



GE VERNOVA

EDGE SOFTWARE & SERVICES

PREDIX EDGE TECHNICIAN CONSOLE

User Guide

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, GE Vernova 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 GE Vernova. Information contained herein is subject to change without notice.

© 2024 GE Vernova and/or its affiliates. All rights reserved.

Trademark Notices

“VERNOVA” is a registered trademark of GE Vernova. “GE VERNOVA” is a registered trademark of GE Aerospace exclusively licensed to GE Vernova. The terms “GE” and the GE Monogram are trademarks of GE Aerospace, and are used with permission. All other trademarks are the property of their respective owners.

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

Contents

- Get Started with Predix Edge Technician Console..... iv
 - About Predix Edge Technician Console..... iv
 - Downloading and Running Predix Edge Technician Console..... v
 - Accessing Predix Edge Technician Console..... vi
 - Configuring Predix Edge Technician Console..... vii
 - Device Status..... ix
- Device Setup..... xi
 - About Device Setup..... xi
 - Configuring the Network and Proxy Settings..... xi
 - Configuring the Network Time Service..... xiv
 - Configuring SNMP..... xv
 - Updating the Host OS..... xvii
 - Device Reset..... xvii
 - Rebooting the Predix Edge OS VM..... xviii
- Device Monitoring..... xix
- Cloud Device Enrollment..... xx
 - About Predix Cloud Device Enrollment..... xx
 - Adding a Device to Predix Edge Manager..... xxi
 - Using Predix Edge Technician Console to Enroll Devices with Predix Cloud..... xxiv
 - Using Predix Edge Technician Console to Delete Enrollment Information from Devices with Predix Cloud..... xxv
- Application and Configuration Management..... xxvii
 - Applications Manager Page..... xxvii
 - Package Size Guidelines..... xxviii
 - Uploading Packages..... xxix
 - Deploying Packages..... xxx
 - Applying Configurations..... xxxi

Viewing Package Status.....	xxxii
Deleting Packages.....	xxxiv
Viewing Operations History for Applications and Configurations.....	xxxv
User Management.....	xxxvi
About User Management.....	xxxvi
Adding Users.....	xxxvii
Deleting Users.....	xxxviii
Logging.....	xxxix
About Device Logging.....	xxxix
Viewing Logs.....	xxxix
Secure Deployment Guide.....	xli
Introduction.....	xli
Required Firewall Rules.....	xli
NTP Server Configuration.....	xlii
Managing Access to Predix Edge Technician Console.....	xliii
Device Enrolment Best Practices.....	xliii
Monitor Your System.....	xliv
Predix Edge Virtual Machine Appliance	xliv
Predix Edge Gateway 3002.....	xliv
Edge Agent for Ubuntu.....	xlv
Other Platforms.....	xlvii
Troubleshooting.....	xlix
Troubleshoot Predix Edge Technician Console.....	xlix
Predix Edge Technician Console Release Notes.....	lii
Predix Edge Technician Console Release Notes 2.5.0.....	lii
Predix Edge Technician Console Release Notes 2.4.0.....	lii
Predix Edge Technician Console Release Notes 2.3.0.....	lii
Predix Edge Technician Console Release Notes 2.2.0.....	liv
Predix Edge Technician Console Release Notes 2.1.0.....	lv

Get Started with Predix Edge Technician Console

About Predix Edge Technician Console

Predix Edge Technician Console is an on-premise, local edge management UI to manage edge devices that may or may not have connectivity to the cloud. Predix Edge Technician Console provides the following capabilities:

- **Device setup and management**
 - Configure the network time protocol
 - Configure network settings including DNS
 - Upload and apply host OS updates
- **Application Management**
 - Upload and deploy packages
 - View application status
 - Start, stop, and delete applications on the device
 - Apply configurations to packages
 - View application details
- **Security**
 - Predix Edge Technician Console uses OAuth-based user authentication and authorization
 - Certificate-based device enrollment
- User management (Admin and Technician roles)
- **Full journal logging**
 - Query specific logs
 - Preview logs
 - Download logs

Supported Browsers

Predix Edge Technician Console has been tested for support on these browsers:

Brows-er	Version
Chrome	Last two ver- sions
Firefox	Last two ver- sions

Related information

About Predix Edge Technician Console (*on page*)

Downloading and Running Predix Edge Technician Console

About this task

Predix Edge Technician Console is bundled with Predix Edge and requires Predix Edge to run.

