware required for this.

Cluster Component	Processor (per instance)	RAM / Hard Drive
Fortify Audit Assistant portal Recommended: 2 instances	2 CPU cores	1 GB / 10 GB ephemeral local volume
Predict daemon Recommended: 2 instances	4 CPU cores	4 GB / 50 GB ephemeral local volume
Train daemon (one instance only)	3 CPU cores	6 GB / 50 GB ephemeral local volume Note: A training data set that includes a large volume of data (over five million issues) requires increased RAM.
Util daemon (one instance only)	1 CPU core	1 GB / 10 GB ephemeral local volume
Predict-V2 daemon Recommended: 2 instances	4 CPU cores	4 GB / 50 GB
Train-V2 Recommended: 3 instances	3 CPU cores	6 GB / 50 GB

Related Documents

This topic describes documents that provide information about OpenText 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

All Products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the [Micro Focus Product Documentation](#) website.

Document / File Name	Description
<i>About Fortify Software Documentation</i> 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.
<i>Fortify License and Infrastructure</i>	This document describes how to install, configure, and use

Document / File Name	Description
<i>Manager Installation and Usage Guide</i> LIM_Guide_<version>.pdf	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.
<i>Fortify Software System Requirements</i> Fortify_Sys_Reqs_<version>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Fortify Software Release Notes</i> 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.
<i>What's New in Fortify Software</i> <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 Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-software-security-center>.

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

Chapter 2: Preparing for Fortify Audit Assistant Deployment

The following steps describe how to prepare for Fortify Audit Assistant on premises deployment. For information about supported versions of the required software, see "[System Requirements](#)" on page 5.

To prepare for your Fortify Audit Assistant deployment on premises, do the following:

1. Install and set up kubectl. For instructions, see <https://kubernetes.io/docs/tasks/tools/install-kubectl>.
2. Download and install PostgreSQL for your Linux operating system. (See <https://www.postgresql.org/download/>.)
3. Create a PostgreSQL database. (For instructions, see <https://www.postgresql.org/docs/11/sql-createdatabase.html>.)

Important! The database must be configured to use the UTF-8 character set.

4. Install Helm. (To download the software, see <https://github.com/helm/helm/releases>. For installation instructions, see https://helm.sh/docs/using_helm/#installing-helm.)

See Also

["Fortify Audit Assistant Installation" on page 11](#)

Chapter 3: Fortify Audit Assistant Installation

Once you have prepared for Fortify Audit Assistant installation ("[Preparing for Fortify Audit Assistant Deployment](#)" on page 10), you must decide how you want to deploy the application.

You can deploy Fortify Audit Assistant on a machine that has Internet access, or in an air-gapped environment.

If you can deploy the application on a machine with Internet access, you can use a remote repository. If you must deploy the application in an air-gapped environment, you must use a private registry for the installation.

Installing Fortify Audit Assistant

The procedure used to install Fortify Audit Assistant on a machine with Internet access is almost identical to the procedure used to install the product in an air-gapped environment. The only difference is that, for an air-gapped installation, you must push the Fortify Audit Assistant images to a private registry.

To install Fortify Audit Assistant:

1. Create a Docker Hub account, and then supply your account name to Fortify Support (<https://softwaresupport.softwaregrp.com>).

Note: After you purchase Fortify Audit Assistant on Premises, Fortify sends an email address to which you send your Docker account name. After you send your Docker account information to Fortify, Fortify sends an email response to confirm that your Docker account name was added to Fortify Docker and that you have access to the Fortify repository. If you have access problems, please contact MFI-FortifyDocker@opentext.com with your Docker account information.

2. Create a Kubernetes secret for pulling images from registries (Docker Hub or private registry). For instructions, see <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry> and enter the secret name as the value for the `imagePullSecrets` parameter in the `custom-values-example.yaml` file. (See step 4.)

Note: The `imagePullSecrets` value is required for access to the Docker Hub registry. If you have a private repository that can be accessed without credentials, then there is no need to specify `imagePullSecrets`.

3. Download the Helm chart package and `custom-values-example.yaml` file, as follows:
 - a. Open a web browser and go to <https://github.com/fortify/audit-assistant-helm-charts>.
 - b. Click the folder for the Fortify Audit Assistant release you want to install.

