



Predix Edge Manager

Documentation

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2021, General Electric Company. All rights reserved.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Chapter 1. Predix Edge Manager Overview.....	8
About Predix Edge Manager.....	8
Chapter 2. Get Started with Predix Edge Manager.....	11
Predix Edge Manager Setup.....	11
Registering for a Predix Account.....	12
Requesting Predix Edge Manager.....	12
Signing into Edge Manager.....	14
Predix Edge Manager Dashboard.....	15
Using Predix Edge Manager.....	16
Signing out of Predix Edge Manager.....	17
Chapter 3. Manage Users.....	18
About User Manager.....	18
Creating Users and Assigning User Roles.....	19
Viewing Predix Edge Manager Users.....	20
Editing Predix Edge Manager User Roles.....	20
Deleting Predix Edge Manager Users.....	21
Resetting Your Password.....	21
Chapter 4. Device Management.....	23
Device Management.....	23
About Predix Edge Manager Device Management.....	23
Adding a Device to Predix Edge Manager.....	24
Importing a Device List.....	26
Searching the Device List.....	27
Performing Bulk Device Operations on Devices.....	27
Editing Device Information.....	28
Deleting Devices from Predix Edge Manager.....	28
Assigning and Reassigning Devices to Technicians.....	29
Moving Devices to a Different Device Group.....	29
Viewing the Device Summary.....	30
Debugging a Device.....	33
Editing Configurations.....	34
Managing Edge Apps.....	34

Managing Containerized Predix Machine.....	35
Exporting Device Details.....	35
Assigning Predix Services to Devices.....	36
Device Enrollment in the Cloud.....	36
About Predix Cloud Device Enrollment.....	36
Adding a Device to Predix Edge Manager.....	38
Enroll a Device using Predix Edge Technician Console.....	40
Using Predix Edge Technician Console to Enroll Devices with Predix Cloud.....	40
Enroll a Device using the Predix Machine Technician Console.....	41
Predix Machine Technician Console-based Device Enrollment.....	41
Accessing Predix Machine Web Console.....	43
Enrolling a Predix Machine-enabled Device with the Cloud.....	44
Manage Predix Edge Manager Groups.....	45
About Predix Edge Manager Groups.....	45
Adding Groups in Predix Edge Manager.....	45
Editing Predix Edge Manager Device Groups.....	46
Deleting Device Groups in Predix Edge Manager.....	46
Manage Devices with Filters.....	46
About Device Filters.....	46
Enabling and Disabling Global Filters and Saved Filter Sets.....	47
Filtering Devices by Group.....	48
Creating and Saving Filters.....	50
Applying Filters to the Device List.....	51
Editing and Deleting Device Filters.....	51
Clearing Device Filters.....	52
Device Operations.....	52
About Device Operations.....	52
Viewing Operations History.....	53
Viewing Details for Operations.....	54
Operation and Task Status Messages.....	56
Device Models.....	56
Adding Custom Device Models.....	56

Editing and Deleting Custom Device Models.....	58
Chapter 5. Deployment and Analytics.....	59
Package Deployment.....	59
About Deployment.....	59
Deploying Edge Apps.....	59
Deploying Configurations.....	61
Deploying Software.....	63
Deploying a Bill of Materials to Multiple Devices.....	65
Deploying a Bill of Materials to a Single Device.....	66
Deploying Analytics Templates and Data Maps.....	68
Deploying Containers to Devices.....	69
Redeploy Failed Packages.....	69
Analytics.....	70
Chapter 6. Predix Edge Manager Commands.....	73
About Predix Edge Manager Commands.....	73
About Custom Commands.....	78
Adding a Custom Command.....	78
Deleting Custom Commands.....	79
Executing Commands.....	79
Executing or Canceling Commands for a Single Device.....	80
Viewing Command History and Canceling Pending Commands for a Single Device.....	81
Chapter 7. Settings and Alerts.....	83
Monitor Devices.....	83
About Alerts.....	83
Viewing and Filtering Alerts.....	83
Creating Policies for Alerts.....	85
Setting and Removing Alert Policies.....	86
Editing and Deleting Alert Policies.....	87
Predix Edge Manager Settings.....	88
About Predix Edge Manager Settings.....	88
Viewing Settings.....	88
Creating Webhooks.....	89

Setting the Time Format.....	90
Edge Manager Predix Cloud Service Configuration.....	90
Chapter 8. Repository and BOM.....	93
Predix Edge Manager Repository.....	93
About Predix Edge Manager Repository.....	93
External Application Installation and Update.....	94
Uploading Software and Configuration Packages to the Predix Edge Manager Repository.....	95
Package Guidelines and Size Limits.....	97
Creating the Edge Application Package.....	98
Downloading Software Packages from the Predix Edge Manager Repository.....	99
Bill of Materials.....	99
Bill of Materials.....	99
Viewing the Bill of Materials List.....	101
Adding a Bill of Materials.....	101
Deleting a Bill of Materials.....	102
Chapter 9. Data Pumps.....	103
Data Pumps.....	103
Configuring Data Pumps.....	103
Chapter 10. Connectivity and SSH.....	106
Predix Edge Manager Connectivity.....	106
About Predix Edge Manager Connectivity.....	106
Ordering SIM Cards.....	106
SIM Card Life Cycle.....	107
Viewing the SIM Card List.....	107
Exporting the SIM List.....	109
Troubleshooting SIM Cards.....	109
Changing the Rate Plan and Lifecycle Stage For a SIM Card.....	109
Performing a Batch Update.....	110
VPN Management.....	111
SSH Access.....	112
About SSH Access.....	112

Requesting SSH Access.....	113
Uploading a Signed SSH Key.....	113
Activating SSH Online with Edge Manager.....	114
Activating SSH Offline with PETC.....	114
Downloading SSH Keys.....	115
Revoking SSH Online with Edge Manager.....	115
Revoke SSH Offline with PETC.....	116
Chapter 11. Unsubscribe from Edge Manager.....	117
Unsubscribe From Edge Manager.....	117
Chapter 12. Troubleshoot Predix Edge Manager.....	118
Retrieving Predix Machine Logs.....	118
Retrieving Predix Edge Device Logs.....	118
Predix Edge Manager Common Errors.....	120
Filing a Support Ticket.....	121
Troubleshooting Devices.....	121
Chapter 13. Reference.....	124
Related Documentation.....	124
Contacting Support.....	124
Chapter 14. Predix Edge Manager Release Notes.....	126
Predix Edge Manager Release Notes 2.4.0.....	126
Predix Edge Manager Release Notes 2.3.0.....	128
Predix Edge Manager Release Notes 2.2.0.....	129
Predix Edge Manager Release Notes 2.1.0.....	131
Predix Edge Manager Release Notes Q2 2018.....	133
Predix Edge Manager Q1 2018.....	135
Predix Edge Manager Q4 2017.....	138
Predix Edge Manager Q3 2017.....	140
Edge Manager Q2 2017.....	142
Edge Manager Q1 2017.....	144
Edge Manager 2016.....	146
Chapter 15. Index.....	a

Chapter 1. Predix Edge Manager Overview

About Predix Edge Manager

Predix Edge Manager provides a single point of entry for deploying and monitoring fleets of devices remotely.

Use Predix Edge Manager to administer your applications and configuration files at both the device and fleet level. Predix Edge Manager enables you to manage the lifecycle of your edge devices at scale. Remotely and centrally manage large fleets of edge devices to deploy configurations, perform software updates, and install edge apps and analytics.

Predix Edge Manager is available on the cloud, or can be deployed on select edge servers for use cases with limited or no cloud connectivity.

Edge Manager works with Predix Edge to receive and monitor data from connected edge devices. Edge Agent has a layer on top of Docker to manage multi-container applications. Edge Manager supports uploading, deploying, and viewing the status of these multi-container applications.

Prerequisites

Note:

Predix Edge Manager has the following prerequisites:

- You must have a Predix account with an org, space, and UAA service instance. See *(page)*.
- To manage edge apps, install Predix Edge OS
- You must have the Predix Machine SDK version 17.1.x or later. See *Downloading the Predix Machine SDK (page)*.

Edge Manager Microservices

Edge Manager architecture includes the following microservices:

- Application configuration and management service – enables you to upload, maintain, edit, and deploy applications (including multi-container edge applications), bill of materials, and configuration packages.
- Command service – sends commands to Predix Edge or applications that are running on the device.

- Device management service – stores, retrieves, and updates device metadata such as device ID, name, model, and attributes.
- Health monitoring service – displays the internal health status of Edge Manager to enable deep monitoring of service status.
- Scheduler service – provides an endpoint for scheduling tasks for devices based on time and priority.
- Alert management service – generates events from sources that need attention.
- Statistics service – stores and retrieves device resource usage and status history.
- API service – provides a single entry point for API requests that are then routed to the Predix Edge Agent, or other backend service.
- User management service – create users and assign roles.

Supported Browsers

Predix Edge Manager has been tested for support on these browsers:

Browser	Version
Chrome	Last two versions
Firefox	Last two versions

Predix Edge Manager Roles

The following table shows the user interface areas available to each Predix Edge Manager role.

Role	Description	Access to
Technician	<p>This role is assigned by the Predix Edge Manager administrator. For Predix Machine devices, technicians can enroll devices in the cloud using the Predix Machine Technician Console. For Predix Edge devices, technicians can enroll devices in the cloud using Predix Edge Technician Console.</p> <p>The Technician role is assigned to the individual responsible for performing the enrollment activity in the Web Console for each device.</p>	<ul style="list-style-type: none"> • Settings > Enrollment

Role	Description	Access to
Operator	<p>This role has the same access to Predix Edge Manager functionality as the administrator, with the exception of user management.</p> <p>The Operator role is assigned to the individual responsible for creating device instances in Predix Edge Manager with the appropriate Device Name, Device ID, and Device Model according to how the devices should be identified.</p>	All Predix Edge Manager pages except User Manager .
Administrator	The administrator has access to all Predix Edge Manager functionality.	All Predix Edge Manager pages and functionality. No restrictions.
Viewer	The viewer role has read-only access to most Predix Edge Manager pages but has limited ability to perform actions.	<p>Read-only access to all pages, except User Manager. A viewer can perform the following actions:</p> <ul style="list-style-type: none"> • Create filters (but cannot save filters). • Apply filters. • Download software packages from the Repository.

Related tasks

[Requesting Predix Edge Manager \(page 12\)](#)

Chapter 2. Get Started with Predix Edge Manager

Predix Edge Manager Setup

Review the requirements and dependencies before requesting Predix Edge Manager.

- [Required Predix Services \(page 11\)](#)
- [Optional Predix Services \(page 12\)](#)
- [Registering for a Predix Account \(page 12\)](#)
- [Requesting Predix Edge Manager \(page 12\)](#)
- [Predix Edge Manager Dashboard \(page 15\)](#)
- [Using Predix Edge Manager \(page 16\)](#)
- [Signing out of Predix Edge Manager \(page 17\)](#)

Required Predix Services

Predix Edge Manager requires the Predix User Account and Authentication (UAA) and Tenant Management Service (TMS) services.

Predix UAA service

Predix Edge Manager uses the Predix UAA service to manage user authentication access. UAA is an OAuth provider that issues security tokens for client applications to use when acting on behalf of users. UAA provides endpoints for managing user accounts and registering OAuth2 clients to secure Predix Edge Manager.


If you already have one, you can use your existing UAA service when you sign up for Predix Edge Manager.

For more information about UAA, see (page).

Predix TMS service

Predix Edge Manager contains a number of resources that are logically isolated and may require different access privileges for different users. The Predix TMS service provides the ability to provision multiple service instances for one tenant. This allows you to integrate and provision different Predix services (for example, Time Series, Event Hub, and Analytics) with your Predix Edge Manager tenant.

If you already have one, you can use your existing TMS service when you sign up for Predix Edge Manager.

 **Note:** The TMS service instance you use must be bound to the same UAA service instance you are using for Predix Edge Manager.

For more information about TMS, see (page).

Optional Predix Services

There are other Predix services you can integrate with Predix Edge Manager to create a comprehensive Edge-to-Cloud solution.

 **Note:** All services integrated with Predix Edge Manager must use the same UAA service instance.

Time Series

Use the Time Series service to ingest, store, and retrieve time series data. See (page).

Event Hub

Use Event Hub to stream high volumes of data from Predix Machine to the cloud. See (page).

Registering for a Predix Account


When you register for a Predix account, a user account is created and you are given an org and space.

An individual account gives you one org and one space within that org. An Enterprise account gives you one org with one or more spaces. Individual users can add additional spaces to an org assigned to them. Enterprise users can add additional users and spaces to the org assigned to them using the Predix.io user interface.

1. To register as an individual user, go to <http://predix.io> and click **Sign Up**. If you are an enterprise user, contact Predix Customer Support at gedigital@ge.com for help setting up your account.
2. Select your **Country**, choose **Personal** or **Company** account, enter your **Email Address**, and click **Continue**.
3. Enter your information on the Sign-up form and click **Verify Information**. A four-digit pin is delivered to the email address you provided.
4. Enter the four-digit PIN sent to your Work Phone or Work Email.
5. Check your email for details about registration.

Requesting Predix Edge Manager

Provide the information required to request Predix Edge Manager.

 **Note:** If you have a Predix Europe account, you must contact support to request Predix Edge Manager. You must also contact support if you are requesting a Predix Edge Manager with APM account. See [Contacting Support \(page 124\)](#).

 **Note:** Predix Edge Manager has the following prerequisites:

- You must have a Predix account with an org and space. See [Registering for a Predix Account \(page 12\)](#).
- Predix UAA and TMS services are required for Predix Edge Manager. You can use your existing UAA and TMS service instances, if you have them, or you can request new service instances when you request Edge Manager.
- For Predix Machine, you must have the Predix Machine SDK version 17.1.x or later. See [Downloading the Predix Machine SDK \(page \)](#)
- Predix Edge


1. Go to the Predix services catalog, and click **Subscribe**.

2. Fill out the required information in the **New Subscription** form:

- **Org** – The organization email associated with the Predix account that has been created for your business.
- **Space** – The space created in your Predix account org.
- **User Account & Authentication (UAA)** – The UAA service instance to use for Predix Edge Manager. You can use an existing UAA service instance if you have one.

If you do not have an existing UAA service instance, click **Subscribe to New UAA**.

For a new UAA service instance, enter the following information:

Field	Description
Org	Select your organization.
Space	Select the space for your application.
Service instance name	Enter a unique name for this UAA service instance.
Service plan	Select a plan.
Admin client secret	Enter a client secret (this is the admin password for this UAA instance). The client secret can be any alphanumeric string.  Note: Record the client secret in a secure place for later use.
Subdomain	(Optional) Enter a subdomain you might need to use in addition to the domain created for UAA. You must not add special characters in the name of the subdomain. The value of sub-domain is case-insensitive.


Your UAA service instance is created with the following specifications:

- The client identifier ("admin").
- The client secret (that you specified while creating the service).

- **Tenant Management Service** – The TMS service instance to use for Predix Edge Manager. You can use an existing TMS service instance (as long as it is bound to the same UAA service instance you are using for Edge Manager) if you have one.

If you do not have an existing TMS service instance, click **Subscribe to New TMS**.

- **Time Series** – Optionally, select an existing Time Series service instance, or click **Subscribe to New Time Series** to create a new Time Series service instance.
- **Event Hub** – Optionally, select an existing Event Hub service instance, or click **Subscribe to New Event Hub** to create a new Event Hub service instance.
- **UAA client id** – The client identifier ("admin") of the UAA service instance associated with Predix Edge Manager.
- **UAA client secret** – The client secret you specified for the UAA service instance associated with Predix Edge Manager.
- **Edge Manager tenant name** – This will be used as a custom sub-domain name in the provisioned Predix Edge Manager URL and cannot be changed.

 **Note:** The tenant name can contain only alphanumeric characters and hyphens, and must be more than two characters but less than 32 characters long.

The tenant name cannot contain the word "edgemanager."

3. Click **Subscribe**.

You will receive an email containing the provisioned Predix Edge Manager URL.

[Sign into Edge Manager \(page 14\).](#)

Related concepts

[Predix Edge Manager Setup \(page 11\)](#)

[Using Predix Edge Manager \(page 16\)](#)


Related tasks

[Viewing and Filtering Alerts \(page 83\)](#)

Signing into Edge Manager

You can sign into Predix Edge Manager after receiving your provisioned URL service instance.

1. Use a web browser to go to the URL of your provisioned Predix Edge Manager service instance.

 **Note:** Supported browsers are Chrome (minimum version 54) and Firefox (minimum version 45).

2. (Optional) If this is your first time signing into Predix Edge Manager, you are prompted to change your password. In the **User Settings** dialog box, enter the following:

- **Old Password** – Enter the password you logged in with.
- **New Password** – Enter a new password.
- **Confirm Password** – Re-enter your new password.



Note: Your password must:

- Be at least eight characters long and not more than 15 characters long
- Contain at least two uppercase letters
- Contain at least one lowercase letter
- Contain at least two numbers
- Contain at least one special character
- Not contain the user name
- Not contain spaces

3. If this is not the first time you are signing into Edge Manager, enter your user name and password, and click **Sign in**.

You see the Predix Edge Manager Dashboard, and the Control Panel pane on the left, where you can access Edge Manager features like Device Manager, Operations, Alerts, Repository, Bill of Materials, Commands, Connectivity, User Manager, Settings, and so on.



Note: If you are a technician, you see only the **Settings > Enrollment** page. When you enroll devices in the Technician Console, you can copy and paste the Certificate Enrollment URL from this page into the required fields on the device enrollment page.

Related tasks

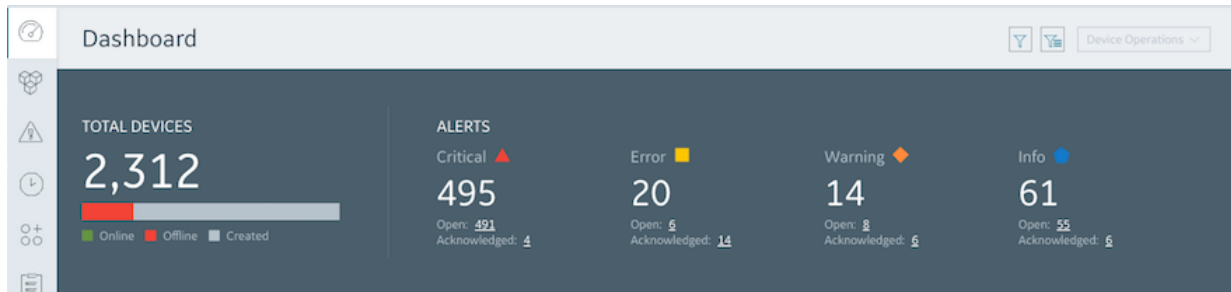
[Resetting Your Password \(page 21\)](#)

[Enrolling a Predix Machine-enabled Device with the Cloud \(page 44\)](#)

[Using Predix Edge Technician Console to Enroll Devices with Predix Cloud \(page 40\)](#)

Predix Edge Manager Dashboard

When you initially sign into Predix Edge Manager, you see the Alerts dashboard at the top of the page. If you have no enrolled devices, all of the number values are zeroes. Once you have enrolled devices, the Alerts dashboard gives you a quick summary view of current alerts, along with how many devices are currently online, offline, or in the created state.



You can apply filters to the information you see on the Alerts dashboard by clicking . You can also create new filters by clicking .

The Predix Edge Manager dashboard also shows device lists, with information about enrolled devices, such as unassigned and offline devices. You can click on the device name link to go to the device details page for that device.

Related tasks

[Creating and Saving Filters \(page 50\)](#)

[Applying Filters to the Device List \(page 51\)](#)

Using Predix Edge Manager

These are some of the basic tasks the administrator and operator roles perform when using Predix Edge Manager.

Task	Description
Create Users.	See Creating Users and Assigning User Roles (page 19) . Note: Only administrators can create and manage users.
Create groups.	See Adding Groups in Predix Edge Manager (page 45) . Create device groups to organize your device inventory by the criteria you specify, such as device type or geographic location.
Import devices into groups.	See Importing a Device List (page 26) . Add multiple devices to a group by importing a list of devices in a CSV file format.
Assign technicians to devices.	See Assigning and Reassigning Devices to Technicians (page 29) .

Task	Description
Enroll devices with Predix Machine.	After the administrator assigns a device, the technician uses the Predix Machine Technician Console or Predix Edge Technician Console to enroll the device with the cloud. See Using Predix Edge Technician Console to Enroll Devices with Predix Cloud (page 40) and Enrolling a Predix Machine-enabled Device with the Cloud (page 44) .
Deploy software packages, a BOM, and configurations to devices.	See Deploying Configurations (page 61) .

Signing out of Predix Edge Manager

Sign out of Predix Edge Manager to end your session.

In the top right of Edge Manager, click your user name, and select **Sign Out**.
You are signed out of Predix Edge Manager and returned to the sign-in screen.

Chapter 3. Manage Users

About User Manager

Only users who are administrators can see and manage user information. The administrator sets up and manages users, roles, and permissions. You can use the **User Manager** page to perform the following tasks:

- View all registered users.
- Create users.
- Delete users.
- Reset user passwords.
- Assign and edit user roles to manage different levels of user permissions.

Predix Edge Manager Roles


The user interface you see depends on your role. The following table shows the areas of Predix Edge Manager different roles can access.


Role	Description	Access to
Technician	<p>This role is assigned by the Predix Edge Manager administrator. For Predix Machine devices, technicians can enroll devices in the cloud using the Predix Machine Technician Console. For Predix Edge devices, technicians can enroll devices in the cloud using Predix Edge Technician Console.</p> <p>The Technician role is assigned to the individual responsible for performing the enrollment activity in the Web Console for each device.</p>	<ul style="list-style-type: none">• Settings > Enrollment
Operator	<p>This role has the same access to Predix Edge Manager functionality as the administrator, with the exception of user management.</p> <p>The Operator role is assigned to the individual responsible for creating device instances in Predix Edge Manager with the appropriate Device Name, Device ID, and Device Model according to how the devices should be identified.</p>	All Predix Edge Manager pages except User Manager .

Role	Description	Access to
Administrator	The administrator has access to all Predix Edge Manager functionality.	All Predix Edge Manager pages and functionality. No restrictions.
Viewer	The viewer role has read-only access to most Predix Edge Manager pages but has limited ability to perform actions.	Read-only access to all pages, except User Manager. A viewer can perform the following actions: <ul style="list-style-type: none"> • Create filters (but cannot save filters). • Apply filters. • Download software packages from the Repository.

Creating Users and Assigning User Roles

Create Predix Edge Manager users and assign roles according to the tasks the user must perform.

1. In the left navigation pane, click  **User Manager**.
2. In the User Manager page, click **Action > Create**.
3. In the **Create User** dialog, enter the user's information, select the user's role, and click **Create**.
 - **User Name** – Name of the user.

 **Note:** The user name cannot contain spaces or special characters other than the following:

- + (plus sign)
 - \ (backslash)
 - - (hyphen)
 - _ (underscore)
 - . (period)
 - @ (at sign)
 - ' (single quote)
 - ! (exclamation point)
- **Email** – Valid email address for the user.
 - **Password** – Password for the user.
 - **Confirm Password** – Re-enter the password you assigned to the user.


When the user logs in the first time, they are prompted to change their password.

- **Role** – Select a role for the user:

- **Administrator** – Administrative access and permissions. Administrators can create groups, import devices, create users, and assign roles to users, and change user passwords.
- **Operator** – Operators can access all the same functionality as the administrator, except for User Manager.
- **Technician** – Can access the Settings page, which displays the certificate enrollment URL.
- **Viewer** – Can view all the Edge Manager pages, except for User Manager, but has limited ability to perform actions.

See [About User Manager \(page 18\)](#) for more information about user roles.


 **Note:** You can assign multiple roles to a user.

 **Note:** You cannot make changes to your own user role when you are logged in with that role.

The new user appears in the user list.

Viewing Predix Edge Manager Users

In the **User Manager** page, you can view users and associated details such as email address, date the user was created, assigned roles, and time and date of last login.

1. In the left navigation pane, click  **User Manager**.
When using User Manager the first time, you see the Welcome screen. Otherwise, you see a list of registered users.
2. (Optional) You can click **Name**, **Email**, **Created**, and **Last Login** to change the order in which the users appear in the list.
3. (Optional) In the **Rows per page** drop-down list, select the number of rows to display on the page.


Related tasks

[Creating Users and Assigning User Roles \(page 19\)](#)



[Deleting Predix Edge Manager Users \(page 21\)](#)

Editing Predix Edge Manager User Roles

In the User Manager page, you can edit user roles.

