ptc

thingworx®

ThingWorx Manufacturing Apps Setup and Configuration Guide

8.1.0

Copyright © 2017 PTC Inc. and/or Its Subsidiary Companies. All Rights Reserved.

User and training guides and related documentation from PTC Inc. and its subsidiary companies (collectively "PTC") are subject to the copyright laws of the United States and other countries and are provided under a license agreement that restricts copying, disclosure, and use of such documentation. PTC hereby grants to the licensed software user the right to make copies in printed form of this documentation if provided on software media, but only for internal/personal use and in accordance with the license agreement under which the applicable software is licensed. Any copy made shall include the PTC copyright notice and any other proprietary notice provided by PTC. Training materials may not be copied without the express written consent of PTC. This documentation may not be disclosed, transferred, modified, or reduced to any form, including electronic media, or transmitted or made publicly available by any means without the prior written consent of PTC and no authorization is granted to make copies for such purposes. Information described herein is furnished for general information only, is subject to change without notice, and should not be construed as a warranty or commitment by PTC. PTC assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is provided under written license agreement, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in the software licenses agreement except with written prior approval from PTC.

UNAUTHORIZED USE OF SOFTWARE OR ITS DOCUMENTATION CAN RESULT IN CIVIL DAMAGES AND CRIMINAL PROSECUTION.

PTC regards software piracy as the crime it is, and we view offenders accordingly. We do not tolerate the piracy of PTC software products, and we pursue (both civilly and criminally) those who do so using all legal means available, including public and private surveillance resources. As part of these efforts, PTC uses data monitoring and scouring technologies to obtain and transmit data on users of illegal copies of our software. This data collection is not performed on users of legally licensed software from PTC and its authorized distributors. If you are using an illegal copy of our software and do not consent to the collection and transmission of such data (including to the United States), cease using the illegal version, and contact PTC to obtain a legally licensed copy.

Important Copyright, Trademark, Patent, and Licensing Information: See the About Box, or copyright notice, of your PTC software.

UNITED STATES GOVERNMENT RIGHTS

PTC software products and software documentation are “commercial items” as that term is defined at 48 C.F. R. 2.101. Pursuant to Federal Acquisition Regulation (FAR) 12.212 (a)-(b) (Computer Software) (MAY 2014) for civilian agencies or the Defense Federal Acquisition Regulation Supplement (DFARS) at 227.7202-1(a) (Policy) and 227.7202-3 (a) (Rights in commercial computer software or commercial computer software documentation) (FEB 2014) for the Department of Defense, PTC software products and software documentation are provided to the U.S. Government under the PTC commercial license agreement. Use, duplication or disclosure by the U.S. Government is subject solely to the terms and conditions set forth in the applicable PTC software license agreement.

PTC Inc., 140 Kendrick Street, Needham, MA 02494 USA

Contents

About This Guide 4

Installing ThingWorx Manufacturing Apps....5
- Product Requirements 6
- Import as a ThingWorx Extension....7
- Configure Communication with KEPServerEX 9
- Configure Java for Tomcat.... 11

Introducing ThingWorx Manufacturing Apps 13
- Console Overview 15

Administration and Configuration....16
- Configure Users and Roles....17
- Manage Resources....19
- Alert Editing....33
- Configure Email and Text Delivery....35

Apps Overview....37
- Controls Advisor 39
- Production Advisor....50
- Asset Advisor 52
- Alert Monitoring 60
- Trending and Troubleshooting 61

Advanced Configuration 62
- Creating Custom Roles 63
- Configuring the URL Shortening Service 64
- Modifying Data Retention Settings 65
- Configuring Remote Access and Control 66
- Configuring Anomaly Detection....69

Asset Simulator....76
- Installing the Asset Simulator....77
- Asset Simulator Configuration 80
- Using the Asset Simulator 82

Frequently Asked Questions 84

Release Notes 86

About This Guide

This ThingWorx Manufacturing Apps guide describes the following:

- Installation of ThingWorx Manufacturing Apps as an extension to ThingWorx.
- Initial setup and configuration steps to get started with ThingWorx Manufacturing Apps

This guide assumes that the prerequisite products on page 6 are installed and configured, including a KEPServerEX with connected devices.

Related Documentation

It may be useful to refer to the following documents located at the PTC Reference Documents website under the product categories: ThingWorx Manufacturing Apps Family and ThingWorx Service Apps Family.

- *What's New in ThingWorx Manufacturing Apps*
- *ThingWorx Manufacturing and Service Apps Customization Guide*

Comments

PTC welcomes your suggestions and comments on its documentation. To submit your feedback, you can send an email to documentation@ptc.com. To help us more quickly address your concern, include the name of the PTC product and its release number with your comments. If your comments are about this book, include the *ThingWorx Manufacturing Apps Setup and Configuration Guide* book title.

1

Installing ThingWorx Manufacturing Apps

Product Requirements 6
Import as a ThingWorx Extension 7
Configure Communication with KEPServerEX 9
Configure Java for Tomcat 11

This chapter describes product requirements and installation for ThingWorx Manufacturing Apps.

Product Requirements

This product works in connection with ThingWorx servers and Kepware servers. To use ThingWorx Manufacturing Apps, you must have the support identified below.

Related Documentation

ThingWorx Manufacturing Apps shares the same core system requirements and compatibility matrix with ThingWorx Core. It is useful to refer to the following document located at the PTC Reference Documents website under the product category: ThingWorx

- *ThingWorx Core 8.1 System Requirements*

For more information about ThingWorx, refer to the ThingWorx Help Center.

Platform and Operating System Support

ThingWorx Manufacturing Apps are compatible with ThingWorx 8.1. For operating system support, please refer to the compatibility matrix located in the document ThingWorx Core 8.1 System Requirements.

Note

- Windows Server 2008 R2 SP1, Windows 2012 R2, and Cent OS 7.1 are recommended and fully tested for production.
- Servers running Japanese OS are not supported.

KEPServerEX Support

ThingWorx Manufacturing Apps supports data from KEPServerEX Version 6.2 or KEPServerEX Version 6.3, which include ThingWorx Native Interface. Non-Kepware servers and earlier versions of KEPServerEX can be connected to either a KEPServerEX 6.2 or KEPServerEX 6.3 server used as an aggregator.

Note

- If you plan to install the Asset Simulator, when prompted to Select Features during KEPServerEX installation, do the following:
  - Expand the Communication Drivers tree and OPC Connectivity Suite subtree. Select OPC UA Client.
  - Ensure that OPC Quick Client is selected for installation in the Communications Server tree.

KEPServerEX and ThingWorx can be installed on the same machine. However, for production we recommend separate machines.

For more information, see KEPServerEx Version 6 Install Guide.

Database Support

ThingWorx Manufacturing Apps are compatible with ThingWorx 8.1. For database support, please refer to the compatibility matrix located in the document ThingWorx Core 8.1 System Requirements.

Client Browser Support

ThingWorx Manufacturing Apps are compatible with ThingWorx 8.1. For client browser support, please refer to the compatibility matrix located in the document ThingWorx Core 8.1 System Requirements.

Import as a ThingWorx Extension

ThingWorx Manufacturing Apps are imported as a ThingWorx extension.

Note

`AssetRemoting.zip` is an optional extension that you can choose to import along with ThingWorx Manufacturing Apps. This extension enables you to use the remote access and control capability available in Asset Advisor. For more information, see Configuring Remote Access and Control on page 66

Prerequisites

Before importing this product as a ThingWorx extension, consider the following prerequisites:

- Review Product Requirements on page 6.
- Review the ThingWorx 8.1 requirements. For more information, see ThingWorx Core 8.1 System Requirements.
- Install ThingWorx 8.1. For more information, see Installing ThingWorx 8.1.
- Follow the instructions to Configure Java for Tomcat on page 11.

Import

You import this product as a ThingWorx extension into an existing ThingWorx platform install (version 8.1). To locate the download, go to the PTC Software Downloads page and expand the following folders: `PTC Smart Connected Applications | Release APPs | ThingWorx Manufacturing Apps Extension | <most recent datecode>`.

1. Do the following:
   a. Download and unzip the contents of the following file:

      `ThingWorx-Manufacturing-Apps-8.1.0-extension-bundle.zip`

   b. **Optional:** Download, but do not unzip the file `AssetRemoting.zip`
2. From ThingWorx Composer, navigate to **Import/Export** ▸ **Import**.

> **Note**
>
> The extension files must be imported in the correct order as described in the following steps.

3. In the **Import Extensions** window, navigate to:

   `ThingWorx-Manufacturing-Apps-8.1.0-extension-dependencies.zip`
4. Click **Import** and refresh the window if prompted.
5. Again, select **Import/Export** ▸ **Import**.
6. In the **Import Extensions** window, navigate to:

   `ThingWorx-Manufacturing-Apps-8.1.0-extension.zip`
7. Click **Import** and refresh the window if prompted.

> **Note**
>
> Complete the next three steps only if you have downloaded the optional `AssetRemoting.zip` extension.
>
> Otherwise, proceed to the last step.

8. Again, select **Import/Export ▸ Import**.
9. In the **Import Extensions** window, navigate to:

   `AssetRemoting.zip`
10. Click **Import** and refresh the window if prompted.
11. View the extensions after the import by selecting **Import/Export ▸ Manage**.

Verify

To verify that you can access the apps, go to the following URL on your ThingWorx server. You need to enter your port number.

https://localhost:<port>/Thingworx/FormLogin/Welcome

The default user name is `Administrator`. The password is the one you specified during the installation and configuration of ThingWorx.

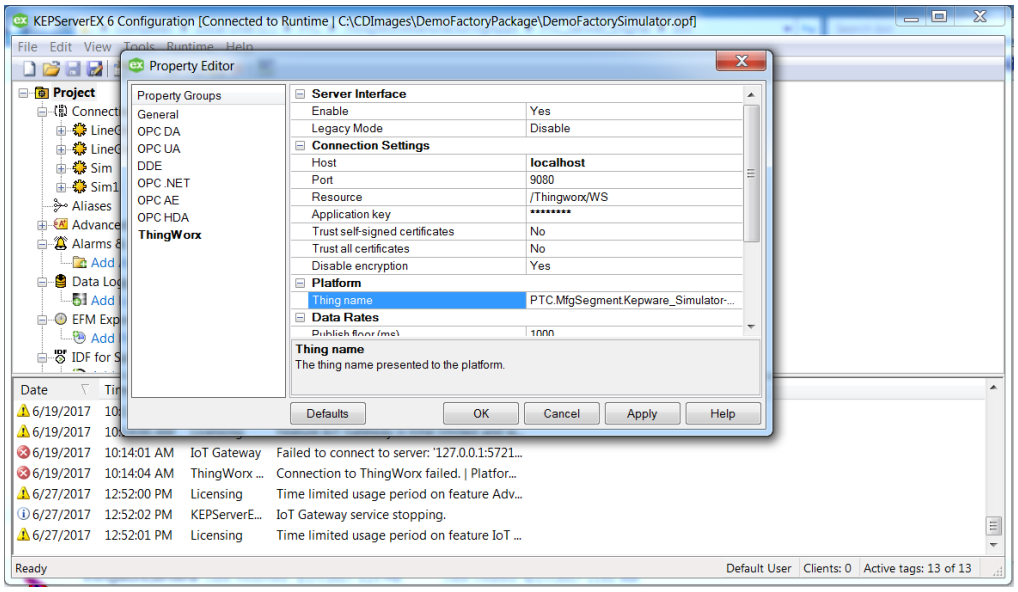
Configure Communication with KEPServerEX

The connection with KEPServerEX provides the data needed by ThingWorx Manufacturing Apps. One or more KEPServerEX servers can be connected. KEPServerEX can be on the same server or a different server than ThingWorx.

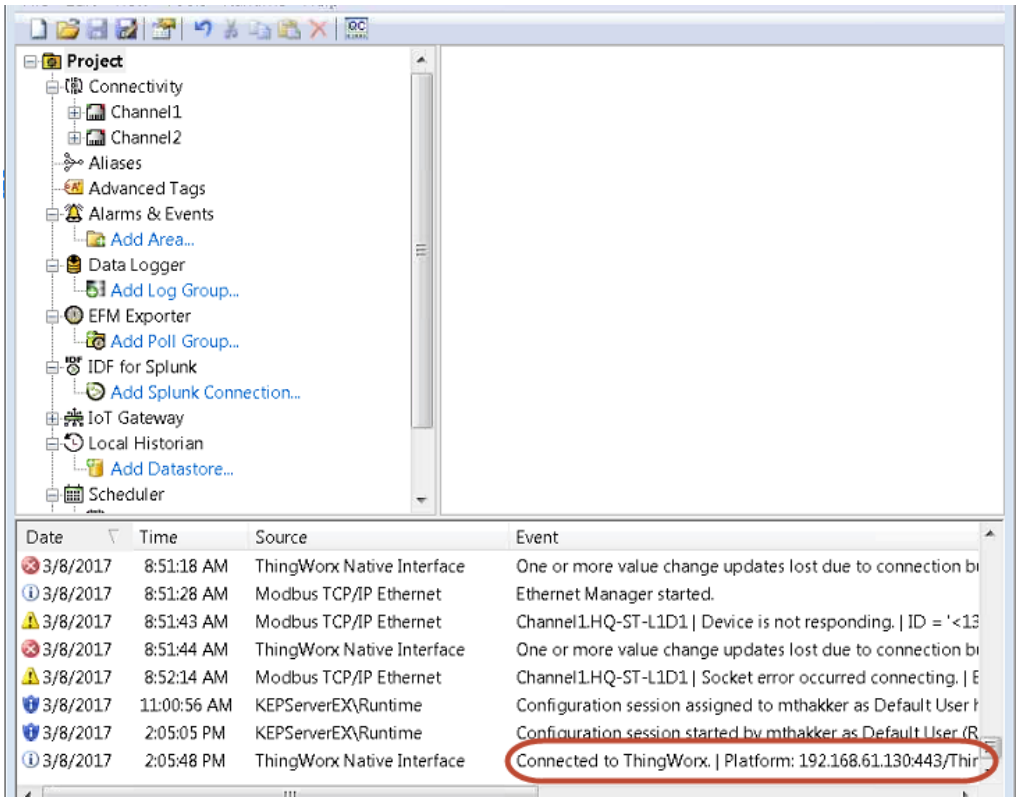
To configure communication with KEPServerEX:

1. When you open ThingWorx Manufacturing Apps for the first time using the link provided on the last page of the installer or one of the shortcut created during the installation, you are guided to create your first connection to your KEPServerEX server. You are prompted to enter a server or Thing name. Ensure that the name is one you can use to identify this KEPServerEX instance. A list of configuration parameters is generated automatically. Print or copy that information before launching ThingWorx Manufacturing Apps.
2. Input the configuration parameters under the ThingWorx tab of your instance of KEPServerEX. Right-click Project, select Properties, and then click the ThingWorx tab.

KEPServerEX then solicits the connection with your product.



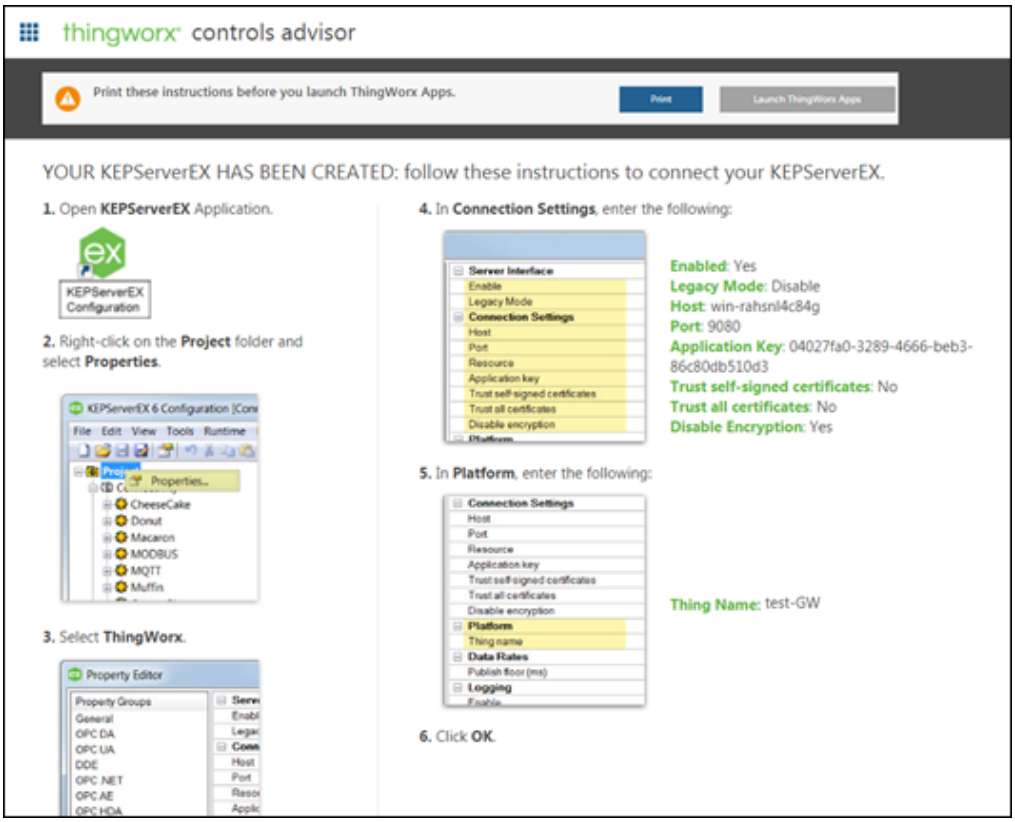
3. In the KEPServerEX configuration, a confirmation regarding a connection to ThingWorx displays in the Event column, as shown in the following figure.



If you receive an error message indicating that the connection to the ThingWorx platform failed and could not initialize a secure socket connection, follow these steps:

- Verify that the host, port, resource, application key, and Thing name are valid and correct.
- Verify that the host of KEPServerEX can reach the machine on which your product is installed. To do so, ping the hostname or IP address of the ThingWorx Manufacturing Apps host.
- Verify that the proper certificate settings are enabled.

4. Launch ThingWorx Manufacturing Apps.



5. Later, you can click **Controls Advisor** from the main console to create and manage additional server connections.

   For more information, see Controls Advisor on page 39.

Configure Java for Tomcat

To assure that ThingWorx Manufacturing Apps runs properly, you must make the following changes to your Java for Tomcat configuration.

To change your Tomcat configuration:

1. From the **Start** menu, launch the **Configure Tomcat** program.
2. Enter values in the **Initial memory pool** and **Maximum memory pool** fields.

   The recommended value is 5120.
3. Increase the default cache settings that affect static file caching. To do so, add the following line within the tags in the `$TOMCAT_HOME\conf\context.xml` file:

   ```
   <Resources cacheMaxSize="501200" cacheObjectMaxSize="2048" cacheTtl="60000"/>
   ```

2

Introducing ThingWorx Manufacturing Apps

Console Overview 15

ThingWorx role-based manufacturing apps simplify the digital transformation of manufacturing and accelerate time-to-value with unmatched deployment flexibility.

ThingWorx Manufacturing Apps include the following applications.