Procedure

1. Install Predix Edge for your operating system.
2. SSH into to the Predix Edge image and sign into Predix Edge using the default credentials:
 - user: root
 - password: root
3. To access Predix Edge Technician Console, find the assigned IP address of Predix Edge. If you are using the **Developer** image of Predix Edge, enter the following command:

```
ifconfig | grep inet
```

The IP address is displayed in the `inet addr` field in the "enp" section.

If you are using the **Production** image of Predix Edge, SSH is disabled, so you cannot access Predix Edge internally. To find the assigned DHCP address, you can use nmap to scan the IP range of the gateway to see what IP address is assigned to Predix Edge. To do this:

- a. Download nmap from <https://nmap.org/download.html>. and install it on the host machine.
- b. Enter the following command:

```
nmap ip_address_of_gateway/24
```

For example:

```
nmap 172.16.200.1/24
```

This scans all IP addresses on the subnet (0 to 255 on the last digit).

On VMWare Fusion, if you select **Share with my Mac**, the IP address of the gateway is the inet address of the vmnet8 device.

**Note:**

If you created a custom network, use that device instead.

On ESXi server, use the server address.

Related information

Installing Edge on Mac (*on page*)

Installing Edge on Windows (*on page*)

Installing Edge on ESXi (*on page*)

Accessing Predix Edge Technician Console

Use a Web browser to sign into Predix Edge Technician Console.

Before you begin

Predix Edge OS must be running to access the Predix Edge Technician Console.

Procedure

1. Open a Web browser and navigate to `https://<predix_edge_OS-ip-address>`

**Note:**

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

On Chrome, click **Advanced**, proceed to _____(unsafe).

On Firefox, select **Advanced > Add Exception > Confirm Certificate Exception**.

2. Enter your user name and password. If this is your first time logging into the Predix Edge Technician Console, use the following default credentials:
 - **User name** – admin
 - **Password** – admin
 - a. If this is your first time logging in, you are prompted to changed your password.
Enter:

- **Old password** – Enter your current password.
- **New Password** – Enter the new password.
- **Re-enter New Password** – Re-enter the new password.

To unmask the passwords, click **Show Passwords**.



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

- b. Click **Reset Password**.

After you reset the password, you have to sign into Predix Edge Technician Console again, using your new password.

You are signed into Predix Edge Technician Console, where the **Device Status** page is displayed. If you have not yet set up the device, some information is not displayed.

Related information

[About Device Setup \(on page xi\)](#)

Configuring Predix Edge Technician Console

If you do not want to use the default settings for Predix Edge Technician Console, you can configure certain settings by creating and deploying your own `settings.json` file.

About this task

Predix Edge Technician Console includes default configurations, so it is not necessary to create and deploy your own `settings.json` file unless you want to change certain default values.

When Predix Edge Technician Console starts, it checks for a `settings.json` file. If one exists, Predix Edge Technician Console parses the file and overwrites the default configuration parameters. If the file does not exist, Predix Edge Technician Console uses its default configuration parameters.

**Note:**

If you deploy a `settings.json` file, Predix Edge Technician Console continues to use the values set in that file until a new `settings.json` file is deployed, even if the default configuration values for Predix Edge Technician Console change on the backend.

Procedure

1. Create a file and name it `settings.json`.
2. Configure the parameters in JSON format, and save the file.

The following is an example `settings.json` file:

```
{
  "maxOSUpdateFileSizeMB": 500,
  "maxStagingAggregateSizeMB": 1000,
  "sessionTimeoutSeconds": 600
}
```

The following table contains information about the configurable parameters.