1. In the left navigation pane, click  **User Manager**.
2. In the user list, select the user to edit the role, and click **Action > Edit**.
You can select only one user at a time for editing.
3. In the **Edit User** dialog, select the roles to apply to the user, then click **Finish**.
The new roles for the user appear in the **Roles** column.


Deleting Predix Edge Manager Users

1. In the left navigation pane, click  **User Manager**.
2. Select the user to delete and click **Action > Delete**.
 **Note:** You can delete multiple users at once.
3. In the confirmation dialog, click **Confirm** to delete the user.
Click **Cancel** to cancel the deletion and return to the user list.

Resetting Your Password

Reset your password if you want to change it, or if you forget it and need to reset it.

1. In the Predix Edge Manager Sign in page, click **Reset Password**.
2. Enter your user name, and click **Send reset password link**.
You will receive an e-mail with a link to reset your password. If you do not receive the e-mail, check your spam (junk) mail folder.
3. Click the reset password link.
You are taken to the **Reset Password** page.
4. Enter and re-enter your new password, and click **Create new password**.

-  **Note:** Your password must:
- Be at least eight characters long and not more than 15 characters long
 - Contain at least two uppercase letters
 - Contain at least one lowercase letter
 - Contain at least two numbers
 - Contain at least one special character

- Not contain the user name
- Not contain spaces

You are logged into Predix Edge Manager.

Chapter 4. Device Management

Device Management

About Predix Edge Manager Device Management

The Predix Edge Manager **Device Manager** page is the entry point for performing many tasks, such as adding and deleting devices, moving devices, assigning devices, and viewing and filtering the device list.



Select **Device Manager > Devices** to view the list of devices. The **Device Manager** page displays a list of registered devices, including the name, device ID, model, status, assigned technician, description, and associated VPNs for each device.

You can use the **Device Manager** page to perform the following tasks:

- Add and delete single, or multiple, devices
- Move devices to other groups.
- View device status and other information about the device, such as Device ID, model, assigned technician, and description.

In the VPN column, if there are associated VPNs for the device, you can click **View** to see the VPN details page.

- Apply filters to the device list to view only devices that meet the criteria you specify.
- Assign and reassign devices to technicians.
- Export a CSV file with device details to your local device.
- Click the device name to view details and perform actions for individual devices.
- Perform bulk device operations, including:
 - Deploy edge apps, BOMs, configurations, containers, templates, and software to a filtered list, or list of selected devices.
 - Executing commands.
 - Setting and removing alert policies.
 - Assigning services.

Related concepts

[Device Summary Page \(page 32\)](#)

[Edge Manager Predix Cloud Service Configuration \(page 90\)](#)

Related tasks

[Creating Policies for Alerts \(page 85\)](#)

Adding a Device to Predix Edge Manager

When you add a device to Predix Edge Manager, information that is specific to the device is added so that when you enroll the device with Predix Machine or Predix Edge Agent, the device can be verified through the security certificate.

Before a device that has Predix Machine or Predix Edge Agent installed can be enrolled and brought online, you must add the device to Predix Edge Manager. This procedure is for adding a single device to Predix Edge Manager. To add multiple devices, see [Importing a Device List \(page 26\)](#).


1. Sign into Predix Edge Manager.


2. In the left navigation pane, select  **Device Manager > Devices**.

3. In the Device Manager page, select **Action > Add**.


4. In the **Add a Device** dialog box, enter the information for the device:

- **Device Name** – the name of the device should be unique and descriptive, and can consist of upper and lower case characters and numbers.
- **Device ID** – used to identify the device with Predix Edge or Machine. The device ID must be unique in a Predix Edge Manager tenant. While the Device ID is typically a serial number, another option is using the MAC address of the WAN interface, which is auto-populated on the Predix Cloud Enrollment page in the local technician console.

 **Note:** The Device ID can consist of lower-case characters and numbers, however, any upper-case characters entered during device creation will be converted to lower-case.


 **Note:** The device ID must follow these conventions:

- Must be a minimum of 3 characters.
- Must not exceed 63 characters.
- Must start with an alphanumeric character (0-9 or a-z).
- The remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).
- Do not use colons (:).
- The Device ID is case-insensitive, but is always stored as lower-case. If you enter upper-case characters in Predix Edge Manager, they are converted to lower-case.

 **Note:** Write down or copy your Device ID for use when enrolling the device with Predix Machine or Predix Edge later.

- (Optional) **Group** – Select the target group for the device.
- (Optional) **Technician** – Select a technician to whom to assign the device.
- **Device Model** – Select the device model from the drop-down list.

- (Optional) **Manufacturer Installed BOM** – A manufacturer BOM lists packages installed before the device is shipped to the user (the packages are not installed through Edge Manager).
 - a. Click **Choose BOM**.
 - b. Select a BOM from the list, and click **Confirm**.

 **Note:** Once a manufacturer BOM is installed, it cannot be modified. Any BOMs deployed at a future date are compared against the initial manufacturer installed BOM, and any packages that are already installed as part of the initial manufacturer BOM are skipped.

- (Optional) **Description** – Add a description for the device.
- **Shared Secret** – Enter the **Shared Secret**. The shared secret provides an initial form of authentication for a device that otherwise does not have an existing identity when you enroll it with Predix Edge. Certificate-based device authentication and enrollment allows a device to enroll itself to Predix Edge Manager at startup and obtain a certificate signed by a root authority.
- **Confirm Secret** – Re-enter the shared secret.
- (Optional) Click **Next** to assign a service to the device.
- Click **Finish** to add the device.

5. If you clicked **Next** in the previous step, in the **Assign Service** dialog box, select the service, or services, to assign to the device.
 - (Optional) Click **Next** to add location details for the device.
 - Click **Finish** to add the device.

6. (Optional) If you clicked **Next** in the previous step, in the **Location** dialog box, enter location details for the device.

 **Note:** The **Elevation** value must be in meters.

- Click **Next** to add custom attributes for the device.
- Click **Finish** to add the device.

7. (Optional) If you clicked **Next** in the previous step, in the **Custom Attributes** dialog box, enter custom attributes as key/value pairs, then click **Finish**.
Key/value custom attributes can be used to add more details about a device, for example, `Region:West`.
Click **+** to add more attributes, and **X** to delete attributes.

8. Click **Finish**.

You receive a confirmation that the device has been successfully added. The device list automatically refreshes and displays the device you added. This may take a moment.

Once you have added the devices to Predix Edge Manager and assigned the technician, the technician can enroll them with Predix Machine or Predix Edge Agent. The technician needs to know the following information in order to enroll the devices:

- Device ID
- Certificate enrollment URL (found on the Settings page)
- Shared secret

Related concepts

[About Predix Edge Manager Groups \(page 45\)](#)

[Edge Manager Predix Cloud Service Configuration \(page 90\)](#)

Related tasks

[Viewing Devices in a Specific Group \(page \)](#)

[Enrolling a Predix Machine-enabled Device with the Cloud \(page 44\)](#)

[Using Predix Edge Technician Console to Enroll Devices with Predix Cloud \(page 40\)](#)

[Viewing the Device Summary \(page 30\)](#)


[Importing a Device List \(page 26\)](#)

Importing a Device List

Import a list of devices in a CSV file format to add multiple devices to Predix Edge Manager.

The CSV must contain the following fields:

- modelID
- did
- name
- sharedSecret

 **Note:** The device ID must follow these conventions:

- Must be a minimum of 3 characters.
- Must not exceed 63 characters.
- Must start with an alphanumeric character (0-9 or a-z).
- The remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).
- Do not use colons (:).
- The Device ID is case-insensitive, but is always stored as lower-case. If you enter upper-case characters in Predix Edge Manager, they are converted to lower-case.

- 1.
2. Select **Action > Import**.
3. In the **Select Group** dialog box, choose the group to import the devices to, and click **Next**.
4. Navigate to the CSV file to import, then double-click.

The devices are imported into the selected group.

5. In the **CSV Upload Status** dialog box, click **Close**.
6. Refresh the device list to see the imported devices.

Searching the Device List

You can search for devices by entering a value for device ID or name.

- 1.
2. Enter your search criteria in the search box.
The search begins when you stop typing.
You can use the following criteria to search for devices:
 - Name
 - Device ID

 **Note:** To clear the search results, delete the search term from the search box.

You can also filter devices to search only devices that meet the filter criteria. For example, if you want to search devices in a specific group instead of all devices.

The device list is updated to display the results of the search. The device list remains filtered according to the search criteria you entered until you delete it from the search field.


Related tasks

[Applying Filters to the Device List \(page 51\)](#)

[Filtering Devices by Group \(page 48\)](#)

Performing Bulk Device Operations on Devices

Use the **Device Manager** page to perform bulk operations like deploying edge apps, software, BOMs, and configurations, as well as executing commands, setting and removing alert policies, and assigning services to devices.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. In the device list, select, or filter, the devices to perform the operation on.
3. In the upper right corner of the Device Manager page, click **Device Operations**, and select the operation to perform.
Device operations include:
 - [Deploy BOM \(page 65\)](#)
 - [Deploy Configuration \(page 61\)](#)
 - [Deploy Container \(page 69\)](#)

- [Deploy Software \(page 63\)](#)
- [Execute Command \(page 79\)](#)
- [Remove Alert Policy \(page 86\)](#)
- [Set Alert Policy \(page 86\)](#)
- [Assign Services \(page 36\)](#)

Editing Device Information

Edit device details such as name, model, assigned technician, and so on.



1. In the left navigation pane, select **Device Manager > Devices**.
2. In the device list, click the link for the device to edit.
3. In the Device page, click **Edit**.
4. In the **Edit Device** dialog box, you can edit the following information for a device:
 - **Device Name** – Name of the device.
 - **Device Model** – Select the device model from the drop-down list.
 - (Optional) **Technician** – Select a technician to whom to assign the device.
 - (Optional) **Description** – Add a description for the device.
 - a. (Optional) Click **Next** to add, or edit, location details for the device.
 - b. Click **Next** to add, or edit, the custom attributes for the device.
 - c. Click **Finish** to save the changes to the device.

Deleting Devices from Predix Edge Manager

When you delete a device, it is completely deleted from the cloud and removed from the Predix Edge Manager UI.

Once you delete a device, you can add it back to inventory and re-enroll it using the same device ID and name.



1. In the left navigation pane, select **Device Manager > Devices**.
2. Select the devices to delete, and select **Action > Delete**.



Note: The **Delete** action is disabled if no filters are applied to the device list to prevent you from deleting all devices.

3. In the confirmation dialog, click **Confirm** to delete the devices.
Devices are permanently deleted, and a confirmation dialog appears.

4. Click **Close**.

Related tasks


[Applying Filters to the Device List \(page 51\)](#)

Assigning and Reassigning Devices to Technicians

Assign devices to technicians so they can complete cloud enrollment using the local technician console.

- Create a user with the technician role.
- Import a device list, or add devices to Predix Edge Manager.

- 1.
2. Select the devices to assign, and select **Select Action > Assign**.

 **Note:** The Assign action is disabled if no filters are applied to the device list.

Select the check box to the left of **Status** to select all devices on the page. If your device list spans more than one page, you have to perform this action on each page.

3. In the **Assign** dialog box, select the technician from the drop-down list, add a description, then click **Assign**.
 - **Technician** – Select a technician or group from the drop-down list.
 - **Description** – Enter the device description.
4. To reassign a device to a different technician, follow steps 1 - 3, then click **Confirm** in the confirmation dialog box to complete reassigning the device.
You return to the device list, where you can view the name of the technician assigned to the device in the Assigned Technician column, and the device description in the Description column.

Related concepts

[Predix Machine Technician Console-based Device Enrollment \(page 41\)](#)

Related tasks


[Enrolling a Predix Machine-enabled Device with the Cloud \(page 44\)](#)

Moving Devices to a Different Device Group

In Predix Edge Manager, you can move devices to a different parent group.



1. In the left navigation pane, select **Device Manager > Devices**.
2. In the device list, select the devices to move, then select **Action > Move**.

 **Note:** The Move action is disabled if no filters are applied to the device list.

3. In the **Move Devices** dialog, select **Move devices under** and select the new parent group, then click **Move**.
4. In the **Move Status** confirmation dialog box, click **Close**.




Viewing the Device Summary

In the device summary page, you can view device details, including device ID, technician assignment, health status, and resource usage.

1. The Device Manager page appears.
2. In the device list, click a device name.

The device's Summary page appears. The Summary page displays the following device details:

Field	Description
Device	Includes information about the device, such as: <ul style="list-style-type: none"> • ID – unique ID assigned to the device. • OS – operating system the device is running on. • Assigned to – the technician the device is assigned to. • Enrollment type – displays the enrollment type (certificate or OAuth). • Container enabled – shows whether the device is enabled for containers. • First seen – timestamp of the first time the device connects to Edge Manager. • Description – brief description of the device, if given. • Location information. • Created by – name of the user who added the device to Edge Manager.
Model	Information about the device model, such as description, processor, memory, and storage.

Field	Description
Health	<p>Device status (for example, "online" or "offline"), the last status change, time since the device was last restarted, and the polling interval (the time interval set to synchronize device data with the database).</p> <p> Note: If the System Up Time for the device is displayed as "Unknown," this indicates there may be a clock issue with the device. See Predix Edge Manager Common Errors (page 120) for more details.</p>
Alert Policy	Displays the associated alert policy for the device (if one is used).
Resource Usage	<p>CPU, memory, and disk usage for the device.</p> <p> Note: CPU and memory utilization is not supported on Windows.</p>
Power Supply Status	<p>Displays the power supply type, the state of the power supply (charging, discharging), percentage of how full the power is, and the description if applicable.</p> <p> Note: Percentage Full and Description are optional, so they are only displayed for certain power supply types, such as battery.</p> <p>Power supply type and state are always displayed for each power type.</p> <p>If there is no power supply "Not available" displays.</p>
Wireless	Displays the wireless connection status.
Bluetooth	Displays the device's Bluetooth connection status.
VPN	VPN client information for the device, including client ID, public IP, IPv4 (internet protocol version 4), and IPv6 (internet protocol version 6).
Connectivity	<p>Number of SIM cards associated with the device, ICCID (integrated circuit card identifier), IMEI (international mobile equipment identity), carrier, provider, and status.</p> <p>If there is a SIM card associated with the device, you can click the ICCID link to view the details for the SIM card.</p>

3. (Optional) Click **Edit** to update the following:

- Device name
- Device model
- Assigned technician
- Description
- Location information

- Custom attributes
- a. Click **Finish** to save the changes.

Related concepts

Device Detail Service ([page 61](#))

Related tasks

[Deploying Configurations \(page 61\)](#)


[Editing Device Information \(page 28\)](#)



Device Summary Page

The **Devices > Summary** page displays information about the selected device and provides access to other device management functionality, such as troubleshooting, configurations, software, BOM, commands, and other pages.

On the **Device Manager** page, click the link for any device in the device list to see details for that device.

The following table describes the functionality of each page.

Page	Description
Summary	See Viewing the Device Summary (page 30) .
Troubleshooting	Use this page to view usage information for the CPU, memory and disk for a device within a specified time period.
Configurations	<ul style="list-style-type: none"> • View the device configuration list and deployment schedule for the device. • Edit configuration files and device information such as device name, model, description, assigned technician, and location. • Assign services to the device. • Deploy selected configurations to a single device.
Edge Apps	<p>View the edge app instances that are deployed to the device, and their corresponding status.</p> <ul style="list-style-type: none"> • Click Start to start the app instance on the device. • Click Stop to stop the running app instance. • Click the trashcan icon to delete an app instance from the device. • Select an application in the list to view the list of containers for that app. <p> Note: This tab is displayed only for devices running on Predix Edge.</p>

Page	Description
Software	<ul style="list-style-type: none"> • View the deployment schedule for Predix software packages and non Predix software packages. • Deploy selected software to a single device. • Edit the name, device model, assigned technician, description, location, and attributes for the device. • Assign services to the device.
BOM	<p>Use this page to:</p> <ul style="list-style-type: none"> • View the current BOM for the device. • View the BOM installation status. • Deploy a BOM to the device.
Commands	View the commands history, cancel pending commands, and execute commands for the device.
Analytics	View the deployed analytics templates for the device.
Containers	<p>This page displays a list of the containers deployed to the device.</p> <p> Note: This tab is displayed only if the device has container images.</p>
Data Pumps	<p>Use this page to create data pumps and view and edit existing data pumps and their status.</p> <p> Note: This tab is displayed only for devices running on Predix Edge.</p>

Related concepts

[About Predix Edge Manager Commands \(page 73\)](#)

Related tasks

[Viewing the Device Summary \(page 30\)](#)

[Deploying Configurations \(page 61\)](#)

[Editing Configurations \(page 34\)](#)

[Troubleshooting Devices \(page 121\)](#)

Debugging a Device

View details about the Predix Machine bundles that are running on the device.

1. In the left navigation pane, select  **Device Manager > Devices**.

2. In the device list, select a device.

The device's **Summary** page appears.


3. In the upper right-hand, click .

The **Debug Details** window appears, displaying details about Machine bundles on the device.


4. Click **Close** when you are finished viewing the debug information.


Editing Configurations

You can edit and deploy configurations for an individual device in Predix Edge Manager.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. Click the link for a device to edit its configuration files.
3. In the Devices page, click the **Configurations** tab.
The **Deployment Schedule** displays a list of configurations for the device, along with the corresponding details and deployment status.
4. Click the configuration package name to edit.
5. In the **Configuration** dialog box, click the file to edit.
6. In the **Edit File** window, make your changes, and click **Save**.
7. In the **Configuration Package** dialog, click **Schedule**.
8. In the **Schedule Deployment** dialog, select the date and time to deploy the configuration to the device and click **Submit**.
The updated configuration package is deployed to the device at the time you scheduled it. The list of configuration files displays and shows the revision number in the Revision column.

Managing Edge Apps

 **Note:** The **Edge Apps** tab is displayed only for devices running on Predix Edge.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. Click the name of the device with the edge apps you want to manage.
3. Click the **Edge Apps** tab.
The **Deployment Schedule** table shows a list of edge apps that are scheduled for deployment, along with the corresponding details and deployment status.

The **Applications** table displays the edge apps that are deployed to the device and their status.

4. Select the action to perform.

- Click **Start** to start the edge app on the device.
- Click **Stop** to stop the edge app on the device.
- Click the trash can icon to delete an edge app from the device.

The **Status** column shows the results of your action, and the **Timestamp** column displays the time and date the action was executed.


If the device is offline, the **Status** is displayed as "pending" until the device is online and the action takes effect.

5. (Optional) Click an Application ID to view the status of individual containers contained in the edge app.

If there are errors associated with the container, click **View** in the **Errors** column to view the error message for the container.

Managing Containerized Predix Machine

Use the **Containers** tab to manage a Predix Machine container on a device from Predix Edge Manager.

 **Note:** The **Containers** tab is displayed only for devices running containerized Predix Machine.



1. In the left navigation pane, select **Device Manager > Devices**.

2. Click the name of the device with the container you want to manage.

3. Click the **Containers** tab.

The **Container Images** section displays the containers running on the device.

4. Select the action to perform.

- Click **Start** to start a container.
- Click **Stop** to stop a container.
- Click the trash can icon to delete a container.


The **Status** column shows the results of your action, and the **Timestamp** column displays the time and date the action was executed.

Exporting Device Details

You can export a list of devices and their corresponding details from Predix Edge Manager to your local machine as a CSV file.

1.

2. Select the devices to export details for, and select **Action > Export**.

 **Note:** The Export action is disabled if no filters are applied to the device list.


3. In the **Export Device Details** dialog, click **Export**.


The device details are compiled and exported to your local machine in a CSV file.

Assigning Predix Services to Devices

Assign Predix services like Time Series and Event Hub to devices.

You must configure services before you can assign them to devices.

 **Note:** You can have multiple services assigned to a device, but all assigned services must be bound to the same UAA service instance that is bound to your instance of Predix Edge Manager so Edge Manager can issue a token with rights to that service instance.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. In the device list, select, or filter, the devices to assign services to.
3. In the upper right corner of the Device Manager page, click **Device Operations > Assign Services**.
4. In the **Assign Service** dialog, select the services to assign, and click **Assign**.
The operations for assigning services to the device ID are started.

Related information

(page)

Device Enrollment in the Cloud

About Predix Cloud Device Enrollment

For cloud enrollment, devices must be added to Predix Edge Manager by an administrator or operator before enrolling the device with the technician console. Enroll devices with Predix Edge Technician Console for devices running Predix Edge Agent, or Predix Machine Technician Console for devices running Predix Machine.

When the device is initially added to Predix Edge Manager, it has no identity associated with the Predix cloud until an identity is created on the cloud through certificate enrollment and associated with the device using Predix cloud authentication.

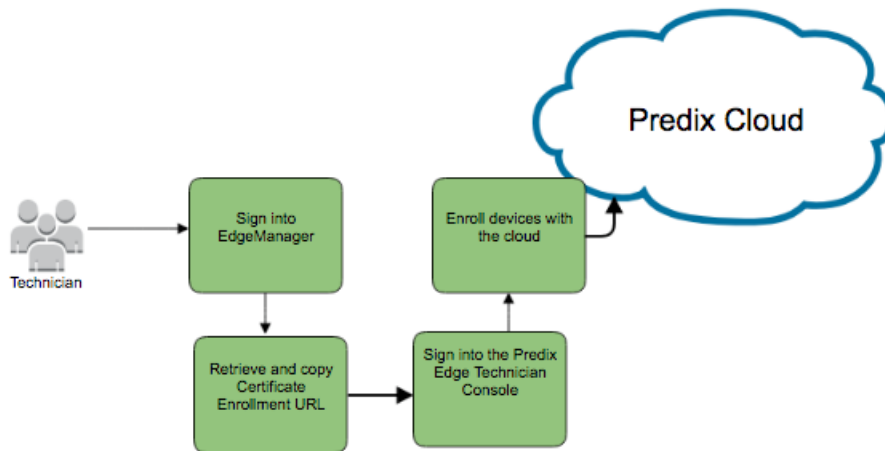
Certificate-based device authentication and enrollment allows a device to enroll itself with Predix Edge Manager at startup and obtain a certificate signed by a GE root authority so that no device-specific credentials are required. Once a device is configured with the Edge Manager URL, device ID, and shared secret, it can communicate with the cloud environment at startup and obtain its own certificate and credentials.

Administrator Tasks

1. The administrator creates the technician user with the Technician role in Predix Edge Manager, and provides the technician with Predix Edge Manager login credentials.
2. The administrator or operator adds devices to Predix Edge Manager and enters a shared secret for the device.

Technician Tasks

Task	Description
1. Login to Predix Edge Manager and change password.	The administrator provides initial sign-in credentials and the URL to access Predix Edge Manager to the technician. When the technician logs in for the first time, they are prompted to change their password.
2. Go to Settings .	The technician is directed to the Settings > Enrollment page and makes note of the appropriate certificate enrollment URL.
3. Sign into the local technician console.	Sign into the technician console. For Predix Machine, see Accessing Predix Machine Web Console (page 43) . For Predix Edge Agent, see Using Predix Edge Technician Console to Enroll Devices with Predix Cloud (page 40) .
4. Finish enrollment process.	The technician finishes enrolling the device with either Predix Edge Technician Console or the Predix Machine Technician Console. This creates an identity for the device in the cloud.

Figure: Technician Workflow for Predix Edge Technician Console**Related concepts**

Predix Cloud Identity Management Service ([page 39](#))

Related tasks

[Adding a Device to Predix Edge Manager \(page 24\)](#)

[Using Predix Edge Technician Console to Enroll Devices with Predix Cloud \(page 40\)](#)

Adding a Device to Predix Edge Manager

When you add a device to Predix Edge Manager, information that is specific to the device is added so that when you enroll the device with Predix Machine or Predix Edge Agent, the device can be verified through the security certificate.

Before a device that has Predix Machine or Predix Edge Agent installed can be enrolled and brought online, you must add the device to Predix Edge Manager. This procedure is for adding a single device to Predix Edge Manager. To add multiple devices, see [Importing a Device List \(page 26\)](#).


1. Sign into Predix Edge Manager.


2. In the left navigation pane, select  **Device Manager > Devices**.

3. In the Device Manager page, select **Action > Add**.


4. In the **Add a Device** dialog box, enter the information for the device:

- **Device Name** – the name of the device should be unique and descriptive, and can consist of upper and lower case characters and numbers.
- **Device ID** – used to identify the device with Predix Edge or Machine. The device ID must be unique in a Predix Edge Manager tenant. While the Device ID is typically a serial number, another option is using the MAC address of the WAN interface, which is auto-populated on the Predix Cloud Enrollment page in the local technician console.


 **Note:** The Device ID can consist of lower-case characters and numbers, however, any upper-case characters entered during device creation will be converted to lower-case.

