



Analytics™ GuardianAI™

Quick Installation Guide

Version 1.00.00

Rockwell Automation Publication FTGAI 95055-IN010A-EN-P



**Rockwell
Automation**

Original Instructions

Contents

- Edge Manager Deployment..... 3**
 - Prerequisites..... 3
 - Getting Started..... 3
 - Deploy FactoryTalk Analytics GuardianAI Redis Database..... 4
 - Deploy FactoryTalk Analytics GuardianAI..... 7
 - Accessing FactoryTalk Analytics GuardianAI..... 11
- Manual Container Deployment..... 13**
 - Prerequisites..... 13
 - Installation Files..... 13
 - Installing FactoryTalk Analytics GuardianAI..... 13
 - Accessing FactoryTalk Analytics GuardianAI..... 14
 - Uninstalling FactoryTalk Analytics GuardianAI..... 15
 - Resetting FactoryTalk Analytics GuardianAI Login Password..... 16
 - Adding a user to the sudoers list..... 16

Edge Manager Deployment

This section provides information about deploying FactoryTalk Analytics GuardianAI using FactoryTalk Edge Manager.

Prerequisites

Ensure the following prerequisites are fulfilled.

- Edge Node Minimum Hardware Spec
 - Processor: Intel Atom 4 core
 - Ram: 8 GB
 - SSD: 120 GB
- Edge Node is certified for Deployment with FactoryTalk Edge Manager
- FactoryTalk Edge Manager access and license are available
- FactoryTalk Analytics GuardianAI application license is available
- Ensure that the Edge Node is onboarded and status is **Online**
- Client PC Accessing FactoryTalk Analysis GuardianAI
 - OS – Windows
 - Web Client: Chrome or Edge

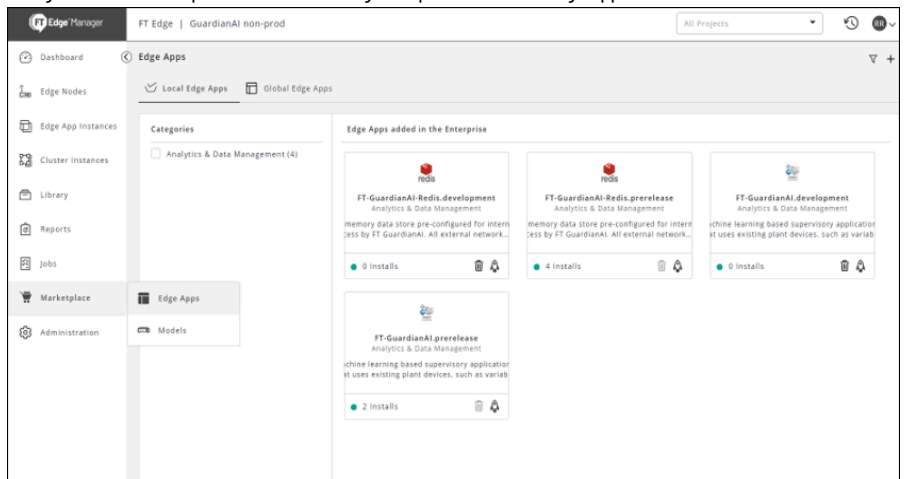
Getting Started

FactoryTalk Analytics GuardianAI has the following two containers within Edge Manager used to deploy the application.

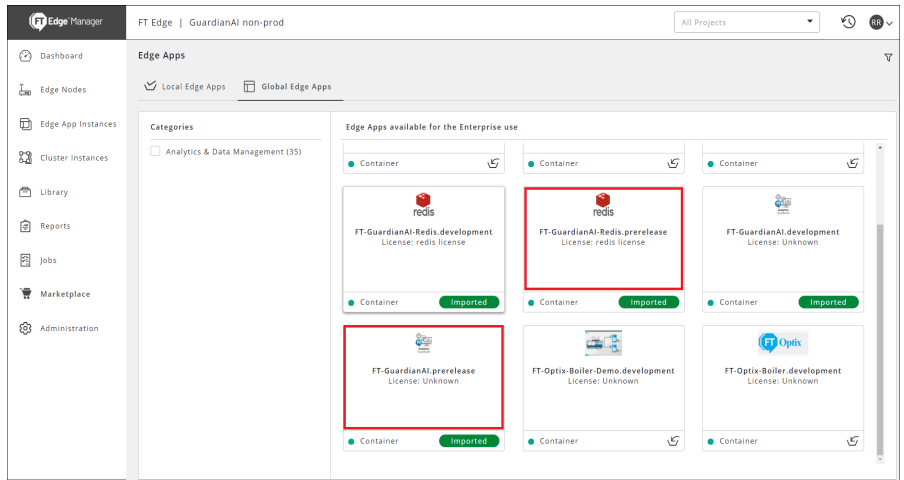
- **FT-GuardianAI-Redis:** The database container used by FactoryTalk Analytics GuardianAI.
- **FT-GuardianAI:** The FactoryTalk Analytics GuardianAI application container.