Parameter	Description	Default Value
<code>sessionTimeoutSeconds</code>	Maximum time Predix Edge Technician Console can be idle before the user is logged out. <ul style="list-style-type: none"> ◦ Default value is 900 seconds (15 minutes) ◦ Minimum value is 300 seconds (5 minutes) ◦ Maximum value is 3600 seconds (one hour) 	900
<code>maxStagingAggregateSizeMB</code>	Maximum allocation, in megabytes, that can be used for all staged config packages, prior to applying them to applications.	1000
<code>maxOSUpdateFileSizeMB</code>	Maximum file size of the OS update image that you can upload to Predix Edge Technician Console.	500

3. Deploy the configuration package.

You can deploy the configuration using Predix Edge Technician Console or Edge Manager.

**Note:**

When you apply a new configuration, Predix Edge Technician Console restarts and you are signed out. You will need to sign into Predix Edge Technician Console again.

Related information

[Applying Configurations \(on page xxxi\)](#)

Uploading Software and Configuration Packages to the Predix Edge Manager Repository (on page)

Deploying Configurations (on page)

Device Status

Use the Predix Edge Technician Console **Device Status** page to view information about the device, monitor the device, and edit settings.

When you sign into Predix Edge Technician Console, the **Device Status** page is displayed. This page displays information about the device and also allows you to perform certain actions.

Table 1. Device Information

Details	<ul style="list-style-type: none"> • Last Restart – Date and time the device was last restarted. • Model – Device model. • Processor – Processor installed on the device. • Number of Cores – Number of cores installed on the device. • Polling Interval – The time interval set to synchronize how often the edge devices communicate with Edge Manager in the cloud. • Operating System – The operating system running on the device. • Last Updated – Displays the date the host operating system was last updated.
Device	<ul style="list-style-type: none"> • ID – The device ID. • Container Enabled – Displays whether or not the device is container-enabled.
Date/Time	Displays the current time and time zone for the device, for example, UTC.
Summary	
Network	<p>This section displays information about the network settings, including DNS domain information and proxy settings.</p> <p>Click Edit to set up the device, or to change the network configuration settings.</p>
Time Service	<p>Configure the time servers to which the device will synchronize its time.</p> <p>Click Edit to configure the time service.</p>

Table 1. Device Information (continued)

Enrollment Info	<p>Displays enrollment status for the device.</p> <ul style="list-style-type: none"> • Enrolled – Status of device enrollment (yes, it is enrolled; no, it is not yet enrolled). • Enrollment Type – • Edge Manager URL – If the enrollment type is certificate, the Predix Edge Manager certificate enrollment URL is displayed.
Network Adapters	<p>Displays information about the network LAN adapters, including MAC address, IP address, subnet mask, and default gateway.</p> <p>Click Edit to configure the network and proxy settings (on page xi).</p>

Device Setup

About Device Setup

The Predix Edge Technician Console **Device Setup** page allows you to configure the network settings and time format for the device, as well as update the host OS.


Configuring the Network and Proxy Settings


Configure the network and proxy settings for the device to enable communication between the device and Predix Edge Manager.

Procedure

1. Sign into the Predix Edge Technician Console.
The **Device Status** page is displayed.
2. To go to the **Device Setup** page:
 - In the left navigation pane, click **Device Setup**, or
 - In the **Summary > Network** section, click **Edit**.
 The **Device Setup** page is displayed.
3. In the **Network** section, configure the network settings for the device.

Setting	Description	Configurations
Network Adapters	The network adapter settings are automatically populated with the IP address, subnet mask, and default gateway of the Edge OS.	Select: <ul style="list-style-type: none"> ◦ DHCP – select for dynamic host configuration protocol. The IP address for your device is automatically assigned by the server and not configurable by the Predix Edge Technician Console administrator. The IP address may change periodically, or when the device is restarted. MTU is configured with a default of 1500 bytes.