 **Note:** The device ID must follow these conventions:

- Must be a minimum of 3 characters.
- Must not exceed 63 characters.
- Must start with an alphanumeric character (0-9 or a-z).
- The remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).
- Do not use colons (:).
- The Device ID is case-insensitive, but is always stored as lower-case. If you enter upper-case characters in Predix Edge Manager, they are converted to lower-case.

 **Note:** Write down or copy your Device ID for use when enrolling the device with Predix Machine or Predix Edge later.

- (Optional) **Group** – Select the target group for the device.
- (Optional) **Technician** – Select a technician to whom to assign the device.
- **Device Model** – Select the device model from the drop-down list.
- (Optional) **Manufacturer Installed BOM** – A manufacturer BOM lists packages installed before the device is shipped to the user (the packages are not installed through Edge Manager).
 - a. Click **Choose BOM**.
 - b. Select a BOM from the list, and click **Confirm**.

 **Note:** Once a manufacturer BOM is installed, it cannot be modified. Any BOMs deployed at a future date are compared against the initial manufacturer installed BOM, and any packages that are already installed as part of the initial manufacturer BOM are skipped.

- (Optional) **Description** – Add a description for the device.
- **Shared Secret** – Enter the **Shared Secret**. The shared secret provides an initial form of authentication for a device that otherwise does not have an existing identity when you enroll it with Predix Edge. Certificate-based device authentication and enrollment allows a device to enroll itself to Predix Edge Manager at startup and obtain a certificate signed by a root authority.
- **Confirm Secret** – Re-enter the shared secret.
- (Optional) Click **Next** to assign a service to the device.
- Click **Finish** to add the device.

5. If you clicked **Next** in the previous step, in the **Assign Service** dialog box, select the service, or services, to assign to the device.
 - (Optional) Click **Next** to add location details for the device.
 - Click **Finish** to add the device.

6. (Optional) If you clicked **Next** in the previous step, in the **Location** dialog box, enter location details for the device.

 **Note:** The **Elevation** value must be in meters.

- Click **Next** to add custom attributes for the device.
- Click **Finish** to add the device.

7. (Optional) If you clicked **Next** in the previous step, in the **Custom Attributes** dialog box, enter custom attributes as key/value pairs, then click **Finish**.

Key/value custom attributes can be used to add more details about a device, for example, Region:West.

Click + to add more attributes, and X to delete attributes.

8. Click **Finish**.

You receive a confirmation that the device has been successfully added. The device list automatically refreshes and displays the device you added. This may take a moment.

Once you have added the devices to Predix Edge Manager and assigned the technician, the technician can enroll them with Predix Machine or Predix Edge Agent. The technician needs to know the following information in order to enroll the devices:

- Device ID
- Certificate enrollment URL (found on the Settings page)
- Shared secret

Related concepts

[About Predix Edge Manager Groups \(page 45\)](#)

[Edge Manager Predix Cloud Service Configuration \(page 90\)](#)

Related tasks

[Viewing Devices in a Specific Group \(page 30\)](#)

[Enrolling a Predix Machine-enabled Device with the Cloud \(page 44\)](#)

[Using Predix Edge Technician Console to Enroll Devices with Predix Cloud \(page 40\)](#)

[Viewing the Device Summary \(page 30\)](#)

[Importing a Device List \(page 26\)](#)

Enroll a Device using Predix Edge Technician Console

Using Predix Edge Technician Console to Enroll Devices with Predix Cloud

You must install Predix Edge Technician Console ([page](#)).

For devices running Predix Edge, with connectivity to Predix cloud, you can use the Predix Edge Technician Console to configure the device with the Predix Edge Manager certificate enrollment URL, device ID, and shared secret, so it can communicate with the cloud environment at startup and obtain its own certificate and credentials.

1. Sign into Predix Edge Technician Console.
2. In the **Device Status** page, click **Enroll**.
3. In the **Enroll Device** dialog box, enter the following information:
 - **Device ID** – Identifies the device with Predix Edge OS. The device ID you enter must match the device ID assigned when the device was added to Edge Manager by the administrator.
 - **Shared Secret** – Enter the shared secret that was entered with the device was added to Predix Edge Manager.
 - **Certificate Enrollment URL** – URL of the Predix Edge Manager tenant. You can find the correct certificate enrollment URL in the Predix Edge Manager **Settings** page.
4. Click **Enroll**.
A green banner displays at the top of the Device Status screen confirming enrollment was successful and the device status displays "enrolled."

In Edge Manager, the device status displays "online" (this may take a moment).

Enroll a Device using the Predix Machine Technician Console

Predix Machine Technician Console-based Device Enrollment

A technician can use the Predix Machine Technician Console to enroll devices after an administrator or operator has added the device to Predix Edge Manager.

The flow for enrolling devices using the Predix Machine Technician Console is as follows:

Administrator Tasks

1. The administrator creates the technician user with the Technician role in Predix Edge Manager, and provides the technician with login credentials.

- The administrator or operator adds devices to Predix Edge Manager and enters a shared secret for the device.

Technician Tasks

Task	Description
1. Login to Predix Edge Manager and change password.	The administrator provides initial sign-in credentials and the URL to access Predix Edge Manager to the technician. When the technician logs in for the first time, they are prompted to change their password.
2. Go to Settings.	The technician is directed to the Settings > Enrollment page and makes note of the appropriate certificate enrollment URL.
3. Sign into the Machine Technician Console.	Sign into the Predix Machine Web Console and go to Technician Console > Predix Cloud Enrollment . See Accessing Predix Machine Web Console (page 43) .
4. Finish enrollment process.	The technician finishes enrolling the device with Predix Machine. This creates an identity for the device in the cloud. See Enrolling a Predix Machine-enabled Device with the Cloud (page 44) .

Figure: Technician Device Enrollment Flow

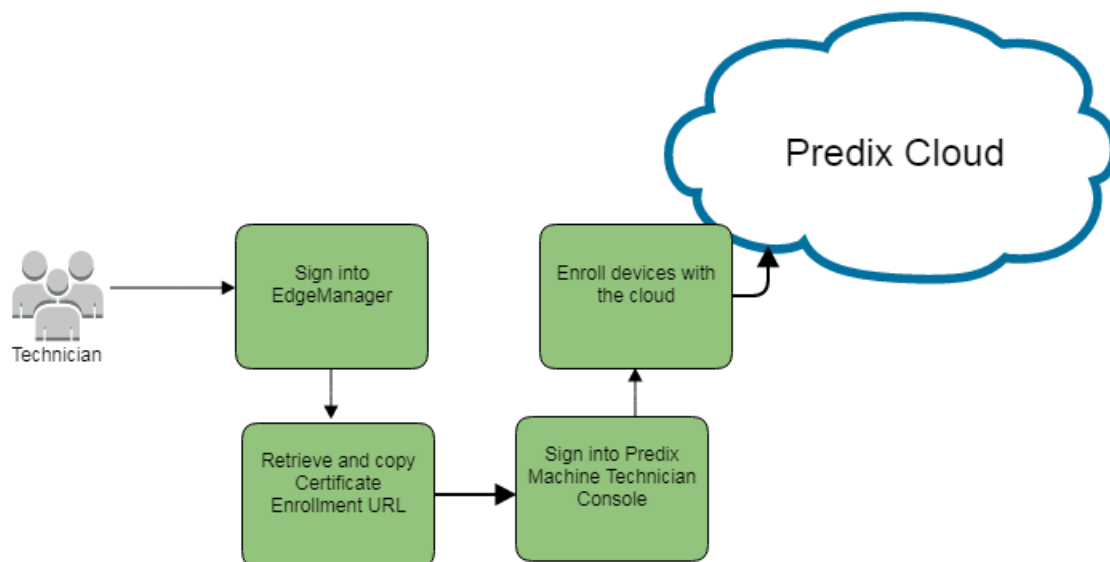
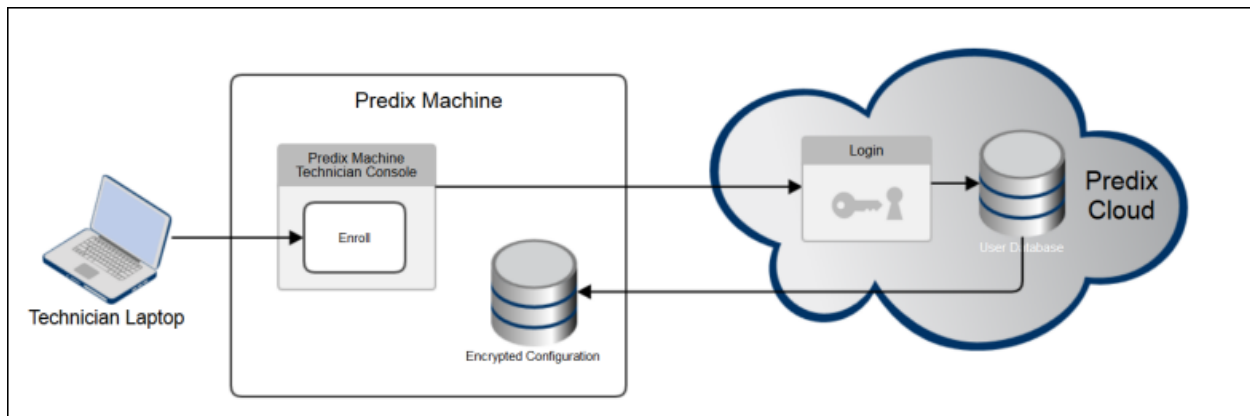


Figure: Predix Machine Device Enrollment Process



Accessing Predix Machine Web Console

You can access and manage the bundles in your Predix Machine environment using the Predix Machine Web Console.

Start a Predix Machine provisioning (PROV) container.

Note: You can only access the Predix Machine Web Console for Predix Machine DEBUG, PROV, OR TECH container types; you must specify one of these types when you generate the container from the Predix SDK.

1. Open a web browser and navigate to:

```
https://localhost:8443/system/console/
```

Note: Since the Web Console uses a self-signed certificate, the browser will warn that the connection is not private. You can proceed.

A login prompt is displayed.

2. Enter your user name and password. If this is your first time logging into the Predix Machine Web console, use the following defaults:

Username: predix

Password: predix2machine

Note: Your password must:

- Be at least eight characters long and not more than 15 characters long
- Contain at least two uppercase letters
- Contain at least one lowercase letter
- Contain at least two numbers
- Contain at least one special character

- Not contain the user name
- Not contain spaces

The Predix Machine Web Console opens, using an Apache Felix web interface. For more information on using the Apache Web Console, see <http://felix.apache.org/documentation/subprojects/apache-felix-web-console.html>.


3. If you use a proxy server, set HTTP Client proxies.
 - a. In the Predix Machine Web Console, click **OSGi > Configuration**.
 - b. Click the Apache HttpClient OSGI bundle in the Name column. For example, **CM_GENERATED_PID.0**.
 - c. Select the **proxy.enabled.name** check box.
 - d. In the **proxy.host.name** box, enter the proxy host.
 - e. In the **proxy.port.name** box, enter the proxy port number.
 - f. Complete the **proxy.password.name** and **proxy.exceptions.name** box, and click **Save**.

Enrolling a Predix Machine-enabled Device with the Cloud

Technicians use the Predix Machine Technician Console to enroll a Predix Machine-enabled device in the Predix cloud.

Administrators or operators must add a Predix Machine-enabled device to Predix Predix Edge Manager before the technician enrolls the device with Predix Machine. See Adding a Device to Predix Edge Manager (*page*).

1. Sign into the Predix Machine Web Console.
2. Click **Technician Console > Predix Cloud Enrollment**.
3. Enter the following information:
 - **Device ID** – Device ID from Predix Edge Manager device summary. This matches the device ID you entered when you added the device to Predix Edge Manager.

 **Note:** The device ID must follow these conventions:

 - Must be a minimum of 3 characters.
 - Must not exceed 63 characters.
 - Must start with an alphanumeric character (0-9 or a-z).
 - The remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).
 - Do not use colons (:).
 - The Device ID is case-insensitive, but is always stored as lower-case. If you enter upper-case characters in Predix Edge Manager, they are converted to lower-case.
 - **Certificate Enrollment URL** – URL of your Predix Edge Manager tenant.

- **Shared Secret** – Provides an initial form of authentication for a device that otherwise does not have an existing identity.

4. Click **Enroll Device**.

The **Enroll Device** button is disabled while the device generates a certificate and sends the corresponding Certificate Signing Request (CSR) to the Predix cloud for signing. This process can take up to 30 seconds to complete before an enrollment success message is displayed.

When certificate enrollment is complete, Predix Machine restarts itself before it appears in Predix Edge Manager with an **Online** status.

Related tasks

[Viewing the Device Summary \(page 30\)](#)

Manage Predix Edge Manager Groups

About Predix Edge Manager Groups

Use the Predix Edge Manager **Groups** page to add, edit, and delete groups.

You can use groups to organize devices by the criteria you specify. A group of devices shares common, unique characteristics, which distinguishes it from other device groups in your network. For example, you can create a group for devices based on their geographic location, or by device type, with sensors in one group and diagnostic devices in another.

Adding Groups in Predix Edge Manager

Create device groups in Predix Edge Manager to organize your device inventory by the criteria you specify, such as device type or geographic location.

1. In the left navigation pane, select **Device Manager > Groups**.
2. In the **Groups** page, click **Action > Add**.
3. In the **Add Group** dialog window enter the information for the group:
 - a. In **Group Name**, enter a name for the group.




Note: Group names must:

- Begin with an alphanumeric character and can contain alphanumeric, dashes, underscores and spaces
- Be between 3 and 63 characters long

- b. (Optional) Select the **Nest Group Under** check box to nest your group under a parent group, then select the parent group from the list.

By default, groups are not nested.

 **Note:** If this is the first group you are creating, no entries are visible in the **Select Parent Group** field because there are no groups.

Creating subgroups can help you refine the way your device groups are organized.

- c. Click **Add**.

The group appears in the group list.


Editing Predix Edge Manager Device Groups

In the Predix Edge Manager Groups page, you can edit group names and change their parent group.

1. In the left navigation pane, select **Device Manager > Groups**.
2. In the **Groups** page, select the group to edit, then click **Action > Edit**.
3. To change the name of the group, or parent group:
 - In **Group Name**, enter the new name for the group, and click **Save**.
 - Select the check box next to **Nest group under**, select the new parent group from the list, and click **Save**.

Deleting Device Groups in Predix Edge Manager

You can delete single groups, or multiple groups.

 **Note:** When you delete a parent group, the subgroups and devices within the parent group are not deleted, but instead move up one level in the hierarchy.

1. In the left navigation pane, select **Device Manager > Groups**.
2. In the **Groups** page, select one or more groups and click **Action > Delete**.
3. In the confirmation dialog box, click **Confirm**.
4. In the **Delete Status** dialog box, click **Close**.

Manage Devices with Filters

About Device Filters

In Predix Edge Manager, create and apply filters so you can more easily work with large numbers of devices.

When you are working with a large number of devices, you may want to manage only on a specified subset of all devices. For example, you may want to filter the list of devices so that only devices of a certain model that have an online status are displayed. This allows you to perform actions (such as deploying configurations and software, and executing commands) on only the set of devices that meet the criteria you specify when you create the filter.

You can create and apply filters on the following pages:

- **Dashboard**
- **Device Manager > Devices**
- **Alerts**
- **Operations**

When filters are applied, the number of filters and number of devices included in the applied filter displays to the left of the filter icons. Click on **Filter Applied** to see a list of all the currently applied filters.

1 Filter Applied 9 Devices  

Related concepts

[About Device Operations \(page 52\)](#)

Enabling and Disabling Global Filters and Saved Filter Sets

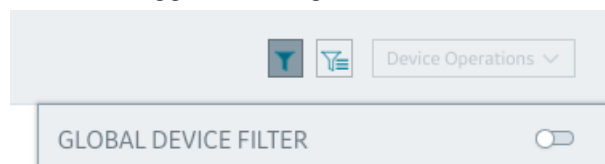
You can change whether or not applied filters will be global and persist across all Edge Manager pages that display a device list.

By default, filters are global, which means that when you apply the filter, the filtered list of devices displays on every page of Edge Manager that has a device list (Dashboard, Device Manager > Devices, Operations, and Alerts > List). Filters persist until you clear them.

Applying filters also enables the Device Operations so that you can deploy a BOM, configurations, containers, and software to the filtered devices. You can also execute commands on the list of filtered devices.

1. To disable the global filter functionality, click the filter icon .

a. Click the toggle to the right of **Global Device Filters**.

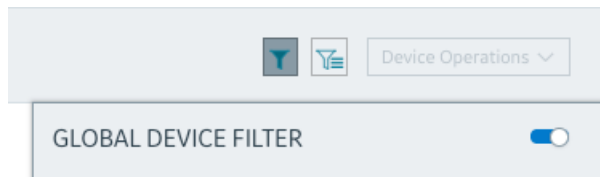



When the toggle is gray, it indicates that global filters are disabled. This means that any filter you set on this page is not propagated to the other Device Manager pages where the device list appears.

2. To enable global filters, click the filter icon .

a. Click the toggle to the right of **Global Device Filters**.

When the toggle is blue, it indicates that global filters are enabled so that the filter applied to this page is propagated to all other Device Manager pages where the device list appears.



3. By default, saved filter sets are enabled, which means you can access and apply saved filters. To disable saved filter sets, click the saved filter set icon ()

a. Click the toggle to the right of **Saved Filter Sets**.


When the toggle is gray, saved filter sets are disabled, and you are unable to select and apply any of the saved filters in the list.

Filtering Devices by Group

In Predix Edge Manager, you can filter the device list in Device Manager to view and perform actions on only devices in a specified group.

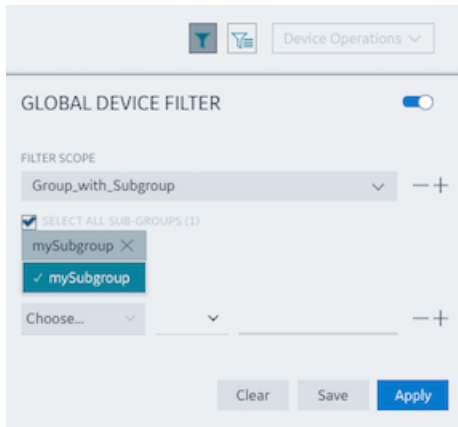
By default, the **Device Manager > Devices** page displays all devices.

1. In the left navigation pane, select  **Device Manager > Devices**.

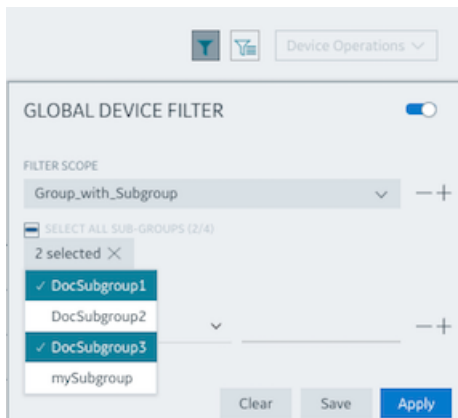
2. Click the filter icon .


3. In **Filter Scope**, select the group to view devices for.

If the group you selected has subgroups (children), The **Select All Sub-Groups** drop-down list appears. You can check the box on the left to select all sub-groups, as shown in the below image.



You can also expand the list of sub-groups, and select only specific sub-groups, as shown in the below image.



 **Note:** If the group you selected has subgroups, devices belonging to the subgroups are not added unless you select this option. If you select this option, when you deploy the BOM, it is deployed to all the subgroups and all the devices in the subgroup.

4. Click **Apply**.

The device list is updated so that only devices in the selected groups appear in the device list.

5. (Optional) Click **Save** to save the filter for future use.


- a. Enter a name for the filter.
- b. (Optional) From **Device Filters** select attributes from the list to further narrow filter results.
- c. Click **Save**.
Your filter appears in the **Saved Filter Sets** list.

Creating and Saving Filters

If you often use the same criteria for filtering the device list, you can create your own custom filters for later reuse.


1. Go to any of the following pages to create filters:
 - **Dashboard**
 - **Device Manager > Devices**
 - **Alerts**
 - **Operations**
2. Click the **Filters** icon (▼) to expand the filter fields.
By default, all device groups are in the **Filter Scope** unless a group filter is applied. To create and save filters for devices in specific groups, see [Filtering Devices by Group \(page 48\)](#).
3. From the **Device Filters** list, select the criteria for the filter, then click **Apply**.
 - Available attributes include default attributes that all devices have, and any custom device attributes you have created.
 - In the middle field, select the operator for the filter. The operator choices that you see depend on the data type of the attribute.
 - In the box on the right, select the value for the filter. For example, if you chose **Device Status** as the attribute and **equal** as the operator, you can select from:
 - **Online** – the device is online.
 - **Created** – the device has not yet connected to Edge Manager and is not enrolled.
 - **Offline** – the device has connected to Edge Manager at some point, but is now unreachable.

To add additional filters, click the + on the right side of the **Device Filters** boxes.


 **Note:** When you use multiple filters, each additional filter is treated as an **and** operation. So you are applying Filter1 **and** Filter2 **and** Filter3, and so on.

Click the minus - to the right of a filter to remove it.


4. Click **Save**.
5. Enter a name for the filter, and click **Save**.

 **Note:** Filter names must be unique and follow these rules:

- A minimum of 3 characters.
- A maximum of 63 characters.
- Must start with an alphanumeric character (0-9 or a-z).
- Remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).

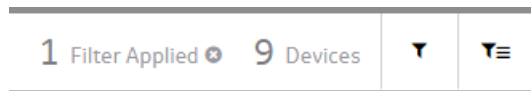
Your filter is created and now appears in the  **Saved Filter Sets** list so that you can select it in the future.

Applying Filters to the Device List

- You can apply filters to the device list from any of the following pages:
 - **Dashboard**
 - **Device Manager > Devices**
 - **Alerts**
 - **Operations**
- Click the filter icon () to expand the filters list.
- In the filter list, select the filter to apply, and click **Apply**.
The device list is updated to display only the devices that meet the applied filter criteria.

 **Note:** Filters are global so the device list displayed reflects the results of the filter you apply on all pages where the device list is displayed.

The image below shows the summary of the results of the applied filter. The number on the left of **Filter Applied** displays the number of filters that were applied, and the number on the left of **Devices** displays the number of devices that were returned based on the filter's criteria.




- Click **Filter Applied** to see a list of all the currently applied filters.
- Click the **x** to the left of **Filter Applied** to clear all filters.

Editing and Deleting Device Filters

You can edit and delete device filters in Predix Edge Manager.

You can edit and delete filters from any of the following pages:

- **Dashboard**
- **Device Manager > Devices**
- **Alerts**
- **Operations**

- In the left navigation pane, select one of the pages with filters.
- Click the saved filter sets icon () to expand the filter list.
- To edit a filter:

- a. Click the filter to edit.
 - b. Make the changes, and click **Save**.
4. To delete a filter:
 - a. In the filter list, click the filter to delete.
 - b. Click the trashcan icon to the right of the filter name.
 - c. In the **Delete Filter** confirmation dialog box, click **Confirm**.

Clearing Device Filters

Filter applied to the device list in Predix Edge Manager persist until you clear them.

When you apply filters, the number of filters applied and number of devices in the filter set displays at the top of the page to the left of the filter icons.



To clear the filter, you can either:

- Click the **x** to the left of **Filter Applied**, or
- Apply a different filter.

Related tasks

[Applying Filters to the Device List \(page 51\)](#)

Device Operations

About Device Operations


In Predix Edge Manager, device operations allow you to deploy edge apps, BOMs, configurations, and software to devices. You can also execute commands on devices.

When you have filters applied to devices, you can perform device operations from the following pages:

- **Dashboard**
- **Device Manager > Devices**
- **Alerts**
- **Operations**

Device Operations are located in the top right corner of the Predix Edge Manager screen.

The **Device Operations** drop-down list is disabled if there are no filters applied to the device list.

 **Note:** You cannot perform the same operation on the same set of filtered devices within one minute of the most recent operation. For example, you cannot deploy configurations to the same set of filtered devices within one minute of the last time you deployed configurations to that set of filtered devices.

Related concepts

[About Predix Edge Manager Commands \(page 73\)](#)

[About Device Filters \(page 46\)](#)

Related tasks

[Executing Commands \(page 79\)](#)

[Deploying a Bill of Materials to Multiple Devices \(page 65\)](#)

[Deploying Containers to Devices \(page 69\)](#)

[Deploying Configurations \(page 61\)](#)


[Applying Filters to the Device List \(page 51\)](#)

Viewing Operations History

View the deployment and commands history for devices in Predix Edge Manager.