The GitHub page lists the Fortify Audit Assistant Helm chart package (`audit-assistant-<chart_version>+<audit_assistant_version>.tgz`) and a sample values chart (`custom-values-example.yaml`) file that you use to configure the deployment.

- c. Download the `custom-values-example.yaml` file and the Helm chart package (TGZ file).

Caution! Do not extract the contents of the `audit-assistant-<chart_version>+<audit_assistant_version>.tgz` file. Leave the file as it is.

4. Open the `custom-values-example.yaml` file and provide all required values (except for the license information, which is addressed in step 6) and values for any additional parameters you want to specify. (For the values that are absolutely required for installation, see ["Additional Requirements" on page 7.](#))

Note: If you are using a private repository, specify a value for the `image.repositoryPrefix` parameter. The value you specify must include a trailing forward slash (/). Depending on your deployment, you may want to specify `service.type`. (Supported type values are ClusterIP, NodePort, and LoadBalancer. The default is ClusterIP.)

Important! You must add the secret name as the value of the `imagePullSecrets` parameter. For example, if you generated a secret with name "regcred," then you would specify the parameter value in following format:

```
imagePullSecrets:
  - name: regcred
```

Note: Any values you specify for parameters in the `custom-values-example.yaml` file can always be changed later. You can then redeploy Fortify Audit Assistant to implement the changes.

5. (Perform this step only for an air-gapped installation, or if you are using a private registry.) Transfer the Fortify Audit Assistant images to your private registry, as follows:

- a. To log in to Docker, run:

```
docker login
```

- b. To log in to your private registry, run:

```
docker login
<private_registry_host_and_port>
```

- c. For each image (`audit-assistant-webapp`, `audit-assistant-daemon`, `audit-assistant-install`, and `audit-assistant-data`), run the following.

Note: In the following, the `<tag>` for all images except for `audit-assistant-data` is equivalent to `<audit_assistant_version>`. The `<tag>` for `audit-assistant-data` is the same as the value of `image/dataTag` in the `custom-values-example.yaml` file.

- i. `docker pull fortifydocker/<image_name>:<tag>`
- ii. `docker tag fortifydocker/<image_name>:<tag> <private_registry_host_and_port>/<private_registry_path>/<image_name>:<tag>`
- iii. `docker push <private_registry_host_and_port>/<private_registry_path>/<image_name>:<tag>`

6. To deploy Fortify Audit Assistant run one of the following:

```
helm template --name <unique_name> -f custom-values-example.yaml --set-
file=productLicense=<path_to_license_file> ./audit-assistant<chart_
version>+<application_version>.tgz | kubectl --namespace <deployment_namespace>
apply -f-
```

Or, if Helm Tiller is installed in the Kubernetes cluster, run:

```
helm install --name <unique_name> -f custom-values-example.yaml --set-
file=productLicense=<path_to_license_file> ./audit-assistant<chart_
version>+<application_version>.tgz --namespace <deployment_namespace>
```

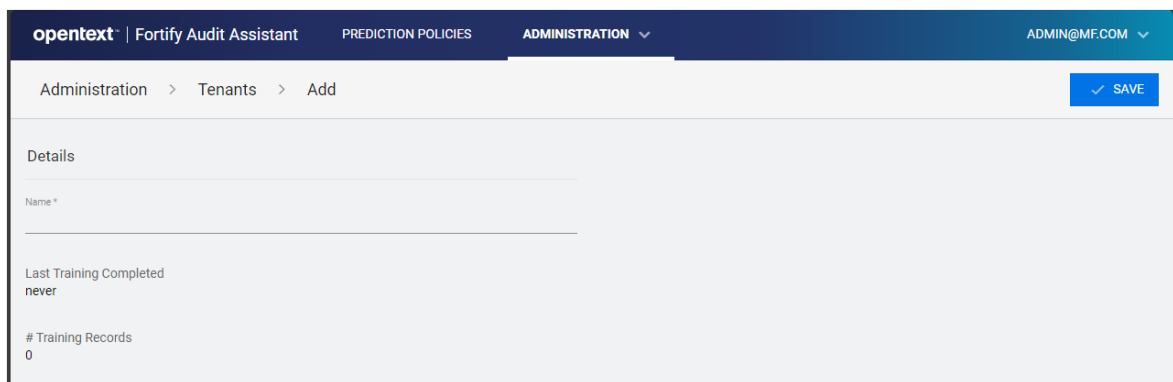
7. Set up reverse proxy with SSL offloading to provide for secure HTTPS access. (For example, you can use a load balancer, Kubernetes Ingress, HAProxy, NGINX, and so on.)

