Micro Focus
Fortify Audit Assistant on Premise

Software Version: 19.2

Installation and Administration User Guide

Document Release Date: August 2019
Software Release Date: August 2019

Legal Notices

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

https://www.microfocus.com

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

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

This document was produced on August 09, 2019. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

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

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

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.microfocus.com/solutions/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

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

Chapter 1: Welcome to Fortify Audit Assistant

Micro Focus Fortify Audit Assistant (Fortify Audit Assistant) helps you to predict which of the issues returned from Micro Focus 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. This data consists of the decisions users have made during scan audits about how to characterize various issues uncovered in code scans. These audit decisions are sent to Fortify Audit Assistant when a user submits a Fortify Static Code Analyzer scan as training data through Fortify Software Security Center. Fortify Audit Assistant predictions regarding the actual threats that issues represent become more accurate as it receives more quality training data.

Fortify Audit Assistant can also learn through corrections that are included in a training data set. A correction is registered after a user reviews the assessment that Fortify Audit Assistant assigned to an issue, disagrees with it, adjusts the value, and then includes the issue in the data set for additional training.

Fortify provides a pre-trained policy based on the decisions on own auditors make when auditing static results in our managed application security service, Fortify on Demand. You can either use this data set, or supply data from your own tenants for contextually specific predictions.

Intended Audience

This content is written for users who are responsible for deploying and maintaining an instance of Fortify Audit Assistant on Premise. It provides all of 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 Scan Analytics online help, which is available in the user interface after deployment.

Related Documents

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

Note: You can find the Micro Focus Fortify Product Documentation at https://www.microfocus.com/support-and-services/documentation. Apart from the Release Notes, all guides are available in both PDF and HTML formats. Product help is available within the Fortify WebInspect products.

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

Micro Focus Fortify Software Security Center

The following documents provide information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Micro Focus Fortify Software Security Center User Guide SSC_Guide_<*version*>.pdf	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. 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

Document / File Name	Description
	team leads with a high-level overview of the history and current status of a project.

System Requirements

This section describes the system requirements for any Micro Focus 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

Kubernetes Cluster

Cluster Component	Processor (per instance)	RAM / Hard Drive
Fortify Scan Analytics 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

Software Requirements

Product	Supported Versions
PostgreSQL	11.x

Product	Supported Versions
Note: This requires manual installation. Fortify recommends that you install and manage the database on a Linux system.	
Kubernetes cluster	1.11.x, 1.12.x, 1.13.x, 1.14.x (recommended), 1.15.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 • Helm Tiller (server-side component) installed In the Kubernetes cluster **Note:** Tiller is recommended only if it is already installed in the cluster and is in use.	2.12.x, 2.13.x, 2.14.x (recommended)
Kubectl **Note:** Kubectl is not required if Helm Tiller is installed in the Kubernetes cluster.	Any version that is compatible with the Kubernetes cluster (version 1.11 or later)
Docker (client and server) **Note:** Required only for the transfer of Fortify Audit Assistant images to a private registry.	18 and later

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 1.11.x and 1.12.x
- Helm (either client-only or both client and a Helm Tiller service provisioned in the Kubernetes cluster) version 2.12.x

Additional Requirements

At minimum, you must prepare the following information, which you 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, Micro Focus 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 FortifyDocker@microfocus.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	42 or later
Google Chrome	75 or later
Mozilla Firefox	68 or later
Safari	12 or later

Fortify Audit Assistant also supports mobile browser screen resolutions.

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 7.

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.)

Chapter 3: Fortify Audit Assistant Installation

Once you have prepared for Fortify Audit Assistant installation ("Preparing for Fortify Audit Assistant Deployment" on page 11), 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: Fortify Support will provide you with access to the Fortify repository on Docker (fortifydocker/).

2. (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`, and `audit-assistant-install`), run the following:
      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>`
3. 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 6.)

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`.

4. 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.

5. 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 9.)

   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.

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>
```

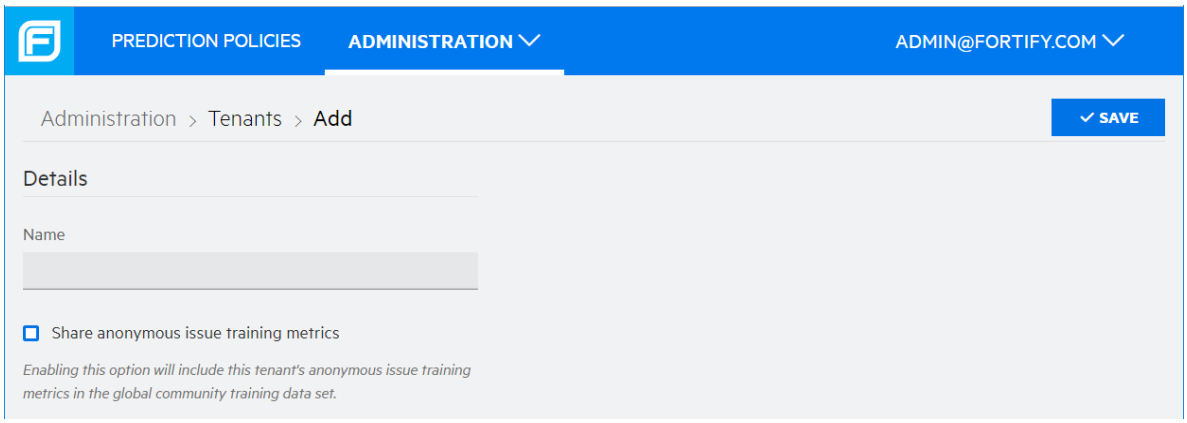
7. Set up reverse proxy with SSL offloading to provide for secure HTTPS access. (For example, you can use a load balancer, Kubernetes Ingress, HAProxy, NGINX, and so on.)

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 Scan Analytics 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 **+ ADD**.



4. In the **Name** box, type a name for the tenant.
5. If you want to include this tenant's anonymous issue training metrics in the shared data set, select the **Share anonymous issue training metrics** check box.
6. 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 17.

See Also

"Switching Tenants" on page 16

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 15

Chapter 6: Managing User Accounts

The following procedures describe how to create, edit, and delete Fortify Audit Assistant 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 15.

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 **+ ADD**.
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. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation and Administration User Guide (Fortify Audit Assistant on Premise 19.2)

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@microfocus.com.

We appreciate your feedback!