Controls Advisor

ThingWorx Controls Advisor is a web/mobile application that rapidly connects to and remotely visualizes data from virtually any PLC in the factory. Controls engineers are notified instantly of data communication errors that may cause the loss of critical production data. Simple tools enable users to trend and visualize data for rapid troubleshooting.

Key features include:

- Real-time visibility of asset and device status
- Instant notification and alerts of device connectivity errors
- The ability to easily trend tags in minutes

ThingWorx Controls Advisor readily connects to Kepware® to provide instant connectivity to your various assets and is built on the ThingWorx industrial IoT platform. This allows for accelerated time-to-value and the ability to quickly kick start your manufacturing journey.

Asset Advisor

Remotely monitor physical assets in real-time, automatically detect anomalies and trigger alerts to improve efficiency and quality. ThingWorx Asset Advisor is a web/mobile application that provides maintenance and service technicians with real-time visibility into the health and status of critical assets. It alerts you to potential problems that may impact production while delivering simple, easy-to-use tools for trending and troubleshooting issues.

Key features include:

- Unified connectivity to disparate assets
- Real-time anomaly detection
- Condition-based monitoring
- Asset trending and troubleshooting

ThingWorx Asset Advisor readily connects to KEPServerEX® and other OPC servers, providing instant connectivity to your assets. Built on the ThingWorx IoT platform, it provides accelerated time-to-value so you can kick start your manufacturing journey.

Production Advisor

Real-time visibility and insight into production line performance and status. ThingWorx Production Advisor is a web/mobile application for production managers that rapidly unifies disparate sources of operational and business data. Users have real-time visibility into production status and critical KPIs such as availability, performance, quality and OEE.

Key features include:

- Real-time visibility into performance and issues
- The ability to drill down into underlying data for root cause analysis
- Normalized manufacturing KPIs with historical trending

ThingWorx Production Advisor readily connects to KEPServerEX® and other OPC servers, providing instant connectivity to your various assets. Built on the ThingWorx IoT platform, it provides accelerated time-to-value so you can kick start your manufacturing journey.

Console Overview

ThingWorx Manufacturing Apps are a set of role-based apps built on ThingWorx that solve common problems in the factory. The apps unify data from enterprise business systems, physical assets, and sensors to deliver user information and insights in context to make better decisions faster.

The tiles available on the console are described by role below. The tiles you see depend on your company's implementation as well as on your user role. For more information, see Configure Users and Roles on page 17.

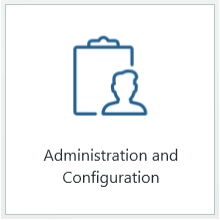
From any window in the app, click the tile icon to quickly move between tiles.

3

Administration and Configuration

Configure Users and Roles 17
Manage Resources 19
Alert Editing 33
Configure Email and Text Delivery 35

This chapter describes the tasks required for the initial setup of ThingWorx Manufacturing Apps. Most tasks are completed using the **Administration and Configuration** tile on the console.



Configure Users and Roles

To configure ThingWorx Manufacturing Apps users and roles:

1. Go to **Administration and Configuration ▸ Users and Access Control**.
2. Click Create User .
3. Enter profile information for the user.
   - The user name must be unique.
   - The cell phone number is required for alert notification. Use the format: `+<number with international code>`
   - Passwords are case sensitive and must contain at least 15 characters.
   - Role Assignments

Tip

You can create a user with multiple roles. For example, you could assign a user all of the following roles.

- Controls Engineer
- Production Manager
- Maintenance Engineer
- A user can be assigned to two roles. However, the result is permissions common to both roles – not the union of the role permissions.

Each role is described in the following table. Begin by creating a user for yourself in the Controls Engineer role.

Role	Access
Controls Engineer	All tiles
Production Manager	• Alert Monitoring • Trending and Troubleshooting

Role	Access
Maintenance Manager	Asset Advisor Administration and Configuration: • Manage Resources • Alert Editing • Trending and Troubleshooting • Alert Monitoring
Maintenance Engineer	Asset Advisor Administration and Configuration: • Alert Editing • Trending and Troubleshooting • Alert Monitoring

Note

The **Notification Preference** selections for each user determine if and how alerts are delivered to that user. The **Email** and **Mobile Phone** values entered are used for the **Email** and **SMS** notification methods, respectively.

4. Repeat steps 2 and 3 to add additional users.

Manage Resources

The procedures in the following sections describe how to create and configure your resources in ThingWorx Manufacturing Apps.

Resources are collections of lines, assets, and sites. Sites allow you to group your lines and assets by location. Sites and lines are used in **Production Advisor**. For more information, see Relate a Site to a Resource on page 32.

Create Resources

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Click new resource .
3. Select a type, either **Asset**, **Line**, or **Site**.

Delete Resource

1. Go to the **Administration and Configuration** ▸ **Manage Resources** page.
2. Select the resources to be removed.
3. Click **Delete Resource**.
4. Confirm the deletion.

Configure Resources

Once resources are created, configure the resources to establish relationships, properties, status, performance metrics, and alerts.

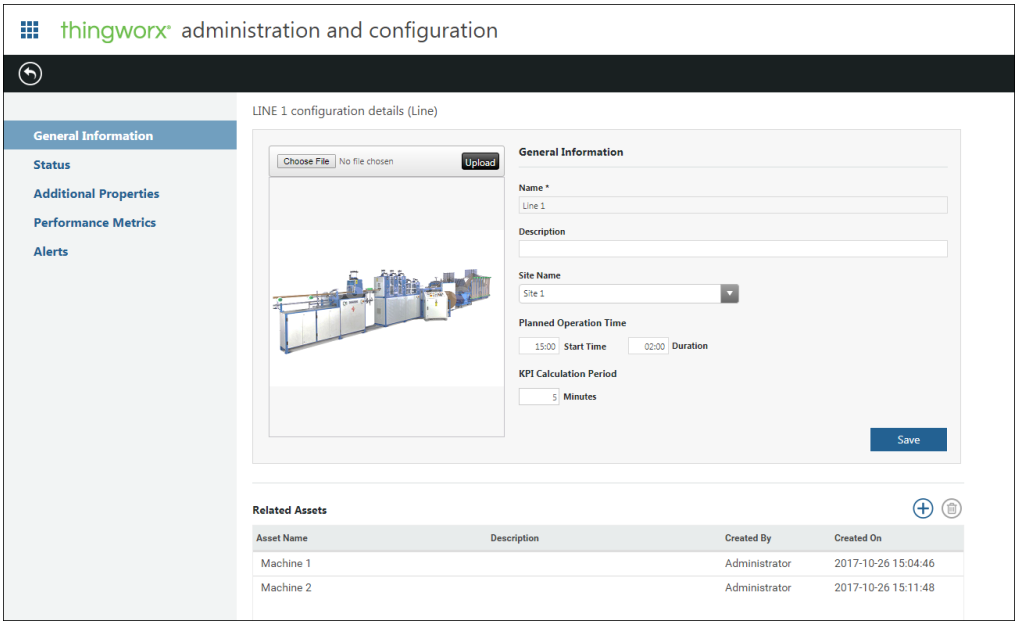
1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resources from the table and click Configure Resource .
3. From the details page of the resource, enter information on each page as described in the following steps. Remember to click **Save** before moving to a different page.

   Here is the suggested workflow:

   a. Create lines and assets. For more information, see Create Resources on page 19
   b. Relate assets to a line. For more information, see Relate Asset to Line on page 30.
   c. Define the status for your assets based on the tags selected from KEPServerEx. For more information, see Configure Status on page 23.
   d. Create properties on your assets. For more information, see Configure Additional Properties on page 24.
   e. Define performance metrics for your assets (optional). For more information, see Configure Performance Metrics on page 26.
   f. Create alerts for your assets. For more information, see Configure Alerts on page 29.
   g. Create properties for your line. For more information, see Configure Additional Properties on page 24.
   h. Define the status for your line based on the assets in the line. For more information, see Configure Status on page 23.
   i. Define performance metrics for your line. For more information, see Configure Performance Metrics on page 26.
   j. Create alerts for your line. For more information, see Configure Alerts on page 29.

Configure General Information

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource
3. On the **General Information** page of the resource, do the following.



a. Upload an image to depict the resource.

   i. Click **Browse**, then select an image file.

   ii. Click **Upload** to display the image, then click **Save**.

b. In the **General Information** area for the resource, enter text in the **Description** field.

c. Select the **Site Name** for the resource from the drop-down list.

d. Enter numbers in the following fields.

   - **Planned Operation Time** (enter time as HH:MM)
   - **Start** and **Duration** (enter time as HH:MM)

> **Tip**
>
> **Start** and **Duration** describes the planned time when the resource is available for use. It is defined in the system using a start time and a duration time.

   - **KPI Calculation Period**

> **Tip**
>
> **KPI Calculation Period** is the time range over which a key performance indicator is calculated for display to others. It is defined in minutes and cannot be set to less that one minute.

e. Click **Save** to persist the configuration.

> **Tip**
>
> Configuration data is lost if you navigate away from the page without saving.

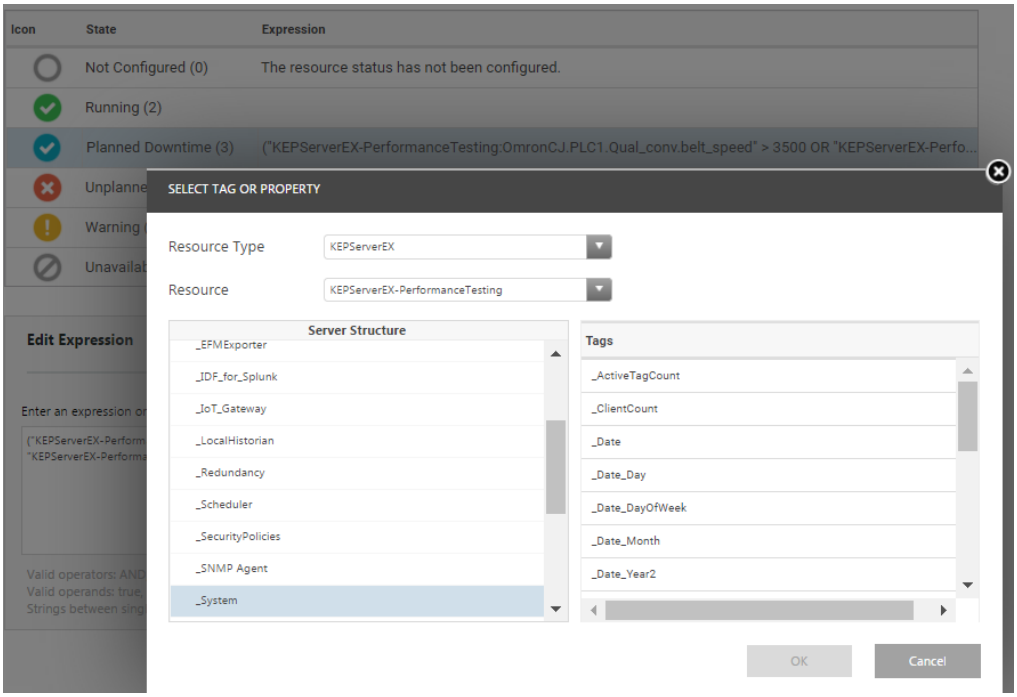
> **Note**
>
> - The **Name** field is not editable once the resource is created.

Configure Status

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource .
3. For each state, enter an expression. For more information, see Status Calculations on page 23

   You can enter the expression manually, or browse to select tags. You can also select properties from other resources.

   For more information, see Configure Additional Properties on page 24



   For lines, the expressions can relate to the assets of the line. For example, a line could be in planned downtime if either of the two assets in the line are in planned downtime. Copy the planned downtime expressions for each appropriate asset and paste them into the planned downtime expression for the line.
4. Click **Save**.

Status Calculations

- There are 6 states provided by default. You can define 4 of them.
- The Warning status is defined by default to appear when the asset has active alerts. The default can be changed to whatever you like.

- The expressions appear in the table in the order they are evaluated. You can change that order by selecting the **Move Up** and **Move Down** arrows.
- After you define the expression of each of the states, make sure they are in the table in the correct order.
- “not Configured” and “unavailable” status cannot be moved.
- If none of the expressions can be evaluated, then the status is “unavailable”.
- If a state does not have an expression defined it is ignored.
- When writing an expression the following can be used.
  - Valid operators: AND, OR, <, >, <=, >=, =, !=, (,)
  - Valid operands: true, false, numbers and tags
  - Strings must appear between single quotes ('). KEPServerEX tags between double quotes (").

Configure Additional Properties

Properties added to assets here display on the **Additional Properties** page of an asset detail in Asset Advisor.

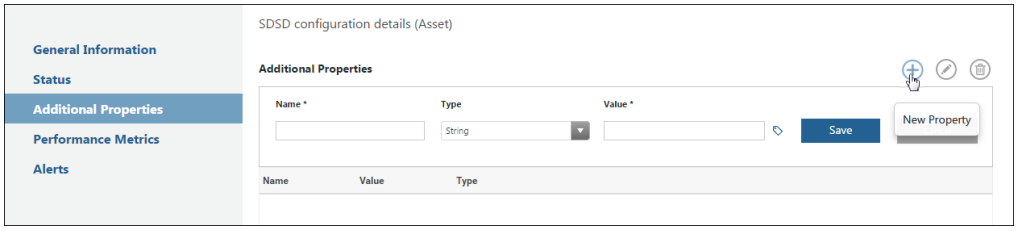
Add properties or tags from KEPServerEX. You can add:

- static properties by specifying the name, type and value
- properties that pull the value from a KEPServerEX tag

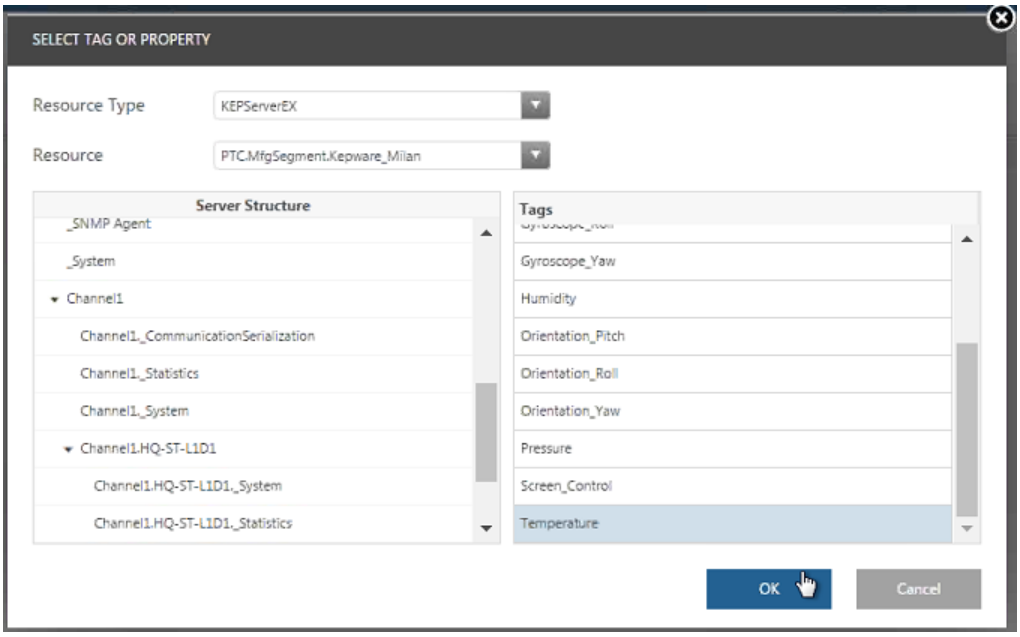
The following example pulls the temperature tag from KEPServerEX.

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource .
3. On the **Additional Properties** page, click new property .

   You can either create static properties by entering a name, type, and value, or properties for which the value is driven by a KEPServerEX tag, where you enter the name and select the tag. The property type is automatically inherited from the KEPServerEX tag type.
4. Enter information in the **Name** and **Type** fields.



5. For **Value**, click the icon to browse for a tag. Locate and select the information from your KEPServerEX..



6. Click **OK**, then click the **Save** button to save the property.

Configure Performance Metrics

The following table explains how performance metrics are calculated by default.

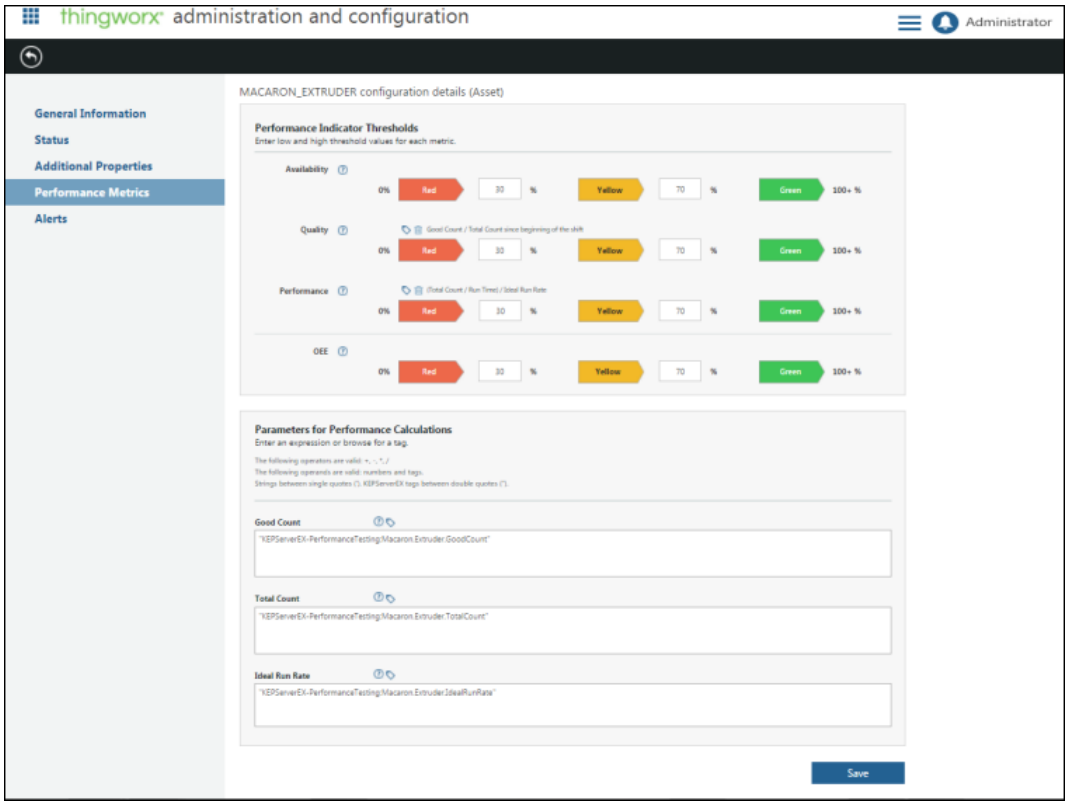
Metric	Default Calculation
Availability	Run Time/Planned Production Time Run Time = Warning Time + Running time Planned Production Time = Warning Time + Running time + Unplanned Downtime + Unavailable time
Quality	Good Count / Total Count since the beginning of the planned operation time.
Performance	(Total Count / Run Time) / Ideal Run Rate Run Time = Warning Time + Running Time
OEE	Availability * Performance * Quality

To configure custom performance metrics for a resource:

1. Go to the **Administration and Configuration** ▸ **Manage Resources** page.
2. Select a resource from the table and click Configure Resource .
3. On the **Performance Metrics** page, enter information for your performance thresholds and calculations as described in the example below and detail the required equations.