1. In the left navigation pane of Edge Manager, click **Operations**.

The following information is displayed for deployments and commands on the **Operations** page:

Column	Description
Name	Click the link to see details about the deployment or command, such as what device it was run on, the status, and what time the deployment or command was started.
Type	Type of package deployed, for example, edge app, configuration, BOM. (Displayed on the Deployments page only.)
Pending	Displays the number of devices on which the deployment or command operation is pending.
In Progress	Displays the number of devices on which the deployment or command operation is progress.
Timeout	<p>Displays the number of devices on which the deployment or command timed out.</p> <p> Note: Timeout means one of two things.</p> <ol style="list-style-type: none"> a. The device has not reported back to Edge Manager with the final status of the command/task within the time specified when the deployment was scheduled. The command/deployment is still in progress and will retry until it succeeds or fails. b. The command/deployment did not receive a response back from the Edge device. This is the final state of the task.
Failed	Displays the number of devices on which the deployment or command execution failed.
Successful	Displays the number of devices on which the deployment or command was successful.
Cancelled	Displays the number of devices on which the deployment or command was cancelled.

Column	Description
Scheduled/ Executed on	The date and timestamp for when the deployment or command was scheduled.
Scheduled/ Executed by	The name of the user who scheduled the deployment or command.
Started	The date and timestamp for when the deployment or command started.
Ended	The date and timestamp for when the deployment or command ended.
Elapsed	Time that has elapsed from the start to the end of the deployment or command operation.

2. (Optional) If the devices on the **Operations** page are part of a filtered list, you can select **Device Operations** to perform the following actions on the device:

- Deploy edge apps, BOMs, configurations, containers, data maps, templates, and software
- Execute commands
- Set and remove alert policies

Related tasks

[Deploying Configurations \(page 61\)](#)

[Deploying a Bill of Materials to Multiple Devices \(page 65\)](#)

[Deploying Containers to Devices \(page 69\)](#)


Viewing Details for Operations


View details for device operations, including status, the time the operation was scheduled to begin, the time the operation completed and so on.

1. In the left navigation pane, click **Operations**.
2. In the **Name** column, click the operation to view its details.
The Operations details page displays deployment details for the operation.

Table 1. Deployment Details

Operation Detail	Description
Device	The device the task was run on. Click the device to view its details.

Operation Detail	Description
Status	<p>The status of the task. Statuses include the following:</p> <ul style="list-style-type: none"> • Pending – All tasks have a pending status before a task starts. • Success – The task succeeded. • In Progress – When one or more tasks begins progress, and some tasks are successful, some are pending, and no failure occurs, a number displays how many are still incomplete, for example, <code>In Progress (4)</code>. • Failed – The task failed. <p> Note: The Failed status is a clickable link, which launches a window with an error message about why the task failed, if the installation script saves messages to a status file.</p> <ul style="list-style-type: none"> • Canceled – The task was canceled. This status applies only to commands. • Unknown – The status is unknown.
Retries	Displays the number of retry attempts made for the task.
Time Acknowledged	The date and timestamp of when the operation request was acknowledged by the device.
Execution Start	The date and timestamp for when the task is execution is started.
End	The date and timestamp for when the task execution ends.
Elapsed	The time elapsed since between execution start and end.
Execution Logs	Once a task has a status of "Finished," you can click the details link to view the detailed log for the task. Until the task is finished, "Not available" is displayed.

 **Note:** This feature is not supported on some devices, in which case, "Not available" is displayed.

If the device is part of a filtered list, you can select **Device Operations** to perform the following actions on the device:

- Deploy edge apps, BOMs, configurations, containers, data maps, templates, and software
- Execute commands
- Set and remove alert policies

Related tasks

[Executing Commands \(page 79\)](#)

Operation and Task Status Messages

These tables describe the status messages you see when performing operations in Predix Edge Manager.

The following table describes the status messages you see when operations are performed.

Table 2. Operation Level

Message	Description
Pending	All tasks have a pending status before an operation starts.
In Progress	When one or more tasks begins progress, and some tasks are successful, some are pending, and no failure occurs, a number displays how many are still incomplete, for example: <code>In Progress (4)</code> .
Successful	When all tasks under an operation are successful.
Failed	When any one task in an operation fails, a number displays how many tasks have failed, for example: <code>Failed (2)</code> .
Unknown	All of the tasks in an operation are unknown.

The following table describes the status messages you see when tasks are performed.

Table 3. Task Level

Message	Description
Pending	The task has not started.
In Progress	The task is in progress.
Timeout	The task timed out prior to completion.
Success	The task completed successfully.
Cancelled	The task was cancelled.
Failed	The task failed to complete.
Unknown	A task can "lose" its status if the back-end service goes down while something is in progress. The task may or may not recover its status. For example, if the task was in progress, it may eventually finish, which will fix it. This status is rare.


Device Models

Adding Custom Device Models

You can create a device model that includes custom attributes you specify, such as OS, processor, memory, custom icon and photo.

1. In the left navigation pane, select **Device Manager > Models**.
The Models page displays a list of existing device models and attributes. Select the device model to see its attributes and, if applicable, its associated BOM.
2. Select **Action > Add**.
3. In the **Add Device Model** dialog, enter the information for your custom device model, then click **Next**.

- **ID** – Enter the device ID.

 **Note:** The device ID must follow these conventions:

- Must be a minimum of 3 characters.
- Must not exceed 63 characters.
- Must start with an alphanumeric character (0-9 or a-z).
- The remaining characters can be any combination of alphanumeric, underscore (_), or hyphen (-).
- Do not use colons (:).
- The Device ID is case-insensitive, but is always stored as lower-case. If you enter upper-case characters in Predix Edge Manager, they are converted to lower-case.

- **Attributes**

- **Description** – Enter a description for your custom device model.
- **OS** – Enter the operating system for the device.
- **Processor** – Enter the processor for the device.
- **Core Number** – Enter the core number for the processor.
- **Memory GB** – Enter the memory size in gigabytes.
- **Storage GB** – Enter the storage size in gigabytes.


- **Manufacturer Installed BOM** – If applicable, select the manufacturer installed BOM.

A manufacturer BOM lists packages installed before the device is shipped to the user (the packages are not installed through Edge Manager).

- **Default Device Model BOM**


- a. Click **Choose BOM**.
- b. Select a BOM from the list, and click **Confirm**.

Optionally, click **Choose File** to add an icon and/or image to represent the device in the device summary. If you do not add your own image, the default image and icon are used.

 **Note:** Icons must be PNG files. Device model images must be JPEG files, and less than 2 MB in size.

4. (Optional) In Custom Attributes, enter a key-value pair for any additional attributes to add to the device, and click **Next**.
You can add additional attributes by clicking (+), or remove attributes by clicking (x).
5. (Optional) Select a BOM from the list to associate a default BOM with the device model, and click **Add**.

When you assign a default BOM to a device model, when you add devices with this model in the future, the same default BOM is automatically assigned to the device, and will be deployed to the device when the it comes online.

 **Note:** If you change the model for an existing device, it does not affect the BOM associated with that device.

You are returned to the Models page, where your new device model appears in the Model list.


Editing and Deleting Custom Device Models

You can edit and delete device models you created.

1. In the left navigation pane, select **Device Manager > Models**.
2. To edit a device model, from the Model list, select the device model to edit, then click **Edit**.
 - a. In the Edit Device Model dialog box, make the desired changes, then click **Next**.
 - b. In the Custom Attributes dialog, make your updates, then click **Update**.

You can edit any existing attribute by editing its associated fields. You can also add (+) or remove (x) custom attributes.
3. To delete a device model, from the Model list, select the device model to delete, then click **Delete**.

You can select multiple device models for deletion.

 **Note:** You cannot delete a device model that is linked to registered devices.

- a. Click **Confirm** in the confirmation dialog box.

Chapter 5. Deployment and Analytics

Package Deployment

About Deployment

You can use Predix Edge Manager to deploy the different types of packages to multiple devices (a fleet) at once, or to single devices.

Bill of Materials (BOM)

A BOM is a comprehensive list of all the packages or applications, and their related dependencies, installed on a device. The BOM lists the software packages with their version numbers in the order they should be installed on the device.

Configurations

Configuration files contain the settings specific to an application.

Edge Apps

Edge apps are composed of multiple containers, which provides a more modular, lightweight, and secure way of managing applications. You can package multiple services in one application (for example, an OPC-UA adapter and the Time Series Gateway service) and each service can be packaged with the operating environment and tools it specifically needs to run.

Containers

Containers are stand-alone executable packages of software. Currently, Docker and Predix Machine containers are supported. Containers, in the context of Predix Edge Manager, apply only to Docker containers that run on Predix Machine.

Software

Software, in the Predix Edge Manager context, refers to any type of software that is not an edge (multi-container) app, for example, operating system, Predix Machine bundles, or external software.


Deploying Edge Apps

In Predix Edge Manager, you can deploy edge apps to multiple devices at once, or to single devices.




1. In the left navigation pane, select **Device Manager > Devices**.
2. To deploy edge apps to a single device, follow these steps.
 - a. Click the link for the device to which to deploy the edge app.
 - b. Click the **Edge Apps** tab.
 The **Edge Apps** tab only displays if the selected device is running Predix Edge.
 If there are applications already deployed to the selected device, they are displayed in the **Applications** list, where you can also start, stop, or delete applications on the device.
 - c. Click **Deploy Edge Apps**.
3. To deploy edge apps to multiple devices, create and apply filters to the device list, or select multiple devices, then select **Device Operations > Deploy Edge App**
4. In the **Select Edge Applications** dialog, select the applications to deploy and click **Next**.
5. In the **Add Edge Applications Identifiers**, add the unique application identifiers for the app, then click **Next**.
 If you are deploying multiple instances of the same edge app on a single device, each edge app instance must have a unique Application ID. When you deploy configurations, you must know the App ID for the instance of the edge app to which to apply the configuration.

 Application IDs must follow these rules:
 - Must begin with an alpha-numeric character.
 - Must be 50 characters or less.
 - Can consist of alpha-numeric characters, hyphens and underscores.
 The **Schedule Deployment** dialog box appears.
6. In the **Schedule Deployment** dialog, select the date and time for deployment to the device.

 **Note:** You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

 - a. In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

 **Note:** When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.
 - b. (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).

- c. Click **Next**.
- d. In the **Edge Applications Confirmation** dialog box, click **Submit**.
- e. In the **Deployment Status** dialog box, click **Close**.


Deploying Configurations

Use the **Device Manager** page to deploy configurations and apply them to deployed applications.


The software and configurations must be uploaded to the Predix Edge Manager Repository.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. To deploy configurations to multiple devices, [Create and apply filters \(page 51\)](#), or select devices by clicking the box on the left of the device.
 - a. Once the devices are selected, select **Device Operations > Deploy Configuration**, then go to Step 4.
3. To deploy configurations to a single device, click the device in the device list, then click the **Configurations** tab.

The **Deployment Schedule** section displays information about software and configuration packages deployed to the device, including:

- **Name** – The name of the software or configuration package.
 - **Version** – The version of the software or configuration package.
 - **Revision** – This field displays only for configurations.
 - **Status** – The status of the deployment. Statuses include:
 - **In Progress** – When one or more tasks begins progress, and some tasks are successful, some are pending, and no failure occurs, a number displays how many are still incomplete, for example, **In Progress (4)**.
 - **Pending** – All tasks have a pending status before an operation starts.
 - **Success** – The deployment succeeded.
 - **Failed** – The deployment failed.
-  **Note:** If the installation script for the package saves messages to a status file, the **Failed** status is a clickable link, which launches a window with an error message about why the installation failed.
- **Canceled** – The deployment was canceled.
 - **Unknown** – The status is unknown.
 - **Retries** – The number of times the task has been retried.
 - **Scheduled On** – The date and timestamp for when the deployment is scheduled.
 - **Scheduled By** – The name of the user who scheduled the deployment.


- **Start** – The date and timestamp for when the deployment starts (the package begins downloading to the device).
- **Execution Start** – The date and timestamp for when the installation of the package starts on the device.
- **End** – The date and timestamp for when the installation is complete.
- **Description** – The description for the package.
- **Execution Logs** – Once the installation has a status of "Finished," you can click the **details** link to view the detailed log for the installation. Until the installation is complete, "Not available" is displayed.

 **Note:** This feature is not supported on some devices, in which case, "Not available" is displayed.


- Click **Deploy Configurations**, then go to Step 4.
- In the drop-down list at the top right of the configurations list, select:
 - **Predix Machine** – Select if you are deploying configurations to apply to applications that are deployed to devices running Predix Machine.
 - **Predix Edge** – Select if you are deploying configurations to apply to applications that are deployed to devices running Predix Edge OS.

Click on a configuration name to display the files included in the configuration package. Click **Back** to go back to the configurations list.

- If you selected **Predix Edge** in the previous step, click **Next** to specify the application ID to which you are applying the configuration, then click **Next**.
- If you are deploying to Predix Edge, click **Next** again to schedule the deployment, otherwise, click **Schedule**.
- In the **Schedule Deployment** dialog, select the date and time for deployment to the device.

 **Note:** You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

- In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

 **Note:** When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.

- (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).
- Click **Submit**.

The **Deployment Status** dialog appears.

8. In the **Deployment Status** dialog box, click **Close**.

The configuration is deployed and applied to the application.

Related tasks

[Deploying Software \(page 63\)](#)


[Filtering Devices by Group \(page 48\)](#)

Deploying Software

In Predix Edge Manager, you can deploy software packages to multiple devices at once, or to single devices.


You can also use the device **Software** page to view software packages installed on the device, as well as the software deployment history for the device.

1. To deploy a software package to a single device, follow these steps.

- a. In the left navigation pane, select  **Device Manager > Devices**.
The **Device Manager** page appears, with the list of devices.
- b. In the device list, click the device to which to deploy the software package.
- c. Click the **Software** tab.


The **Deployment Schedule** section displays information about software and configuration packages deployed to the device, including:

- **Name** – The name of the software or configuration package.
- **Version** – The version of the software or configuration package.
- **Revision** – This field displays only for configurations.
- **Status** – The status of the deployment. Statuses include:
 - **In Progress** – When one or more tasks begins progress, and some tasks are successful, some are pending, and no failure occurs, a number displays how many are still incomplete, for example, **In Progress (4)**.
 - **Pending** – All tasks have a pending status before an operation starts.
 - **Success** – The deployment succeeded.
 - **Failed** – The deployment failed.

 **Note:** If the installation script for the package saves messages to a status file, the **Failed** status is a clickable link, which launches a window with an error message about why the installation failed.

- **Canceled** – The deployment was canceled.
- **Unknown** – The status is unknown.
- **Retries** – The number of times the task has been retried.


- **Scheduled On** – The date and timestamp for when the deployment is scheduled.
- **Scheduled By** – The name of the user who scheduled the deployment.
- **Start** – The date and timestamp for when the deployment starts (the package begins downloading to the device).
- **Execution Start** – The date and timestamp for when the installation of the package starts on the device.
- **End** – The date and timestamp for when the installation is complete.
- **Description** – The description for the package.
- **Execution Logs** – Once the installation has a status of "Finished," you can click the **details** link to view the detailed log for the installation. Until the installation is complete, "Not available" is displayed.

 **Note:** This feature is not supported on some devices, in which case, "Not available" is displayed.

If the selected device is running on the Predix Machine platform, the **Non Predix Machine** section displays a list of non Predix Machine software installed on the device and information about the software such as vendor, type of software, version, status (for example, active or inactive), the time the software was installed, and a description.

d. Click **Deploy Software**.


e. In the **Select Software** dialog box, select the boxes to the left of the software package (application, container, operating system, virtual machine) to deploy, and click **Schedule**.

 **Note:** If you schedule a deployment to a device with the status of "created" or "offline," the status displays "Pending" until the device comes online, at which time the deployment begins automatically and the status changes to "In progress."


2. To deploy software to multiple devices follow these steps.

- [Create and apply filters \(page 51\)](#), or select devices from the device list.
- Select **Device Operations > Deploy Software**, and in the Select Software dialog, select the software package to deploy.
- In the **Select Software** list, select the software to deploy to the devices, and click **Schedule**.

3. In the **Schedule Deployment** dialog, select the date and time for deployment to the device.

 **Note:** You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

- In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

 **Note:** When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.

- b. (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).
- c. Click **Submit**.

The **Deployment Status** dialog appears.

4. In the **Deployment Status** dialog box, click **Close**.

The software package is deployed, downloaded to the device, and saved in the Repository on the date and time you specified.

Related tasks

[Deploying Configurations \(page 61\)](#)

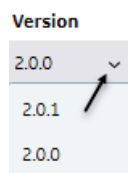
Deploying a Bill of Materials to Multiple Devices

Use Predix Edge Manager to deploy a BOM to a filtered set of devices.

A BOM is a comprehensive list of all the packages or applications, and their related dependencies, installed on a device.


1. Go to any of the following pages to [Create and apply filters \(page 51\)](#):
 - **Dashboard**
 - **Device Manager > Devices**
 - **Alerts**
 - **Operations**
2. In the **Select BOM** dialog box, select the BOM to deploy and click **Schedule**.

If there are multiple versions of the BOM file, you can click in the version column to select the version of the BOM to deploy.




When a BOM is updated and redeployed, packages specified in the BOM that are already installed on the device are skipped (not downloaded and deployed again). Only new packages


are deployed to the device. The status of skipped packages is displayed as "installed" rather than "success."

 **Note:** If you schedule a deployment to a device with the status of "created" or "offline," the status displays "Pending" until the device comes online, at which time the deployment begins automatically and the status changes to "In progress."

3. In the **Schedule Software Deployment** dialog, select the date and time for deployment to the device.

 **Note:** You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

- a. In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

 **Note:** When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.

- b. (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).
- c. (Optional) Select the **Force BOM installation** box if there is already a package with the same name and version installed on the device and you want to overwrite it.
- d. Click **Submit**.

The **Deployment Status** dialog appears.

4. Click **Close** in the confirmation dialog box.


The BOM deployment appears in **Operations > Deployment History**.

Related tasks

[Viewing Details for Operations \(page 54\)](#)

Deploying a Bill of Materials to a Single Device

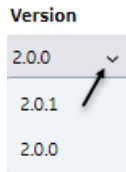
Use the **Device Manager** page to deploy a BOM to a single device.

1. In the left navigation pane, select  **Device Manager > Devices**.
2. Click the link for the device to which to deploy the BOM.
3. Click the **BOM** tab.

4. Select **Deploy BOM**.

5. In the **Select BOM** dialog box, select the BOM to deploy, and click **Schedule**.

If there are multiple versions of the BOM file, you can click in the version column to select the version of the BOM to deploy.



When a BOM is updated and redeployed, packages specified in the BOM that are already installed on the device are skipped (not downloaded and deployed again). Only new packages are deployed to the device. The status of skipped packages is displayed as "installed" rather than "success."

Note: If you schedule a deployment to a device with the status of "created" or "offline," the status displays "Pending" until the device comes online, at which time the deployment begins automatically and the status changes to "In progress."

6. In the **Schedule Software Deployment** dialog, select the date and time for deployment to the device.

Note: You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

- a. In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

Note: When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.

- b. (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).
- c. (Optional) Select the **Force BOM installation** box if there is already a package with the same name and version installed on the device and you want to overwrite it.
- d. Click **Submit**.

The **Deployment Status** dialog appears.

7. In the Deployment Status dialog box, click **Close**.

The BOM deployment appears in the Last Created Operation section.


Deploying Analytics Templates and Data Maps

Use Predix Edge Manager to deploy analytics templates and data maps to devices.


Before you can deploy data maps and analytics templates, you must first upload the following types of packages to the Predix Edge Manager repository.



1. In the left navigation pane, select **Device Manager > Devices**.
2. Select the devices to which to deploy the analytics template or data map.
3. To deploy a data map, follow these steps:
 - a. Select **Device Operations > Deploy Data Map**.
 - b. In **Select Analytic Data Map**, select the data map to deploy, then click **Schedule**.
4. To deploy the analytics template, follow these steps.
 - a. Select **Device Operations > Deploy Template**.
 - b. In the **Select Analytic Template** dialog box, select the templates to deploy, then click **Schedule**.
5. In the **Schedule Software Deployment** dialog, select the date and time for deployment to the device.

 **Note:** You can set the time zone timestamp formatting (UTC or local) in the **Settings** page.

- a. In **Timeout**, set the timeout for each operation in weeks, days, hours, minutes, or seconds, per device.

 **Note:** When the operation is not scheduled, the timeout starts from the moment you create the task. When the operation is scheduled, the timeout is the scheduled time plus the timeout time you set.

- b. (Optional) In the **Retries** field, enter a number for how many times to retry the deployment in case of failure (including if the deployment times out).
- c. (Optional) Select the **Force BOM installation** box if there is already a package with the same name and version installed on the device and you want to overwrite it.
- d. Click **Submit**.

The **Deployment Status** dialog appears.

6. In the Deployment Status dialog box, click **Close**.

Related tasks

[Uploading Software and Configuration Packages to the Predix Edge Manager Repository \(page 95\)](#)

Related reference

[Package Guidelines and Size Limits \(page 97\)](#)

Deploying Containers to Devices

Use Predix Edge Manager to deploy containerized applications to a filtered list of devices.

1. [Create and apply filters \(page 51\)](#).



2. In the left navigation pane, select **Device Manager > Devices**.

3. Select the devices to deploy the container to.

You can select devices by checking the box to the left of the device, or to deploy a container to devices in specific groups, you can apply a group filter. See [Filtering Devices by Group \(page 48\)](#).

4. In the upper-right corner of the screen, select **Device Operations > Deploy Container**.

5. In the **Select Container** dialog box, select the containers to deploy, and click **Schedule**.

6. In the **Schedule Deployment** dialog box, select the date and time to deploy the container, and click **Schedule**.

The **Deployment** status confirmation dialog, shows the status of the deployment.

7. Click **Close**.


Redeploy Failed Packages

The deployment of packages (applications, software, configurations, etc.) may sometimes be unsuccessful. Use the following procedure to redeploy failed packages.

1. Log into Predix Edge Manager.
2. On the **Operations** page select the **Deployments** tab.
3. Select the **Name** of the failed deployment operation (as indicated in the **Failed** column).
4. Use the **Filter** to select tasks with a status of **Failed**.
5. Use the checkboxes to select the failed task(s).
6. Select **Retry Deployment**. In the confirmation window that appears, select **Confirm**.

7. In the **Select...** window that appears, select the item(s) to redeploy. Select **Next**.

At this point, follow the specific deployment procedure for the type of item(s) selected as outlined in [Package Deployment \(page 59\)](#).

 **Note:** If attempts to redeploy a package repeatedly fail, you can [file a support ticket \(page 121\)](#).

Analytics

Predix Edge Analytics enable you to upload the analytics runtime engine, template, and data map and deploy these to Predix Edge devices.

Analytic Engine

To successfully run analytics on the edge device, a supported analytic engine must be deployed to the device. (See [Deploying Edge Apps \(page 59\)](#) for instructions.) Predix Edge currently supports two analytic engines – Csense and Foghorn.

- Upload an Analytic Engine:
 - Csense and Foghorn engines are regular Predix Edge Apps that can be uploaded to the Edge Manager repository as a Predix Edge platform application.
- Deploy an Analytic Engine:
 - Deploy the uploaded engine to a device or set of devices as you would for any other Predix Edge application.

Once the analytic engine is successfully deployed to a device, the **Analytics** tab should appear on the **Device** page. At this point, analytic templates and data maps can be deployed to that device.

Analytic Templates and Data Maps

Once a device has an analytic engine successfully running, analytic templates and data maps can be deployed. Templates must be uploaded and deployed before data maps, which rely on the templates.

- **Upload**
 - Analytic Template:
 1. Go to the **Repository** page.
 2. Click the **Action** drop-down menu.
 3. Select **Upload**.
 4. Enter a **Name** and **Version** for the analytic template package.
 5. Select **Type** > **Analytics Template**.
 6. Select **Platform** > **Predix Edge**.
 7. **Capabilities** is a field that did not previously exist for Predix Machine. It defines any capabilities the package depends upon to run. In this case, analytic

templates will run successfully only if there is an analytic engine on the device. The analytic engines listed above that are supported by Predix Edge will provide one of two capabilities (`Predix.Edge.AnalyticEngine.CSense` or `Predix.Edge.AnalyticEngine.Foghorn`). Add the corresponding capability in the **Capabilities** field when uploading the analytic template. A single template should be able to run on only one of the engines (i.e., a Foghorn template cannot run on the CSense engine and vice versa).