Perform the following steps to import the FactoryTalk Analytics GuardianAI application from Marketplace:

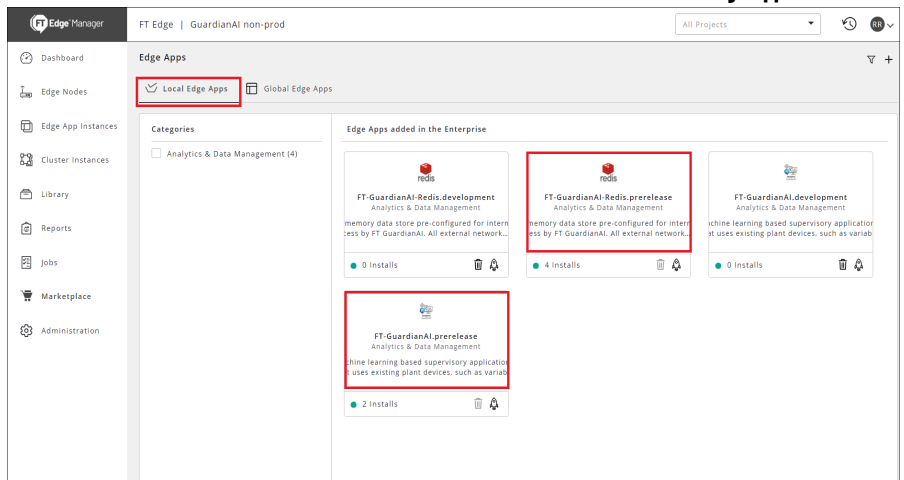
1. Navigate to the Marketplace on the left navigation panel and click Edge Apps.



2. Go to the **Global Edge Apps** tab, scroll down and click the **FT-GuardianAI-Redis** app from the list.



3. Check the details and click the import icon [].
4. Repeat the step for FT-GuardianAI and click the import icon [].
5. Both the **FT-GuardianAI-Redis** and **FT-GuardianAI** will be now available on the **Local Edge Apps**.

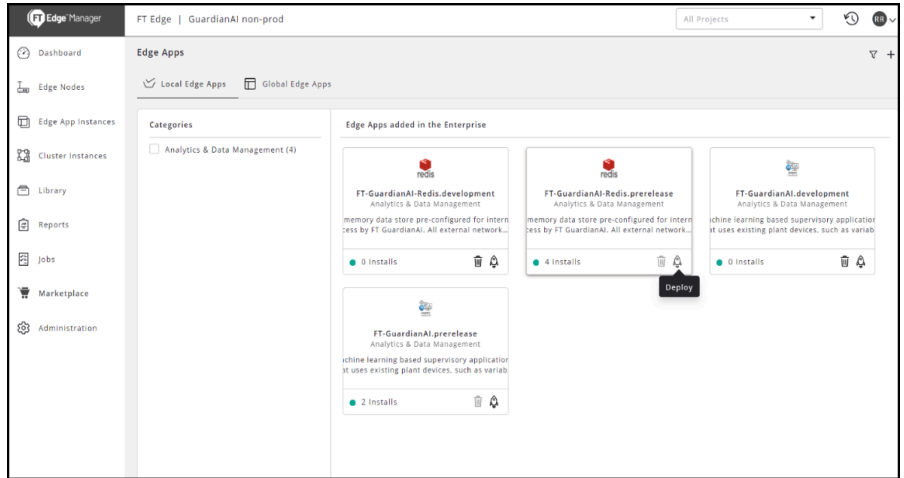



Deploy FactoryTalk Analytics GuardianAI Redis Database

Perform the following steps to deploy the FactoryTalk Analytics GuardianAI Redis database.

1. On the left navigation panel, go to the Marketplace and click Edge Apps.

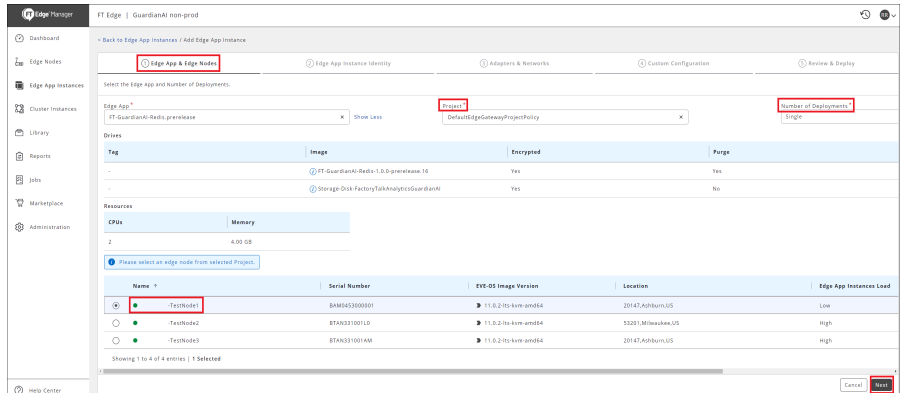
NOTE: It is important to first deploy the **FT-GuardianAI-Redis** application before the main FT-GuardianAI.



2. Click the [] icon on FT-GuardianAI-Redis to deploy the app. The **Add Edge App Instance** page displays.
3. On the **Edge App & Edge Nodes** tab, provide the following details and Click **Next**.

NOTE: It is recommended to set the other details as defaults.

- o **Project:** Select the project from the drop-down list.
- o **Number of Deployments:** Select Single for single deployment.
- o **Select an edge node from selected Project:** Select the appropriate Edge Node.



4. On the Edge App Instance Identity tab, provide the following details and click Next.
 - o **Name:** Provide a unique application name. The application name cannot be changed.
 - o **Title:** Provide a title.
 - o **Description:** Provide a detailed explanation about Edge App instance.

- On the **Adapter & Networks** tab, select the **Network Instance** from the drop-down list, review the details and click **Next**.