Setting	Description	Configurations
		<ul style="list-style-type: none">◦ Static – select if you are using a static IP address for the device. When using a static IP address, only the primary DNS server can be configured. MTU is configured with a default of 1500 bytes. <div data-bbox="1133 695 1421 1837" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"><p> Note:</p><p>When the IP address is changed, or when changing from Static to DHCP, a new tab will automatically pop up. If the popup blocker is enabled on your browser, a notification is displayed at the top of the browser to indicate that a popup has been blocked. You must disable the popup blocker to open the Predix Edge Technician Con-</p></div>

Setting	Description	Configurations
		<div data-bbox="1133 268 1419 373" style="border: 1px solid #0070c0; border-radius: 10px; padding: 5px; margin-bottom: 10px;">  sole in a new tab. </div> <ul style="list-style-type: none"> ◦ Disabled – select to disable a network adapter.
	Host-Level DNS	<ul style="list-style-type: none"> ◦ Primary DNS – primary host-level DNS server configuration. ◦ Alternative DNS – alternative host-level DNS server configuration.
	Dell 3002-specific settings	<p>For Dell 3002, the following conventions are recommended for network adapter configuration:</p> <ul style="list-style-type: none"> ◦ lan1 is intended for LAN use. ◦ lan2 is intended for WAN use. <p>It is recommended that you configure the gateway for lan2 (intended for WAN) only.</p>
DNS	The domain name servers are automatically populated with the primary and secondary DNS servers of the network Predix Edge OS is running on. This section contains all the host-level DNS server settings.	This section is view-only.
Proxy	If the network uses a firewall, enter the proxy server information.	<ul style="list-style-type: none"> ◦ HTTP – enter the HTTP proxy, for example: <div data-bbox="1143 1745 1386 1789" style="background-color: #f0f0f0; padding: 2px; margin-top: 5px;"> <code>http://<host>:<port></code> </div>

Setting	Description	Configurations
		<ul style="list-style-type: none"> ◦ HTTPS – enter the HTTPS proxy, for example: <div style="background-color: #f0f0f0; padding: 2px; margin: 5px 0;"><code>https://<host>:<port></code></div> ◦ No Proxy – enter the text for no proxy, for example: <div style="background-color: #f0f0f0; padding: 2px; margin: 5px 0;"><code><domain></code></div>

4. Click **Save**.

The **Save Settings** confirmation dialog box appears.

5. To proceed with saving the settings, click **Save and Restart**.

When you set, or reset, the proxy settings, Predix Edge Technician Console restarts and you are redirected to the sign-in screen.



Note:

Upon restart, a new IP address may be assigned if you are using DHCP.

Configuring the Network Time Service

Enter the NTP servers the device will poll to synchronize its UTC time.

Procedure

1. From the **Device Status** page, click **Device Setup** in the left navigation pane.
2. In the **Device Setup** page, click the **Time Service** tab.
3. In the **NTP** field, enter up to ten addresses for the time servers.

Typically, the device should be set up to poll at least three servers on different networks to get the most accurate time.

Use commas, spaces, or returns to separate multiple entries, for example:

NTP

```
0.pool.ntp.org,  
1.pool.ntp.org,  
2.pool.ntp.org,  
3.pool.ntp.org
```

4. Click **Save**.
5. (Optional) Click **Reset** to revert to the last saved configuration.

Configuring SNMP

You can use PETC to configure SNMP settings on your device.

Before you begin

Only an admin user can use PETC to configure SNMP. Other users can view the settings.

Supported MIBs and their definitions are listed here: <http://www.net-snmp.org/docs/mibs/>.

They include:

- HOST-RESOURCES-MIB
- SNMPv2-MIB
- UCD-SNMP-MIB

SNMPv3 is supported and described here: http://www.snmp.com/snmpv3/snmpv3_intro.shtml

About this task

Device health metrics from SNMPv3 standard MIBs will be available through SNMP for systems to poll from.

Procedure

1. From the **Device Status** page, click **Device Setup** in the left navigation pane.
2. In the **Device Setup** page, click the **SNMP** tab.
3. To enable SNMP, slide the Enable/Disable icon to the right.
4. Configure your SNMP settings.