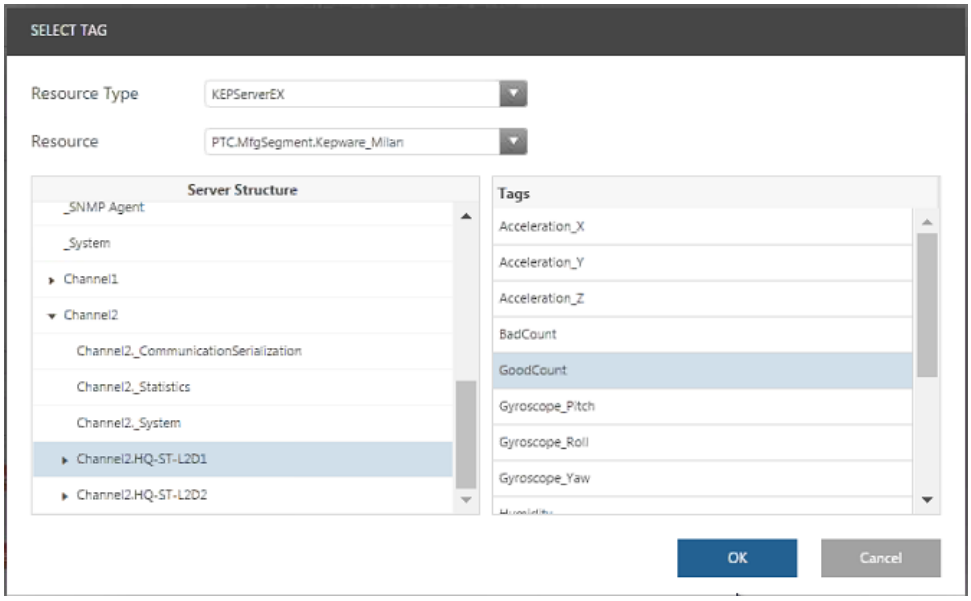
> **Tip**
>
> Quality and Performance can be overridden by selecting a KEPServerEX tag directly.

> **Note**
>
> The following example assumes you have a KEPServerEX tag from which you can access the number of good parts and bad parts for the day.


thingworx administration and configuration
Administrator
General Information
Status
Additional Properties
Performance Metrics
Alerts
MACARON_EXTRUDER configuration details (Asset)
Performance Indicator Thresholds
Enter low and high threshold values for each metric.
Availability
Quality
Performance
OEE
0%
Red
30
%
Yellow
70
%
Green
100+ %
Parameters for Performance Calculations
Enter an expression or browse for a tag.
Good Count
"KEPServerEX-PerformanceTesting.Macaron.Extruder.GoodCount"
Total Count
"KEPServerEX-PerformanceTesting.Macaron.Extruder.TotalCount"
Ideal Run Rate
"KEPServerEX-PerformanceTesting.Macaron.Extruder.IdealRunRate"
Save

Quality
Good Count / Total Count since beginning of the shift
0%
Red
30
%
Yellow
70
%
Green
100+ %
Performance
(Total Count / Run Time) / Ideal Run Rate
0%
Red
30
%
Yellow
70
%
Green
100+ %

1. **Good Count**
   - For assets, enter or browse for the KEPServerEX tag that identifies good parts for the asset.



   - For lines, enter the good counts for each asset in the line.
2. **Total Count**
   - For assets, enter or browse for your bad count, and then add your good count.

> **Tip**
>
> You can copy and paste the good count from the previous field.

3. **Ideal Run Rate**

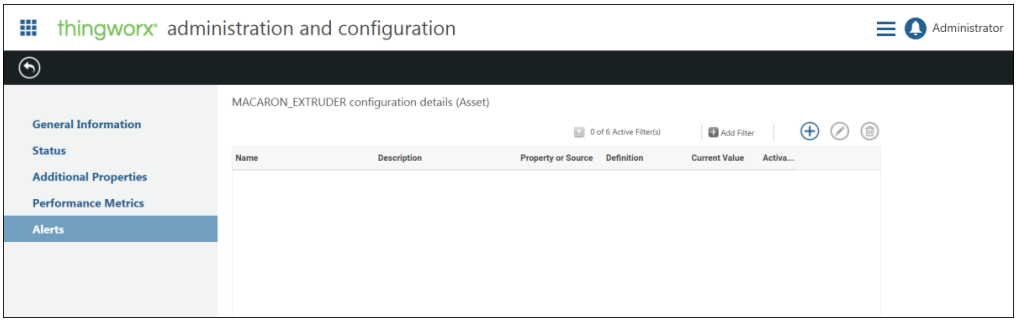
Identify how quickly your factory would be producing parts for the asset or line in an ideal situation. Expressed in parts per minute.

4. Click **Save**.

   Production Advisor and **Asset Advisor** display the performance metrics you have defined for the lines and assets.

Configure Alerts

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource .
3. On the **Alerts** page, you can add, edit, or delete alerts for this resource.



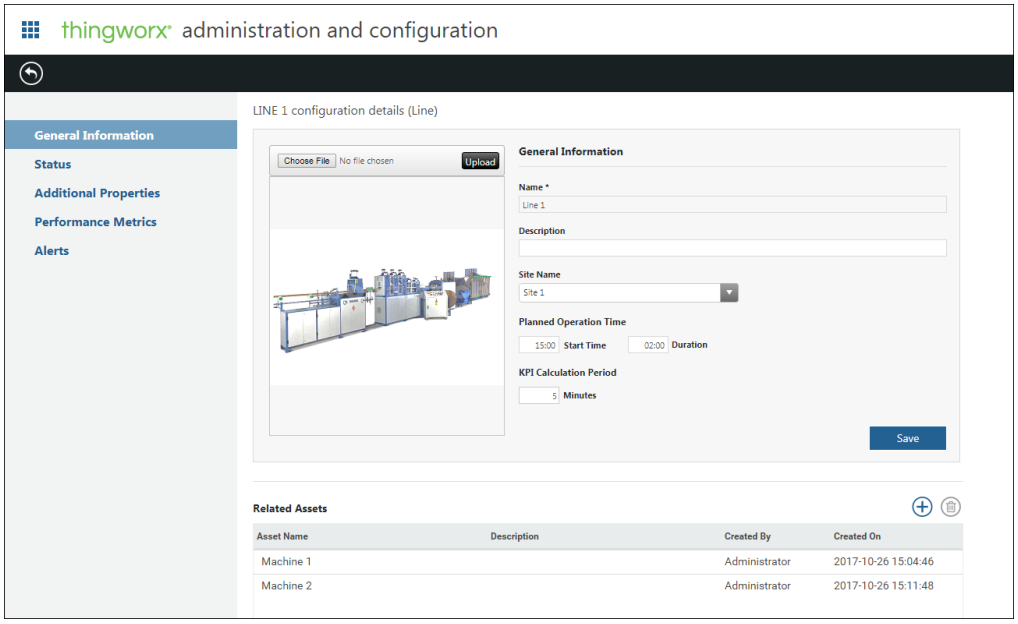
For more information, see Alert Editing on page 33.

Relate an Asset to a Line

Note

An asset does not have to be associated with a line. It can also be related to multiple lines.

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource .
3. On the **General Information** page, go to the **Related Lines** table and relate the line to the asset.



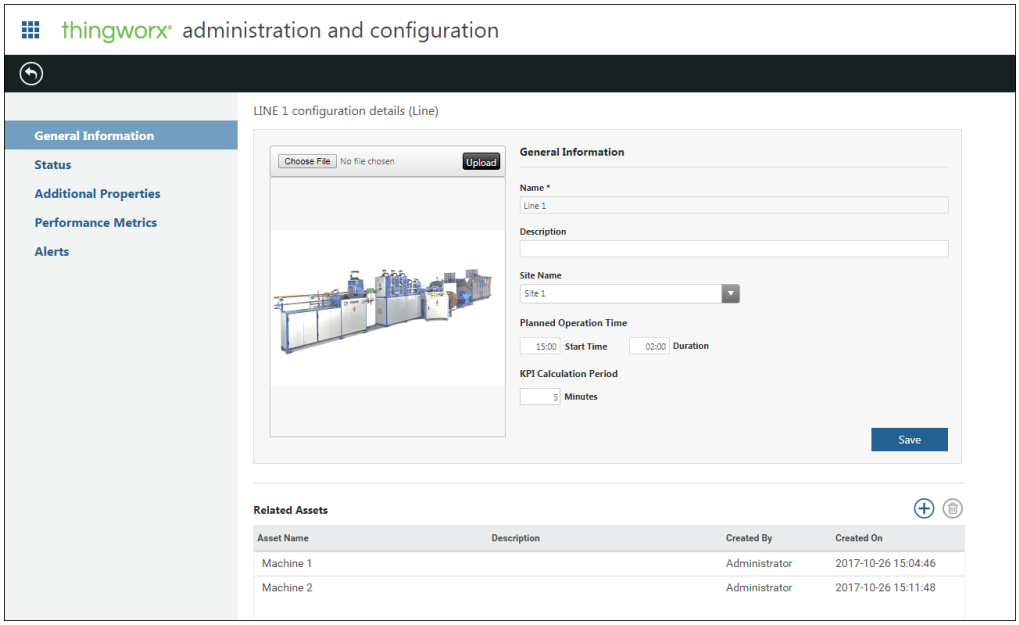
SELECT ASSETS

Asset Name	Description	Created By	Created On
1-1_SinkingEDM		SuperUser	2017-05-17 13:13:36
1-1_WireEDM		SuperUser	2017-05-17 13:13:36
1-2_GantryRobot		SuperUser	2017-05-17 13:13:36
1-2_WeldingRobot		SuperUser	2017-05-17 13:13:36
1-3_CNCMill		SuperUser	2017-05-17 13:13:36
1-3_CNCTurning		SuperUser	2017-05-17 13:13:36
2-1_Bender		SuperUser	2017-05-17 13:13:36
2-1_LaserCutter		SuperUser	2017-05-17 13:13:36
2-2_Grinder		SuperUser	2017-05-17 13:13:36

Relate a Site to a Resource

Sites need to be created in the system before one can be related to an asset or line. For more information, see Create Resources on page 19.

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select a resource from the table and click Configure Resource .
3. On the **General Information** page, select a site from the **Site Name** list.



4. Click **Save**.

Clear Data History

If a resource has captured data incorrectly, it can be removed from the system so that the resource history does not retain incorrect data.

1. Go to **Administration and Configuration** ▸ **Manage Resources**.
2. Select one or more resources from the table and click Clear Data History .

> **Tip**
>
> This does not clear any expressions; only the data captured up to this point in time.

Alert Editing

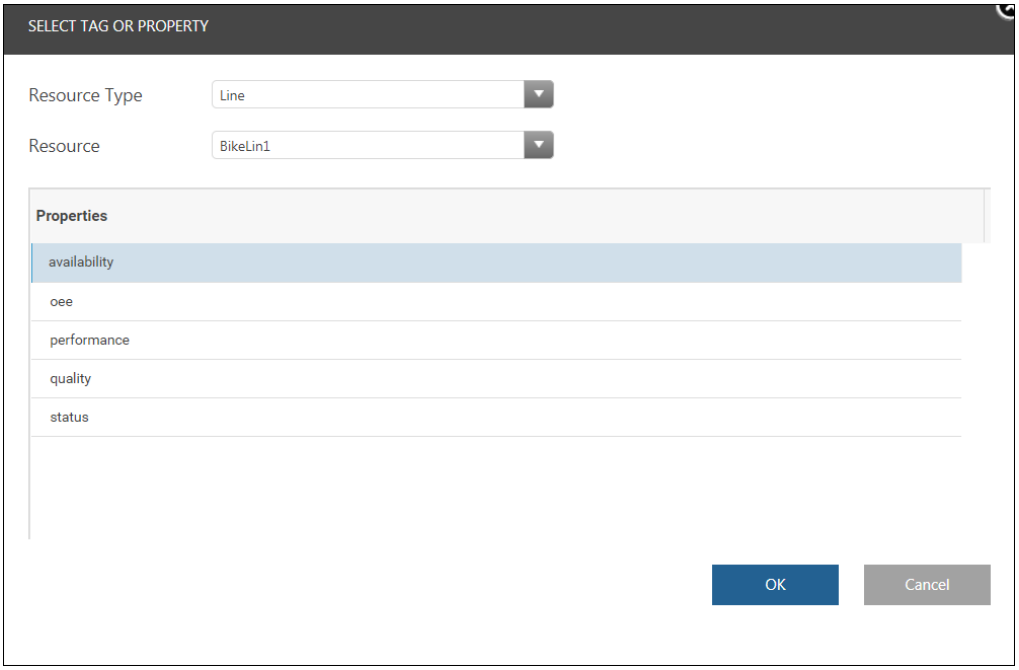
You create alerts using the status expressions set when you Configure Resources on page 20.

To edit an alert:

1. Go to **Administration and Configuration** ▸ **Alert Editing**.
2. Click New Alert .
3. Set the **Resource Type** and **Resource** (ID).

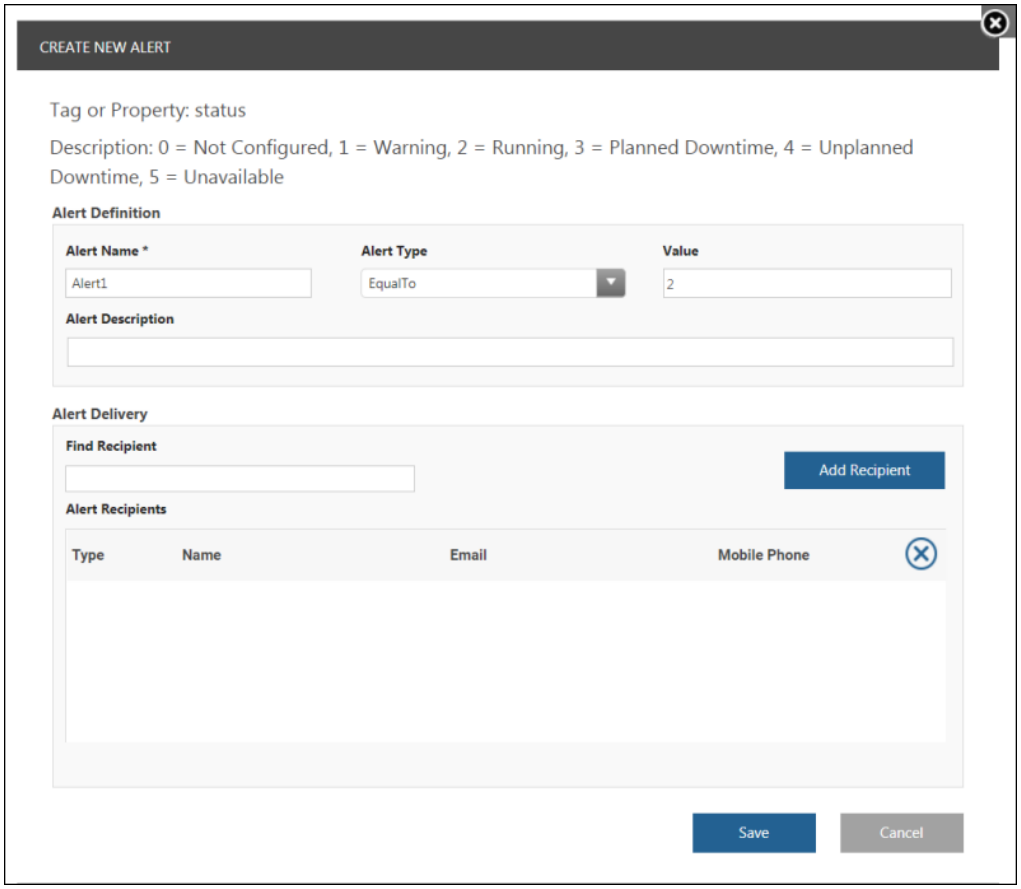
   This example uses **Line**.
4. Select the property used to trigger the alert, then click **OK**.

   This example uses **availability**.



5. Create the alert. For **Value**, use one of the numbers listed in the description.

   This example uses 2 (running).



6. Search for and add recipients for the alert.

> **Tip**
>
> Only users that have an alert delivery method specified (email or SMS) show up in the search results

The alerts are delivered to each recipient based on their notification preferences in **Users and Access Control**

.

7. Click **Save** to create the alert.

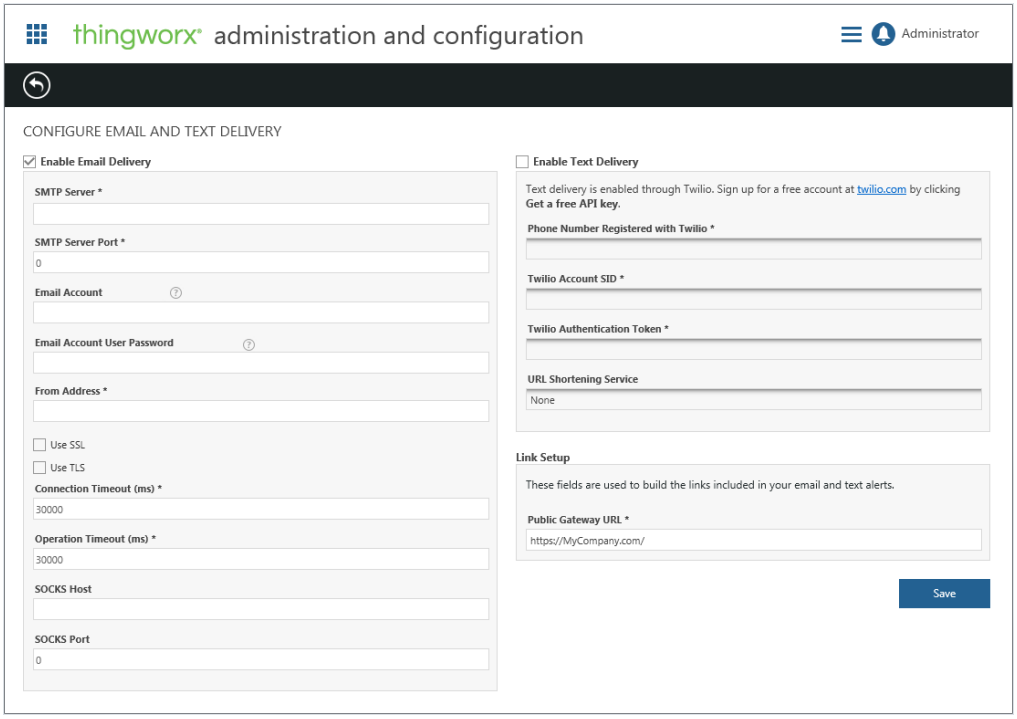
   Once defined, alerts can be viewed in multiple ways. For example, from the **Alert Monitoring** tile.

   For more information, see Alert Monitoring on page 60 and Asset Advisor on page 52.