Network Adapter Name	Firewall Rules	Network Instance*
Eth0	Edge App Configured	defaultLocal-GuardianAI-TestNode1

- The Custom Configuration page is displayed. The Redis database has no custom configuration parameters.
- Click **Next**.
- On the **Review & Deploy** tab, review all the selected options and click **Deploy**.

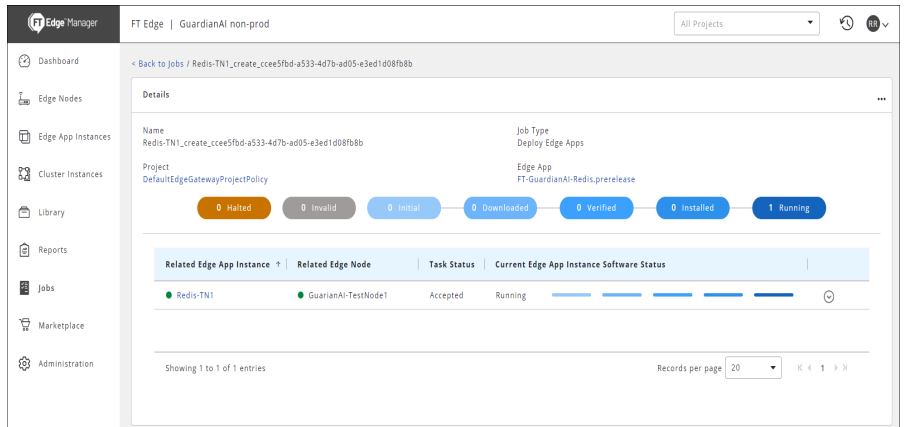
Tag	Image	Encrypted	Purge	Mount Path
-	FT-GuardianAI-Redis-1.0.0-prerelease-16	Yes	Yes	-
-	Storage-Disk-FactoryTalkAnalytics-GuardianAI	Yes	No	/data

Edge App Instance *	Edge Node	Project
Redis-TN1	GuardianAI-TestNode1	DefaultEdgeGatewayProjectPolicy

You can click **Previous** to return to the previous tabs and edit or update the details.

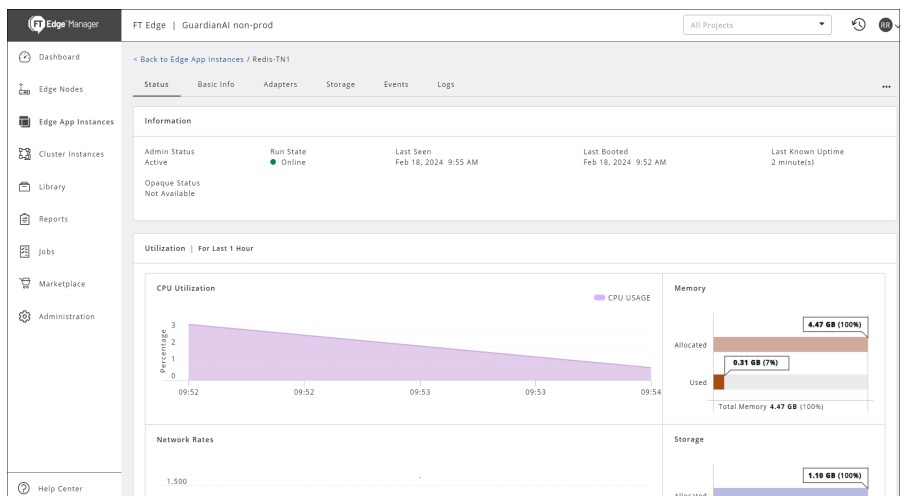
- The FactoryTalk Edge Manager will deploy to the edge node and provide a status update as Redis gets loaded and updates to a running status.

NOTE: The initial status will display as Invalid, this is normal while FactoryTalk Manager initiates the deployment.



10. The **Edge App Instance** will also provide a status view of the Redis database.

NOTE: Look for the unique application name created in step 4.

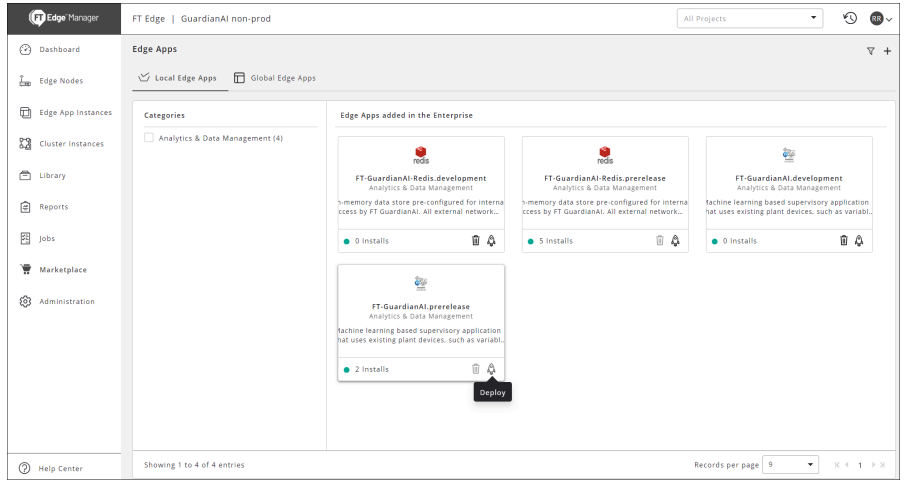



Deploy FactoryTalk Analytics GuardianAI

Perform the following steps to deploy the FactoryTalk Analytics GuardianAI application.