Chapter 4: Adding Tenants

Fortify Audit Assistant on Premises supports any number of tenants, but you must create at least one for your users.

To add a tenant to the system:

1. Log on to Fortify Audit Assistant as an administrator.
2. On the Fortify header, select **ADMINISTRATION**, and then select **TENANTS**.
3. In the upper right corner of the Administration > Tenants page, click the **+ ADD** button.



The screenshot shows the Fortify Audit Assistant interface. The top navigation bar includes the logo 'opentext | Fortify Audit Assistant', menu items 'PREDICTION POLICIES' and 'ADMINISTRATION', and a user profile 'ADMIN@MF.COM'. Below the navigation bar, the breadcrumb trail reads 'Administration > Tenants > Add'. A blue 'SAVE' button with a checkmark is in the top right corner. The main content area is titled 'Details' and contains three fields: 'Name *' with an empty text input box, 'Last Training Completed' with the value 'never', and '# Training Records' with the value '0'.

4. In the **Name** box, type a name for the tenant.
5. Click **SAVE**.

Now you can add users to the system and assign them to this tenant or another tenant you create. For information about how to add and manage users, see ["Managing User Accounts" on page 15](#).

See Also

["Switching Tenants" on page 14](#)

Chapter 5: Switching Tenants

A user in the administrator role can create tenants and assign users to those tenants. In addition, an administrator can impersonate a tenant user to troubleshoot potential tenant issues, examine its prediction policies, or view its usage statistics.

To log into a tenant as a user assigned to that tenant:

1. Log on to Fortify Audit Assistant as an administrator.
2. At the right end of the Fortify header, select your email address, and then select **SWITCH TENANT**.
3. From the **Tenants** list, select the name of the tenant you want to look at.
4. Click **OK**.

See Also

["Adding Tenants" on page 13](#)

Chapter 6: Managing User Accounts

The following procedures describe how to create, edit, and delete Fortify Audit Assistant user accounts:

[Creating User Accounts](#)

[Editing User Accounts](#)

[Deleting User Accounts](#)

Note: Before you can add users to the system, you must have at least one tenant to which to assign users. For information about how to create tenants, see ["Adding Tenants" on page 13](#).

Users who forget their passwords can use the **Forgot your Password?** link on the Fortify Audit Assistant login page to receive an email with a link to a password reset page.

Creating User Accounts

To create a new Fortify Audit Assistant user account:

1. On the Fortify header, select **ADMINISTRATION**, and then select **USERS**.
2. In the upper right corner of the Administration > Users page, click the **+ ADD** button.
3. Provide the following:
 - In the **Email** box, type the email for the user.
 - In the **First Name** and **Last Name** boxes, type the first and last names of the user, respectively.
4. From the **Role** list, select either **Administrator**, or **Security Lead**.
5. If you assigned the user the security lead role, then from the **Tenant** list, select the tenant to which you want to assign the user.

Note: You can specify a unique email address for a new user that you assign to one tenant. You cannot use a given email for a security lead across multiple tenants, or for an administrator *and* a security lead.

6. Click **SAVE**.

After you create the account, the user receives an email that contains a link for a password reset.

Editing User Accounts

To edit a user account:

1. On the Fortify header, select **ADMINISTRATION**, and then select **USERS**.
2. From the list of users on the Administration > Users page, select the email address for the user whose account you want to edit.

The Administration > Users > Edit page displays the account details.
3. Make your changes, and then click **SAVE**.

Deleting User Accounts

1. On the Fortify header, select **ADMINISTRATION**, and then select **USERS**.
The Administration > Users page opens.
2. On the row for the account you want to delete, select the delete icon (✕).
3. In the Confirm dialog box, click **YES**.

Accessing Online Help

For additional information about how to use Fortify Audit Assistant, see the online documentation.

To access online documentation:

- At the right end of the Fortify header, click your account name, and then select **DOCUMENTATION**.

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 Administration User Guide (Fortify Audit Assistant on Premises 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!