Configure Email and Text Delivery

To configure the email and text delivery for sending alert notifications to designated recipients:

1. Go to **Administration and Configuration ▸ Configure Email and Text Delivery**.
2. Enable one or both services by checking the appropriate boxes at the top of the page.
3. Enter the necessary information for your company.



- **Email Delivery**—Provide the necessary information for the system to send email notifications for alerts:
  - The address and port for the SMTP mail server used to send emails.
  - The email account used to send the alert notifications, and its password, if required by the SMTP mail server.
  - Select whether to use SSL or TLS for encryption, or neither.
  - The email address that is to appear in the From field of the email message.
  - Specify the connection and operation timeouts in milliseconds, or accept the defaults.

- Specify the SOCKS proxy server host name and the port for the SOCKS proxy server, if one is used with the SMTP mail server.

- **Text Delivery**—
  - To use texts to send email notifications, sign up for a free account at twilio.com. The fields here should match the fields that appear after you complete your sign up with Twilio.
  - If configured, select a URL shortening service. For more information, see Configuring the URL Shortening Service on page 64.
- **Link Setup**—This information is used to build the links included in your email and text alerts.
  - Specify the public gateway portion (basic http: address to the server) of the URL for links to your system.

    The following example shows what a URL would look like from outside your company using the Public Gateway URL.

    This URL:

    ```
    http://10.155.20.100:8080/Thingworx/Runtime/
    index.html#master=
    PTC.Factory.AlertMonitoring.Master=
    PTC.Factory.AlertManager.AlertMonitor=false=
    sensor1=Asset_Pump1=true
    ```

    would appear as a hyperlink in the email message as:

    ```
    https://acme.com/Thingworx/Runtime/
    index.html#master=
    PTC.Factory.AlertMonitoring.Master=
    PTC.Factory.AlertManager.AlertMonitor=false=
    sensor1=Asset_Pump1=true
    ```

    if the Public Gateway URL was set to https://acme.com/

Tip

The public gateway URLs are located at the beginning of the example strings.

4

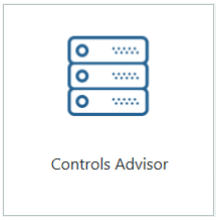
Apps Overview

Controls Advisor 39
Production Advisor 50
Asset Advisor 52
Alert Monitoring 60
Trending and Troubleshooting 61

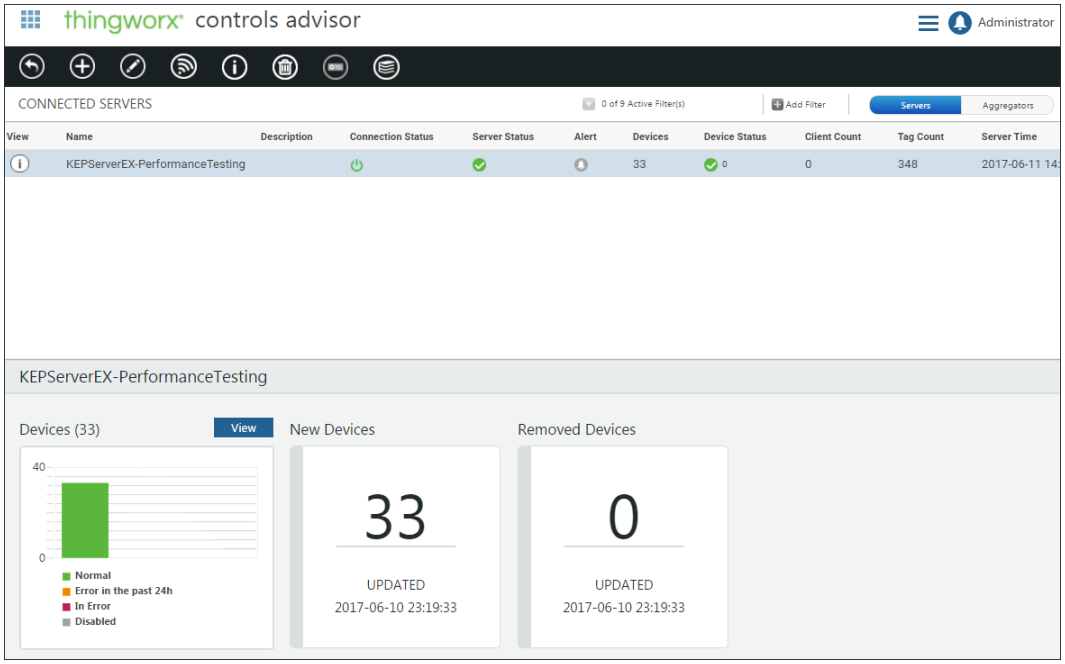
The ThingWorx Manufacturing Apps console can include one or more of the following tiles. The tiles you see depend upon your user role, as well as your company's implementation of the product.

- Controls Advisor
- Production Advisor
- Asset Advisor
- Alert Monitoring
- Trending and Troubleshooting
- Administration and Configuration

Controls Advisor



Controls Advisor enables a controls engineer to connect and remotely monitor KEPServerEX and aggregator connections and devices in real time. After the connections are set up, the controls engineer is notified instantly of data communication errors that may result in a loss of critical production data.



The following list highlights the features of Controls Advisor.

- **Discover** — Scans the server and creates the devices in ThingWorx Manufacturing Apps . Repeat this action as you add and remove devices from KEPServerEX.
- **Create Server** — Add new servers. Aggregators are created when you select the checkbox at the bottom of the **Create Server** window.
- Switch the **CONNECTED SERVERS** table view between Servers and Aggregators using the toggle button in the upper right corner of the page. For more information on aggregators, see the following sections.

Connecting KEPServerEX to ThingWorx

KEPServerEX can be used to directly connect to devices (direct connection), or as an aggregator to connect to legacy KEPserverEX and 3rd party OPC Server. The Controls Advisor App provides the capability to monitor all KEPServerEX and 3rd party OPC server connected directly or via aggregator to the ThingWorx instance in a single page.

In order to make a connection between KEPServerEX and ThingWorx, an industrial gateway must be created in ThingWorx. The industrial gateway is a ThingWorx thing that is used to establish the connection information between ThingWorx and KEPServerEX as it holds some of the connection information.

In addition to the industrial gateway thing, a remote thing is created. The remote thing represents the Server (KEPServerEX or 3rd party OPC server) being monitored within controls Advisor. This remote thing holds the properties mapped to a tag.

Finally, the project property on the KEPServerEX server connecting to ThingWorx, must then be configured to establish the connection to the remote thing via the industrial gateway.

Creating a Server Connection

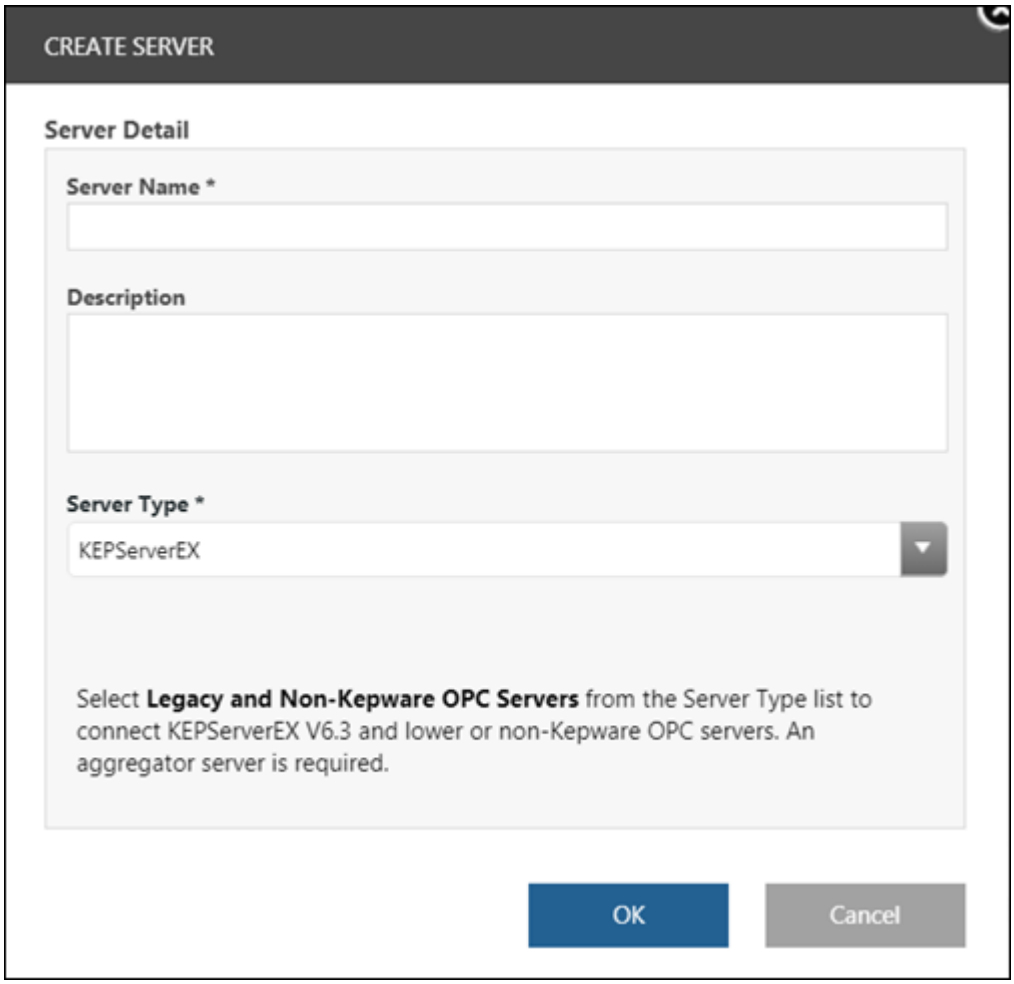
The first time the controls engineer logs into the app, a check is made to determine whether or not a server connection already exists.

- If a sever does not exist, the controls engineer is guided to create his first connection to a KEPServerEX.
- If a server does exist, the controls engineer is taken directly to the console page.

During the initial flow, the controls engineer is asked for a server name, the type of connection (aggregator or direct connection to devices), and information required to configure its KEPServerEX project properties. The controls engineer is then automatically directed to the server list page where he can monitor the server.

To connect to additional KEPServerEX servers, a **Create Server** action is available in the action toolbar of the server list page. This enables the controls engineer to create a remote thing in ThingWorx representing the connection to a specific KEPServerEX server. Selecting this action opens a window where the following information can be specified.

- **Server Name** — This corresponds to the remote thing name that is displayed in Controls Advisor.
- **Description** — A pull down is available with options to specify the type of connection to be established. Direct or Aggregator.



Tip

- A direct connection indicates that KEPServer EX is directly connected to devices.
- An aggregator connection indicates that KEPServerEx is used as an aggregator to connects legacy KEPServerEX or other 3rd party OPC servers that are themselves connected to devices.

The controls engineer is then presented with instructions on how to configure the project properties on the KEPServerEX server. These instructions can be printed for future reference.

Note

Controls Advisor does not support cases where KEPServerEX is connected directly to devices and used as an aggregator simultaneously.

Displaying Connected Servers

When accessing Controls Advisor, the controls engineer is presented with a page that displays server information.

There are two views in this page.

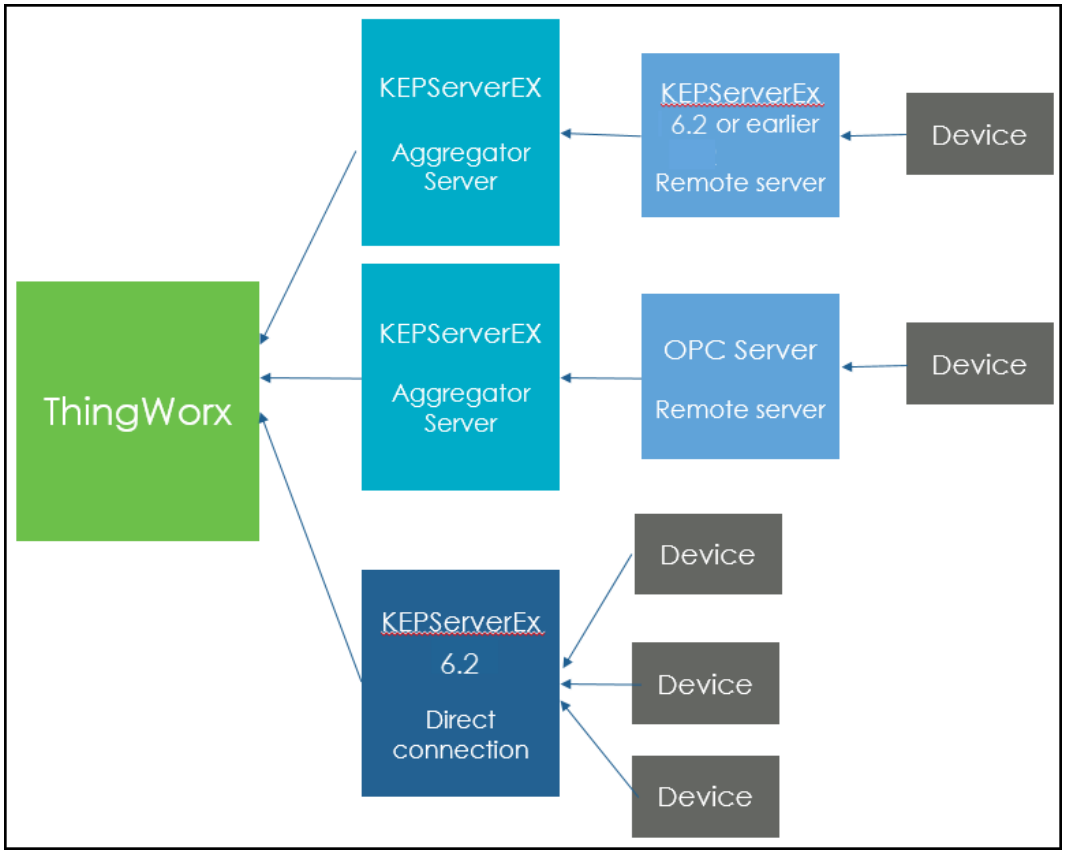
- **Server** — Displays servers connected to devices (directly connected or thru an aggregator).
- **Aggregators** — Displays Servers that are used as aggregators.

Note

- The first server in the list is selected by default when accessing the page.
- It is not possible to deselect items in the list.

Understanding Aggregators

An aggregator server is required for non-Kepware servers and KEPServerEX servers prior to version 6.2. The graphic below describes the relationships among the server and devices.



Working with Aggregators

Discoverting Remote Servers

When creating a server connection and selecting the **Connect to legacy and Non Kepware OPC Servers** check box in the **Create Server** window, the system assumes that the KEPServerEX has remote OPC or legacy KEPServerEX servers connected as OPC devices.

The action **Discover Legacy KEPServerEX and OPC Servers** is available in the Aggregator view of Controls Advisor. Selecting a KEPServerEX aggregator and invoking this action, produces the following result.

The list of remote servers associated to the selected aggregate server is scanned and compared to the list of remote servers already discovered.

- If a remote server of the same name is already in the list it is kept.
- If a remote server is not in the list, but on the aggregate, it is added.
- If a remote server is in the list, but not on the aggregate, it is deleted from ThingWorx.

Note

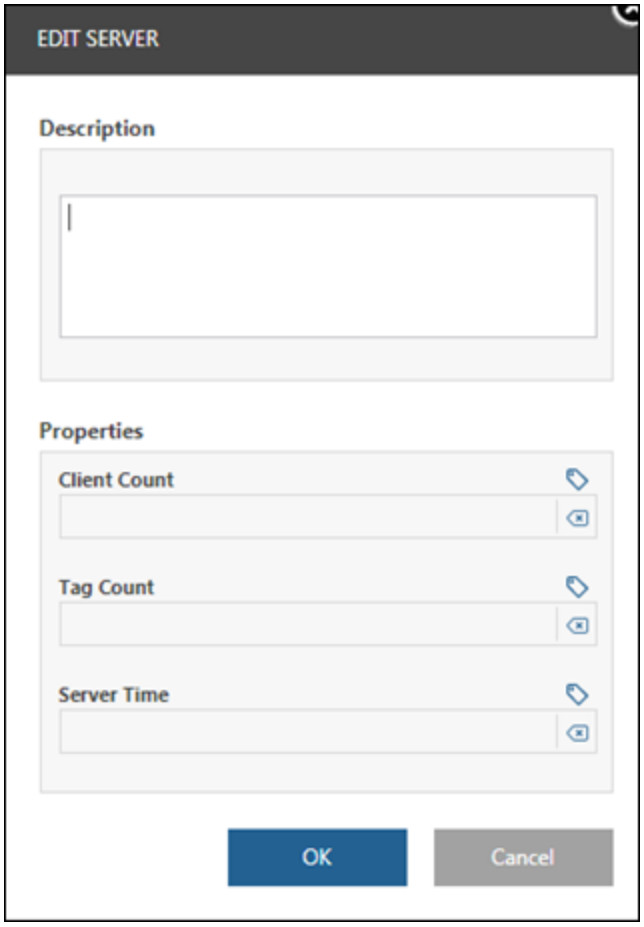
A server name must be unique in ThingWorx. if there is an uniqueness conflict, the server is ignored and the next remote server is created. At the end of the discovery, a system message displays the path of the ignored remote servers and explains why they were not created. You must then rename the servers in Kepware and re-discover them.

Editing a 3rd party OPC Remote Server

3rd party OPC vendors have their own tag structure that can be different from the KEPServerEX tag structure. When a remote server is connected via an aggregator, KEPServerEX, system tags cannot be bound automatically. In the **Edit Server** window, the controls engineer is able to manually map the following system tags to any data point of the selected remote server. The following system tags can be mapped.

- Client Count (integer)
- Tag Count (integer)
- Current Server Time (date)

When browsing the remote server, the tag picker automatically selects the remote server, the tags with improper types are automatically filtered out.



Note

- You cannot edit system tags of a KEPServerEX.
- As the server status is calculated based on the Current Server Time property changing, the 3rd party OPC server status shows as OFF until the Current Server Time is mapped to a tag.

Working with Devices

Discovering Devices

A **Discover Devices** action is available in the action toolbar of the Server View page. The discovery of the device is scheduled and occurs automatically once a day at midnight. During the initial discovery, the system scans the server and for each device, creates a remote thing in ThingWorx corresponding to the device. No device is created when the remote server is not a KEPServerEX. Devices for 3rd party OPC servers must be created manually.

Discoveries scan the list of devices on the server and compare it to the list of devices already discovered.

- If the device of the same Device Name is already in the list, it is kept.
- If a device is not in the list but on the server, it is added.
- If a device is in the list, but not on the server, it is deleted from ThingWorx.

When a device is deleted, the device is deleted in ThingWorx and all data associated to the Thing properties are deleted as well. The binding is removed and tags are unsubscribed. After discovery is complete, a warning indicator is displayed in the **Devices** column of the servers list indicating that a change occurred (some devices were added or removed during last discovery).