1. On the left navigation panel, go to the Marketplace and click Edge Apps.

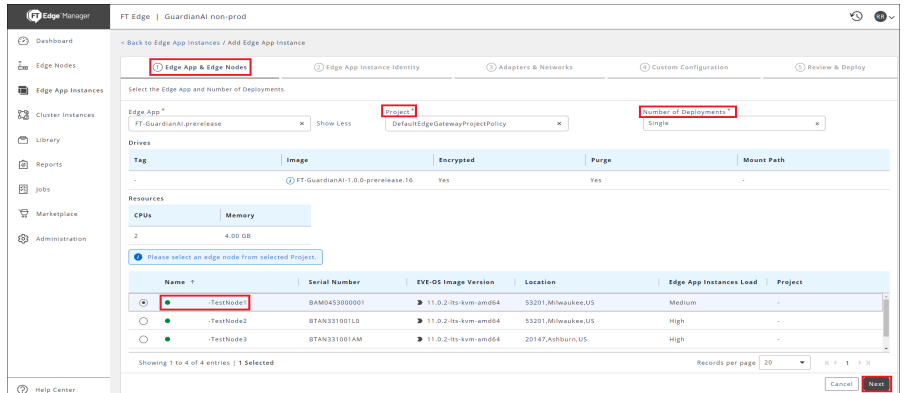
NOTE: Note: It is important to first deploy the FT-GuardianAI-Redis application before the main FT-GuardianAI.



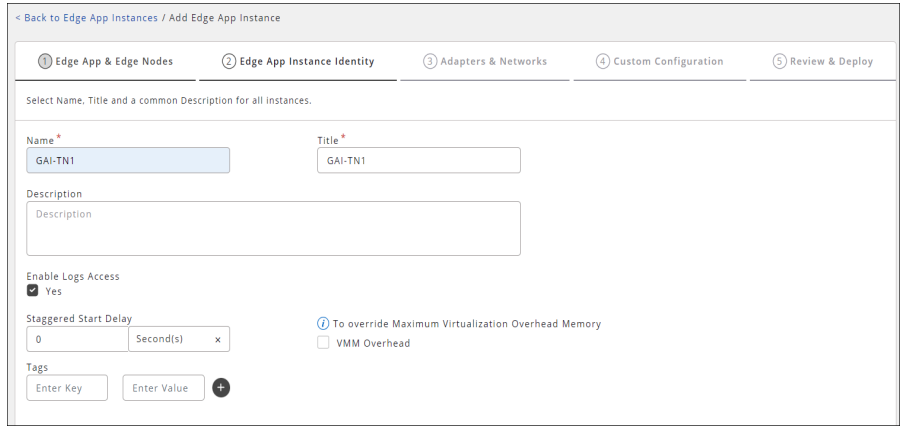
2. Click the [] icon on FT-GuardianAI to deploy the app. The **Add Edge App Instance** page displays.
3. On the **Edge App & Edge Nodes** tab, provide the following details and Click **Next**.

NOTE: It is recommended to set the other details as defaults.

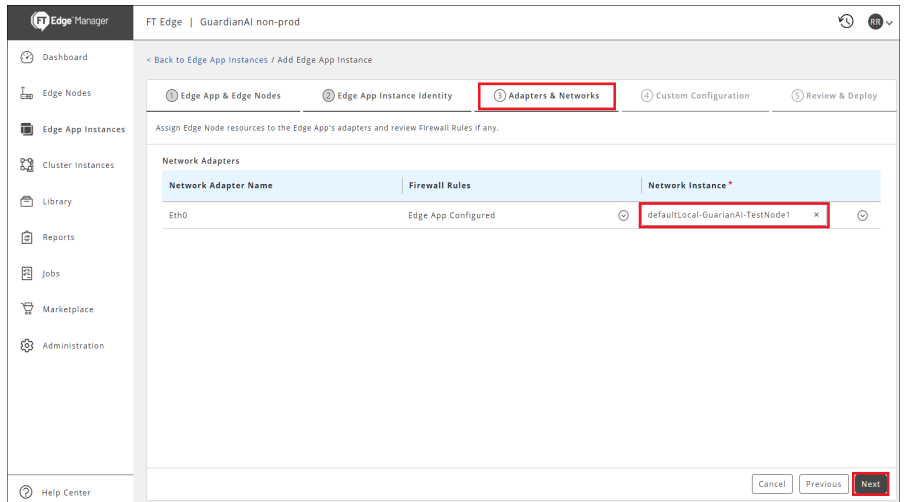
- o **Project:** Select the project from the drop-down list.
- o **Number of Deployments:** Select Single for single deployment.
- o **Select an edge node from selected Project:** Select the appropriate Edge Node.



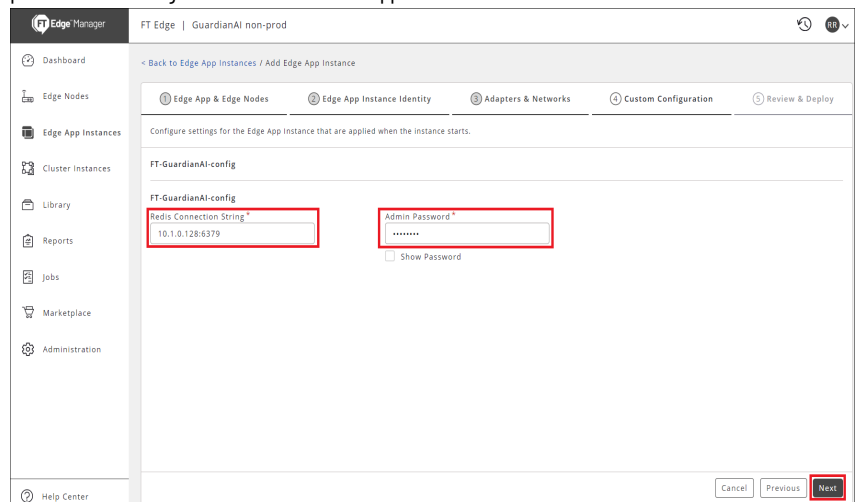
4. On the **Edge App Instance Identity** tab, provide the following details and click **Next**.
 - o **Name:** Provide a unique application name. The application name cannot be changed.
 - o **Title:** Provide a title.
 - o **Description:** Provide a detailed explanation about Edge App instance.