- The first time you configure, you will need to set your authentication phrase and privacy phrase for the default user **edgeos-snmpd-user**.
- Optionally, you can change the authentication phrase and privacy phrase for the default user **edgeos-snmpd-user**

Setting	Description
Authentication Phrase	<p>(Optional) The SNMPv3 USM (User-based Security Model) authentication passphrase for the specified SNMPv3 user name for the authentication protocol.</p> <p>References:</p> <ul style="list-style-type: none"> ◦ http://net-snmp.sourceforge.net/tutorial/tutorial-4/commands/snmpv3.html ◦ https://docs.microfocus.com/NN-Mi/10.30/Content/Administer/nm-AdminHelp/nmAdm0100AboutSNMPv3.htm
Privacy Phrase	<p>(Optional) The SNMPv3 USM privacy passphrase for the specified SNMPv3 user name. This is the encryption passphrase to be used with the privacy protocol.</p> <p>References:</p> <ul style="list-style-type: none"> ◦ http://net-snmp.sourceforge.net/tutorial/tutorial-4/commands/snmpv3.html ◦ https://docs.microfocus.com/NN-Mi/10.30/Content/Administer/nm-AdminHelp/nmAdm0100AboutSNMPv3.htm
Reset	Reset your SNMP settings to their previously saved settings.

5. Click **Save** to submit your changes.
6. Verify that SNMP has been enabled on the **Device Status** page.

Results

You can now use SNMP for your device communication.

Updating the Host OS

You can update the Predix Edge OS in the Predix Edge Technician Console.

Procedure

1. To update Predix Edge in the **Device Status** page, you can either click **Update OS** or click **Device Setup** in the left navigation pane.
2. In the **Device Setup** page, click the **Host OS** tab.
3. Click **Upload OS Update**.
4. In the **Upload** dialog box, click **Choose File**, select the OS file, then click **Upload**.



Note:

Unpack the Predix Edge tar.gz image and use the signed software update file inside it (predix_edge_OS.swu.tar.gz or predix_edge_OS.swu, for example).



Note:

The OS update file must be packaged as a tar file (tar.gz) and has a size limit of 512 MB. For production environments, the OS image must be a GE-signed image and contain the installation script.

5. (Optional) Click **Cancel** to cancel the upload.
6. When the upload is complete, click **Apply Update** to update the operating system.
When you apply the update, the OS is updated and restarts. You will need to sign into Predix Edge Technician Console again once the OS restarts. The **Device Status** page displays the **Last Updated** date in the device **Details**.
7. (Optional) Click the trashcan icon to delete the uploaded OS update file if you do not want to apply the update.

Device Reset

From the Predix Edge Technician Console, you can perform a device reset of any connected device.

Before you begin

Only an admin user can see the **Device Reset** option and perform this operation.

Procedure

1. From the **Device Status** page, click **Device Setup** in the left navigation pane.
2. Click the **Utilities** tab.
3. Click the **Device Reset** button.

Predix Edge OS and the VM on which it is running restarts. This also restarts the Predix Edge Technician Console, which means you will need to sign in again.

4. Enter your password.

Results

This should reset all data on the Predix Edge device. It will reset the device to the currently installed operating system default, which is a fresh image of the current Edge OS version.

**Note:**

This operation does not perform a secure delete.

Rebooting the Predix Edge OS VM

From the Predix Edge Technician Console, you can reboot the VM on which Predix Edge OS is running.

Procedure

1. From the **Device Status** page, click **Device Setup** in the left navigation pane.
2. Click the **Utilities** tab.
3. Click **Reboot**.

Predix Edge OS and the VM on which it is running restart. This also restarts the Predix Edge Technician Console, which means you will need to sign in again.

Device Monitoring

Netdata is a real-time monitoring utility that has been incorporated into PETC for monitoring your devices. To see the Netdata dashboard (i.e., **System Overview**):

1. Sign into the PETC. The **Device Status** page is displayed.
2. Click the **Resource Monitor**.

As currently configured in PETC, the **System Overview** displays statistics for CPU, memory and disk usage.