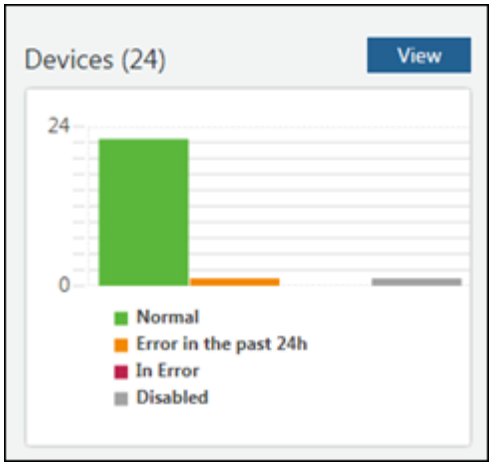
You are notified in two widgets about the number of devices added or removed.

- The number of **New Devices** corresponds to the total number of devices added during the discovery. This value is persisted until the next discovery.
- The number of **Removed Devices** corresponds to the total number of devices removed during the discovery. This value is persisted until the next discovery.
- The **Date** is the date of the last discovery.

> **Tip**
>
> The widgets are not refreshed until you select another row/server.

The devices that have been discovered on the server are displayed in the **Devices** widget shown in the following figure. Each bar represents the number of devices within a specific status for the devices connected (already discovered) to the server.

- Running
- In Error
- Errors in the past 24h
- Disabled

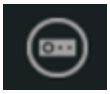


After each discovery the **Devices** widget is updated along with the **New Devices** and the **Removed Devices** widgets. A **View** button is available in the Devices widget to access the device list page.

Note

When a device is renamed in Kepware, it is not automatically renamed in the app. Upon next discovery, the device is removed and a new device with the new name is added.

Creating Devices

A **Create Device**  action is available in both the server view page and the device list page. This action is only valid when the selected server is a remote 3rd party OPC Server. You can only create devices manually by selecting the **Create Device** action.

Tip

- The **Create Device** action is disabled when selecting a KEPServerEX server (remote or not).
- The **Discover Devices** action is disabled when selecting a remote 3rd party OPC Server.

When creating a device, you can specify or map pre-defined properties to tags by browsing the remote server using the tag picker CC (only the selected remote server can be browsed)

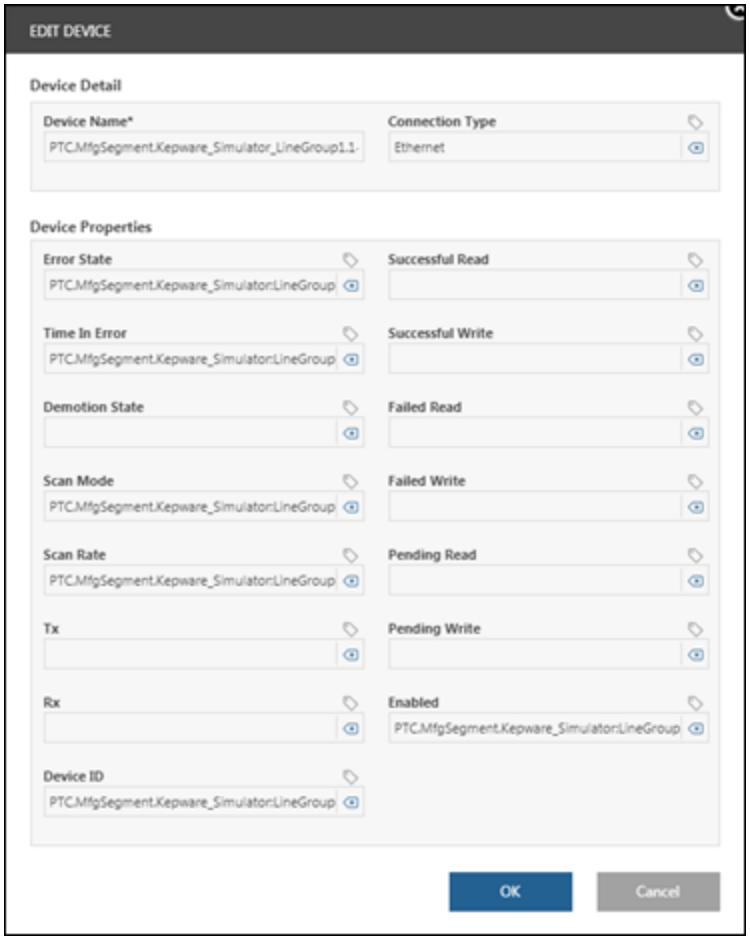
Note

If a value is entered manually, it becomes a static value for the property. No automatic binding occurs if a path to a tag is entered

You cannot edit the fields. A**Clear** action is available to clear the tag name. After selecting **OK** the binding is done, the table is refreshed, and the values appear in the table. Unless there is a mapping for those tags, the values appear blank in the server list page and in the device list page.

Editing Devices

Devices can be edited from the device list page. When selecting a device and the **Edit Device** action, the window displays all the properties associated to the devices. Any device can be edited, and the tag mapping of the device properties changed. However, the name of the device cannot be edited.



Deleting a Server Connection

The Controls Engineer can delete a server from the server list. A pop-up appears to confirm the action. When deleting a server, all ThingWorx artifacts with respect to the server are deleted including devices. All local bindings from the remote server Things properties to any Assets/Lines/Trends properties are also deleted

When you delete a remote server connected to an aggregator, the following occurs.

- All devices that are associated to the remote server are deleted.
- All local binding from the remote servers Thing properties to any Assets/Lines/Trends properties are also deleted.

When you delete an aggregator, the following occurs.

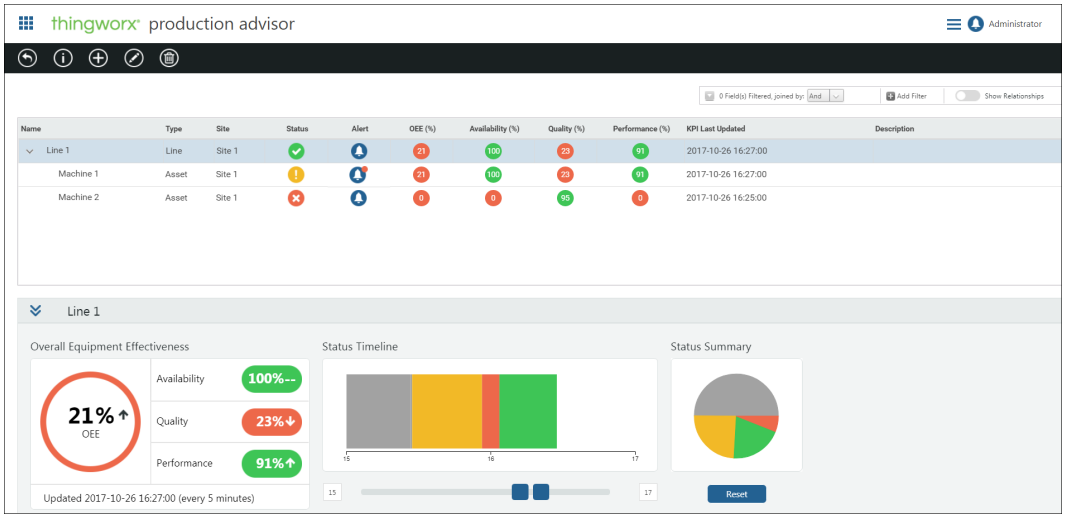
- All remote Servers related to the aggregator are deleted.
- All devices that are associated to each remote servers are deleted.
- All local binding from the remote servers Thing properties to any Assets/Lines/Trends properties are also deleted.

Note

Data associated to the server properties that are stored in the ThingWorx database are not deleted and are re-used in trends if a new remote thing is created with the same name.

Production Advisor

With Production Advisor, plant managers have the ability to view real-time operational performance data that is unified from disparate sources. This enables fast-informed decisions with contextual information, as well as the ability to drill down for root cause analysis. Sample pages are shown in the following figures.



Production Advisor Features

- Use the create, configure, and delete resources shortcut actions to manage production resources. For more information, see Manage Resources on page 19
- Use the filter options at the top of the page to create filters for the lines and assets that display.
  - Add multiple filters.
  - Determine the logical operator between created filters.
  - Display related lines or assets with the **Show Relationships** option.
- The unassigned assets node groups assets that have not been related to a line.
- Click on the View Production History icon for detailed information on the resource, such as performance and status history.

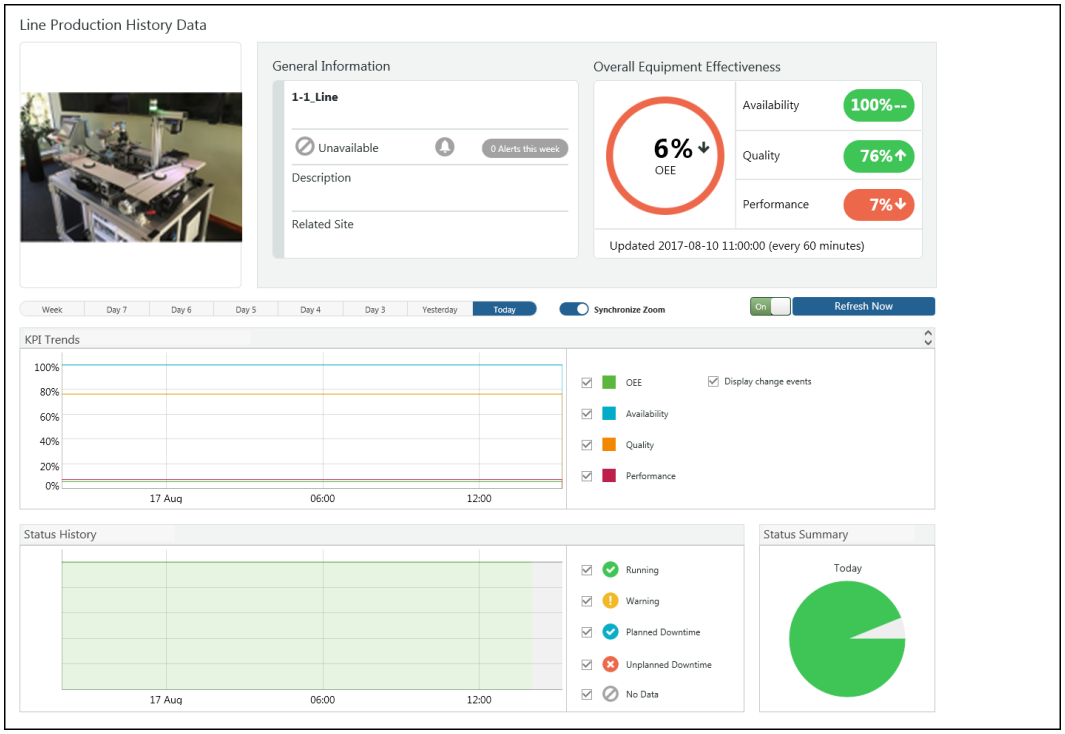
- On the graphs, click and drag to zoom in and double-click to zoom out. **Synchronize Zoom** means when you zoom in on one graph, the other graph zooms to the same time frame.
- Navigate back in time using preset time ranges (radio buttons) to show up to a week of data.
- Refresh data on the graphs manually or automatically using the **Refresh Now** option.

• On the **KPI Trends** graph, show and hide change events using the **Display Change Events** check box. These events are flagged on the graph and listed below the check box.

Tip

The system can display the following types of change in the KPI Trends graph.

- Change to the ideal run rate value
- Change to KPI calculation period value
- Change to KPI parameter expressions (good count, total count, ideal run rate, quality, and performance)

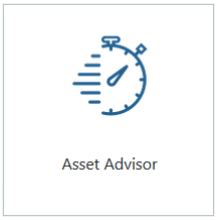


Note

OEE KPIs are calculated periodically (for a specific period of time) – the KPI calculation period.

The KPI calculation period is the time range over which a KPI is calculated for display to users. In Production Advisor, this is configurable per asset and line and is calculated across multiple operation times if applicable. This applies to OEE, Availability, Performance, and Quality KPIs. For more information, see Configure General Information on page 20.

Asset Advisor



Asset Advisor connects to your equipment and provides real-time feedback of sensor details, alerts, and anomalies. This allows you to understand how your equipment is being utilized, how it performs, and ultimately improves the efficiency of that equipment.

The following sections highlight features of Asset Advisor.

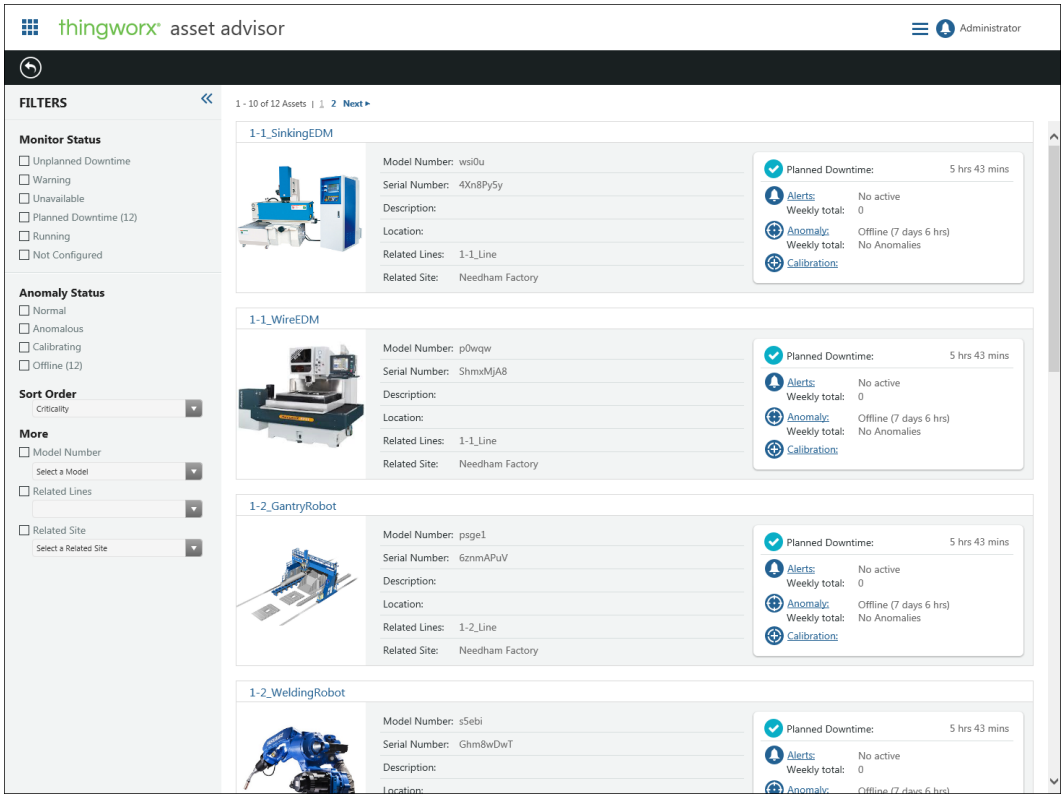
Asset List

- The asset list page provides a summary view of all assets in the system, including their status and any automatically detected threshold alerts and anomalies.
- Filter the list to show only those assets in certain states, or by model number, related asset, or related line.
- Assets can be sorted by Name, Model Number, Serial Number, or Criticality.
- At a glance, view the status of threshold alerts as well as the anomaly status for the asset. Weekly totals, anomaly duration, and sensor calibration status are also included.

Tip

The status icons display a red dot in the upper right corner enabling you to visually detect when threshold alerts or anomalies are currently active.

- Click the **Alerts** link in the status message to open the **ALERT MONITOR** page that displays detailed information for threshold alerts.
- Click the **Anomaly** link in the status message to open the **ALERT MONITOR** page that displays detailed information for anomaly alerts.
- Click the **Calibration** link in the status message to open the **Monitored Properties** page that displays detailed information for sensor calibrations.
- Click on the asset name or image to view the asset in more detail.



Asset Detail

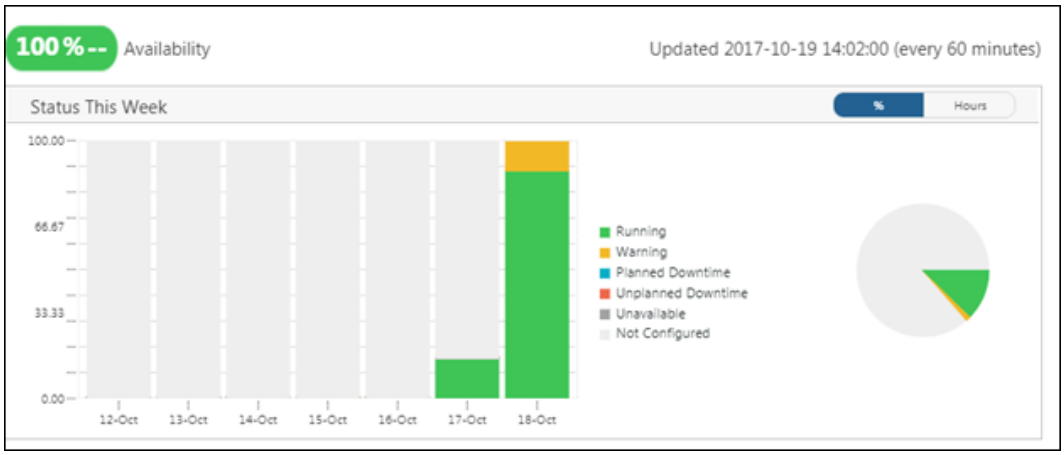
You can further investigate asset issues on the detail page of the asset.

- Switch between viewing **Performance**, **Monitored Properties**, or **Additional Properties**.
- Optionally, perform actions on assets remotely using **Remote Access**, **File Transfer** and **File Transfer History**.

- View general asset profile information such as model and serial numbers.
- View asset alert, anomaly, and sensor calibration status messages. Click on the Alerts or Anomaly icon to open the Alert Monitoring page for additional details.