8. Select the **File**, which is the analytic template to upload.
 9. If the analytic engine requires a handler, enter it in **Package Handler**.
 10. Click **Upload**.
- Analytic Data Map:
 1. Go to the **Repository** page.
 2. Click the **Action** drop-down menu.
 3. Select **Upload**.
 4. Enter a **Name** and **Version** for the analytic data map package.
 5. Select **Type > Analytics Data Map**.
 6. Select **Platform > Predix Edge**.
 7. Select the **Target Template** to which the data map should be tied.
 8. The **Capabilities** and **Package Handler** fields are identical to the capabilities and handler that were specified when uploading the analytic template, and therefore appear as read-only fields when uploading the analytic data map.
 9. Select the **File**, which is the analytic data map to upload.
 10. Click **Upload**.
 - **Deploy to Multiple Devices**
 - Analytic Template:
 1. Go to the **Device Manager** page.
 2. Click the **Device Operations** drop-down menu.
 3. Select **Deploy Template**.
 4. Select **Predix Edge** as the platform type on the top right.
 5. Select the appropriate analytic template and version.
 6. Click **Schedule**.
 7. Enter the **Date and Time** for deployment, the desired **Timeout** period and select the **Application ID** of the analytic engine to which the template should be deployed.
 8. Click **Submit**.
 - Analytic Data Map:
 1. Go to the **Device Manager** page.
 2. Click the **Device Operations** drop-down menu.
 3. Select **Deploy Data Map**.
 4. Select **Predix Edge** as the platform type on the top right.
 5. Select the appropriate analytic data map and version.
 6. Click **Schedule**.
 7. Enter the **Date and Time** for deployment, the desired **Timeout** period and select the **Application ID** of the analytic engine to which the data map should be deployed.
 8. Click **Submit**.
 - **Deploy to a Single Device**
 - Analytic Template

1. Go to **Device Manager > Devices**.
2. Select the device to which the template should be deployed.
3. On the device details page, select **Analytics**. If the **Analytics** tab does not appear, you must deploy the analytics engine for the device and ensure it is running.
4. Click the **Deploy Analytics** drop-down menu.
5. Select **Deploy Template**.
6. Select the appropriate analytic template and version.
7. Click **Schedule**.
8. Enter the **Date and Time** for deployment, the desired **Timeout** period and select the **Application ID** of the analytic engine to which the template should be deployed.
9. Click **Submit**.
- Analytic Data Map
 1. Go to **Device Manager > Devices**.
 2. Select the device to which the data map should be deployed.
 3. On the device details page, select **Analytics**. If the **Analytics** tab does not appear, you must deploy the analytics engine for the device and ensure it is running.
 4. Click the **Deploy Analytics** drop-down menu.
 5. Select **Deploy Data Map**.
 6. Select the appropriate analytic data map and version.
 7. Click **Schedule**.
 8. Enter the **Date and Time** for deployment, the desired **Timeout** period and select the **Application ID** of the analytic engine to which the data map should be deployed.
 9. Click **Submit**.

Analytic Template Status

This feature allows you to see analytic template details and control the templates.

1. Go to **Device Manager > Devices**.
2. Select the device.
3. Select **Analytics**. This will display a list of the analytic engines deployed to the device.

 **Note:** If an analytic engine is running, but no analytic templates have been deployed, no information will be displayed on the Analytics tab.

4. Click an engine to list its deployed analytic templates.
5. For each template you will see:
 - **Template Name:** the name specified when the template was uploaded.
 - **Version:** the version specified when the template was uploaded.
 - **Status:** will indicate if the template is **Running** or **Stopped**.
 - **Description:** if a description of the template was specified when it was uploaded, it will appear here.
 - **Data Map:** the data map deployed with the template on the device.
 - **Action:** here you can **Start** the template; **Stop** the template; or **Delete** the template (using the trash can icon).

Chapter 6. Predix Edge Manager Commands

About Predix Edge Manager Commands

Use the **Commands** page to:

- View all system-defined and custom commands.
- View the details of each command.
- Add and delete custom commands.

On the **Commands** page, you can choose to view commands in list view or tile view by clicking the corresponding icons in the top right of the page.






The following table describes the system defined commands for Predix Edge Manager, the applicable platform, and the associated handler. The "Created On" and "Created By" columns display additional information about custom commands, including the user who added the custom command and the timestamp and date of when the command was added.


System-defined Default Commands for Predix Machine

Table 4.

System Commands	Description	Handler	Has Output?
Delete Application Container	Deletes a container from the device. You must know the container ID to execute this command.	ContainerManager	No
Get Application Containers	Returns a list of available Docker containers, with basic information about each.	ContainerManager	Yes
Get Available Logs	Returns a list of available logs on the device.	Machine	Yes
Get IP Address	Posts the network interface information with all available device IP addresses to the provided URL endpoint.	Machine	Yes
Get Log	Retrieves the Predix Machine log from the device.	Machine	Yes

System Commands	Description	Handler	Has Output?
HTTP Tunnel: Disable	Disables the HTTP tunnel to prevent data transfer from the device to the cloud.	Machine	No
HTTP Tunnel: Enable	Enables data transfer from the device to the cloud.	Machine	No
Install Debian Package	<p>Installs a list of Debian packages and their dependencies from configured apt repositories.</p> <p> Note: Only for Linux devices that support apt-get.</p>	debianPackages	Yes
List Installed Packages	<p>Returns a list of all packages installed on the device.</p> <p> Note: Only for Linux devices that support dpkg.</p>	Machine	Yes
Predix Connectivity: SetVPN Log Verbosity	Set the log verbosity for the VPN connection.	Machine	No
Predix Connectivity: StartVPN Management	Start managing VPN on the device.	Machine	No
Predix Connectivity: Stop VPN Management	Stop managing VPN on the device.	Machine	No
Refresh	Restarts the Predix Machine OSGi container process. This command is not permitted if the watchdog is not running.	Machine	No

System Commands	Description	Handler	Has Output?
Refresh Device Detail	<p>Sends all device detail information in the next sync. This command overrides the Cloud Gateway's polling interval and schedules a sync immediately.</p> <p>This command also overrides the sync intervals of the following device detail categories. Information about the following, together with all other device detail information, if available, will be included in the next sync.</p> <ul style="list-style-type: none"> • <code>com.ge.dspmicro.cloud.gateway.machineInfoUploadInterval</code> • <code>com.ge.dspmicro.cloud.gateway.deviceStatusUploadInterval</code> • <code>com.ge.dspmicro.cloud.gateway.dockerInfoUploadInterval</code> 	Machine	No
Restart	Restarts the Predix Machine OSGi container.	Machine	No
Restart all Application Containers	Restarts a list of application containers.	Machine	No
Restart Application Container	Restarts an application container running on the device.	Machine	No
Run ifconfig Command	<p>Runs the system command <code>ifconfig</code> on the device and returns the command output.</p> <p> Note: This is only for devices that support <code>ifconfig</code>.</p>	Machine	Yes

System Commands	Description	Handler	Has Output?
Run journalctl Command	<p>Queries the default system journal on the device using system command journalctl according to the filtering and formatting values specified in the command parameters.</p> <p>All command parameters are optional. However, journals usually contain a lot of entries, therefore, it is best practice to use the filtering parameters to reduce the size of output that will be sent to the cloud.</p> <p> Note: Only for Linux devices that support journalctl.</p>	Machine	Yes
Run top Command	<p>Runs the system command top on the device for one iteration.</p> <p> Note: This applies only to devices that support the top command.</p>	Machine	Yes
Set Polling Interval	Sets the polling interval for synchronizing the device data with the database.	Machine	No
Start Application Container	Starts a running container on the device. You must specify the container ID to execute this command.	Machine	No
Stop Application Container	Stops a running container on the device. You must specify the container ID to execute this command.	ContainerManager	No
Upload Configurations	<p>Uploads the configuration files specified in the current Command Handler configuration.</p> <p> Note: To run this command, you must first deploy configurations to the device. See Uploading Software and Configuration Packages to the Predix Edge Manager Repository (page 95).</p>	Machine	No

System Commands	Description	Handler	Has Output?
Technician Console: Disable	Disables the Predix Machine Technician Console on the device.	Machine	No
Technician Console: Enable	Enables the Predix Machine Technician Console on the device.	Machine	No

System-defined Default Commands for Predix Edge

Table 5.

System Commands	Description	Handler	Has Output?
Allow Third-Party Applications	Allows for the deployment of third party applications. This may result in reduced security for an edge device.	ApplicationManager	No
Reboot Device	Reboots the device.	Edge	No
Get Journal Log	Runs the system command "\journalctl\" on the device for the given parameters and returns the output.	JournalLogs	Yes
Start Edge Application	Starts an Edge Application with the specified Application ID.	ApplicationManager	No
Stop Edge Application	Stops an Edge Application with the specified Application ID.	ApplicationManager	No
Delete Edge Application	Deletes an Edge Application with the specified Application ID.	ApplicationManager	No
Set Polling Interval	Sets the duration of the polling interval, which is used to schedule communications from the device to the cloud.	Edge	No
Run ifconfig	Runs the system command "\ifconfig\" on the device and returns the output.	Networking	Yes
Run top	Runs the system command "\top\" on the device for one iteration and returns the output.	Troubleshooting	Yes
Start Analytics Template	Starts the specified analytics template on the device.	Analytics	No

System Commands	Description	Handler	Has Output?
Stop Analytics Template	Stops the specified analytics template on the device.	Analytics	No
Delete Analytics Template	Removes the specified analytics template and associated data map on the device.	Analytics	No
Get Edge Log	Retrieves the contents of the given log file name and returns the output	Edgelog	Yes
List Edge Log	Returns a list of Edge log files	Edgelog	Yes

 **Note:** System-defined default commands cannot be edited or deleted.

Related reference

Commands and Command Formats ([page](#))

About Custom Commands

Application custom commands allow application developers to expose functionality that can be interacted with via Predix Edge from within their applications. As developers create complex applications, they need to be able to expose their capabilities, send status information, deploy content, and issue commands into their applications from both Predix Edge Manager and Predix Edge Technician Console (PETC).

For Example, the analytics framework that leverages all the underlying infrastructure of application custom commands to expose that it supports the AnalyticEngine capability can deploy analytic templates or data maps, send status to Edge Manager, and issue commands such as Delete, Stop, and Start of a specific analytic into the application.

Adding a Custom Command

You can add custom commands to manage devices.

Before you can execute any commands, you need to set up the Command Framework service and configure the Machine Command Handler so that Edge Manager can communicate with Predix Machine. See Command Framework Overview ([page](#)).

1. In the left navigation pane, click **Commands**.

2. Click **Select Action > Add**.
3. In the **Add Custom Command** dialog box, enter the information for the new command, then click **Add**.
 - **Command Display Name** – Enter the name displayed to the user.
 - **Command** – Enter the command in the following format: `"command" : <command>`
 - **Handler** – Enter the name of the package handler.
 - **Has Output** – Select the check box if the command will produce output.
 - **Description** – Enter a short description of the command.
 - **Platform** – Select the platform (Predix Machine or Predix Edge) on which the command will run.
 - **Parameters Name** – Enter the display name for the parameter, such as UNIT.
 - **Key** – Enter the parameter that corresponds to the parameter name, for example, `unit`.
 - **Value** – Enter the value that corresponds to the key.
 - **Editable** – Select the check box to enable editing of command parameters.

Related tasks

Creating a Command Handler (*page*)
 Configuring Package Handler (*page*)

Deleting Custom Commands

You can delete custom commands, but you cannot delete system-defined commands.

1. In the left navigation pane, select **Commands**.
2. In the **Commands List**, select the commands to delete.
3. Click **Select Action > Delete**.
4. In the confirmation dialog box, click **Confirm**.
 The Delete Status dialog box confirms your action, and you no longer see the command in the Commands List.
5. In the Delete Status dialog box, click **Close**.


Executing Commands

Once you have applied filters, you can execute commands from any of these pages:


- **Dashboard**
- **Device Manager > Devices**


- Alerts
- Operations

You can also execute commands on a single device using the **Commands** tab in the device details page.

 **Note:** Before you can execute commands on devices running Predix Machine, you must set up the Command Framework service and configure the Machine Command Handler so Predix Edge Manager can communicate with Predix Machine. See [Command Framework Overview \(page 51\)](#).

1. [Create and apply filters \(page 51\)](#), or select devices in the **Device Manager** page.
2. In the upper-right corner of the screen, select **Device Operations > Execute Command**.
3. In the **Execute Command** window, select the platform from the drop-down list, then select the command tile for the command to execute and click **Next**.
Click the three dots in the upper right of the command tile to see information about the command.

 **Note:** You cannot execute commands to the same set of filtered devices within one minute of the most recent command execution.

 **Note:** You cannot execute commands on devices with a status of "Created."

4. In the **Execute Command** dialog box, enter a value for **Timeout** and select the unit of time (minutes, hours, or days).
5. (Optional) If the command contains parameters, enter values for the parameters.
Entering a parameter value is optional. Parameters are associated with the command, so different parameters apply to different commands, and these fields will vary.
6. Click **Execute**.
7. In the confirmation dialog box, click **Close**.

Related tasks

[Filtering Devices by Group \(page 48\)](#)

Executing or Canceling Commands for a Single Device

You can use the **Commands** tab on the device details page to execute commands on a single device.

To execute commands on multiple devices, see [Executing Commands \(page 79\)](#).



1. In the left navigation pane, select **Device Manager > Devices**.
2. From the device list, click the device to run commands for, and click the **Commands** tab.
The Commands page shows the command history for the device (if applicable).
3. To execute the command, click **Execute Command**.
4. In the **Execute Command** window, select the platform from the drop-down list, then select the command tile for the command to execute and click **Next**.

 **Note:** You cannot execute commands on devices with a status of "Created."

5. In the **Execute Command** dialog box, enter a value for **Timeout** and select the unit of time (minutes, hours, or days).
6. (Optional) If the command contains parameters, enter values for the parameters.
Entering a parameter value is optional. Parameters are associated with the command, so different parameters apply to different commands, and these fields will vary.
7. Click **Execute**.
8. In the confirmation dialog box, click **Close**.
9. To cancel pending commands, select the commands to cancel, and click **Cancel Pending Commands**.


Viewing Command History and Canceling Pending Commands for a Single Device

Use the selected device's **Commands** tab to view its command history. You can also cancel pending commands and download output from the device.


1. In the left navigation pane, select **Device Manager**.
2. From the device list, click a device link to view its command history.
3. Click the **Commands** tab.
If commands have been sent to the device, the **Commands History** list shows commands issued to the device, including the command status, start time, end time, and result.
 - Name – Displays the commands issued to the device.
 - Status – Displays the status for the issued command.

Status messages include:

- Pending – All commands have a pending status before a command begins executing.
- Success – The command succeeded.
- In Progress – When one or more commands begins progress, and some commands are successful, some are pending, and no failure occurs, a number displays how many are still incomplete, for example, `In Progress (4)`.
- Failed – The command failed.

 **Note:** If the installation script for the package saves messages to a status file, the **Failed** status is a clickable link, which launches a window with a message about why the command failed,

- Canceled – The command was canceled.
- Unknown – The status is unknown.
- Start/End – Displays the start and end timestamps for the executed commands.
- Execution Logs – Once the command has a status of "Finished," you can click the **details** link to view the detailed log for the command execution.

 **Note:** This feature is not supported on some devices, in which case, "Not available" is displayed.

Until the command is complete, "Not available" is displayed.

- Output – If the command you issued (for example, `Get Log`) supports file output, you can click the **Download** link to download the output file for the command.

4. (Optional) In **Commands History**, click **Cancel Pending Commands** to cancel all pending commands for the device.

Chapter 7. Settings and Alerts

Monitor Devices

About Alerts

Alerts allow you to monitor managed devices, VPN connections, and SIMs by providing information such as current status (online, offline, created, and so on).

In Predix Edge Manager, you can create custom alert policies and view and filter alerts.

Related concepts

Device Detail Service (page)

Related reference

Edge Alerts JSON Requirements (page)

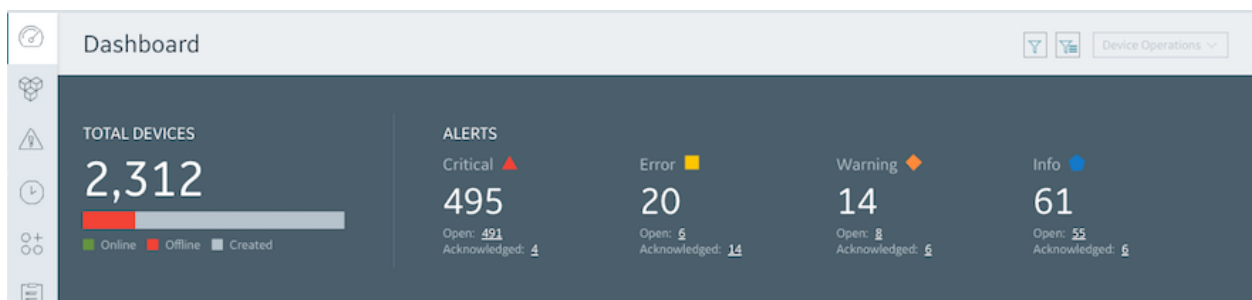
Viewing and Filtering Alerts

View and filter alerts for managed devices in Predix Edge Manager.

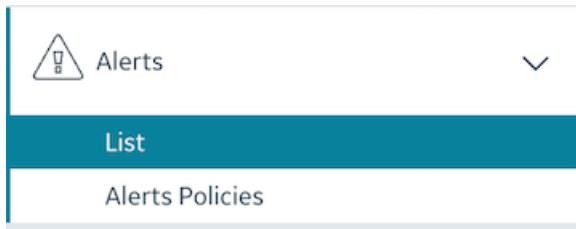
When you initially sign into Predix Edge Manager, you see the Alerts dashboard at the top of the page, which gives you a quick summary view of current alerts, along with how many devices are currently online, offline, or in the created state.

The numbers in the alerts section relate to the number of current alerts with the relevant severity (critical, error, warning, and info) and statuses (open and acknowledged).

Clicking links in the **Alerts** section takes you to the Alerts page with a list of alerts filtered by severity and disposition. Clicking on the **Online**, **Offline**, and **created** links in the total devices section takes you to the devices page with the associated status filter.



1. For the detailed list view for all current alerts, click **Alerts > List** in the left navigation pane to view the Alerts page.



The Alerts page displays information about alerts for enrolled devices. The table shows the latest alerts for each source and the alert type, so for each source and alert type only one alert is displayed. Alert information is displayed in sortable columns, and includes the following:

- Severity – the severity of the alert.
- Status – the status of the alert.
- Alert Type – the type of alert.
- Device ID – the ID associated with the device for which the alert is triggered.
- Source Type – the type of device for which the alert was triggered, including SIM, VPN, device, and cellular.
- Source – the source (device, SIM, VPN, and so on) ID of the alert .

Click the source link to see more details for the device.

- Triggered Time – the time the alert was triggered.

Click **Triggered Time** to sort alerts by the time they were triggered (ascending or descending).

- Last Updated – the time the alert was last updated.
- By – displays the user name of the user who updated the alert.
- Description – if there is a description associated with the alert, it is displayed here.

Click on column headings to sort the information in the column.

2. Use the drop-down lists in the **Filters** section to filter alerts using the following criteria, then click **Apply**:

Filter	Description
Severity	Filter by alert severity. Severity levels include: <ul style="list-style-type: none"> • Info • Warning • Error • Critical
Status	Filter by the status of the alert, including: <ul style="list-style-type: none"> • Open – the alert is open and has not been acknowledged. • Acknowledged – the alert has been acknowledged and is still open. • Closed – the alert has been closed.
Source Type	Source types include: <ul style="list-style-type: none"> • Device • SIM • VPN

Filter	Description
Alert Type	<ul style="list-style-type: none"> • Device Offline – when the device is offline, a critical alert is displayed. • SIM usage – alerts are displayed for the following conditions: <ul style="list-style-type: none"> ◦ When the data usage limit for a SIM is over 80%, a warning alert is displayed. ◦ When the data usage limit is over 100%, a critical alert is displayed. • VPN status – when a device's VPN connection is down, a critical alert is displayed. • Cellular strength – cellular signal strength status, for example, "Cellular signal weak."

3. Click **Clear** to clear the filters.

Related tasks

[Creating and Saving Filters \(page 50\)](#)

Related reference

Edge Alerts JSON Requirements (page)

Creating Policies for Alerts

You can create customized time-based alert policies for devices, VPN connections, and SIMs.

You can create customized time-based alert policies that override the default alert policies (provided by the Device Detail service) when applied to selected, or filtered, devices.

1. In the left navigation pane of Predix Edge Manager, select **Alerts > Alerts Policies**.
2. Click **Create New**.
3. In the **Create a New Threshold** dialog box:
 - a. In **Name**, enter a name for the alert policy.
 - b. Select the severity level for the alert from the "**Send a ...**" drop-down list.
Severity levels include:
 - **Info**
 - **Warning**
 - **Error**
 - **Critical**

Note:

Severity escalation starts when the device goes offline and continues as long as the alert status is not "closed." The recommended severity escalation is to go in order from the lowest level of "info" to the highest level of "critical" (info, warning, error, then critical).

It is recommended that you do not set time intervals between escalations for less than five minutes to avoid possible issues in situations where a large number of devices goes offline at the same time. For example, if you set up an alert policy to send an "info" alert when a device is offline for 10 minutes, do not set up the next escalation alert ("warning") for 30 seconds later.

Alerts Policies

TIME-BASED THRESHOLDS

Create A New Threshold

Name
Device offline alert

Send a **Info** alert when a device is offline for 10 Minutes - +

Send a **Warning** alert when a device is offline for 15 Minutes - +

Send a **Critical** alert when a device is offline for 20 Minutes - +

Cancel Submit

- c. Enter a number for the time threshold, select the unit of time from the drop-down, then click **Submit**.

Units of time can be:

- **Seconds**
- **Minutes**
- **Hours**
- **Days**

For example, if you want to create a policy so that when a device is offline for one hour, a critical alert is triggered for that device, enter **1** for the number and select **Hours** from the drop-down.

The new alert policy appears in the list.

Setting and Removing Alert Policies


Apply or remove custom alert policies from selected, or filtered, devices.

1. In **Device Manager > Devices**, select the devices to set or remove alerts for, or go to any of the following pages to [Create and apply filters \(page 51\)](#) to set or remove alerts for a filtered set of devices:
 - **Dashboard**
 - **Device Manager > Devices**
 - **Alerts**
 - **Operations**
2. To set an alert policy:
 - a. Select **Device Operations > Set Alert Policy**.
 - b. In the **Set Alert Policy** confirmation dialog box, from the drop-down list, select the alert policy to apply, and click **Apply**.
The custom alert policy is applied and overrides the default alert policy.
3. To remove an alert policy:
 - a. Select **Device Operations > Remove Alert Policy**.
 - b. In the **Remove Alert Policy** confirmation dialog, click **Confirm**.
The custom alert policy is removed and the default alert policy takes effect.

Editing and Deleting Alert Policies

Edit or delete alerts policies you have created.

1. In the left navigation pane of Predix Edge Manager, select **Alerts > Alerts Policies**.
2. Click the > to the left of any alert in the list to expand details for an alert.
3. To delete an alert policy:
 - a. Click the trash can icon on the right of the alert policy to delete.
 - b. In the **Delete Threshold Policy** confirmation dialog, click **Confirm**.
The custom alert policy is removed from the devices, and the default alert policy takes effect.
 - c. Click **Cancel** to cancel the delete operation.
4. To edit an alert policy:
 - a. Click the pencil icon on the right of the alert policy to edit.
 - b. Make the changes, and click **Submit**.

 **Note:** You cannot change the name of the alert policy.

Predix Edge Manager Settings

About Predix Edge Manager Settings

Use the **Settings** page to view enrollment URLs, create Webhooks, set timestamp format, and see the version of Predix Edge Manager you are using.


Use the **Settings** page to do the following:

- **Enrollment** – View the enrollment URLs for enrolling devices with Predix Machine.
- **Webhooks** – Create Webhooks so that when device status changes, a notification is sent.
- **Time** – Set the format for the timestamps that appear in Edge Manager.
- **Services** – Configure Predix cloud services and assign them to devices.
- **About** – Displays version information for Edge Manager.

Viewing Settings

The **Settings** page allows you to see the certificate enrollment URL used for enrolling devices with Predix Machine, create webhooks, set the timestamp format, and configure cloud services.

1. Sign in to Predix Edge Manager.

 **Note:** If you are assigned the Technician role, when you sign in (after changing your password), the **Settings** page is displayed, showing the certificate enrollment URL. This is the only page you see in Predix Edge Manager.

2. Click **Settings** in the left navigation pane.

The tabs you see depend on your role. The administrator and operator have access to all the tabs on the Settings page. The viewer role has access to the Enrollment and About tabs only.