As part of its monitoring function, Netdata will raise alarms when certain conditions are met. To see alarm details, click the **Alarms** button located in the top-right of the **System Overview** screen. The **Alarms** window has three tabs:

- **Active:** currently active alarms
- **All:** current settings that trigger an alarm condition; these thresholds are pre-configured by GE Digital and cannot be modified
- **Log:** a register of all alarms/status changes detected

Cloud Device Enrollment

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.

When the device is initially added to 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 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

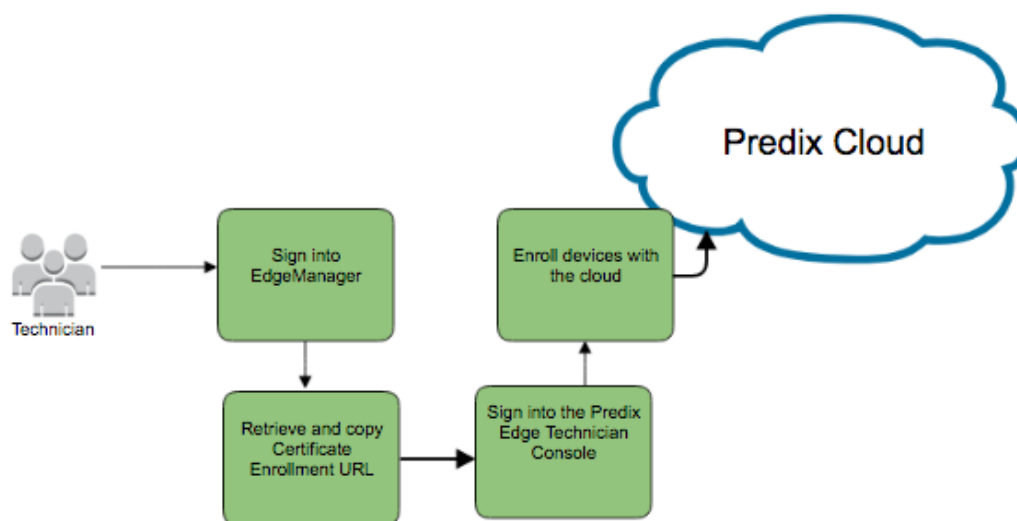
1. The administrator creates the technician user with the Technician role in Edge Manager, and provides the technician with Edge Manager login credentials.
2. The administrator or operator adds devices to Edge Manager and enters a shared secret for the device.

Technician Tasks

Task	Description
1. Login to Edge Manager and change password.	The administrator provides initial sign-in credentials and the URL to access 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.

Task	Description
	For Predix Edge Agent, see Using Predix Edge Technician Console to Enroll Devices with Predix Cloud (on page xxiv) .
4. Finish enrollment process.	The technician finishes enrolling the device with either Predix Edge Technician Console. This creates an identity for the device in the cloud.

Figure 1. Technician Workflow for Predix Edge Technician Console



Related information

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

[Predix Cloud Identity Management Service \(on page \)](#)

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


Adding a Device to Predix Edge Manager

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

Before you begin

Before a device that has Predix Edge or Predix Edge Agent installed can be enrolled and brought online, you must add the device to Edge Manager. This procedure is for adding a single device to Edge Manager. To add multiple devices, see [Importing a Device List](#) (on page [10](#)).

Procedure

1. Sign into 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. The device ID must be unique in a 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 Edge Manager, they are converted to lower-case.

**Note:**

Write down or copy your Device ID for use when enrolling the device with 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 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.

What to do next

Once you have added the devices to Edge Manager and assigned the technician, the technician can enroll them with Predix Edge 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 information

About Predix Edge Manager Groups (*on page*)

Viewing Devices in a Specific Group (*on page*)

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

Viewing the Device Summary (*on page*)

Importing a Device List (*on page*)

Edge Manager Predix Cloud Service Configuration (*on page*)

Using Predix Edge Technician Console to Enroll Devices with Predix Cloud

Before you begin

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

About this task

For devices running 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.