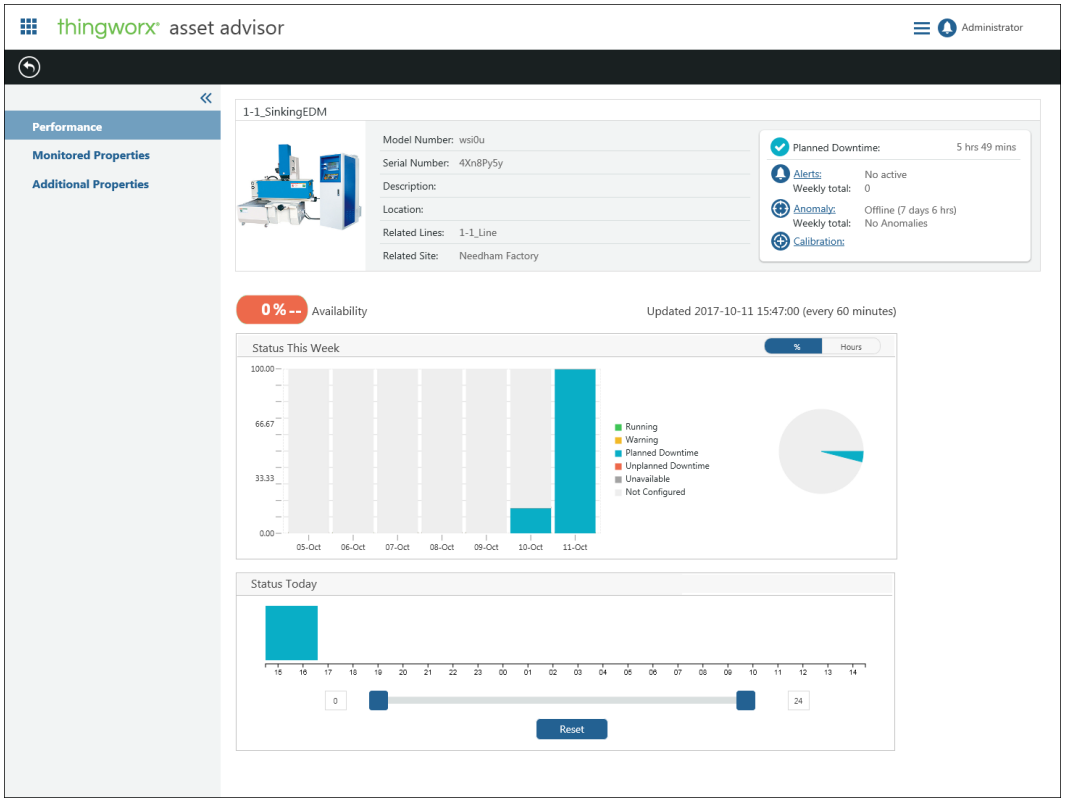
Asset Detail — Performance

You can view the distribution of the monitor status over this week in a bar graph or in a pie chart. You can also toggle between viewing by percentage or hours.



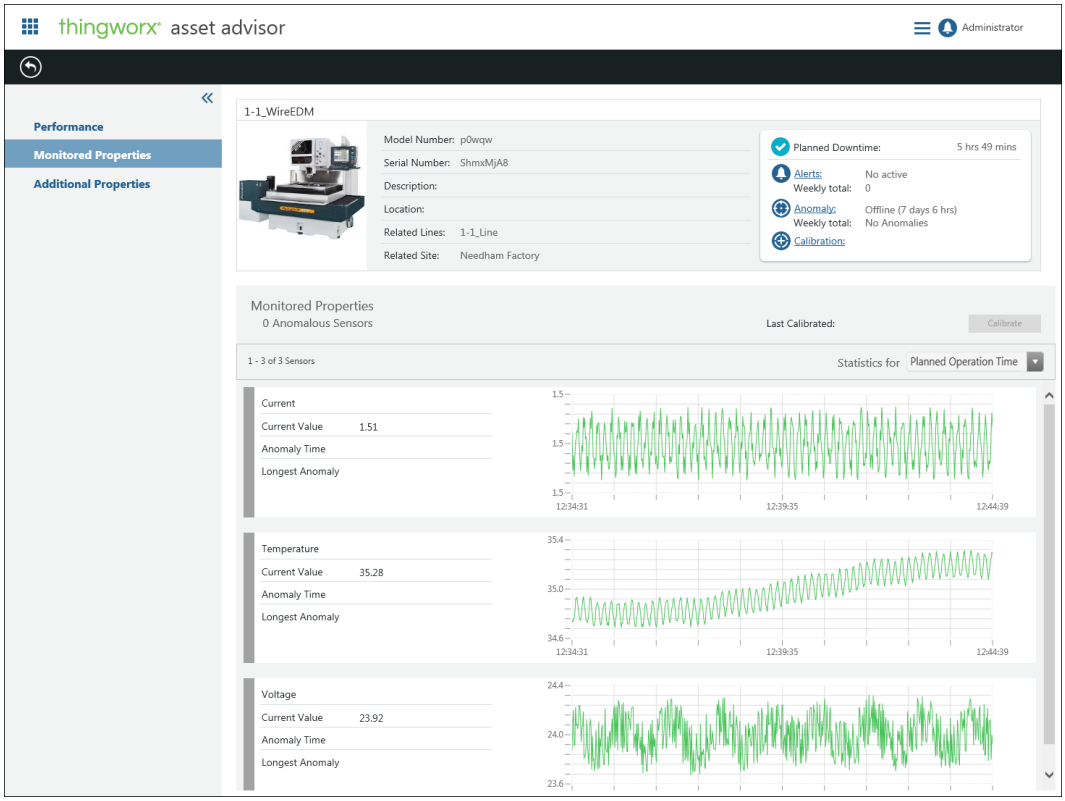
Both the availability calculation and graph are updated in a configurable frequency and the default is 60 minutes.

You can also view the performance distribution over the current day with a slider, allowing you to view the performance in the desired time period.


thingworx asset advisor
Administrator
Performance
Monitored Properties
Additional Properties
1-1_SinkingEDM
Model Number: wsi0u
Serial Number: 4Xn8Py5y
Description:
Location:
Related Lines: 1-1_Line
Related Site: Needham Factory
Planned Downtime: 5 hrs 49 mins
Alerts: No active
Weekly total: 0
Anomaly: Offline (7 days 6 hrs)
Weekly total: No Anomalies
Calibration:
0 % -- Availability
Updated 2017-10-11 15:47:00 (every 60 minutes)
Status This Week
%
Hours
100.00
66.67
33.33
0.00
05-Oct
06-Oct
07-Oct
08-Oct
09-Oct
10-Oct
11-Oct
Running
Warning
Planned Downtime
Unplanned Downtime
Unavailable
Not Configured
Status Today
Reset

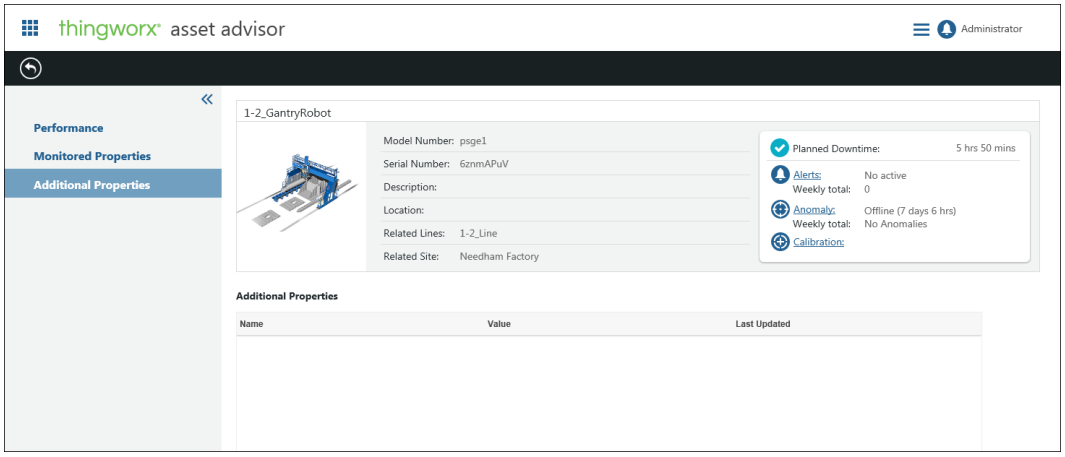
Asset Detail — Monitored Properties

- View real-time data from all sensors configured on the asset, their current readings, and whether that reading is normal (green) or anomalous (orange).
- Select the time frame over which sensor data displays anomaly KPI (**Planned Operation Time**, **1 Minute**, **15 Minutes**, **1 Hour**, **1 Day**, or **1 Week**). Note that this does not affect the data displays.
- Click the calibration link in the status message to open the Monitored Properties page to re-calibrate sensors.
- Calibration causes the system to re-train the anomaly detection model based on new sensor data. Calibration is useful if the operating conditions for the asset have changed and the system needs to learn the new normal operating conditions.



Asset Detail — Additional Properties

Additional properties configured on the asset display here. These properties are configured in **Administration and Configuration ▸ Manage Resources**.



Asset Detail — Remote Access

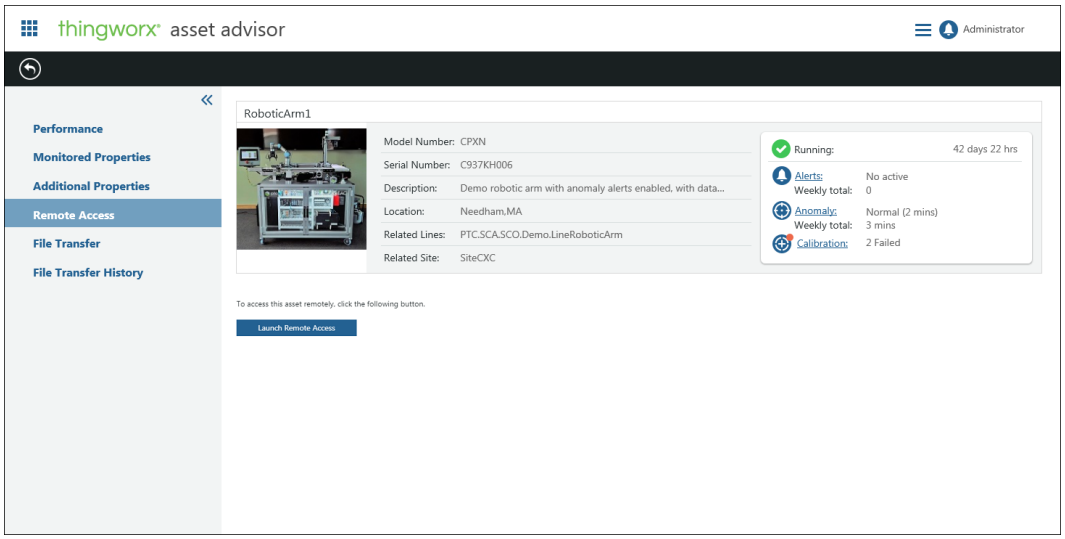
- **Remote Access** is a set of optional features that can be added to Asset Advisor by importing the Asset Remoting extension using ThingWorx Composer. For more information, see Configure Remote Access and Control on page 66.

  The extension includes the following features.

  - Remote Access
  - File Transfer
  - File Transfer History

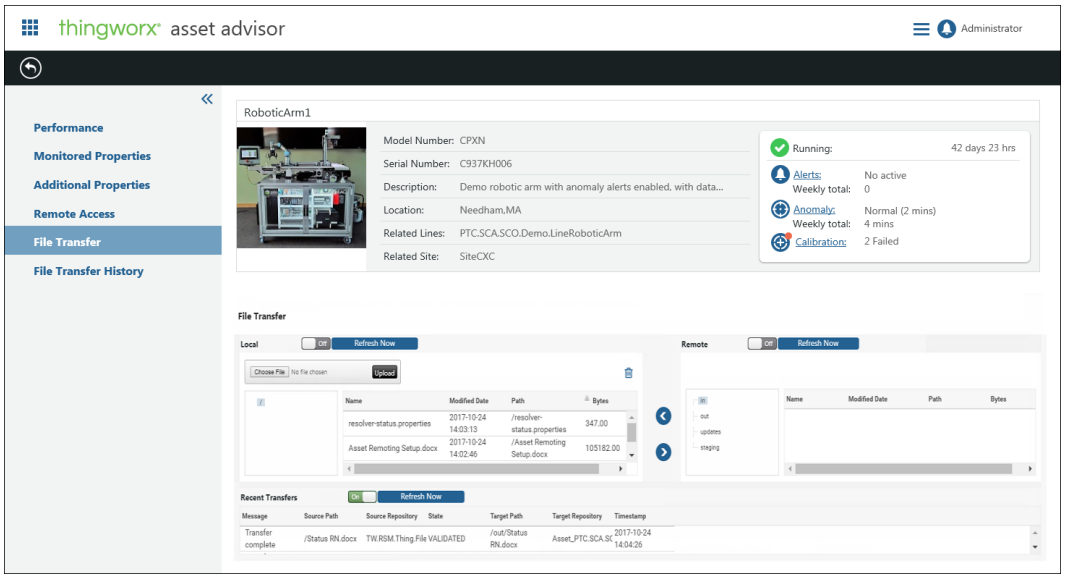
> **Note**
>
> - Once the extension has been imported, assets also need to be configured to be remotely accessed. For more information, see Configure Remote Access and Control on page 66.

- If the asset is already configured for remote access, click the **Launch Remote Access** button to connect directly to the asset for the purpose of executing software patches or changing configuration settings – without the need to make a field trip.
- If the extension has been imported, but the asset has not been configured for **Remote Access**, a message is displayed in the page asking you to notify your system administrator.



Asset Detail — File Transfer

- If the asset is configured for file transfer, you can upload files to, or download files from the asset for the purpose of software upgrade or configuration changes using the **File Transfer** page.
- If the asset has not been configured for file transfer, a message is displayed in the page asking you to notify your system administrator.

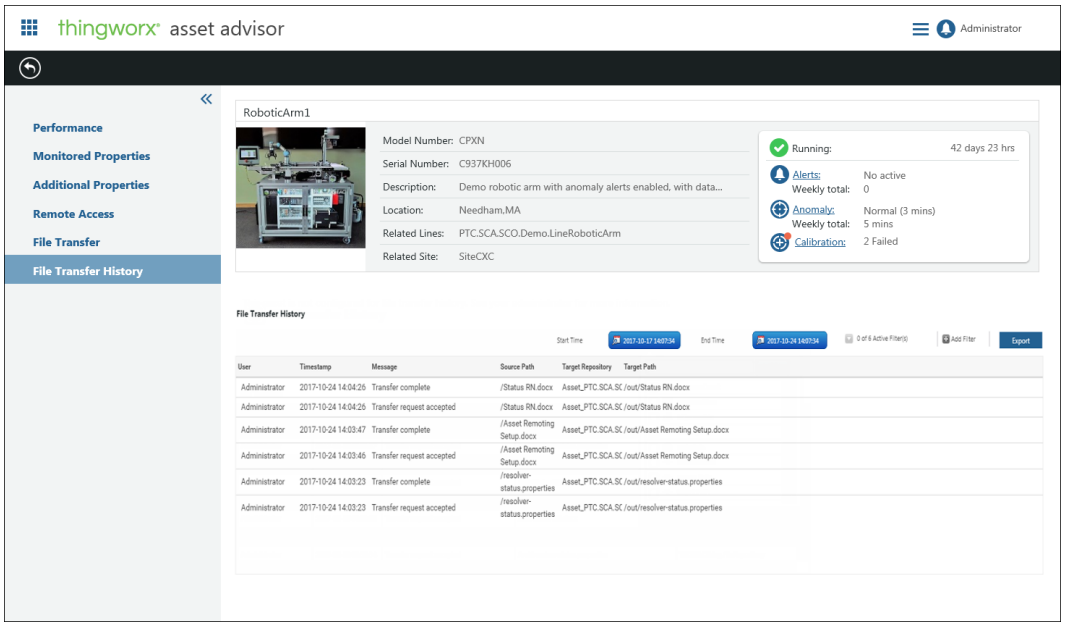


Asset Detail — File Transfer History

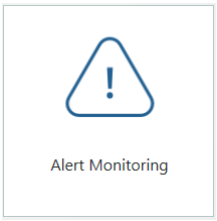
- If the asset is configured to display file transfer history, information is displayed in the lower half of the asset detail page enabling you to manually browse file transfer history or quickly find an entry by entering a date range.

You can also find an entry by applying a standard filter from a drop-down menu.

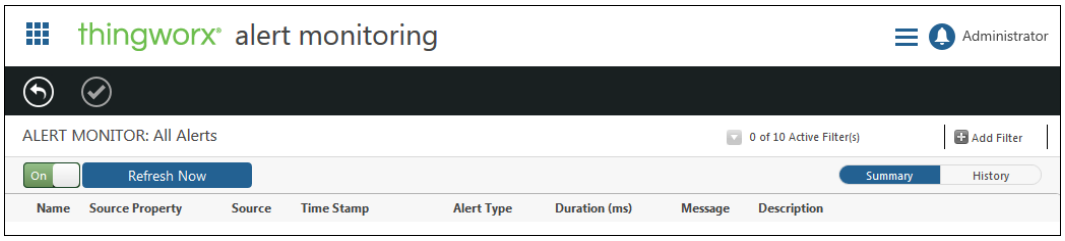
- If the asset has not been configured for file transfer history, a message is displayed in the asset detail page asking you to notify your system administrator.



Alert Monitoring



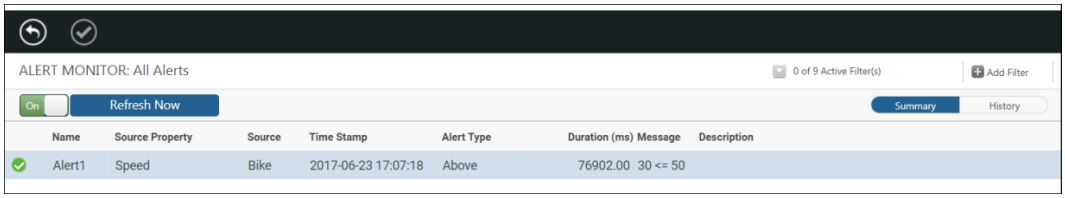
View active alerts and alert history for assets using the **Alert Monitoring** page. All active alerts in the system are displayed in the **Summary** view.



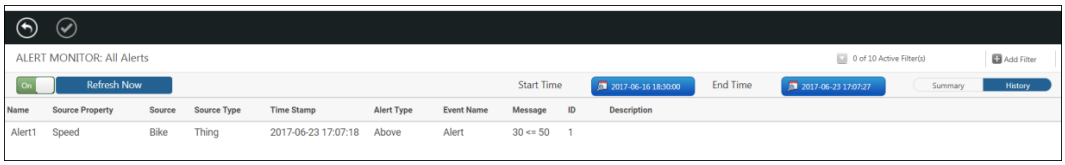
Click an individual alert to see more information about that alert.

To acknowledge an active alert, select the alert and click .

Once an alert has been acknowledged, a checkmark appears in the table and it no longer sends out notification messages.



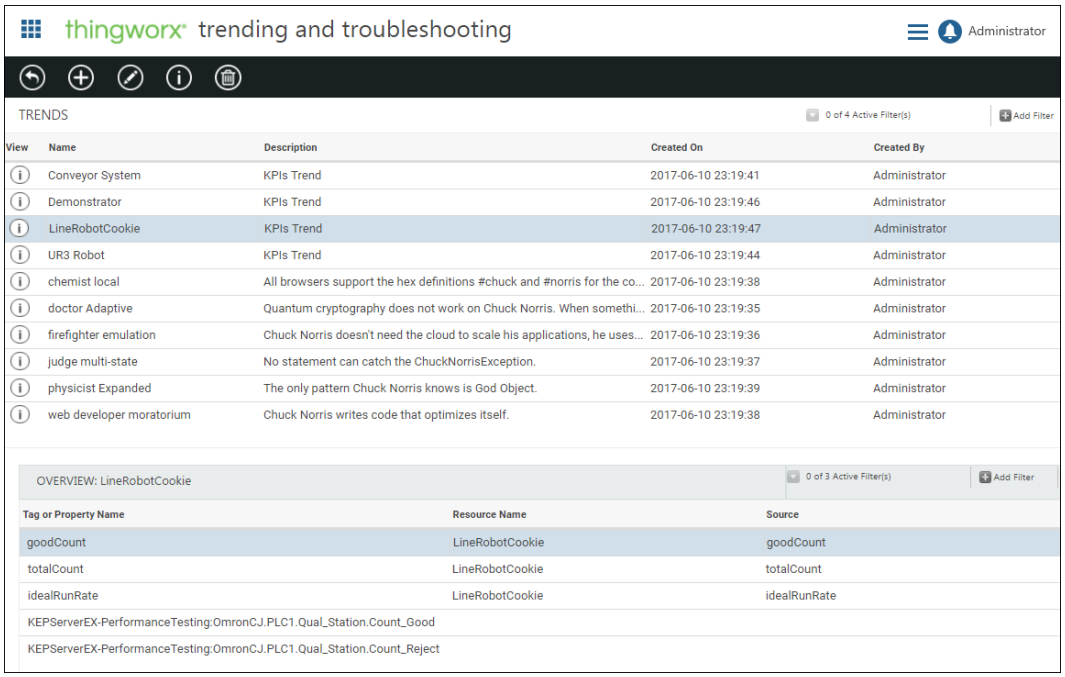
Switch to the **History** view to see alert history for a selected time frame.