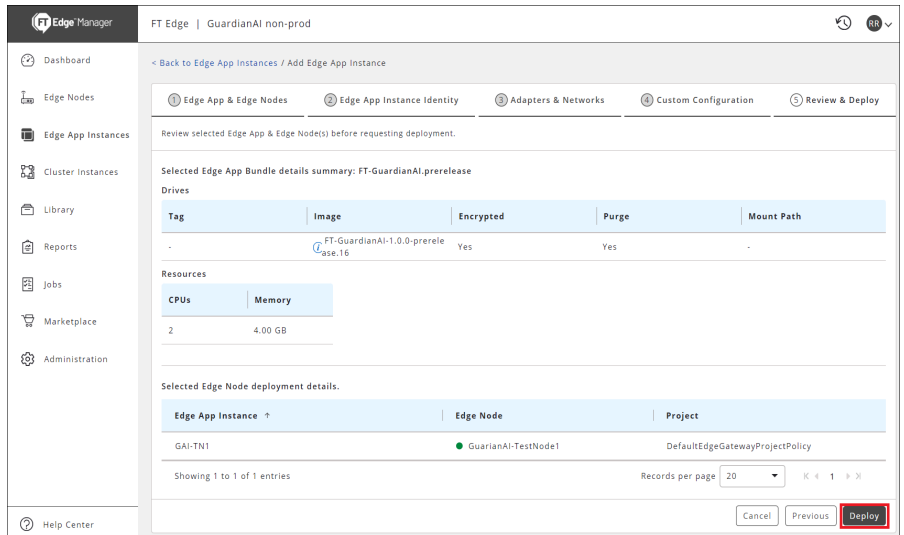
5. On the **Adapter & Networks** tab, select the **Network Instance** from the drop-down list, review the details and click **Next**.



6. The Custom Configuration page is displayed. The FactoryTalk Analytics GuardianAI application has the following parameters to configure
 - a. **Redis Connection String:** Default value is set to connect to the Redis Database. This parameter is the reason why it is important to deploy the Redis Application before FactoryTalk Analytics GuardianAI.
 - b. **Admin Password:** The FactoryTalk Analytics GuardianAI has a main login page. This parameter sets the password for the login screen to access the application



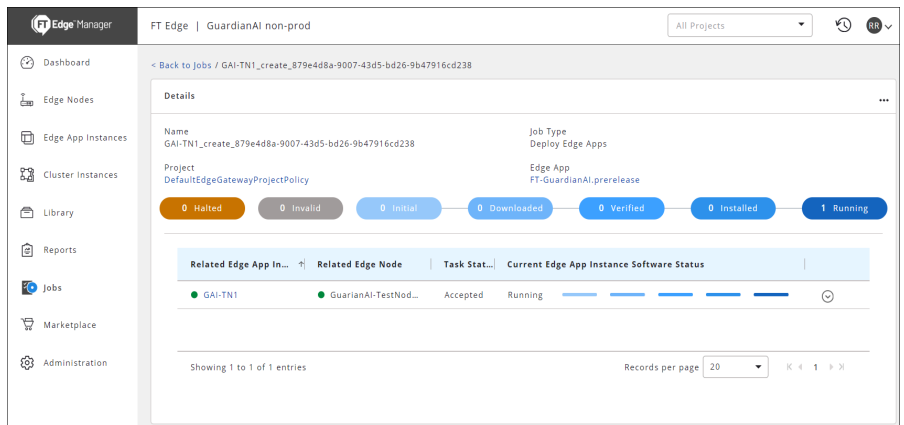
7. Click **Next**.
8. On the **Review & Deploy** tab, review all the selected options and click **Deploy**.



You can click **Previous** to return to the previous tabs and edit or update the details.

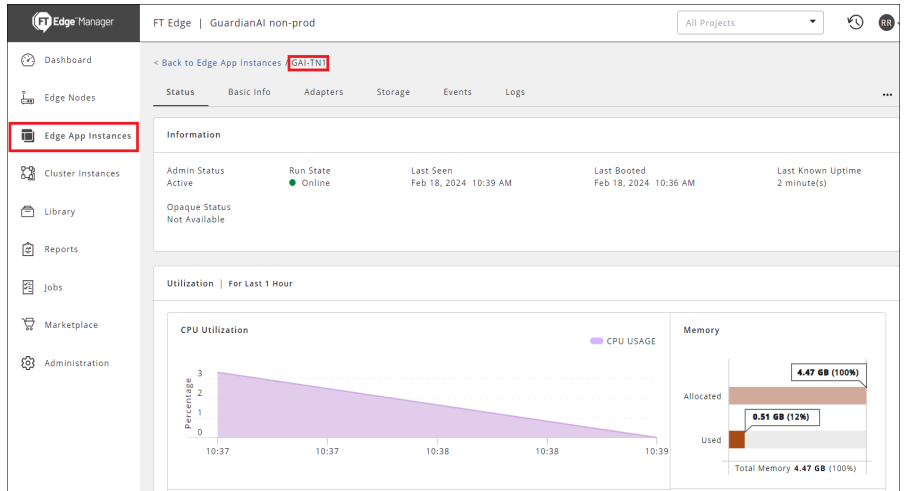
- The FactoryTalk Edge Manager will deploy to the edge node and provide a status update as FactoryTalk Analytics GuardianAI gets loaded and updates to a running status.