Tab	Role	Description
Enrollment	<ul style="list-style-type: none"> • Viewer • Technician • Administrator • Operator 	Displays the certificate enrollment URL.
Webhooks	<ul style="list-style-type: none"> • Viewer • Administrator • Operator 	Administrator and operator can create and view Webhooks. The Viewer role can view this page.

Tab	Role	Description
Time	<ul style="list-style-type: none"> • Viewer • Administrator • Operator 	Administrator and operator can set the timestamp format for Edge Manager. The Viewer role can view this page.
Services	<ul style="list-style-type: none"> • Viewer • Administrator • Operator 	Administrator and Operator can add and configure new service instances. The Viewer role can view this page.
About	<ul style="list-style-type: none"> • Viewer • Administrator • Operator 	View Edge Manager version.

Creating Webhooks

Webhooks allow you to build apps that subscribe to device status events on Edge Manager. When a device status event is triggered, an HTTP POST payload is sent to the webhook's configured URL.

Device status events include:

- Created
- Enrolled
- Online
- Offline
- Deleted

Create up to 10 webhooks for receiving information about changes in device status, for example, when a device changes status from online to offline and vice versa.

1. In Edge Manager, go to **Settings > Webhooks**.
2. Click + and add a new payload URL for the server endpoint that will receive the webhook payload.
The following payload is sent to the webhooks you added.

```
{
  "eventType": string,
  "deviceid": string,
  "created": timestamp,
  "data": {
    "status": string
  }
}
```

Setting the Time Format

Set the format for the timestamps that appear in Edge Manager.

1. In the left navigation pane, select **Settings > Time**.
2. In the **Time Zone** drop-down, select the time zone format, and click **Apply**.

Edge Manager Predix Cloud Service Configuration

You can add and configure existing cloud services in Edge Manager and assign them to devices, which enables the UAA client on the device to access the assigned cloud services.


Before you can configure services in Edge Manager, you must set those services up. All Predix services work with the UAA service. When you request Edge Manager, you can add your UAA service instance to your Edge Manager account, or if you do not already have a UAA service instance, one will be provisioned for you when you request Edge Manager.

 **Note:** All services integrated with your Edge Manager account must use the same UAA service instance that is bound to your Edge Manager instance.

The basic flow for service setup and configuration if you create your own service instances prior to requesting Edge Manager is as follows:

1. Create a UAA service instance ([page 12](#)).
2. Create a Predix Tenant Management (TMS) service instance ([page 13](#)) and bind it to the UAA service instance you created.
3. Create additional Predix service instances, for example, Time Series or Event Hub, and bind it to the same UAA service instance.
4. [Request Predix Edge Manager \(page 12\)](#).
5. Configure the services ([page 13](#)) in Edge Manager.
6. [Add devices \(page 24\)](#) to Edge Manager and [assign services \(page 36\)](#).

You can add services to single devices, or you can bulk assign services to a list of devices. Edge Manager sends the device information to the configured service to map the service to the device ID.

 **Note:** The operation for adding services to a large number of devices is asynchronous and may take some time to complete.

If you do not have existing service instances when you request Edge Manager, a UAA and TMS service instance are provisioned for you. You can add other services later—just make sure they are bound to the same UAA service instance as your Edge Manager instance.

Related information

(page)

Configuring Predix Cloud Services

Use Edge Manager to configure edge device data rivers, with the service instance ID, URL, scopes, and so on, to point to the specified Predix cloud services.

You must set up the services before you can configure them in Edge Manager.

The **Settings > Services** tab In Edge Manager allows you to configure the details (service instance ID, scopes, URL, and so on) for Predix cloud services connected to edge devices. You can also view, reset, and update configured services.

1. In the left navigation pane, click **Settings**.
2. Click the **Services** tab.
3. Enter the information for the service to configure, and click **Save**.
 - **Service Name** – Name of the cloud service, for example, `predix-time-series`.
 - **Service Instance Name** – Name you specified when you created your service instance, for example: `my-predix-time-series-service-instance`.
 - **Service Instance ID** – Unique identifier (GUID) of the service instance. This is generated when the service instance is initially created.
 - **Service URL** – Contains the API endpoint for communicating with the service, which varies according to the region where your Predix account is located. For example, for a US West Predix account:

```
wss://event-hub-pr.svc.aws-usw02.ice.gecis.io/v1/stream/messages/
```

- **Scopes** – Each service requires specific scopes. For example, the Time Series service requires the following scopes:
 - For data ingestion:
 - `timeseries.zones.<Predix-Zone-Id>.user` (added by default)
 - `timeseries.zones.<Predix-Zone-Id>.ingest`
 - For data queries:
 - `timeseries.zones.<Predix-Zone-Id>.user` (added by default)
 - `timeseries.zones.<Predix-Zone-Id>.query`
- (Optional) **Service Attributes** – Enter any additional attributes for the service as a key/value pair.
- **Associate by Default** – Enable this checkbox to automatically assign the service to newly created devices. This attribute can be set for multiple services, which will all be assigned to new devices. At the time of device creation, if no default services have been defined, the system will assign one service with a name containing the string "timeseries" and one with a name containing the string "event hub" as follows:
 - a. If there are no services matching these names, no service will be assigned.

- b. If there is a service with a name containing "timeseries", but no service with a name containing "event hub", the timeseries service will be assigned.
- c. If there is a service with a name containing "event hub", but no service with a name containing "timeseries", the event hub service will be assigned.
- d. If there is service with a name containing "timeseries" and a service with a name containing "event hub", both services will be assigned.



Chapter 8. Repository and BOM

Predix Edge Manager Repository

About Predix Edge Manager Repository

Use the Predix Edge Manager Repository to view and upload software packages, including system, applications, configurations, and containers.

The **Repository** page displays the following information about software uploaded to Predix Edge Manager:

Column	Description
Name	The name of the software package.
Type	<p>The type of software, which includes the following types:</p> <ul style="list-style-type: none">• Application – Application software for the device.• Analytics Data Map – Maps the data defined in the analytics template to the device output structures.• Analytics Template – The analytic template defines the input and output structures required by the analytic.• Configuration – Device configuration software. <p> Note: To upload Predix Machine configurations to the Edge Manager repository, you must include the entire <code><Predix Machine runtime container location>/configuration/machine</code> folder, or write your own custom package handler to handle individual configurations.</p> <ul style="list-style-type: none">• Container – (Predix Machine only) Docker containers package your application software into a standardized unit for automation of application deployment.• Operating System – Unpack the Predix Edge tar.gz image and use the signed software update file inside (<code>predix_edge_OS.swu.tar.gz</code> or <code>predix_edge_OS.swu</code>, for example). <p> Note: Unpack the Predix Edge .tar.gz image and use the signed software update file inside it (<code>predix_edge_OS.swu.signed.tar.gz</code>).</p> <ul style="list-style-type: none">• Virtual Machine – Upload a virtual machine image.

Column	Description
Version	<p>The software version. The most recent version of the software is displayed by default. If a software package has multiple versions, you can select which version you want from the drop-down list in the Version column.</p> <p>Version has the following format:</p> <pre>x.x.xxxxxx</pre> <p>For example:</p> <pre>9.9.999999</pre>
Vendor	The device vendor.
Description	Description for the uploaded software.
Handler	This field is required for the Predix Machine platform only. Enter the name of the package handler you configured.
Notes	Additional notes about the software.

Related concepts

Package Handler Service ([page](#))

External Application Installation and Update

The Predix Machine Package Handler service provides a way for you to deploy and install your own, or external, software packages on the device.


The package handler provides information to the package framework service about how a package should be processed and where the package should be installed after it is downloaded onto the device.

When you upload a package to the Predix Edge Manager repository, you must specify the package handler. The default package handler is "Machine." When you use the "Machine" package handler, when an application or configuration package is deployed through Predix Edge Manager, Predix Machine downloads the package to the device and verifies that it has not been tampered with. Once this verification succeeds, Predix Machine unzips the package and runs the `install.sh` script. This script runs with the same permissions as the Predix Machine process, and it receives the following three parameters:

1. The root directory of the Predix Machine container `<PREDIX_HOME>` is passed as parameter 1.
2. The directory where the contents of the ZIP were extracted `<UPDATE_DIR>` is passed as parameter 2.
3. The base name of the status file to write `<APP_NAME>` is passed as parameter 3.

The installation script performs the following actions:

1. Copies any required files to the correct destination on the file system.
2. Starts the application process in the background (using a command to keep the process running after the installation script exits).

 **Note:** The installation process does not complete until the script exits. Therefore, ensure that the script sets up the application to run in the background. If necessary, the script should also configure the application to start automatically when the system boots. This is often handled using a service like systemd or Upstart.

3. Writes the installation status to a file.
4. Exits the script with a return code—`Exit 0` for success, or a value in the range 50-255 for failure.

Regardless of whether you are using a custom package handler, or the default "Machine" package handler, your installation script must use the following format when recording installation status to the `<PREDIX_MACHINE_HOME>/appdata/packageframework/<APP_NAME>.json` file.

```
{
  "status": "<String>",
  "errorcode": <Integer>,
  "message": "<String>",
  "starttime": <Long>,
  "endtime": <Long>
}
```

- Status – The value must be either "success" or "failure."
- Errorcode – Zero (0) for success, or in the range of 50 - 255 for failure.

For more information about return codes, see [Upgrade Return Codes \(page 100\)](#).

- Message – Enter any string you want.
- Starttime – Time the installation began, in seconds, from epoch.
- Endtime – Time the installation completed, in seconds, from epoch.

Related concepts


[Package Handler Service \(page 100\)](#)

Uploading Software and Configuration Packages to the Predix Edge Manager Repository

To upload edge applications to the Predix Edge Manager repository, you must first create an application package.

For edge apps, the package is a `tar.gz` file containing your application's docker-compose file and an export of all the Docker images used by your application.

1. Create a package that includes the configurations, BOM, or applications you want to install.

 **Note:** Docker containers and edge apps must be packaged as tar files (`tar.gz`), all other software packages must be packaged as ZIP files (`.zip`).

2. For applications being deployed to Predix Machine, create an `install` directory that includes an `install.sh` shell script.

For example, `<Application or configuration>/install/install.sh`

 **Note:** If you do not include an install script, the package upload will fail.

3. In the left navigation pane, click **Repository**.
4. In Predix Edge Manager Repository, select **Action > Upload**.
5. In the **Upload** dialog, enter:


- **Name** – (Required) Name of the software package.
- **Vendor** – Device vendor.
- **Version** – (Required) Software version. Version has the following format:

```
x.x.xxxxxx
```


For example:

```
9.9.999999
```


- **Type** – (Required) Choose from:
 - **Application** – Application software for the device.
 - **Analytics Data Map** – Maps the data defined in the analytics template to the device output structures.
 - **Analytics Template** – The analytic template defines the input and output structures required by the analytic.
 - **Configuration** – Device configuration software.

 **Note:** To upload Predix Machine configurations to the Edge Manager repository, you must include the entire `<Predix Machine runtime container location>/configuration/machine` folder, or write your own custom package handler to handle individual configurations.

- **Container** – (Predix Machine only) Docker containers package your application software into a standardized unit for automation of application deployment.
- **Operating System** – Unpack the Predix Edge tar.gz image and use the signed software update file inside (`predix_edge_OS.swu.tar.gz` or `predix_edge_OS.swu`, for example).

 **Note:** Unpack the Predix Edge .tar.gz image and use the signed software update file inside it (predix_edge_OS.swu.signed.tar.gz).

- **Virtual Machine** – Upload a virtual machine image.
- **Platform** – Choose from:
 - **Predix Machine** – Select this option for Predix Machine containers, applications, and configurations.
 - **Predix Edge** – Select this option for multi-container Predix Edge apps.
- **Description** – Description for the software or container. You should make the description meaningful, for example, add the location of the device group to which you are pushing the application.
- **Notes** – Optionally, you can include additional notes about the package.


 **Note:** Notes have a 1024 character limit.

- **Package Handler** – Name of the Predix Machine package handler you configured. See [Configuring Package Handler](#) (*page 102*).

6. Click **Choose File** to select the files to upload to the repository.

7. Click **Upload**.

8. In the **Confirm Upload** dialog box, click **Done**.

 **Note:** The size limit for uploads is:

- 500 MB for configuration, application, and containers
- 15 GB for OS

If the file upload operation is interrupted for some reason, it will automatically resume from the point at which it was interrupted when the connection is restored. You do not need to re-initiate the upload.

The package is uploaded to the repository and appears in the Repository list.

Package Guidelines and Size Limits

Before uploading packages to Predix Edge Manager, ensure they are packaged correctly and do not exceed the recommended size limits.

The following table shows the guidelines for package size limits when uploading packages to the Predix Edge Manager Repository.

Package Type	Size Limit	File Type	Notes
Configuration	500 MB	ZIP	As best practice, once configuration files are uncompressed on the device, each file should be no larger than 5 MB. Actual limits depend on how much disk space is available at the time.
Application	500 MB	ZIP	
Container	500 MB	gzip	
Edge app	500 MB	tar.gz	
Analytics runtime engine	500 MB	tar.gz	Package and upload the runtime engine as a multi-container (Predix Edge) app.
Templates	500 MB	ZIP	When you upload a template, you do not specify a platform, however, you must specify a package handler, which should be the analytics engine name, for example, FogHorn or CSense. The handler is not the app instance ID.
Data Maps	500 MB	ZIP	When you upload a data map, you must specify the name of the template to which the data map is associated. You do not specify a platform.
Operating system	15 GB	n/a	

Creating the Edge Application Package

Package a multi-container edge application.

1. Navigate to the folder on your machine that contains the `docker-compose.yml` file for your application.
2. Execute the following command to (replacing `<your-image1>`, `<your-image2>`, and `<your-image3>` with the images used by your application):

```
$ docker save -o images.tar <your-image1> <your-image2> <your-image3>
```

3. Create a `tar.gz` file containing the `docker-compose.yml` and `images.tar` file for your application.


```
$ tar -czvf app.tar.gz images.tar docker-compose.yml
```

You now have a packaged application. If you are using a development VM, you can upload the application. If you are using a production VM, you need to take one more step to have your application signed. Only signed apps can run on production Predix Edge OS VMs. See Application Signing ([page](#)) for more information and further instructions.

Downloading Software Packages from the Predix Edge Manager Repository

You can download application, configuration, and container packages from Predix Edge Manager.

1. In the left navigation pane, click **Repository**.
2. Select the software package to download (you can select multiple packages), then select **Action** > **Download**.

 **Note:** If a software package has multiple versions, you can select which version you want to from the drop-down list in the **Version** column and selecting a version.

The software package is downloaded as a ZIP file.

Bill of Materials

Bill of Materials

Create and install a Bill of Materials (BOM) to track dependencies between software packages and applications.

The Bill of Materials (BOM) lists all the software packages and applications, with dependencies among them, that are installed on a GE Digital-provisioned device. The BOM lists the software packages with their version numbers in the order they should be installed on the device.

 **Note:** Software packages can be of the type application, container, or configuration. If you do not specify the type of package in the BOM JSON file, it is application by default.


BOM Definition

The BOM must be in JSON format. Package installation follows the order you define in the BOM. The below shows an example BOM for Predix Machine:

```

{
  "name": "Device-BOM",
  "version": "1.0.0",
  "description": "BOM for device",
  "packages": [
    {
      "version": "16.04.10",
      "vendor": "Ubuntu",
      "name": "Ubuntu Linux",
      "provider": "GE Digital",
      "description": "Operation system on device."
    },
    {
      "version": "1.8.0",
      "vendor": "OpenJDK",
      "name": "OpenJDK",
      "provider": "GE Digital",
      "description": "JVM"
    },
    {
      "version": "1.7.x",
      "name": "Predix Machine Configuration",
      "type": "configuration"
    },
    {
      "version": "1.7.x",
      "vendor": "GE Digital",
      "name": "Predix Machine",
      "provider": "GE Digital",
      "description": "Predix Machine"
    }
  ]
}

```

 **Note:** Vendor, provider, and description are not required, as that information is retrieved from the package repository.

The below JSON shows an example BOM for Edge OS:

```

{
  "name": "Sample-BOM",
  "version": "1.0.0",
  "description": "Sample BOM ",
  "packages": [{
    "version": "1.0.0",
    "name": "QE-EdgeApp",
    "type": "multi_container_app",
    "appInstanceId": "alias1"},
    {
      "version": "1.0.0",

```

```

    "name": "QE-EdgeConfig",
    "type": "configuration",
    "appInstanceId": "alias1"}
  ]}

```

Related tasks

[Deploying a Bill of Materials to Multiple Devices \(page 65\)](#)

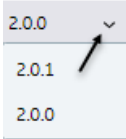
[Deploying a Bill of Materials to a Single Device \(page 66\)](#)

Viewing the Bill of Materials List

View the list of Bill of Materials (BOM) uploaded to Edge Manager.

1. In the left navigation pane, select **Bill of Materials**.

If Bill of Materials files are uploaded to Edge Manager, you see the files listed with the following information:

Name	The file name of the BOM. BOM files are in JSON format.
Version	The version of the BOM. If there are multiple versions of the BOM file, you can click in the version column to see all of the versions. Version 
Created On	The date the BOM was added to Edge Manager.
Description	Description of the BOM.

2. Click a BOM file in the list to see its contents in the **Software** pane.

Adding a Bill of Materials

Add a Bill of Materials (BOM) to Predix Edge Manager so that you can deploy them to enrolled devices.

1. In the left navigation pane, select **Bill of Materials**.
2. Click **Select Action > Add**.
3. In the **Add BOM** dialog box, click **Choose File** to select the JSON file containing the BOM to add, then click **Upload**.

 **Note:** The packages listed in the BOM file you are adding must be active (already uploaded) in the Edge Manager repository.

The BOM appears at the top of the BOM list (by default, the list is sorted by timestamp).

4. Select the BOM to see its contents in the **Software** section.

Related tasks

[Deploying a Bill of Materials to Multiple Devices \(page 65\)](#)

[Deploying a Bill of Materials to a Single Device \(page 66\)](#)


[Deleting a Bill of Materials \(page 102\)](#)

Related information

(page)

Deleting a Bill of Materials

Delete unused Bill of Materials (BOM) from Predix Edge Manager.


 **Note:** You can delete only BOMs that are not currently in use by any installations.

1. In the left navigation pane, select **Bill of Materials**.
2. From the BOM list, select the checkboxes next to the BOM to delete, and select **Select Action > Delete**.
3. In the **Delete BOM** confirmation dialog, click **Confirm** to proceed with the deletion.
A confirmation dialog confirms the deletion.

Chapter 9. Data Pumps

Data Pumps

Data pumps enable you to specify asset data to send to the Predix cloud for use with cloud applications and analytics. Data pumps simplify deployment to a single edge device. Data pumps are comprised of multiple edge applications to ingest and publish data.

 **Note:** Currently, only the OPC-UA protocol (ingress) and the Predix Time Series service (egress) are supported.

You can use the data pump graphical designer in Predix Edge Manager to configure data flow between a protocol adapter (ingress) and gateway service (egress). The most basic example is configuring a device to collect data from an OPC-UA server and sending it to the Time Series service.

The data pump flow design is saved in the Predix Edge Manager database and can then be deployed. Data pumps are deployed as two packages—application and configuration.


Configuring Data Pumps

You need the following information to configure a new data pump:

- OPC-UA server connection settings
- Tags must be in a CSV file and include the following fields:
 - Identifier Type
 - Namespace Index
 - Node ID
 - Published Name

Click **Sample CSV** to download an example CSV file with the required fields.

1. In Predix Edge Manager, select **Device Manager** in the left navigation pane.
2. Select the device for which to configure the data pump.

 **Note:** The Data Pumps tab appears only for devices that are running on the Predix Edge platform.

3. Click the **Data Pumps** tab.
4. In the Data Pumps page click **Create New** to create a new data pump, or click **Select Existing** to edit an existing data pump.
5. In the Setup page, enter the following information, then Click **Next**:
 - **Name** – Populated by default as <device_ID>_DataPump. You can change this—just be sure the name is unique and meaningful.
 - **Version** – Enter a version number. The format must be: <version>.x.x
 - **Description** – (Optional) Enter a description for the data pump.

You can click **Save** at this point to save the data pump in the data base so you can finish configuring it later.

Click **Exit** to exit the data pump designer. A confirmation dialog gives you the opportunity to save or discard the changes.

6. In the **Services** page, enter the information for the protocol adapter and the egress point, then click **Next**.


 **Note:** Currently, only the OPC-UA protocol and the Predix Time Series service as an egress point are supported.

Table 6. OPC-UA

Field	Description
Server IP/ Hostname	Enter the hostname or IP address for the OPC-UA server.
TCP Port	Enter the TCP port for the OPC-UA server.
Server Resource Path	Enter the resource path for the OPC-UA server. The path name begins with a single forward slash.
Update Type	Choose from the following update types: <ul style="list-style-type: none"> • Subscription – Select if the OPC-UA server is configured to use a subscription to read data. • Polling – Select if the OPC-UA server is configured to use polling to read data.

Table 7. Time Series

Field	Description
Time Series Name	Select the time series from the drop-down list.
Time Series Zone ID	Enter the Zone ID for the Predix Time Series service tenant.

Field	Description
Time Series URL	Contains the API endpoint for communicating with the service, which varies according to the region where your Predix account is located. For example: wss://gsvc.aws-usw02.ice.gecis.io/v1/stream/messages

You can click **Save** at this point to save the data pump in the data base so you can finish configuring it later.

Click **Exit** to exit the data pump designer. A confirmation dialog gives you the opportunity to save or discard the changes.

- In the **Tags** window, click **Choose File** to upload a CSV file (or drag and drop the CSV file) containing the tags, then click **Import**.
- In the Deploy window, you can save and deploy the data pump, or save it now and deploy it later.

Option	Description
Save	Saves the data pump in the database.
Save and Deploy	Saves and deploys the data pump.
Exit	Exits the data pump designer. A confirmation dialog gives you the opportunity to save or discard the changes.

If tags already exist in the table, you get an error message with the duplicate node IDs (along with any other errors). If this happens, you need to update your CSV file offline and re-upload it.

Chapter 10. Connectivity and SSH

Predix Edge Manager Connectivity

About Predix Edge Manager Connectivity

Use Predix Edge Manager Connectivity to establish connectivity between edge devices and the cloud over various networks, including cellular, fixed-line, and satellite communication.

In the left navigation pane, click **Connectivity**.

The **Connectivity Dashboard** displays information about VPN connection status, SIM state, SIM connections, and recent critical alerts.

In Edge Manager Connectivity, you can perform the following tasks:

- **SIM List**
 - View and modify SIM lifecycle states.
 - Modify data usage plans.
 - View the current connectivity state for a SIM.
 - View the current billing cycle's usage of the SIM.
 - View SIM details such as ICCID, IP address, provider, and device ID.
 - View alerts for SIM cards.
 - Export the SIM list as a CSV file.
- **Batch Update** – update the rate plans and lifecycle states of multiple SIMs with one upload.
- **VPN** – view Virtual Private Network (VPN) connections and status associated with registered devices.

Ordering SIM Cards

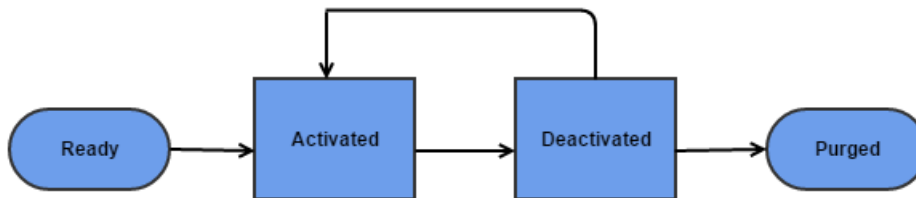
Before ordering SIMs, you must have a Predix account.

1. Go to <http://www.predix.io/catalog>, then click the **Connectivity** tile.
2. Follow the instructions on the Connectivity page.

Once you are registered, the SIM cards you order are added automatically to your account. The default SIM card state is "Ready," unless otherwise specified. See [SIM Card Life Cycle \(page 107\)](#).

SIM Card Life Cycle

The following diagram displays the different states of the SIM card life cycle.



- **Ready**
 - Unless otherwise specified when ordering, Ready is the default state for new SIM cards.
 - When a minimum amount of data is passed on the SIM card, Ready transitions to Activated.
 - Ready is a system state, and is not user-configurable.
- **Activated**
 - Until the SIM card is in the Activated state, there is no billing.
 - The Activated state allows the SIM card to pass data (subject to the associated rate plan).
 - You can customize this state.
- **Deactivated**
 - In the Deactivated state, the SIM card is no longer provisioned to pass data.
 - You can customize this state.
- **Purged**
 - Once the SIM card is in the Purged state, the SIM card cannot be reused.
 - The Purged state is configurable by administrators only.
- **Suspended**
 - When the SIM card exceeds the data usage of its associated plan, it is suspended.
- **Not Available**
 - The Not Available state indicates an error with communication between the service provider and the SIM card.