Procedure

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 Edge Manager.
 - **Certificate Enrollment URL** – URL of the Predix Edge Manager tenant. You can find the correct certificate enrollment URL in the 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).

Using Predix Edge Technician Console to Delete Enrollment Information from Devices with Predix Cloud

Before you begin

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

About this task

For devices running Predix Edge, with connectivity to Predix cloud, you can use the Predix Edge Technician Console to delete enrollment settings from the device in order to re-enroll the device.

Procedure

1. Sign into Predix Edge Technician Console.
2. In the **Device Setup** page, click the **Enrollment** tab.
3. Click **Delete Enrollment**.

A message displays with information about deleting enrollment: "This will delete enrollment settings so that the device can be re-enrolled. No other settings, files or deployed applications will be removed. This does not remove the device from Edge Manager."

4. Delete the device from Edge Manager.

Application and Configuration Management

Applications Manager Page

The **Applications Manager** page provides the access point for viewing uploaded and deployed applications, uploading applications, deploying applications, and deleting applications.

In the left navigation pane, click  **Applications Manager**.

Application List

The **Application List** section displays information about the uploaded packages that are available for deployment (staged), including name, size, and status. You can change the columns that are displayed by selecting and unselecting them in the **Actions** drop-down.

**Note:**

You cannot unselect all the columns—at least one must always be selected.

The **Actions** drop-down in this section allows you to:

- **Upload App** – Upload applications to Predix Edge Technician Console.

**Note:**

The default size limit of the repository for all uploaded packages is 1GB, but you can configure this value. See

- **Deploy** – Deploy application instances to the device.
- **Delete** – Delete staged packages. This does not delete deployed applications.

To delete deployed applications, use the **Delete** action in the **Deployed Instances** section.

Deployed Instances

The **Deployed Instances** section displays application instances that are deployed to the device and their statuses. The **Actions** drop-down in this section allows you to perform the following actions on deployed application instances:

- **Delete** – Delete deployed application instances with any of the following statuses:
 - Running
 - Stopped
 - Error

**Note:**

You cannot delete system containers (for example, predix-edge-technician-console and predix-edge-broker).

- **Start** – Start applications that have a status of "Stopped."
- **Stop** – Stop applications that have a status of "Running."
- **Apply Config** – Apply a configuration to an application with any of the following statuses:
 - Running
 - Stopped
 - Error

Related information

[Viewing Package Status \(on page xxxii\)](#)

[Uploading Packages \(on page xxix\)](#)

[Deploying Packages \(on page xxx\)](#)

Package Size Guidelines

Follow the guidelines in the table below for Predix Edge Technician Console package types and size limits.

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	

Package Type	Size Limit	File Type	Notes
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	


Uploading Packages

Upload applications to Predix Edge Technician Console so you can deploy them to the device.

Before you begin

You must create and package the application. If you are using the production version of Predix Edge OS, the application must be signed.

Procedure

1. In the left navigation pane, click  **Applications Manager**.
2. In the **Available Packages** section, select **Actions > Upload App**.
3. Click **Choose File** to browse for the package to upload.



Note:

Application packages must be packaged as `gzip` files and configurations as `zip` files. See the guidelines in [Package Size Guidelines \(on page xxviii\)](#).

4. (Optional) In **Name**, enter a name for the application.
If you do not enter a name for the package, it defaults to the file name.
5. Click **Upload**.
You are returned to the **Applications Manager** page, where a success message appears at the top of the page and the uploaded package appears in the **Available Packages** list with a status of "Uploaded." You can now deploy the package to the device.


Deploying Packages

Once packages are uploaded to Predix Edge Technician Console, they can be deployed to the device.

Before you begin

You must upload the package to Predix Edge Technician Console before you can deploy it to the device.

Procedure

1. In the left navigation pane, click  **Applications Manager**.
2. In the **Available Packages** section, select the package to deploy, then select **Actions > Deploy**.
3. In the **Deploy** dialog box, click **Deploy**.