NOTE: The initial status will display as Invalid, this is normal while FactoryTalk Edge Manager initiates the deployment.



- The **Edge App Instance** also provides a status view of the FactoryTalk Analytics GuardianAI Application.

NOTE: Look for the unique application name created in step 4.



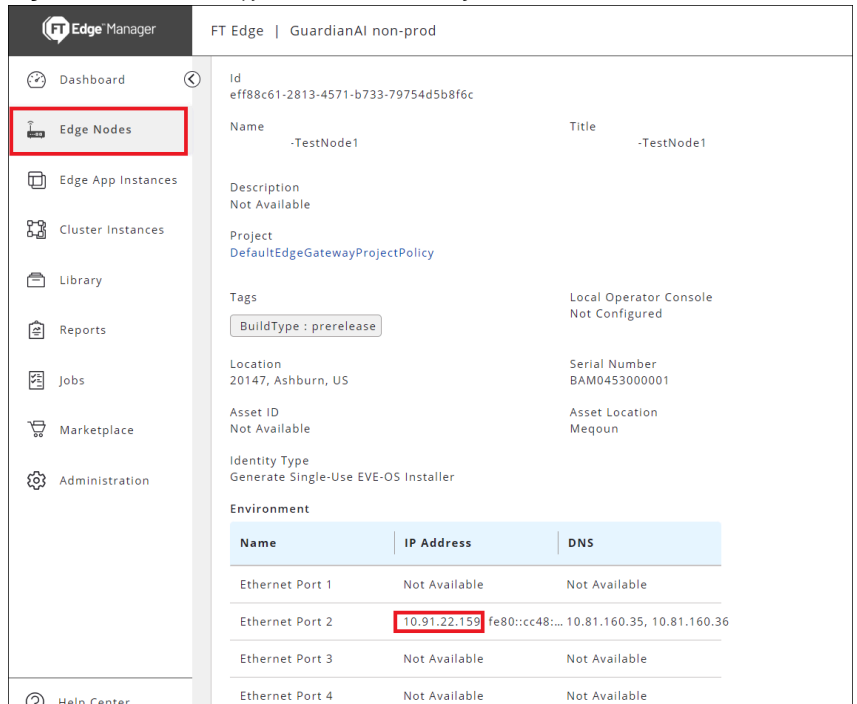
Accessing FactoryTalk Analytics GuardianAI

This section provides information on how to access FactoryTalk Analytics GuardianAI from FactoryTalk Edge Manager.

1. On a web browser, type the following URL in the following format to access the FactoryTalk Analytics GuardianAI application.

https://<Edge Device IP address>

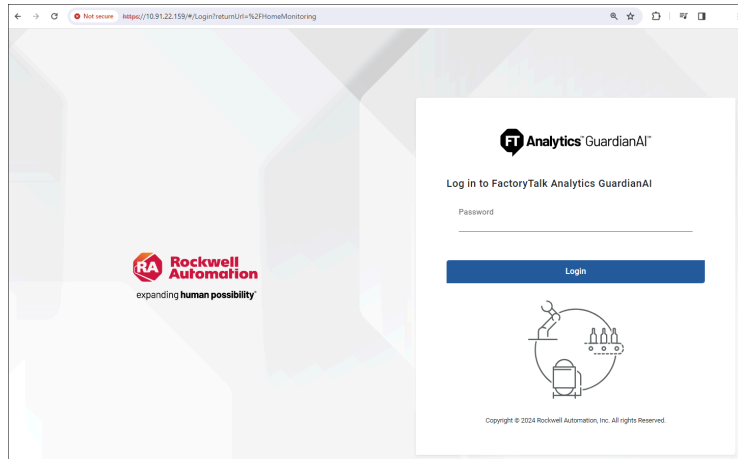
- o **Edge Device IP address:** Copy the address from the Edge Node Basic tab.



2. The application login page is displayed. Provide the password.

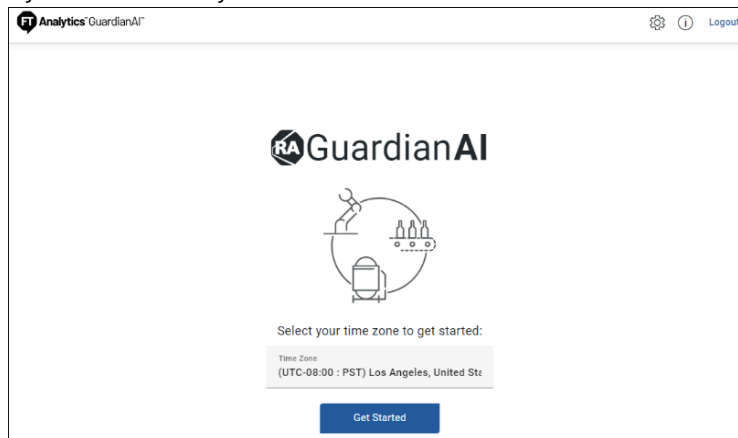
NOTE: The password is set in the custom configuration step 6 of the Deploy FactoryTalk Analytics GuardianAI section.