If the Not Available state persists, contact support.

Viewing the SIM Card List

In Edge Manager, in the left navigation pane, click **Connectivity > SIM List**.

The page displays a list of SIM cards for your account, including the following information:

- **Status** – Displays the status of the SIM, for example, "online."
- **Alerts** – Displays alerts associated with usage, for example, when the data limit for the SIM card is close to the maximum allowed for the associated plan.

- **ICCID** – An Integrated Circuit Card Identifier (ICCID) is inscribed on the back of each SIM card. The ICCID identifies each SIM internationally. It consistently maps your physical endpoint to the logical endpoint within Edge Manager. Click the link to go to the SIM details page.
- **Device Name** – the name of the device.
- **Life Cycle Stage** – Displays the life-cycle stage of the SIM card. See [SIM Card Life Cycle \(page 107\)](#).
- **IP Address** – Read-only field that displays the assigned IP address for the SIM card. IP address management is handled automatically by Predix. Once assigned, the IP address, where supported, can be changed by filing a service request with the Predix support team.
- **MTD Usage (MB)** – Displays the data usage (up to the last 60 minutes) for the SIM card.
- **Provider** – The connectivity provider.
- **Plan** – The selected rate plan provisioned for the SIM card.
- **Session** – Indicates whether the SIM card is currently in session and transmitting data (up to the last 60 minutes).

The Connectivity page also displays messages about cellular service provider maintenance when applicable.

Viewing Details for a SIM Card

1. In the left navigation pane, click **Connectivity > Sim List**.
2. Click the ICCID link for the SIM card to view its details.

The page for the selected SIM card displays the SIM details, including:

- **SIM Details** – Displays details, such as ICCID, primary IMSI, and the device ID the SIM card is associated with.

Click the Device ID link to go to the summary page for the device associated with the SIM card.

- **SIM Usage** – Displays the cycle to date usage, rate plan details, whether the usage limit has been reached, and whether or not the SIM card is suspended.
- **SIM APN Information** – Displays the IP address for the SIM card.
- **Alerts** – Displays any data usage alerts for the SIM card.
- **Signal Strength** – Displays signal strength status, when the status was last updated, and the network mode.
- **Rate Plan** – Displays the rate plan for the SIM card. This field is read-only.
- **Lifecycle Stage** – Displays the lifecycle stage for the SIM card (Activated or Deactivated). This field is read-only.

You can also view details for a SIM card associated with a device by clicking the ICCID link displayed in the device's summary page.

Related tasks

[Viewing the Device Summary \(page 30\)](#)

Exporting the SIM List

You can export the SIM list as a CSV file.

1. In the left navigation, select **Connectivity > Sim List**.
2. In the far left column, select the SIMs you want to export details for, or select the check box next to **Name** to select all SIMs.
3. Click **Export**.

The SIM details are compiled and exported to your local machine in a CSV file.

Troubleshooting SIM Cards

Run diagnostics for the SIM card to view points of failure.

1. In the left navigation pane, select **Connectivity**.
2. In the Connectivity page, click the SIM card to troubleshoot.
The SIM card summary page shows details about the SIM card, including any alerts associated with the SIM card.
3. Click **Run Diagnostic**.
The Troubleshooting window shows the states of connectivity, including the points of failure and success, for the SIM card.

Changing the Rate Plan and Lifecycle Stage For a SIM Card


You can update the rate plan and lifecycle stage for a single SIM card. To update multiple SIM cards with one upload, see [Performing a Batch Update \(page 110\)](#).

1. In Edge Manager, click **Connectivity** in the left navigation pane.
2. Click the ICCID link for a SIM card to view its details.
The page for the selected SIM card displays the SIM details, SIM usage, SIM APN, and session status information.
3. To change the rate plan for the SIM card, select the new rate plan from the drop-down list, then click **Confirm** in the confirmation dialog box.
4. To change the lifecycle stage for the SIM card, select the stage from the drop-down list, then click **Confirm** in the confirmation dialog box.

Performing a Batch Update

You can use the Batch Update feature to update the rate plan and life cycle state for multiple SIM cards with one upload.

1. Log into Predix Edge Manager.
2. In the left navigation pane, select **Connectivity**.
The Connectivity page lists the SIM cards associated with your account.
3. (Optional) Filter the SIM card list by life cycle state or plan by entering search criteria in the search box, such as "Activated."
Skip this step if you want to update all SIM cards.
4. Click **Export** to export a CSV file containing the SIM cards to update, and save the exported CSV file locally.
5. Update the information for the SIM cards, then save the file.
You can go to the SIM card's details page to see the rate plans and states that are available to the SIM card. See [Viewing Details for a SIM Card \(page 108\)](#).
6. In Predix Edge Manager, in the left navigation pane, select **Connectivity > Batch Update**.
7. Click **Upload CSV**.
8. In the Batch Update window, click **Choose File**.
9. Browse to locate and select your CSV file.
Edge Manager validates the file as it is uploaded. The dialog box displays a Batch Update Summary of the following information:
 - Total Sims
 - State changes
 - Rate plan changes
 - IP changes
 - Error records
 If there are errors in the file, click the view link to download the CSV file, which lists any errors detected during validation. To correct the errors before submitting the updates, click **Cancel**, fix the errors, and upload your CSV again.

 **Note:** Only validated records are processed. If you proceed with the update without fixing errors, the error records are not processed.
10. Click **Update** to submit the updated SIM records.
Your update appears in the Batch Update list. The Error column shows the number of records that contained errors, and the Success column shows the number of records that were

successfully updated. The numbers are links, which you can click to download a CSV file with a list of the corresponding SIM cards.

VPN Management


You can perform VPN management on devices using Edge Manager.

To enable VPN management through Edge Manager, you must have a prepared environment with a server and client that are ready to communicate. For more information, see [Predix Machine VPN Service \(page \)](#)

Select **Connectivity > VPN** to view Virtual Private Network (VPN) connections associated with registered devices.

The VPN Connectivity page displays the following information:

- **Status** – Shows the connection status of the VPN client. When the check mark is green, it is connected. When the check mark is gray, it is disconnected.
- **Client ID** – VPN client ID. Click the client ID to see details about the VPN.
- **Device ID** – Unique number associated with the device.
- **IPv4** – VPN client IPv4 address.
- **IPv6** – VPN client IPv6 address.
- **Public IP** – VPN client public address.
- **Server IPv4** – VPN server IPv4 address.
- **Server IPv6** – VPN server IPv6 address.
- **Connected Since** – Timestamp for when the current connection was established.

 **Note:** The IPv4, IPv6, Public IP, Server IPv4, Server IPv6, and Connected Since fields are empty if the VPN is disconnected.

Enter "connected" in the search box to search for connected VPNs.

Related concepts

[Predix Machine VPN Service \(page \)](#)

Starting and Stopping VPN Management

You can start and stop the management of VPN connections on devices.

1. In the left navigation pane, select **Connectivity > VPN**.
2. Click the **Client ID** link for the VPN connection to manage.
3. In the VPN page:

Option	Description
Start	Click to start management of the VPN connection on the device.

Option	Description
Stop	Click to stop management of the VPN connection on the device.

Getting the VPN Log

Get and view the VPN connection log for a device.

1. In the left navigation pane, select **Connectivity > VPN**.
2. Click the **Client ID** link for the VPN connection to manage.
3. On the VPN page, click **Get Log**.

Setting the VPN Log Verbosity

Set the verbosity level for the VPN connection on the device.

1. In the left navigation pane, select **Connectivity > VPN**.
2. Click the **Client ID** link for the VPN connection to manage logs for.
3. Click **Set Log Level**.
4. In the VPN Log Verbosity dialog box, select the log verbosity (1-10) from the drop-down list, and click **Submit**.

SSH Access

About SSH Access

Predix Edge Manager enables you to securely access Predix Edge devices using SSH.

You can use SSH to troubleshoot issues in a production Predix Edge device or instance. The device is not required to have Edge Manager connectivity as both online and offline access is supported.

You can get SSH access in one of two ways:

- Online via Edge Manager:
 1. Use Edge Manager to obtain a signed SSH key.
 2. Use Edge Manager to activate the signed key.
- Offline via Edge Manager and PETC:
 1. Use Edge Manager to obtain a signed SSH key.
 2. Use PETC to activate the signed key.

Requesting SSH Access

To get SSH access, first generate a public SSH key and use that to create a signed SSH key in Edge Manager.

1. In the left navigation pane, select **Device Manager > Devices** to see a list of all devices.
2. Select the Predix Edge device(s).
 - a. For a single device, click the device name.
 - b. Use the checkboxes to select multiple devices. A maximum of 100 devices per request is supported.
3. To request SSH access:
 - a. For a single device, click the **Request** button (located under **SSH ACCESS**).
 - b. For multiple devices, click the **Device Operations** drop-down menu and select **Request SSH Access**.


A dialog will appear with instructions for requesting SSH access.

4. Select an **EXPIRATION DATE** for the SSH access. The default is one week later, the maximum 90 days.

5. Generate a public SSH key on your device.

For further information, see <https://help.github.com/en/articles/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent> (external reference).

 **Note:** RSA is the only algorithm supported by GE for SSH access. It is recommended you generate your public key with RSA-4096 (RSA-2048 will also work).

 **Note:** It is highly recommended you use a passphrase when generating the RSA key pair to protect the private key.

6. Click the **Choose file** button to select the public SSH key you created.
7. (Optional) Enter a description in the **Request Description** field.
8. Click **Download Request File**. This will save a .REQ file in your downloads folder.

Email your .REQ file to digital-ssh-signing@ge.com to obtain a signed SSH key.

Uploading a Signed SSH Key

Within one business day, you should receive an email from GE with your signed key (.SSK file).

For offline use, upload the .SSK key to PETC and activate it as described in [Activating SSH Offline with PETC \(page 114\)](#).

For online use, perform the steps below.

1. In the left navigation pane, select **Signed Keys**.
2. Click the **Action** drop-down menu.
3. Select **Upload SSK(s)**.
A dialog will appear instructing you to select the .SSK file.
4. Click **Choose File** to select the .SSK file.
5. Click **Upload**.

The uploaded file will appear in the **Signed Keys** list.


Activating SSH Online with Edge Manager

To activate a signed key using Edge Manager, perform the following steps.

1. In Predix Edge Manager's left navigation pane, select **Signed Keys**.
2. Click **Activate** (in the **Action** column).
3. A confirmation dialog will appear. Click **Confirm** to activate the key, or **Cancel** to quit.

There are numerous ways to check the status of the key activation.

- In the **Signed Keys** list, click **Pending Activation** for the key.
- When a device is selected, click the **Commands** tab.
- In Predix Edge Manager's left navigation pane, click **Operations** and then the **Commands** tab. Select the specific operation.

 **Note:** Any pre-existing keys in the device that are not managed by Predix Edge will not be preserved after activation.

Activating SSH Offline with PETC

Prior to activating SSH, you are assumed to have completed the following:

- The needed devices have been enrolled in Edge Manager.

- You have generated a signing request for your device(s) via Edge Manager and obtained a signed SSK key (.ssk) file.

1. In the left navigation pane, select **Signed Keys**.
2. In the **Select Action** drop-down, select **Add Key**.
3. In the **Add Signed File** window, click the **Choose File** button and locate the signed SSK key (.ssk) file.
4. Click the **Finish** button.
The signed key has been activated and the **Signed Keys** table shows the activated key at the top of the table with the **Status** Active.

Using the activated key, you can now access the devices enrolled in SSH. If you are prompted for a password when trying to SSH into a device, that device has not been properly enrolled.

Downloading SSH Keys

Use this feature to retrieve a key that you can upload to PETC in order to activate SSH access on an offline device.

1. From Predix Edge Manager's navigation menu, click **Signed Keys**.
2. Use the checkboxes to select the key(s).
3. Click the **Action** drop-down menu and select **Download**.

The key(s) will be saved in your downloads folder.

Revoking SSH Online with Edge Manager

 **Note:** This action can be performed only if the **Key Status** is **Active**.

1. To revoke a single key:
 - a. From Predix Edge Manager's navigation menu, select **Signed Keys**.
 - b. Click **Revoke** for the specific .SSK file you wish to revoke.
2. To revoke multiple keys:
 - a. From Predix Edge Manager's navigation menu, select **Signed Keys**.
 - b. Click the **Action** drop-down menu and select **Revoke**.
3. A confirmation dialog will appear. Click **Confirm** to revoke the key, or **Cancel** to quit.

There are numerous ways to check the status of the key revocation.

- In the **Signed Keys** list, click **Pending Revocation** for the key.
- When a device is selected, click the **Commands** tab.
- From Predix Edge Manager's left navigation menu, click **Operations**, then the **Commands** tab. Select the specific operation.

Revoke SSH Offline with PETC

As with Edge Manager, you can use PETC to revoke any signed SSH key.

1. In the left navigation pane, select **Signed Keys**.
2. On the **Signed Keys** page, select the signed keys that you want to revoke.
3. In the **Actions** drop-down, select **Revoke**.
The **Revoke Signed Key** window appears.
4. To confirm, click the **Revoke** button.

The revoked key disappears from the list.

Chapter 11. Unsubscribe from Edge Manager

Unsubscribe From Edge Manager

Predix Edge Manager allows you to remotely manage your fleet of devices. If you want to stop managing your devices remotely, perform the following steps.

1. Delete all users you created in Edge Manager. See [Deleting Predix Edge Manager Users \(page 21\)](#).
2. Un-enroll and delete the devices you created. See [Deleting Devices from Predix Edge Manager \(page 28\)](#).
3. Contact the [GE Digital Customer Center](#) to have your dependent services and tenant deleted, and billing stopped.

Changes will take effect in your next billing cycle after the tenant deletion has been performed by Customer Support.

Chapter 12. Troubleshoot Predix Edge Manager

Retrieving Predix Machine Logs

You can use Edge Manager to retrieve log files from the Predix Machine device when debugging an application or troubleshooting a device

1. In the left navigation pane, click **Device Manager**, then select the device for which to retrieve logs.
2. Select **Device Operations > Execute Command**.
3. In the **Execute Command** dialog window select **Predix Machine** as the platform, then select either:
 - **Get Log** – Retrieves the Predix Machine log from the device.
 - **Get Available Logs** – Returns a list of available logs on the device.
4. Click **Next**.
5. In the **Execute Command** dialog window, set the **Timeout** value (the default is 30 minutes) for the operation, and click **Execute**.
Edge Manager requests the logs from the device.
6. In the confirmation dialog window, click **Close**.
7. In the **Device Manager** page, click the link for the device, then click the **Commands** tab.
The **Commands History** displays the command history for the device and the status of each command. Once the **Status** displays "Success" you can click the **download** link in the **Output** column to download the log file.

Retrieving Predix Edge Device Logs


You can use Predix Edge Manager to retrieve log files from the edge device when debugging an application or troubleshooting a device.

If you are using the development version of Predix Edge, with ssh enabled, you can also obtain logs from the command line of the device.


1. In the left navigation pane, select  **Device Manager > Devices**.

2. Select the device for which to retrieve logs, then select **Device Operations > Execute Command**.
3. In the **Execute Command** dialog window select **Predix Edge** as the platform, then select the **Get Journal Log** tile, and click **Next**.
4. In the **Execute Command** dialog window, set filters (using boolean values "true" and "false") for the type, quantity, and formatting of the logs to retrieve, and click **Execute**.
Edge Manager requests the logs from the device.
Optionally, to filter the logs for a specific application running on the device, you must first obtain the Container Name from the app. To do this:

- a. On the **Edge Apps** tab for the device, select the **Application ID** and copy the name of the container.

 **Note:** The container name may have a `.1` appended at the end of the name. Do not include that in the copied text.

Devices








QE-UI-EDGEOS-DONOTDELETE Edit 

ROOT

Online


Summary Troubleshooting Configurations **Edge Apps** Software BOM Commands Data Pumps



APPLICATIONS Deploy Edge Apps

APPLICATION ID	STATUS	VERSION	TIMESTAMP	ACTIONS
 idpd_20180828-DataPump-1-0-0	Error			Start Stop 
 predix-edge-technician-console	Error			Start Stop 
 HistorianBeta3RC2	Error			Start Stop 
predix-edge-broker	Stopping			Start Stop 

CONTAINERS (2): PREDIX-EDGE-TECHNICIAN-CONSOLE

NAME	IMAGE NAME	DESIRED STATE	CURRENT STATE	ERRORS
predix-edge-technician-console_petc.1	dtr.predix.io/predix-edge/petc:1.0.5	Pending 2 days ago		
predix-edge-technician-console_petc.1	dtr.predix.io/predix-edge/petc:1.0.5	Shutdown	Orphaned 2 days ago	

Rows per page 10 

1-2 of 2  1 

- b. In the **Execute Command** dialog box, paste the value you copied in the previous step into the **Show Logs from Specified Application Service** field.
5. In the confirmation dialog window, click **Close**.
6. In the **Device Manager** page, click the link for the device, then click the **Commands** tab.

The **Commands History** displays the command history for the device and the status of each command. Once the **Status** displays "Success" you can click the **download** link in the **Output** column to download the log file.

Predix Edge Manager Common Errors

The following are general issues you may experience when using Predix Edge Manager.

500 Internal Server Error When Importing Device List

When importing a device list, you receive the following error:

```
500 Internal Server Error
Failed to upload the devices. An unexpected error has occurred, try again
later.
```

Cause

The device list may not meet the required format.

Solution

Verify the following:

- The file is a valid CSV file with a .csv file extension.
- The file contains only the following required fields:
 - modelID
 - did
 - name
 - sharedSecret

Device System Up Time "Unknown"

On the Device Summary page, in the Health information, if the **System Up Time** is displayed as "Unknown" this can mean there is a timing (or clock) issue on the device itself that is causing a negative up time to be recorded when Predix Machine syncs to the cloud. If you see this status, you should check your device for clock issues.

"Set Up Your Redirect URI" Error

If you try to login and receive the message: "You should not see this page. Set up your redirect URI," your session has timed out.

Solution

Re-enter your Edge Manager URL (for example, <https://<your-tenant-id>.edgemanager.run.asv-pr.ice.predix.io>), and sign in.

Error Messages

If you receive any of the following error messages, [file a support ticket \(page 121\)](#):

- Incorrect application URL
- Unable to get user token
- Unable to create session
- Unable to get tenant configuration
- Network connection to the authorization server for the tenant management service access token has timed out.
- Network connection to tenant management service has timed out.
- Tenant management service request has timed out.
- Request to the authorization server for the tenant management service access token has timed out.
- Unable to get tenant management service access token.
- Unable to get tenant configurations from the tenant management service.

Filing a Support Ticket

1. Go to <https://www.predix.io/support/> and click **File a ticket**.
2. In the **Issue**, **Priority**, and **Products and Services** drop-down lists, select the appropriate criteria.
3. In **Issue description**, provide the following information:
 - Customer Name
 - Tenant ID
 - Email Address
 - Org Name
 - Space Name
4. (Optional) Click **Attach File** to include any relevant files.
5. Click **Create Ticket**.

Troubleshooting Devices


Use the Troubleshooting page to see CPU, memory, and disk usage for a device.

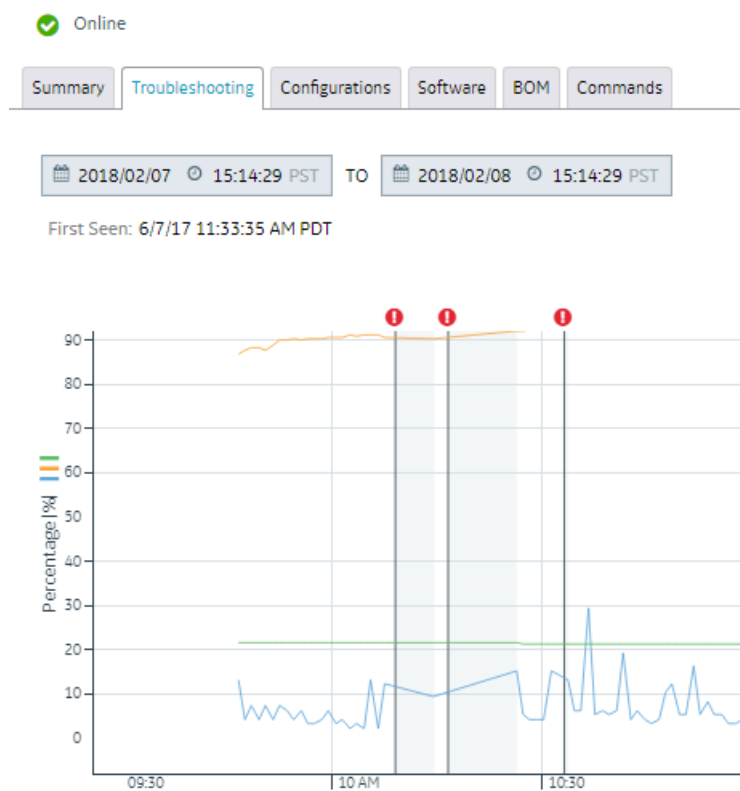
1. In the left navigation pane, select **Device Manager**.

2. Click the link for the device to troubleshoot.

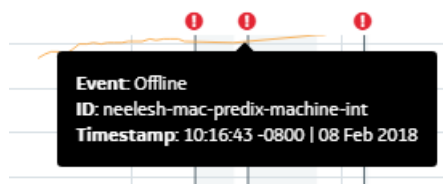
3. Click the **Troubleshooting** tab.

You see a graph representing CPU, memory, and disk usage information for the device. By default, the time window is set for the previous 24 hours from the present time.


 **Note:** Troubleshooting data is displayed only for the times the device is online. For example, if the device was online all day yesterday and is offline all day today, you see only the data for yesterday, when the device was online.



The red circles represent events, for example, the device was offline. The shaded area visually represents the duration of the event. Hover over the red circle for details about the event.



The **First Seen** date and time displays the first time the device connects to Edge Manager. Data does not display for dates and times that are earlier than the **First Seen** date and time stamp displayed for the device.

4. Click the calendar icon to change the time window to view.
 - a. In the calendar view, select the dates and times for the time span to view, and click **Apply**.
You can also click one of the preset time spans (last 7 days, this month, last month).
5. Click the pan icon () to move the graph.
6. Click the magnifying glass icon to zoom in on a data point.

Chapter 13. Reference

Related Documentation

Edge Manager works in conjunction with Predix Machine.

See the [Predix Machine documentation](#) for related documentation.

Edge Manager Topic	Relates to
<ul style="list-style-type: none">• Adding a Device to Edge Manager• Importing a Device List	<i>Predix Machine:</i> Device Enrollment Overview (page) Adding a Device to Predix Edge Manager (page)
<ul style="list-style-type: none">• Adding Custom Device Models• Device Summary• Alerts	<i>Predix Machine:</i> Device Detail Service (page)
Managing Docker Containers	<i>Predix Machine:</i> Predix Machine Containerization Overview (page)
Uploading Software and Configurations to Edge Manager	<i>Predix Machine:</i> Package Handler Service (page)
<ul style="list-style-type: none">• Executing Commands• Adding a Custom Command	<i>Predix Machine:</i> Command Framework Overview (page)


Contacting Support

Follow these instructions to request an instance of Predix Edge Manager if you have a Predix Europe account.

 **Note:** Predix Edge Manager has the following prerequisites:

- You must have a Predix account with an org, space, and UAA service instance. See (page).
- You must have the Predix Machine SDK version 17.1.x or later. See Downloading the Predix Machine SDK (page).


1. Go to the Predix portal at <http://predix.io>, and click **Support**.
2. Click **File a support ticket**, and provide the following information in the **Description** field:
 - **Customer Name** – Your business name, or the business name of the account to create.
 - **Email Address** – The email address where Predix will send the provisioned Predix Edge Manager URL.
 - **Org Name** – The organization name associated with the Predix account that has been created for your business.
 - **Space Name** – The space created in your org.
 - **Tenant ID** – This will be used as a custom sub-domain name in the provisioned Predix Edge Manager URL.

 **Note:** The tenant ID should be short (more than two characters, but less than 32). It can contain only alphanumeric characters and hyphens.

- Reason for requesting Predix Edge Manager access – Description of the use case and customer details. For example, POC or demo.

You will receive an email containing the provisioned Predix Edge Manager URL.

3. If this is your first time logging in, you are prompted to change your password. In the User Settings dialog box, enter the following:
 - **Old Password** – Enter the password you logged in with.
 - **New Password** – Enter a new password.
 - **Confirm Password** – Re-enter your new password.