You can access threshold alerts in the **Alert Monitor** by clicking on the Alert Monitor icon. Anomaly alerts in the**Alert Monitor** are accessed by clicking on the Anomaly icon.

Trending and Troubleshooting

Use the Trending and Troubleshooting page to track trends that use KEPServerEX tags or properties for a given resource. Once a trend is created, you can view any of the selected properties over varying lengths of time.



To create a trend:

1. At the top of the **trending and troubleshooting** page, click new trend .
2. In the **New Trend** window, enter a name and optionally, a description.
3. Select the type and resource.
4. Select up to five properties or tags to trend for the selected resource.
5. View any of the selected properties over varying lengths of time to track the trend.

5

Advanced Configuration

Creating Custom Roles 63
Configuring the URL Shortening Service 64
Modifying Data Retention Settings 65
Configuring Remote Access and Control 66
Configuring Anomaly Detection 69

Certain configurations must be completed using ThingWorx Composer.

For information about customizing the ThingWorx Manufacturing Apps extension, refer to the ThingWorx Manufacturing Apps Customization Guide located on the PTC Reference Documents website.

Creating Custom Roles

You can define your own roles and assign permissions to those roles, in addition to, or instead of the roles provided with ThingWorx Manufacturing Apps. This enables you to tailor the application to your business processes. Custom roles are set up using ThingWorx Composer. Once created, these custom roles appear in the role assignment section of the **Users and Access Control** page within ThingWorx Manufacturing Apps .

To create a custom role:

1. In ThingWorx Composer, click on **User Groups** under **Security**.
2. Click on the **New** button to create a new user group.
3. Enter the name of the role in the **Name** field
4. Select 'PTC.KinexManufacturing' for **Project**.
5. Select the following tags:
   - `PTC:factory-mv`
   - `Role:Factory-UserGroup`
6. Press **Save** to create the User Group.
7. Select **FactoryUsers** from the list of **User Groups** and click on the **Edit** button.
8. Click on the **Edit Members** button.
9. Select the new user group from list on the left and move it to the list on the right.
10. Press the **Save** button to save the changes and close the dialog box.
11. Press the **Save** button on the screen for the FactoryUsers User Group.

To assign access rights to a custom role:

1. In ThingWorx Composer, click on **User Groups** under **Security**.
2. Click on one of the following user groups to apply the same access rights to your custom role.
   - Controls Engineer
   - Maintenance Engineer
   - Maintenance Manager
   - Production Manager
3. Click on the **Edit Members** button.
4. Select your custom role from list on the left, and move it to the list on the right.

5. Click on **Save** to save the change and close the popup window.
6. Repeat these steps if you would like to apply the rights of another group to your custom role.

> **Note**
>
> If you would like your new custom role to replace an existing role or roles, remove the Role:Factory-UserGroup Tag from roles that you don't want to appear in the application after completing the previous steps.

Configuring the URL Shortening Service

To configure the **URL Shortening Service** field on the **Email and Text Delivery Configuration** page, obtain and apply a Google API key as described below. This allows you to use the Google URL shortening service for links sent in email or text alert notifications.

1. Obtain the Google API key:

> **Note**
>
> This option is not available with Express or Developer Edition licenses.

   a. Go to the following URL: https://developers.google.com/url-shortener/v1/getting_started#APIKey.
   b. Sign in with a Google account.
   c. Click **GET A KEY**.
   d. Enter a project name.
   e. Click **ENABLE API**.
   f. The API key is generated. Copy the API key to a known location.
2. Apply the Google API key in ThingWorx Composer:
   a. From **MODELING** ▸ **Things**, search for the **PTC.SCA.Common.GoogleUrlShortener** thing.
   b. Edit the thing.
   c. Select **Configuration**.
   d. Click **Change Password** for **apiKey**.
   e. Paste in the API key obtained in step 1.

f. Click **Save**.

g. The **PTC.SCA.Common.GoogleUrlShortener** thing now appears as a selectable value for the **URL Shortening Service** field on the **Email and Text Delivery Configuration** page.

Modifying Data Retention Settings

By default, sensor data is purged after one week. The purge is done at midnight each day. This means that each day at midnight, the system checks for data that is one week old and removes it from the system.

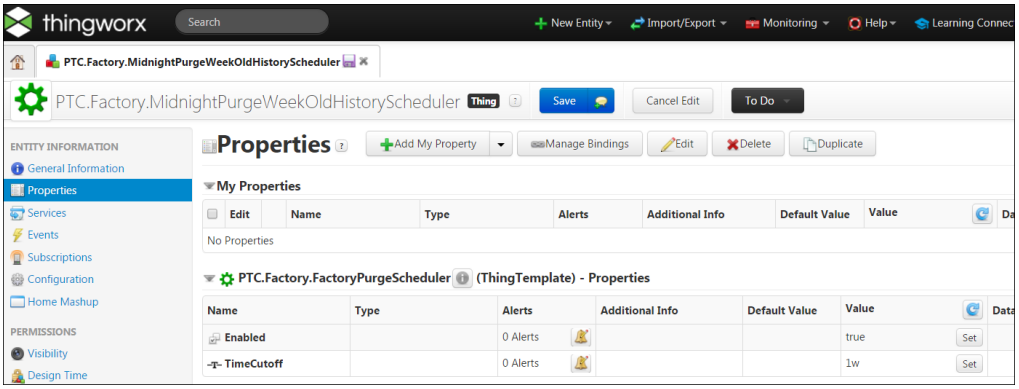
Note

If you have reported feedback on incorrect anomaly status for an asset using the **Report Incorrect Status** action in Asset Advisor, that feedback is stored in the same value stream as the sensor data. To save any reported feedback before a scheduled purge is run, follow the steps in Extracting Anomaly Feedback on page 74.

To modify data retention settings:

1. In ThingWorx Core, locate:

   PTC.Factory.MidnightPurgeWeekOldHistoryScheduler thing.



2. Modify the age of the data purged.

   a. Under **ENTITY INFORMATION**, select **Properties**.

   b. Modify the **TimeCutoff** property by clicking **Set** in the **Value** column.

      The format required is a combination of numbers and letters: w (weeks), d (days), h (hours), m (minutes), and s (seconds). For example, to purge all data older than 3 and a half days, enter `84h` or `3d 12h`.

Case, spaces, and order do not affect the value.

3. Change when the purge occurs.
   a. Under **ENTITY INFORMATION**, select **Configuration**.
   b. Modify the **schedule** property by clicking the **More** button or entering the data manually.

      The property uses CRON format. For more information on CRON, see https://docs.oracle.com/cd/E12058_01/doc/doc.1014/e12030/cron_expressions.htm.

Configuring Remote Access and Control

The remote access extension includes the following optional Asset Advisor features:

- Remote Access
- File Transfer
- File Transfer History

Note

Remote Access only supports VNC. It does not support SSH and Microsoft RDP.

Prerequisites

- Remote access features require the use of either ThingWorx Edge MicroServer or ThingWorx Edge SDK. To meet this prerequisite, do one of the following.
  - Install Edge Micro Server 5.3.4. For more information, see the *ThingWorx WebSocket-based Edge MicroServer Developer's Guide v5.3.4* located at the PTC Reference Documents website under the product category `ThingWorx Edge MicroServer`.
  - Use Edge SDK 6.0. For more information see the *ThingWorx Java SDK Developer's Guide v6.0.0* located at the PTC Reference Documents website under the product category `ThingWorx Edge SDK`

To import the extension:

1. From ThingWorx Composer, navigate to **Import/Export** ▸ **Import**.
2. In the **Import Extensions** window, navigate to: `ThingWorx-Asset-Remoting-8.1.0-extension.zip`.

3. Click **Import** and refresh the window if prompted.
4. You can view the extensions after the import by selecting **Import/Export ▸ Manage**.

To configure an asset for remote access:

1. Connect your Edge device via EMS or Edge SDK. For more information, refer to the guides listed under the heading **Prerequistes**.
2. Verify that the ApplicationKey entity exists on the ThingWorx server so that the EMS or Edge SDK you are using can authenticate with the platform.
3. From Thingworx Composer, navigate to the **Things ▸ Asset_<asset_name> ▸ General Information**.
4. Set the Identifier.
5. Click **Save**.
6. Optional: Configure “Remote Access and Control (RAC)”
    a. From ThingWorx Composer navigate to the**Things ▸ Asset_<asset_name> ▸ General Information** page.
    b. Click on the drop-down menu next to Enable Tunneling and select **Override – Enabled**.
    c. Navigate to the Configuration section and click on the **Add My Tunnel** button.
        i. The Tunnel Name is used to identify what tunnel to use. Enter any name.
        ii. Configure Host and Port from the point of view of the edge device where the server component of the client/server application is running – not the ThingWorx Core. For example, when you want to access the edge device from the VNC Viewer, you would type the IP address of the device, and then the port number.
        iii. The Port value should be the port that the VNC server is listening on. This is typically 5900.
        iv. The App URI should be left as the default, as you are going to rely on ThingWorx built in VNC client.
        v. The # of Connections and Protocol can remain their default values, unless you have a reason to change them.
        vi. Click **Save**.
        vii. From ThingWorx Composer, navigate to **Things ▸ Asset_<asset_name> ▸ Properties**.
        viii. Set your vnc password on the property: *vncProperty*.

> **Note**
>
> The **File Transfer** action enables you to copy files from the local system repository, `TW.RSM.Thing.FileRepositor` to a remote location (an asset). For more information, see the ThingWorx documentation on how to customize a file repository.

Configuring Recommended Subsystem Settings

These are recommended configuration settings for the FileTransferSubsystem and WSCommunicationSubsystem that can improve performance when performing file transfers.

WSCommunicationSubsystem Configuration

If file transfers are expected to involve large files (greater than 20mb in size), increase the timeout value for request response messages to 180 seconds by completing the following steps.

1. In ThingWorx Composer, under System, click **Subsystems**.
2. In the list of subsystems, click **WSCommunicationSubsystem**.
3. In the left-side panel, click **Configuration**.
4. In the **Amount of time a request will wait for the response message before timing out (secs)** field, enter 100.
5. Click **Save**.

Configuring the Other Recommended File Transfer Settings

1. In ThingWorx Composer, under System, click **Subsystems**.
2. In the list of subsystems, click **FileTransferSubsystem**.
3. In the left-side panel, click **Configuration**.
4. Enter the following recommended values for each file transfer setting.

Field	Value
Min. threads allocated to File Transfer pool.	100
Max threads allocated to File Transfer pool	100
Max queue entries before adding new working thread.	10000
Idle thread timeout (seconds).	60
File Transfer idle timeout.	300
Max File Transfer size.	1000000000

5. Click **Save**.

Configuring Anomaly Detection

Anomaly detection uses a machine learning algorithm to model sensor data and compares the current sensor data against the baseline modeled data to identify and report anomalies.

Anomaly Detection Setup

To prepare ThingWorx for anomaly detection, follow the instructions available in the "Implementing Anomaly Detection" section of the ThingWorx Core Help Center, available at the following URL: https://support.ptc.com/help/thingworx_hc/thingworx_8_hc/

1. As described in "Install Anomaly Detection External Services", download and install the `results` and `training` external services.
2. As described in step 1 of "Preparing ThingWorx for Anomaly Detection", configure `AlertProcessingSubsystem` to point to the service locations.
3. You may ignore steps 2–5 of "Preparing ThingWorx for Anomaly Detection", which describes creating and binding a remote Thing.
4. For each property where anomaly detection is configured, perform the following steps:
    a. In New Composer, edit the Connected Server (the Industrial Thing) containing the remote source property.
    b. In Properties and Alerts, edit the remote property and perform the following steps:
        i. Uncheck Persistent. (Non-persistent properties improve the performance of anomaly detection for properties with fast scan rates.)
        ii. Set Scan Rate to the data update frequency in milliseconds.
        iii. Set Push Type to "Always Pushed".
        iv. Save the change to the property, then save the Thing.
    c. In New Composer, edit the asset Thing containing the property.
    d. In Properties and Alerts, edit the property and perform the following steps:
        i. Uncheck Persistent.
        ii. Save the change to the property, then save the Thing.
5. As described in "Creating an Anomaly Alert", use ThingWorx New Composer to create anomaly alerts on any desired properties on the Asset Thing. Refer to Anomaly Detection Configuration Guidelines on page 70 when setting the alert parameters.

Anomaly Detection Configuration Guidelines

This section provides general guidelines for configuring anomaly detection. There are three main configuration parameters: training time, certainty, and outbound anomaly rate. Training time is used in anomaly detection training to build a baseline. Certainty is used to classify whether an observed data stream is anomalous when compared to the baseline. Outbound anomaly rate smooths brief state changes. These parameters are set on each sensor on an asset.

Minimum Data Collection Time (Training Time)

The first thing to consider in anomaly detection is the amount of data that needs to be collected to produce an accurate model of the system. The system works best on periodic data with cycles of fixed length. Ideally, the system should train on non-interrupted data streams which contain at least five cycles. All training must occur on normal, non-anomalous data.

Once training is complete, anomaly detection looks for anomalies in a time window equal to 20% of the training time. For example, if the training time was ten minutes, when an anomaly occurs, it may continue to be reported for up to two minutes after it subsides. This time window allows relatively subtle anomalous patterns to be detected.

Certainty

The certainty parameter defines a percentage threshold, a value between 50 and 100 (exclusive), used to identify whether a new sensor reading should be considered anomalous based on the comparison between the prediction from the baseline model and actual observations. Very high certainty values make it less likely to report a false anomaly, while lower certainty values lead to fewer undetected anomalies.

The choice of certainty is based on business impact. If missing an anomaly will cause critical asset failure, then the certainty should not be set too high. On the other hand, if the asset is very durable or the sensor data has much noise, and frequent anomaly alerts cause too much disruption, set the certainty to a high value to reduce false anomalies. Customers need to adjust the certainty for each sensor until false anomalies are at a manageable level.

Because certainty is defined as a statistical threshold, choosing 99.9999 may produce noticeably fewer false positives than 99.9 (for example), despite the small absolute difference in those values.

Outbound Anomaly Rate

This parameter represents the duration over which to smooth anomaly detection results as well as the interval at which to test for anomalies. An anomaly alert is triggered only while the underlying machine learning algorithm has reported anomalies for more than 50% of data points during the most recent interval. That is, if the parameter is set to 1 minute, then every minute, ThingWorx evaluates

whether more than 30 seconds of the previous minute’s data was anomalous, and sets the alert status accordingly. Increasing this value is the best way to avoid "churn" where brief anomalies appear and disappear.

Outbound anomaly rate must be at least as high as the data scan rate, but should typically be higher to reduce spurious alert activity. The disadvantages of a high value are that the longer test interval can delay reporting an anomaly state change, and that anomalies shorter than the outbound anomaly rate may not be reported at all

Anomaly Detection Limitations

This parameter represents the duration over which to smooth anomaly detection results as well as the interval at which to test for anomalies. An anomaly alert is triggered only while the underlying machine learning algorithm has reported anomalies for more than 50% of data points during the most recent interval. That is, if the parameter is set to one minute, then every minute, ThingWorx evaluates whether more than 30 seconds of the previous minute’s data was anomalous, and sets the alert status accordingly. Increasing this value is the best way to avoid "churn" where brief anomalies appear and disappear.

Note

In the 8.0.0 release, it is not recommended to apply anomaly detection for data streams with any of the following conditions.

- Sensors with multiple normal states. For example, an HVAC unit has a number of different states of operation during the course of a day. All of these states are “normal”, but present very different behavior. For instance, the unit drains more power when actively trying to lower the temperature of the building.
- Sensors with chaotic, unpredictable patterns, such as temperature sensors.
- Sensors with periodic patterns, too fast to be recorded by KEPServerEX, making them appear chaotic.

Understanding Anomaly Detection and Troubleshooting

Anomaly detection in Asset Advisor does not correspond exactly to the judgement of a human eye, and may seem inconsistent at times. Here are some guidelines for interpreting and improving its results.

Expect some false positives

The anomaly detection system works by modeling sensor data and comparing the model's results on recent data against a validation set created during calibration. The system estimates the likelihood that the data sets came from different distributions. If this likelihood exceeds the certainty parameter, the recent data is considered anomalous. For more information on the certainty parameter, see Anomaly Detection Configuration Guidelines on page 70.

Because of the statistical nature of this methodology, sometimes a sensor can be declared as anomalous without the sensor being physically in an anomalous state, especially if certainty or outbound anomaly rate is low or the data is noisy. This can happen even for simulated example data. As a result, brief anomaly reports that are not repeated should not be a major concern for most users. There are some ways to reduce false positive reports, but eliminating them entirely is not always feasible.

Additionally, anomaly detection analyzes a sliding window of data for anomalies, with a length equal to 20% of the training time. A short anomaly (true or false) can continue to be reported for this length of time, even after the sensor data has returned to normal.

If too many false positives, try re-calibrating

False positives are often due to lasting, but harmless, changes in sensor data, such as those caused by environmental changes occurring after the system was trained. These can be fixed by re-calibrating, which is usually the easiest and best thing to try first.

Reducing brief false positives

In many applications, brief anomalies tend to represent statistical noise rather than real problems that require attention. Set the outbound anomaly rate to at least twice the duration of the longest such false positives.

Reducing false positives in un-patterned data

If a sensor's normal variation from moment to moment is mostly noise with no repeated pattern over time, the false positive anomaly reports can be especially common. We recommend setting the certainty parameter to the maximum possible value in this case. This reduces sensitivity to true anomalies, but true anomalies on this kind of sensor usually result in very low or very high values, so the algorithm does not need to be particularly sensitive.

The training time should be long enough to guarantee that a full range of normal data values can be observed several times each. Additional training time is unlikely to help.

If there are still an unacceptable number of false positives at maximum certainty, consider configuring an alert when data falls outside an expected range, rather than using anomaly detection for that sensor.

Reducing false positives in cyclic data

Many types of sensors tend to generate a repeating pattern of data over time. While the anomaly detection in Asset Advisor excels at detecting subtle anomalies in such data, careful configuration is sometimes necessary if too many false positives are observed.