Figure 1. FactoryTalk Analytics GuardianAI Login Page



After login, the user will be prompted to select the time-zone for FactoryTalk Analytics GuardianAI. It is recommended to set the time zone to the locale of the compute surface where FactoryTalk Analytics GuardianAI is installed. The time zone is used by the application to record timestamps of deviation and failure risk events encountered when monitoring assets. The time zone can be modified by going to the general settings page via the gear icon in the upper right corner of the FactoryTalk Analytics GuardianAI application.

Figure 2. Time Zone Configuration



Manual Container Deployment

This section provides information about deploying FactoryTalk Analytics GuardianAI manually using container.

Prerequisites

- Minimum Hardware Specifications
 - Processor: Intel Atom 4 core
 - Ram: 8 GB
 - SSD: 120 GB
- Host Machine OS
 - Linux Debian 11, 12
- Client Computer
 - OS – Windows
 - Web Client: Chrome or Edge
- Ensure the Linux instance has web access to enable the automated script to download dependent packages

Installation Files

The following files are required to perform manual container deployment of FactoryTalk Analytics GuardianAI application.

- **Build Label**- V1.00.00
- **guardianai-install.sh** - This installation script is used to deploy FactoryTalk Analytics GuardianAI application.
- **guardianai-uninstall.sh** - This script is required in case you want to uninstall FactoryTalk Analytics GuardianAI application.
- **guardianai-reset-password.sh** - Script used to reset the Login password for the FactoryTalk Analytics GuardianAI main login screen.
- **guardianai.tar** - This file contains application files and all other dependent scripts required to run the FactoryTalk Analytics GuardianAI application.
- **redis.tar** - This file contains the redis database used as the data storage layer by the FactoryTalk Analytics GuardianAI application.

Installing FactoryTalk Analytics GuardianAI

Perform the following steps to install the FactoryTalk Analytics GuardianAI application.

1. Ensure the user executing the installation has sudo permissions. For additional information please refer to the step below “Adding a user to the sudoers list.”
2. Move the content guardianai-install.sh, guardianai-uninstall.sh, guardianai.tar, and redis.tar files to the target Linux device.
 - Create a GuardianAI directory in your user home directory.

```
guardianaivm@guardianVM12:~$ ls -l
total 36
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Desktop
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Documents
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Downloads
drwxr-xr-x 3 guardianaivm guardianaivm 4096 Feb 14 16:20 GuardianAI
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Music
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Pictures
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Public
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Templates
drwxr-xr-x 2 guardianaivm guardianaivm 4096 Feb  8 10:02 Videos
```

- Place the files in that directory
 - **Note:** WinSCP can be used to transfer files to the Linux Instance
3. Modify the permission to the installation scripts to enable execution
 - `chmod +x guardianai-install.sh`
 4. Execute the Installation script.
 - a. The installation script takes as an argument the login password that will be used for the application.
 - b. `./guardianai-install.sh <GuardianAI Login Password>`
 - c. **Note:** The user will be prompted to enter the sudo password.
 - d. Once the script is executed successfully, the user will see the following:

Figure 3. Installation Script Execution

```
guardianaivm@guardianVM12:~/GuardianAI$ ./guardianai-install_3.sh Rockwell
Starting the setup...
Updating package lists
Installing archive extractor package
Extracting GuardianAI package
Extracting database package
Installing runtime environment
Setting port 80 access
Setting port 443 access
Setting connectivity check from containers
Enabling execution after this session disconnect
Enabling scheduling service
Stopping GuardianAI runtime
Removing GuardianAI runtime
GuardianAI database does not exist
GuardianAI does not exist
Loading GuardianAI
Loading GuardianAI database, previous data is retained
Creating GuardianAI runtime
Creating database
Creating GuardianAI with admin password
Running GuardianAI
Removing GuardianAI installation archive
Removing database installation archive
```

Accessing FactoryTalk Analytics GuardianAI

FactoryTalk Analytics GuardianAI has a self-signed certificate, to access the application the user should bring up a web page using either Chrome or Edge.

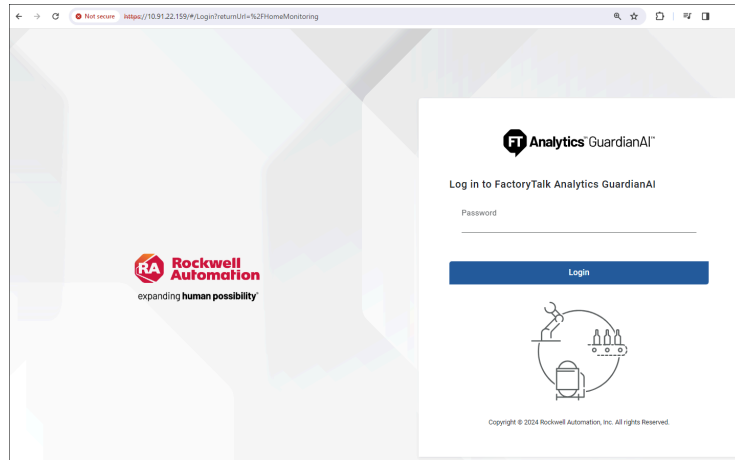
FactoryTalk Analytics GuardianAI Hyperlink: `https://<hostname>`

NOTE: Enter hostname in the Linux shell command line to get the instance hostname for connection.