 **Note:** Your password must:

- Be at least eight characters long and not more than 15 characters long
- Contain at least two uppercase letters
- Contain at least one lowercase letter
- Contain at least two numbers
- Contain at least one special character
- Not contain the user name
- Not contain spaces

You see the Predix Edge Manager Dashboard, and the Control Panel pane on the left, where you can access Edge Manager features like Device Manager, Operations, Alerts, Repository, Bill of Materials, Commands, Connectivity, User Manager, Settings, and so on.

Chapter 14. Predix Edge Manager Release Notes

Predix Edge Manager Release Notes 2.4.0

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

New Features/Enhancements

This release contains the following new features and enhancements:

Device Count

On the **Device Manager > Groups** page, a **Device Count** column has been added to the table. The number in this column will link you to the **Device** page and display a list of only those devices in the group.

Deployment Status on Dashboard

The Edge Manager **Dashboard** now lists the last five deployments for each status (**Upcoming**, **Active** and **Completed**).

Redeploy Failed Packages

The ability to redeploy failed package deployments has been added to the **Deployments** tab on the **Operations** page. See [Redeploy Failed Packages \(page 69\)](#).

Retry Deployment on Timeout

When deploying a package, the **Retries** field will also apply to instances when the package deployment times out. See [Package Deployment \(page 59\)](#).

Certificate Expiry Filters

Two new Global Device Filters have been added:

- **Certificate Expiration Due (Days)** – how long until a device's certificate expires
- **Certificate Expired (Days)** – how long it has been since the device's certificate expired

Location Filters

Three new filters have been added to Edge Manager's Global Device Filters:

- Location City
- Location State
- Location Country

New Fields Added to Device Summary

Two new fields have been added to the Device Summary page:

- **Certificate Status** – displays the current status of the selected device's certificate. The options are **Unknown**, **Valid**, **Pending Renewal** and **Expired**.
- **Certificate Expires** – Displays the date and time when the device's certificate will expire.

Active Directory Integration

It is now possible to integrate Predix Edge Manager with your IDP using SAML.

Bug Fixes

This release contains the following bug fixes:

Link to Output for Executed Commands

The ability to view output from executed commands is now available from the **Commands** tab on the **Operations** page. Click the name of an executed command. If output is available for the command execution you will be able to either **view** or **download** it from the link in the **Output** column.

Errors When Deploying Intelligent Data Pump

Resolved an issue that would result in an "invalid signature" error when deploying the intelligent data pump to Edge devices.

Known Issues

This release has the following known issues:

No link for edited configurations

After deploying an edited configuration to a device, a link for the operation details is not created. All other deployments result in a link to the operation details being provided.

Execution time does not get updated

When you update a Docker container, the Execution Time in the Deployment Schedule does not get updated in Edge Manager. However, Start and End times are updated and displayed correctly.

Time for operations displayed differently

Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.

Software and configuration packages sometimes need to be re-deployed

If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and

needs to be restarted, then those software or configuration packages may need to be redeployed to that device.

Cannot delete groups with large number of devices

There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Release Notes 2.3.0

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

New Features/Enhancements

This release contains the following new features and enhancements:

AppHub

Predix Edge Manager can be configured to work with the AppHub service (*page*), allowing for custom micro-app integration. (BETA)

Edge Manager APIs (V1)

Edge Manager APIs have been made public to allow you to manage alerts, devices, packages, and BOMs, as well as execute commands on devices directly via RESTful API calls.

See API documentation [here](#).

Known Issues

This release has the following known issues:

No link for edited configurations

After deploying an edited configuration to a device, a link for the operation details is not created. All other deployments result in a link to the operation details being provided.

Browser Issues

On Firefox and Chrome browsers, there is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Firefox Workaround: Run Firefox in Safe mode to disable Firefox plug-ins.

Chrome Workaround:

1. Run Chrome in Incognito mode.
2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.

Execution time does not get updated

When you update a Docker container, the Execution Time in the Deployment Schedule does not get updated in Edge Manager. However, Start and End times are updated and displayed correctly.

Time for operations displayed differently

Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.

Software and configuration packages sometimes need to be re-deployed

If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.

Cannot delete groups with large number of devices

There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Release Notes 2.2.0

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

New Features/Enhancements

This release contains the following new features and enhancements:

Edge Analytics Framework

The Edge Analytic Framework gives the ability to compute near the device in order to offer benefits in performance, reliability and bandwidth. A preferred Analytic engine can now be uploaded and deployed to a device. Once the engine has been deployed it can be configured by sending down the actual analytic logic with the Analytic Template file, and a data mapping on the device with the Analytic Data Map file.

Custom Commands

Commands have been extended to allow execution against specific applications as well as the device, allowing for improved customization of edge devices. When creating a command, you can specify that the command is associated with an application. This allows the execution of commands within third-party applications deployed to a device.

Edge Manager External API

The Edge Manager External API exposes a set of API endpoints to be consumed by outside parties. This allows third parties to build applications and tooling that leverages the vast set of Edge Manager capabilities.

Predix Edge Native Commands

Extension of the System Commands available to all Predix Edge devices includes the following commands:

- Ifconfig
- top -b -n 0
- Set Polling Interval

Large File Transfer Support

The previous file size limit when uploading multi container applications was 500MB. This has been extended to 10GB.

Known Issues

This release has the following known issues:

No link for edited configurations

After deploying an edited configuration to a device, a link for the operation details is not created. All other deployments result in a link to the operation details being provided.

Browser Issues

On Firefox and Chrome browsers, there is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Firefox Workaround: Run Firefox in Safe mode to disable Firefox plug-ins.

Chrome Workaround:

1. Run Chrome in Incognito mode.

2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.

Execution time does not get updated

When you update a Docker container, the Execution Time in the Deployment Schedule does not get updated in Edge Manager. However, Start and End times are updated and displayed correctly.

Time for operations displayed differently

Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.

Software and configuration packages sometimes need to be re-deployed

If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.

Cannot delete groups with large number of devices

There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Release Notes 2.1.0

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

New Features

This release contains the following new features:

Additional Protocol Adapter for Data Pumps

The Intelligent Data Pump provides the ability to configure and move data from an asset on the edge to the cloud in order to process that data in the cloud (e.g., run applications, analytics, etc.).

The following protocol was added:

- Modbus: A more general purpose, less GE-focused protocol used across industry, specifically in water, wastewater, and general purpose DCS systems.

UI Re-design

Upgrade of the Edge Manager UI to the new Predix Design System. The upgrade of front-end components enables performance improvements across the application. It also keeps our theme consistent with other Predix Design System applications.

Known Issues

This release has the following known issues:

No link for edited configurations

After deploying an edited configuration to a device, a link for the operation details is not created. All other deployments result in a link to the operation details being provided.

Browser Issues

On Firefox and Chrome browsers, there is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Firefox Workaround: Run Firefox in Safe mode to disable Firefox plug-ins.

Chrome Workaround:

1. Run Chrome in Incognito mode.
2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.

Execution time does not get updated

When you update a Docker container, the Execution Time in the Deployment Schedule does not get updated in Edge Manager. However, Start and End times are updated and displayed correctly.

Time for operations displayed differently

Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.

Software and configuration packages sometimes need to be re-deployed

If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.

Cannot delete groups with large number of devices

There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Release Notes Q2 2018

These are the enhancements and known issues for Predix Edge Manager.

Q2 2018 29 June

This release contains the following:

Deployment Retry

When deploying software, configurations, and BOMs to devices, you can now specify a number for how many times to retry the deployment in case of deployment failure.

Predix Edge

You may see a **Predix Edge** option in the Predix Edge Manager user interface. Predix Edge is a beta feature that not all Predix Edge Manager tenants have access to. Contact [Predix support](#) with questions.

Q2 2018 Resolved Issues

This release contains the following resolved issues:

Duplicate group names

The issue where Predix Edge Manager allowed you to create groups with the same name as an existing group and attach it to the same parent, has been resolved going forward.

If there are existing groups with duplicate names, they remain as is. Any new groups you create cannot have duplicate names, and Edge Manager prevents you from moving a group to another parent group with a duplicate name.

Q2 2018 11 June Enhancements

This release includes the following enhancements:

Commands

- In the **Device Operations > Execute Command** window, commands are displayed as tiles.
- In the **Device Operations > Execute Command** window, you can search for commands.

Fast deployment

When the `uploadTaskStatusOnSubmitEnabled` flag is set to `true` in Predix Machine, poll intervals are skipped for fast deployment of packages.

For more information, see [Configuring Cloud Gateway](#) in the Predix Machine documentation.

Q2 2018 28 May Enhancements

This release includes the following enhancements:

Cancel Package and BOM Deployment

You can now cancel package and BOM deployments from the **Operations** page and device details page (from the **Configurations**, **Software**, and **BOM** tabs).

Commands

On the **Commands** page, you can choose to view commands in list view or tile view by clicking the corresponding icons in the top right of the page.



Q2 2018 30 April Enhancements

This release includes the following enhancements:

Logs are Sent as Part of the Status Detail Message

Predix Edge Manager checks logs sent from Predix Machine and, depending on how Predix Machine sends the logs to Edge Manager, now either displays the log file in Edge Manager when you click the link for the execution log, or downloads the execution log file.

Package Type Displayed

In the **Devices > Software** tab, there is a new column that displays the package **Type** (configuration, application, or container).

Q2 2018 Known Issues

This release has the following known issues:

Partial BOM Update

No link for edited configurations

After deploying an edited configuration to a device, a link for the operation details is not created. All other deployments result in a link to the operation details being provided.

Browser Issues

On Firefox and Chrome browsers, there is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Firefox Workaround: Run Firefox in Safe mode to disable Firefox plug-ins.

Chrome Workaround:

1. Run Chrome in Incognito mode.
2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.

Execution time does not get updated

When you update a Docker container, the Execution Time in the Deployment Schedule does not get updated in Edge Manager. However, Start and End times are updated and displayed correctly.

Time for operations displayed differently

Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.

Software and configuration packages sometimes need to be re-deployed

If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.

Cannot delete groups with large number of devices

There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Q1 2018

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

Predix Edge Manager Q1 2018 New Features

This release contains the following new features:

Partial BOM Deployments

When a BOM is updated and redeployed, packages specified in the BOM that are already installed on the device are skipped (not downloaded and deployed again). Only new packages are deployed to the device. The status of skipped packages is displayed as "installed" rather than "success."

This feature saves time and data when deploying BOMs.

Upload and Deploy Operating Systems

You can now upload operating systems to the Predix Edge Manager **Repository** and deploy the OS to devices. You can check the status of the OS deployment in the **Operations** and **Devices** (in the **Software** tab) pages.


New Commands

New commands to help the administrator troubleshoot various issues have been added. The new commands include:


- **run_dpkg** – Lists all packages installed on the device using system command dpkg.

 **Note:** This command is only for Linux devices that support dpkg.

- **run_ifconfig** – Runs the system command ifconfig on the device and returns the command output.

 **Note:** This command is only for devices that support ifconfig.

- **run_top** – Runs the system command top on the device for one iteration.

 **Note:** This command is only for devices that support top.

- **run_journalctl** – Queries the default system journal on the device using system command journalctl according to the filtering and formatting values specified in the command parameters.

 **Note:** This command is only for Linux devices that support journalctl.

- **refresh_device_detail** – Sends all device detail information in the next sync. This command overrides the Cloud Gateway's polling interval (`com.ge.dspmicro.cloud.gateway.pollingInterval`) and schedules a sync immediately.

See:

- [About Predix Edge Manager Commands \(page 73\)](#)

- Predix Machine Commands and Command Formats ([page](#)) documentation for details about these new commands.

Device Troubleshooting Page

There is a new Troubleshooting tab in the device detail page that displays CPU, memory, and disk usage for the device.

See [Troubleshooting Devices \(page 121\)](#).

Enhancements

This release contains the following enhancements:

Increased File Size Limit

When uploading files, or packages, to the Predix Edge Manager **Repository**, the size limit has increased to the following:

- 500 MB for configuration, application, and containers
- 15 GB for OS

Known Issues

This release contains the following known issues:

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox**: Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- When you update a Docker container, the **Execution Time** in the Deployment Schedule does not get updated in Edge Manager. Start and End times are updated and displayed correctly.
 - Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
 - You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.

- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Q4 2017

These are the new features, enhancements, and known and resolved issues for Predix Edge Manager.

Predix Edge Manager Q4 2017 New Features

This release contains the following new features:

Create Custom Alert Policies

You can now create your own customized time-based alert policies that override the default alert policies (provided by the Device Detail service) when applied to selected, or filtered, devices. See [Creating Policies for Alerts \(page 85\)](#).

Global Filters

When you enable global filters, you can apply filters on the Edge Manager dashboard, Device Manager, Operations, and Alerts pages, and the applied filter persists across all of those pages until it is cleared. This allows you to perform device operations on a filtered list of devices from any page that has a device list.

See [About Device Filters \(page 46\)](#).

Create and Save Filters

You can create and save your own custom filters for later reuse. See [Creating and Saving Filters \(page 50\)](#).

User Manager

There is now a "viewer" role, which allows the user assigned this role to have read-only access to all Edge Manager pages except User Manager. The "viewer" user can also create filters, apply filters, and download software packages from the Repository. See [About User Manager \(page 18\)](#).

Edge Manager APIs (Beta)

Edge Manager APIs have been made public to allow you to manage alerts, devices, packages, and BOMs, as well as execute commands on devices directly via RESTful API calls.

See API documentation at <https://em-api-apidocs.run.aws-usw02-pr.ice.predix.io/swagger-ui.html>.

This initial public release of Edge Manager APIs is in beta, and is subject to regular changes and improvements. Provide comments and feedback, and report issues by filing a support ticket at <https://www.predix.io/support/>.

Enhancements

This release contains the following enhancements:

Asynchronous File Upload

Asynchronous file upload allows file transfers that were interrupted, for example, by a network error, to automatically resume from the point at which the transfer was interrupted.

Perform simultaneous uploads

When you upload a file to the Edge Manager repository, the upload window shows the progress of the upload, and is non-blocking so that you can navigate to other pages in Edge Manager. You can also start another upload while the first one is in-progress as well as cancel an upload that is in-progress.

Connectivity Summary Includes Provider

The Device Summary page now displays the provider for SIM connectivity.

Changed Functionality

This release contains the following changes to functionality:

Password Policy

The password policy for Edge Manager is now enforced by the User Account and Authentication service. See (page).

Groups

Groups are no longer displayed in the upper left corner of Device Manager. You can now filter according to groups using the global filter feature. See [About Device Filters \(page 46\)](#).

Operations History

There is no longer an **Operations > History** page. Previously, this page was used for viewing and filtering operations. You can now use the global filters feature to perform

the actions previously performed on the **Operations > History**. See [About Device Filters \(page 46\)](#).

Known Issues

This release contains the following known issues:

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox**: Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- When you update a Docker container, the **Execution Time** in the Deployment Schedule does not get updated in Edge Manager. Start and End times are updated and displayed correctly.
 - Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
 - You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.

- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Predix Edge Manager Q3 2017

These are the enhancements, and known and resolved issues for Predix Edge Manager.

Important Announcements

Removal of OAuth Enrollment for Edge Manager and Predix Machine

Due to a recently identified security issue with OAuth enrollment, support for OAuth-based device enrollment in Edge Manager is being discontinued effective **August 22, 2017**. If you already have devices in Edge Manager that were originally enrolled using OAuth authentication, they will continue to function normally. However, if you have devices added to (but not yet enrolled in) Edge Manager with OAuth as the specified method of enrollment, you will be required to delete those devices.

You then have to add the devices to US-West Edge Manager, using [certificate enrollment](#).

In preparation for US-East retirement on September 15, 2017, you will not be able to add new devices to US-East Edge Manager tenants starting August 22nd due to a security issue.

Please contact [Predix Support](#) if you have more questions or concerns.

US-East ASV Edge Manager Retirement

Effective September 15, 2017, the Edge Manager instance in US-East will be retired. In preparation for the retirement, you will not be able to add new devices to Edge Manager tenants starting August 22nd due to a security issue.

Please contact [Predix Support](#) if you have questions, or follow these [instructions](#) to get access to US-West Edge Manager.

Known Issues

This release contains the following known issues:

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox**: Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- When you update a Docker container, the **Execution Time** in the Deployment Schedule does not get updated in Edge Manager. Start and End times are updated and displayed correctly.

- Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
- You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.

- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Edge Manager Q2 2017

These are the enhancements, and known and resolved issues for Edge Manager.

Enhancements

This release contains the following enhancements:

Device Manager

If a device has a SIM, the SIM ID is a clickable link that goes to the SIM details page.

Custom Device Model

You can now assign a default BOM when you create a custom device model so that when you add devices with this model in the future, the same default BOM is automatically assigned to the device, and will be deployed to the device when the it comes online.

See [Adding Custom Device Models \(page 56\)](#).

Repository

- You can now download software packages from the repository.

See [Downloading Software Packages from the Predix Edge Manager Repository \(page 99\)](#).

- If there are multiple versions of the software, you can view and select the versions from the Version column.

Resolved Issues

The following issues have been resolved in this release:

- The issue where the BOM did not have support for `.config` files is resolved.

Known Issues

This release contains the following known issues:

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox**: Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- When you update a Docker container, the **Execution Time** in the Deployment Schedule does not get updated in Edge Manager. Start and End times are updated and displayed correctly.
 - Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
 - You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.


- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Edge Manager Q1 2017

These are the new features and known and resolved issues for Edge Manager.

 **Note:** US West users must use Edge Manager with Predix Machine version 17.1.0 or later.

New Features

Edge Manager contains the following new features:

BOM Management

You can now define a BOM and upload it to Edge Manager. The BOM lists all the software packages and applications, with dependencies among them, that are installed on a GE Digital-provisioned device.

Edge Manager BOM management includes:

- Import a BOM to Edge Manager.
- The ability to install BOMs on devices.
- View a list of BOMs that are currently installed on the device.

For more information, see (page).

Alerts

You can now view and filter alerts for managed devices.

For more information, see (page).

Bluetooth and WiFi Status

You can now see Bluetooth and WiFi connection status for a device on the Device Details page.

For more information, see [Viewing the Device Summary \(page 30\)](#).

VPN Management

You can start and stop VPN management on a device using Edge Manager. You can also set the log verbosity for the VPN connection.

Time Zone Setting

Ability to select Local or UTC time as a global setting.

For more information, see [Setting the Time Format \(page 90\)](#).

Add Additional Notes for Packages


You can now add additional notes for packages when you upload them to the Edge Manager repository.

APM and Edge Manager Integration

Edge Manager integration with APM allows users with an APM tenant to use Edge Manager and vice versa.

With this new feature, you can enroll devices with Edge Manager and use the APM Time Series instance to ingest data. All users and devices in Edge Manager are separated by tenancy.

This feature works with both certificate and OAuth based enrollment.

 **Note:** For OAuth, when a device is created, the device ID must be unique across all tenants. If the device ID is not unique, adding the device causes an error.

 **Note:** Contact the [APM Service Ops team](#) to get a tenant provisioned.

Resolved Issues

The following issues have been resolved in this release:

- The issue where devices become unreachable in environments with a large number of devices has been fixed.

Known Issues

This release contains the following known issues:

BOM does not support .config files

BOM does not support .config. This means you cannot use BOM to upgrade a machine to new features.

Workaround: Upload configurations to Edge Manager as an “application” so the BOM can use it.

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox:** Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
 - You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.

- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Edge Manager 2016

Q4 2016

New Features

The following features have been added to Edge Manager.

Deployment Information

You can view information about the software and configuration deployments such as deployment and execution time and the result of the deployment.

Access to Execution Logs

You can use the **Commands** tab to access a detailed execution log for the device. See [Viewing Command History and Canceling Pending Commands for a Single Device \(page 81\)](#).

Device Details

The **Device Summary** page displays more details about the device, including:

- View details for the device including information about the device OS and model.

- Resource Usage information for the device, such as CPU, memory, and disk usage.
- Power Supply information for the device, such as power supply type, power supply status, and percentage of how full the power supply is.
- Health of device displays status, last status change, and up time for the device.
- Connectivity displays the number of SIM cards associated with the device and their status. Click the ICCID link to view details for the SIM card.
- OpenVPN displays client information for the device.

See [Viewing the Device Summary \(page 30\)](#).

Filtering

- Filter by name of filter, attributes, operator, and value.
- Create and save custom filters.
- Edit and delete filters.

Multi group selection

You can now select multiple groups.

Connectivity

The following features have been added to Predix Edge Manager Connectivity:

- Open VPN connection page displays details for VPN connections associated with registered devices.

For more information, see [VPN Management \(page 111\)](#).

Enhancements

Device Manager

- Topology view for groups

Limitations

This release has the following limitations:

Not all functionality is backward compatible

Deployment information, access to execution logs, device details, openVPN, and some attributes in Filter are not supported for devices that are running Predix Machine version 16.3.x or earlier.

Known Issues

This release contains the following known issues:

- Issues with Firefox And Chrome browsers:
 - There is a plug-in conflict that causes the browser to crash (GE internal only) when downloading a file, or when viewing the output of a command.

The same plug-in conflict causes an error when uploading a large file (hundreds of MB).

Workaround:

For **Firefox**: Run Firefox in Safe mode to disable Firefox plug-ins.

For **Chrome**:

1. Run Chrome in Incognito mode.
 2. In **Settings > Extensions**, if you have the DGExtension, ensure that it is disabled by unselecting the checkbox.
- Operations start, execution start, and elapsed time display differently for the top level versus operation details when there is only one operation. This is due to how the summary is calculated versus how the operation detail is calculated.
 - You can create groups with the same name as an existing group and attach it to the same parent.

Workaround: To avoid creating groups with duplicate names, verify that there are no existing groups with the same name.

- You cannot save a filter if the name has more than 63 characters.

Workaround: Use fewer than 63 characters in filter names.

- If a device is placed in inventory but not enrolled, and software or configuration packages are sent to that device, and one of the Edge Manager services fails and needs to be restarted, then those software or configuration packages may need to be redeployed to that device.
- There is a known issue with deleting a group with a large number (over 5,000) of devices. Do not create such large groups, or move devices incrementally out of large groups so you can delete the group.

Q3 2016

New Features

The following features have been added to Edge Manager.

Edge Manager

- From Edge Manager, you can start, stop, and delete Docker images on a device.

For more information, see [Managing Containerized Predix Machine \(page 35\)](#).

Device Manager

In **Device Manager > Devices**, you are now able to perform the following actions:

- Add custom device models to categorize the devices.

For more information, see [Adding Custom Device Models \(page 56\)](#).

- Add custom attributes for devices when adding devices.

For more information, see [Adding a Device to Predix Edge Manager \(page 24\)](#).

- Deploy Docker containers to devices.

For more information, see [Deploying Containers to Devices \(page 69\)](#).

User Manager

You can now edit user roles to add or delete roles associated with a user.

For more information, see [Editing Predix Edge Manager User Roles \(page 20\)](#).

Connectivity

The following features have been added to Predix Connectivity.

- You can now perform batch updates of the life cycle state and rate plan for SIM cards.

For more information, see [Performing a Batch Update \(page 110\)](#).

- Predix Machine can now detect the set of IPs on a device and call a special SIM API daily to detect changes of SIMs. This allows Predix Connectivity to associate SIMs with IPs passed-in with a device id.
- Diagnostic reports for the SIM card gives you information about provisioning or connectivity issues related to the SIM card.

For more information, see [Troubleshooting SIM Cards \(page 109\)](#).

- Alerts for SIM cards based on high and no usage are displayed on the SIM card summary page.

For more information, see [Viewing Details for a SIM Card \(page 108\)](#).

- Messages about cellular service provider maintenance appear on the Connectivity page.

Enhancements

The following enhancements have been added.

Commands

You can now execute commands for a single device on the device summary

Commands page.

For more information see [Executing or Canceling Commands for a Single Device \(page 80\)](#)

Dashboard

Dashboard is now the landing page for Edge Manager, which gives you an overview of your devices and their status.

Q2 2016

New Features

Device Manager

- Create, edit, and delete groups.
- Add and delete devices.
- View the device summary.
- Assign technicians to devices.
- Open an SSH tunnel to remote devices.
- Execute custom commands on multiple devices.
- Get the output for executed commands, including a descriptive error message in case of failure.

Repository

Add software packages – Allows you to add software packages to the cloud repository so you can deploy application, system, and configurations to devices on a managed schedule.

Commands

- Access and manage the default commands for devices.
- Create custom commands.

Connectivity

- Modify SIM states.
- Modify data- usage plans.
- Troubleshoot connectivity issues.
- View logs.

User Manager

- Add and delete users.
- Reset user passwords.
- Assign roles to users.

- Change passwords for users who are signed in.

Index

E

Edge Manager

8