If sequences of false positives seem to appear and disappear periodically, we recommend changing the training time. Examine the data to see how long the data pattern takes to repeat itself. If the pattern is short (less than two minutes), then we recommend training for at least 20 times this cycle length. An even longer training time can help, especially if the data also seems noisy. For longer patterns, instead of increasing the training time, measure the cycle length more precisely and set the training time to an exact multiple of 5 times the cycle length.

After completing this training time, we recommend increasing the certainty until false positives reach an acceptable level.

Missed anomalies

A false negative occurs when sensor data appears anomalous, but Asset Advisor reports that it is normal. This usually means that the certainty has been set too high and should be reduced. (A small number of false negative data points within a correct anomalous report can be safely ignored.)

If Asset Advisor is taking too long to report a real anomaly, or if the missed anomalies are short, try reducing the outbound anomaly rate. Asset Advisor also may not react to anomalies of just a few data points. If true anomalies on a sensor are expected to be this brief, then configuring ThingWorx range alerts for the sensor data may be a useful supplement.

If brief false negative intervals appear within a correct anomalous report, increase the outbound anomaly rate to at least twice the duration of these intervals.

System limitations

Some kinds of data cannot be effectively handled by anomaly detection in Asset Advisor. Avoid configuring anomaly detection for systems with more than one normal state (such as a belt with multiple speeds), or for sensors whose values may have chaotic, non-repeating patterns, or ranges of values that are not seen during a training period (such as temperature).

The system is not very sensitive to changes in cycle period or frequency. If an anomaly manifests as a pattern with normal amplitude but with a faster or slower cycle, the Asset Advisor anomaly detection may not react to changes in the individual intervals between these patterns, although it may detect a change if the activity becomes much more or less frequent overall.

Also note that KEPServerEX generally does not handle incoming data faster than 20 Hz, which causes data patterns with a higher frequency (such as alternating current) to look un-patterned.

Extracting Anomaly Feedback

To extract accumulated reports of incorrect asset status for an individual asset to provide to PTC:

1. Sign into ThingWorx Composer:
   a. Enter `http://<host>:<port>/Thingworx`.
   b. When prompted, enter credentials for an administrator user.
2. In the left pane, scroll down and expand “System”.
3. Select “Subsystems” to display the subsystems in the right pane.
4. In the right pane, select “PlatformSubsystem”.
5. Under “Entity Information:” in the left pane, select “Configuration” to open configuration information in the right pane.
6. Look for “Allow Request Method Switch” and check the check box, then click **Save** at the top of the page.
7. Enter the following URL in the browser address bar:
   `http://<host>:<port>/Thingworx/Things/<AssetName>/Services/QueryInfoTablePropertyHistory?method=POST&Accept=<MediaType>&propertyName=anomalyFeedback&startDate=<startDateInMillis>&endDate=<endDateInMillis>`
   - *<host>*—your host name or IP address.
   - *<port>* –the port on which you have ThingWorx configured to run.
   - *<AssetName>*—the Thing name of the Asset from which you wish to get the anomaly feedback report. For example: PTC.CSLM.PS.Demo.SimPump.Thing.Pump1.
   - *<MediaType>*—type of media acceptable for the response:
     - `text/html` for an HTML report.
     - `application/json` for a JSON report.
   - *<startDateInMillis>*—optional start date and time in milliseconds.
     - Example: convert 1/15/2017 to milliseconds:

`startDate=1484438400000` (this value is only precise to the date and not the time.)

- Date-to-Millis converter: `http://www.epochconverter.com/`.

- *`<endDateInMillis>`*—optional end date and time in milliseconds.
  - Example: convert 1/15/2017 to milliseconds.

    `startDate=1484438400000` (this value is only precise to the date and not the time.)

Configuring Asset Anomaly Status Update Frequency

Asset Advisor calculates and records the anomaly status of each asset at regular intervals, setting the status to Anomalous, Normal, Calibrating, or Unavailable. The update frequency defaults to 30 seconds. It can be made shorter (to improve responsiveness to sensor status changes) or longer (to improve performance or reduce system requirements).

To configure asset anomaly status update frequency:

1. In ThingWorx Composer, open the **PTC.SCA.SCO.AnomalyPropertyUpdateTimer** Thing for editing.
2. Click on the **Configuration** tab.
3. Set a new update rate in milliseconds.
4. Click **Save**.

6

Asset Simulator

Installing the Asset Simulator 77
Asset Simulator Configuration 80
Using the Asset Simulator 82

The Asset Simulator enables you to simulate the behavior of sensors on an asset to model anomaly detection without connecting to a real device. The Asset Simulator system has two main components: the Data Generator and the Asset Simulator. The Data Generator allows you to load or generate sensor data readings. Once sensor data is loaded into the Data Generator, you can simulate several sensor behaviors through the Asset Simulator: normal, anomalous, disconnected, failed, and maintenance states.

Note

Disconnected, failed, and maintenance states are all identical for the purpose of anomaly detection.

In addition to installing the asset simulator and example assets, you can also create new simulated assets.

Installing the Asset Simulator

The Asset Simulator can simulate actual device behavior without having to connect to a physical asset. It does this by replaying data sequences derived from mathematical distributions or actual asset data imported as CSV files. Virtual assets can be configured to reference these data sequences and expose them as asset behavior. The Asset Simulator communicates with KEPServerEX in the same way a real device does. The simulated asset behavior is controlled through an administration console. Typically, both normal and anomalous behaviors are defined for each sensor on the asset.

The Asset Simulator provides 10 simulated Pump assets as part of a reference implementation (5 pump assets and 5 Robotic Arm assets). They are imported with the accelerator extension. Installing the extension creates the 10 assets as Things in ThingWorx. Once the Asset Simulator and KepServerEX are configured, the properties on these Things reflect simulated data.

The following section describes how to install and configure the Asset Simulator to bring life to the reference assets. Then, you can view data streaming through each asset and control their respective sensors' status through the Asset Simulator administration console, to illustrate how Asset Advisor visualizes both normal and anomalous behaviors.

The URLs in these instructions assume that the Data Generator is installed at `localhost:8082` and the Asset Simulator at `localhost:8083`.

Distribution

The Asset Simulator has two main components: the Data Generator and the Asset Simulator. The Data Generator produces data sequences for the Asset Simulator to consume. The Asset Simulator distribution file, ThingworxAssetAdvisorSimulator-<version>.zip is available in the distribution location and contains two sub-distributions and two data files:

- `data-generator-<version>.zip`
- `asset-simulator-<version>.zip`
- `demo-assets.xml`
- `KepwareDemoAssetsProject.json`

Installing the Data Generator

The Data Generator service produces sequences of data points on request. The Asset Simulator takes these data points and exposes them in a protocol that mimics sensor hardware.

Unzip the `data-generator-<version>.zip` file into a directory of your choice. It should contain the following files:

- `demo-dataset.csv`
- `load-demo-dataset.bat`

- `load-demo-dataset.sh`
- `ptc-cslm-data-generator.jar`
- `start.bat`
- `start.sh`

Running the Data Generator

Note

For simplicity, it is recommended that a team run a single instance of the Data Generator on a shared server, to be used by all Asset Simulator instances. This makes setup easier, and also allows users to share data sequences.

1. Install Redis—
   - On Windows—
     a. Download the Microsoft Open Tech Redis 3.2.1 installer (`Redis-x64-3.2.100.msi`) from the following URL: https://github.com/MSOpenTech/redis/releases.
     b. Run the Redis on Windows installer. The default settings are normally fine but may be changed at the user's discretion. Redis is now running as a Windows service.
   - On Linux—
     a. For detailed instructions on installing Redis on Linux, refer to their Quick Start guide at the following URL: https://redis.io/topics/quickstart, or install using your distributions package manager.
     b. Start the Redis server according to your installation instructions.

     Note

     The Data Generator persists its data sequences into Redis. The Data Generator exposes these data sequences through its REST API.

2. Start the Data Generator—
   a. Edit `--spring.redis.host=redis` in the `start.sh` file (for Linux) or `start.bat` file (for Windows), and replace `redis` with the actual host name of the Redis server. For example, `--spring.redis.host=<ip or host name>`.

      The default host:port is `localhost:6379`.
   b. Execute the `start.sh` or `start.bat` file.

c. Visit `http://localhost:8082/swagger-ui.html` to confirm the setup is working.

   If the `swagger-ui` page is loaded, then the Data Generator is up and running.

3. Load the sample data—

   Data sequences can be loaded from files. You can load `demo-dataset.csv` by running `load-demo-dataset.sh` (for Linux) or `load-demo-dataset.bat` (for Windows). Verify that the data is loaded by visiting `http://localhost:8082/Sequences`, and confirm that the page shows data.

> **Note**
>
> On Windows, if you do not have curl installed, you can download it from the following URL: https://curl.haxx.se/download.html. Place the folder containing the curl executable in your system PATH environment variable.

4. Command-line flags—

   The Data Generator service can be executed with several command-line flags which may be added to the start script. These include:

   - `--server.port=<port>` to change the API/UI port from 8082.
   - `--logging.file=<file>` to log to a file (in addition to standard console logging).
   - `--debug` for more detailed logging.
   - `--spring.redis.host=<host>` to specify a Redis location (default is localhost).
   - `--spring.redis.port=<port>` to specify a Redis port (default is 6379).

Installing the Asset Simulator

Unzip the `asset-simulator-<version>.zip` file into a directory of your choice. It should contain the following files:

- `asset-sim-init.json`
- `ptc-cslm-asset-simulator.jar`
- `start.bat`
- `start.sh`

Running the Asset Simulator

1. Start the Asset Simulator—
   a. Execute the `start.sh` file (for Linux) or `start.bat` file (for Windows).
   b. Visit `http://localhost:8083/AssetSimulator`. You should see the interface described in Using the Asset Simulator on page 82.
2. Command-line flags—

   The Asset Simulator can be executed with several command-line flags which can be added to the start script. These include:

   - `--server.port=<port>` to change the API/UI port from 8083.
   - `--logging.file=<file>` to log to a file (in addition to standard console logging).
   - `--debug` for more detailed logging.
   - `--simulator.config=<file>` to specify a non-default name or location for the configuration file.

Asset Simulator Configuration

The Asset Simulator configuration file (typically named `asset-sim-init.json`) names the assets to be simulated and their associated sensors, and maps those sensors to Data Generator data sequences. It also describes the location of the Data Generator and the configuration of the Asset Simulator OPC UA server.

Note

For information on working with the example assets in the Asset Simulator, see Using the Asset Simulator on page 82.

The configuration file uses JSON format. The configurable properties of the top-level JSON object are listed below. Properties are JSON strings unless otherwise noted.

imports

List of strings. This is the only property not shown in the example configuration. It allows partial configurations to be imported from other files. Example syntax is `"imports": ["import1.json", "import2.json"]`.

sensorTypes

List of objects with the following properties. Each sensor type represents a specific sensor on an asset, not just a kind of sensor. For instance, if an asset is fitted with three vibration sensors, each one needs its own sensor type definition. Multiple sensor types can share the same Data Generator sequences.

- `name`—The name of the OPC node for the sensor, also referenced elsewhere in this file.
- `updateIntervalMs`—Time delay before presenting each new data point, in milliseconds.
- `normalSequenceName`—The name of the Data Generator sequence providing this sensor's data while it is in a normal state.
- `anomalySequencename`—The name of the Data Generator sequence providing this sensor's data while it is in an anomalous state.

assetTypes

List of objects with the following properties:

- `name`—Name of the asset type. Used by asset definitions elsewhere in this file.
- `sensorTypes`—List of Strings. The names of the sensor types on each asset of this type.
- `sensorGroups`—Optional List of Objects. Named groups of sensors which might all become anomalous or failed due to a single underlying cause. This is purely a convenience to allow users to change multiple sensors' states at once. The properties of each sensor group object are `name` and `sensors`.

assets

List of objects with the following properties:

- `name`—The name of the OPC folder representing the asset and containing its sensor nodes.
- `assetType`—The asset type, determining the sensors and sensor groups for the asset.

assetBatches

List of objects with the following properties. All assets created in a batch will present the same data for a given sensor in a given state, which allows large numbers of assets to be simulated efficiently. Each asset name has the same prefix

and a zero-padded numeric suffix from 1 to the asset count. That is, setting name to "Pump" and count to "1000" will create assets named Pump0001 through Pump1000.

- `name` – Prefix for names of assets to create.
- `assetType` – The asset type, determining the sensors and sensor groups for the assets.
- `count` – The number of assets to create.

dataGeneratorLocation

The host and port of the Data Generator.

opcHostname

The hostname which should be used by OPC clients for the host machine.

dataBufferMinSeconds

To prevent delays, the Asset Simulator buffers data for each sensor. When the buffer size drops below this level (calculated with `updateIntervalMs`), the simulator requests additional data from the Data Generator.

dataBufferMaxSeconds

When the Asset Simulator makes a request to the Data Generator, it requests enough data to fill its buffer to this level.

sequenceLifetimeHours

The Asset Simulator requests that the Data Generator make temporary copies of its data sequences for each sensor, to avoid collisions in time series requests. This controls the lifetime of the temporary copies.

opcApplicationURI

opcBindPort

opcServerName

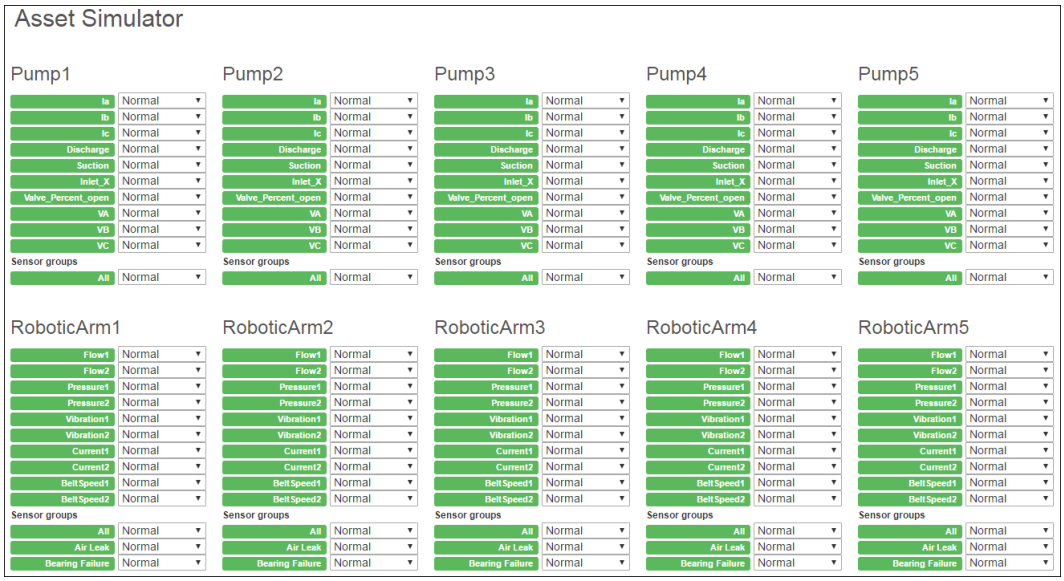
opcApplicationName

These properties control the identity of the simulated OPC server.

Using the Asset Simulator

The Asset Simulator user interface is available at `<host>:<port>/AssetSimulator`, for example: `http://localhost:8083/AssetSimulator`.

The assets, sensors, and sensor groups available in the Asset Simulator UI are largely determined by its configuration file. For more information, see Asset Simulator Configuration on page 80.



Changing sensor states

- To set the state of a sensor on an asset, click on its corresponding drop-down list, and select the new state.
- To set the state of all sensors configured in a group on an asset, click on the group's drop-down list, and select the new state.

Sensor behaviors

- **Normal**—Sensor presents normal data, as defined by the configuration file.
- **Anomalous**—Sensor presents anomalous data, as defined by the configuration file.
- **Failed**—Sensor presents the `BadSensorFailure` OPC UA error code.
- **Disconnected**—Sensor presents the `BadDisconnect` OPC UA error code.
- **Maintenance**—Sensor presents the `BadOutOfService` OPC UA error code.

7

Frequently Asked Questions

Terminology

- What does the term “current shift” mean?

  The term “current shift” is the time frame from midnight to the current time. Midnight is based on the time zone where the server is located.

- What does the term “line” mean?

  The term (production) line refers to a work center that is a collection of equipment dedicated to the manufacture of a specific number of products or product families.

- What is the difference between the terms “asset” and “resource”?

  An asset is a physical object that is uniquely identified and tracked for maintenance and/or financial purposes.

  A resource is a collection of equipment and/or assets that provides the capabilities required to execute an enterprise activity or business process.

- What does the term “site” mean?

  A site is a component of a manufacturing enterprise that is identified by physical, geographical, or logical segmentation.

- What does the term “enterprise” mean?

  An enterprise is one or more organizations that share a mission, goals, and objectives to offer an output such as a product or service.

Reference: ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration − Part 1: Models and Terminology ISBN: 978-1-936007-47-9 International Society of Automation (ISA).

Performance and Scalability

- How many devices are supported for each server?

  A maximum of 250 devices per server are supported. Note that with a large number of devices, discovering devices for a specific server may take several minutes.

KEPServerEX

- Can non-system tags be monitored?

  Update of KEPServerEX system tags only occurs when non-system tags associated to the server are monitored. To monitor a non-system tag, create a trend in **Trending and Troubleshooting** and add any tag from any devices. System tags are found in the `_System` and `_Statistics` tag groups in KEPServerEX.

Alert Notifications

- Why am I not receiving email alert notifications using gmail.com?

  If you are not receiving email alert notifications on domains such as gmail.com or yahoo.com, ensure that the option to allow less secure apps is enabled for those email services. For more information, see https://support.google.com/a/answer/6260879?hl=en.

- How do I set up mobile alert notifications?

  For mobile alert notifications, add any mobile numbers with different country codes to the twilio account before using those mobile numbers.

8

Release Notes

Known Issues and Solutions	
Issue	**Solution**
• When downloading a file whose name contains certain malicious characters ('(' or ')' for example) using the **File Transfer** action in Asset Advisor, the application redirects you to a web page that states “This site can’t be reached”.	The work-around is to rename the file and remove any malicious characters. For more detailed documentation on overriding the default system behavior for FileRespositoryDownloader, see https://support.ptc.com/help/thingworx_hc/thingworx_8_hc/index.html#page/ThingWorx/ThingWorxHelpCenterDITAFiles/GettingStarted/InstallingandUpgrading/ConfiguringESAPIValidatorSettings.html
• When you make administrative changes to an asset and save those changes, other users viewing the same asset from the asset detail page may experience unexpected user interface behavior due to an interruption in websocket communication.	The work-around is to refresh the asset detail page to restore the websocket communication.

Known Issues and Solutions	
• After clicking the **Launch Remote Access** button on an asset detail page to open a remote session, if you attempt to refresh the browser window, a “page not found” message appears giving the impression that the connection has been lost.	The work-around is to return to the asset detail page, click the **Launch Remote Access** button again, and avoid refreshing the browser window during the remote session with the asset.
• When setting a **Start Time** and **End Time** for the Asset Advisor **File Transfer History** action, if the **Start Time** is left in an unconfirmed state while an**End Time** is selected, the events filter for the history window is reset to the current time producing a minimal list of events.	The work-around is to confirm the **Start Time** by selecting **Done** before selecting the **End Time**.