The first access point for FactoryTalk Analytics GuardianAI will be the login page. The login password is the argument set when first installing the application and running the shell script, please refer back to step 4.b of the installation.

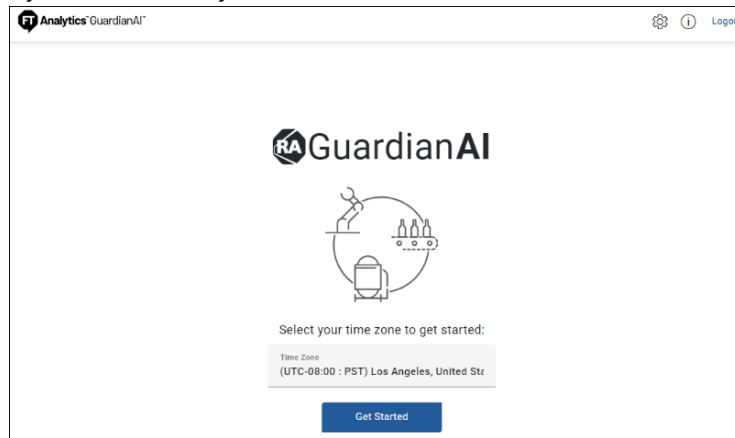
```
./guardianai-install.sh <GuardianAI Login Password>
```

Figure 4. FactoryTalk Analytics GuardianAI Login Page



After login, the user will be prompted to select the time-zone for FactoryTalk Analytics GuardianAI. It is recommended to set the time zone to the locale of the compute surface where FactoryTalk Analytics GuardianAI is installed. The time zone is used by the application to record timestamps of deviation and failure risk events encountered when monitoring assets. The time zone can be modified by going to the general settings page via the gear icon in the upper right corner of the FactoryTalk Analytics GuardianAI application.

Figure 5. Time Zone Configuration



Uninstalling FactoryTalk Analytics GuardianAI

Perform the following steps to uninstall FactoryTalk Analytics GuardianAI.

1. Ensure the user executing the installation has sudo permissions. For additional information please refer to the "Adding a user to the sudoers list."
2. Modify the permission to the uninstall scripts to enable execution.

```
chmod +x guardianai-uninstall.sh
```
3. Execute the Uninstall script.

```
./guardianai-uninstall.sh
```

- Once the script is executed successfully, the user will see the following.

Figure 6. Uninstall Script Execution

```
guardianaivm@guardianVM12:~/GuardianAI$ ./guardianai-uninstall.sh
Starting the uninstall...
Disabling GuardianAI scheduling service
Stopping GuardianAI runtime
Removing GuardianAI runtime
Removing installed GuardianAI database docker.io/guardianai/redis:7.2.4
Removing installed GuardianAI docker.io/library/guardianai:1.0.0-prerelease.17
Removing GuardianAI database files
Removing GuardianAI logs
Removing GuardianAI captured trends
```

NOTE: The uninstall script will delete all the data captured by FactoryTalk Analytics GuardianAI and fully remove the containerized application.

Resetting FactoryTalk Analytics GuardianAI Login Password

In the event a user forgets the login password for the main FactoryTalk Analytics GuardianAI page, the following script can be used to reset the password. The login password will be reset to the original password configured upon installation of the application (refer to step 4 below to query the original password)

- Modify the permission to the reset password script to enable execution.
`chmod +x guardianai-reset-password.sh`
- Execute the reset password script.
`./guardianai-reset-password.sh`
- The script will reset the password to the original value set during the installation of FactoryTalk Analytics GuardianAI.

Figure 7. Password Reset

```
guardianaivm@guardianVM12:~/GuardianAI$ ./guardianai-reset-password.sh
Deleting existing password
The password has been reset to the value that was used during product install
```

- To query the original password set during the installation, use the following command.
`podman inspect guardianai|grep Admin__Password=`

Figure 8. Query Password Set During Installation

```
guardianaivm@guardianVM12:~/GuardianAI$ podman inspect guardianai|grep Admin__Password=
      "Admin__Password=Rockwell",
      "Admin__Password=Rockwell",
```

- Users will now be able to login using the original password set during installation
- To change the password, please go to the settings page via the gear icon in the upper-right corner of FactoryTalk Analytics GuardianAI.

Adding a user to the sudoers list

Add user to the sudoer list

Perform the following steps to add a user to the sudoers list.

NOTE: A root user should add a user to the sudoers list. Before you add the user to the sudoers list, perform the first two steps in the following procedure to switch to a root user.

1. Run command: su
2. Enter the root password
3. Run command: sudo visudo

The visudo command ensures that you do not make syntax errors that can lock you out of the system.

```
GNU nano 5.4 /etc/sudoers.tmp
# This file MUST be edited with the 'visudo' command as root.
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
```

4. Using the down arrow key, scroll down to the line below root ALL=(ALL:ALL) ALL
5. Add the following as shown in the image.
 - <User name> ALL=(ALL) ALL

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
guardianauser ALL=(ALL) ALL
```

6. To exit: ctrl-x
7. Y - enter to save

```
GNU nano 5.4 /etc/sudoers.tmp *
# directly modifying this file.
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
guardianauser ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL

File Name to Write: /etc/sudoers.tmp
^G Help          M-D DOS Format    M-A Append       M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend      ^T Browse
```

8. Enter again to write to sudoers.tmp

Switch back to the user by exiting from root

- Run command: exit

```
root@guardianaivm:/home/guardianauser# exit
exit
guardianauser@guardianaivm:~$
```