Note:

If you have previously deployed a package with the same Application ID as the one you selected, you receive a warning message that the app already exists on the device and will be redeployed (rather than deployed).

You can proceed with redeploying the app; or enter a unique application ID to deploy a separate instance of the app if you want to run multiple instances of the same app on the device.

The package is deployed to the device and appears in the **Deployed Instances** section of the **Applications Manager** page. The package status updates as follows:

- a. Deploying
- b. Starting
- c. Running

Related information


[Uploading Packages \(on page xxix\)](#)

[Viewing Package Status \(on page xxxii\)](#)

Applying Configurations

You can use the **Applications Manager** page in Predix Edge Technician Console to apply configurations to applications.

Procedure

1. In the left navigation pane, click  **Applications Manager**.
2. In the **Deployed Instances** list, select the application to which to apply the configuration, then select **Actions > Apply Config**.



Note:

Configurations must be packaged as zip files, and do not have to be signed.

3. In the **Apply Configuration** dialog box, click **Choose File**, select the configuration to apply, then click **Upload & Apply**.

The application is stopped, and the configuration is applied. The status of the application changes as follows:

- a. Applying Configuration
- b. Starting
- c. Running

Packaging the Edge Application Configuration

If your application uses configuration files they must be packaged as a zip file to be deployed. Once deployed to an Edge device, these files will be available to your application in the `/config` mount within your app.

Procedure

1. Navigate to the folder containing your configuration files and zip them.



Note:

Zip only the actual files, not the folder that contains the files.

2. The following example assumes you have your config files in a folder named `my-config-folder` and all of the files end with a `.json` extension:

```
$ cd my-config-folder
$ zip -X -r config.zip *.json
```

You now have a packaged application configuration that you can deploy. You do not have to sign configuration files.

Viewing Package Status

You can use the **Applications Manager** page in Predix Edge Technician Console to view the status of uploaded and deployed packages.

Procedure

1. In the left navigation pane, click  **Applications Manager**.

The **Applications List** displays packages that are available to deploy to the device (staged), and application instances that are currently deployed to the device, and their respective statuses.

Table 2. Available Packages

Status	Description
Uploading	The package upload is in progress. When a package is uploaded very quickly, you may not see this status.
Uploaded	The package is uploaded to Predix Edge Technician Console and available to deploy to the device (staged).

In the **Deployed Instances** section, you can view the status of applications, as well as individual containers within applications, that are deployed to the device.

Table 3. Deployed Instances

Status	Description
Deploying	The package is in the process of being deployed.
Starting	The application is starting.
Running	The application is running on the device.
Stopping	The application is in the process of stopping.
Stopped	The application has stopped.
Redeploying	<p>The application is being redeployed. This status only occurs if you deploy an application instance that has already been deployed and use the same application ID (application name), rather than giving it a new, unique name.</p> <p>For example, if you deploy an app instance with the name "MyApp," then select the same "MyApp" app instance and click Deploy and do not give the app instance a unique name, it is considered to be redeploying, rather than deploying.</p>
Deleting	<p>The package deletion is in progress. Once deletion is complete, the package no longer appears in the Deployed Instances list. You can delete only packages that have any of the following statuses:</p> <ul style="list-style-type: none"> ◦ Running ◦ Stopped ◦ Error
Applying Configuration	<p>A configuration is being applied to the package. You can apply configurations only to packages that have any of the following statuses:</p> <ul style="list-style-type: none"> ◦ Running ◦ Stopped ◦ Error
Error	<p>An internal error occurred while the application was running. Click the Application ID to see the application details and the error message. If there were multiple errors, view the logs for the application.</p>

2. (Optional) You can view the status of individual containers within an application by clicking on the Application ID, which takes you to the application details screen.
3. Click **Refresh** to refresh the **Applications List**.


Related information

[Viewing Logs \(on page xxxix\)](#)

Deleting Packages

You can use the **Applications Manager** page to delete applications that are uploaded to Predix Edge Technician Console and packages that are deployed to the device.

Procedure

1. In the left navigation pane, click  **Applications Manager**.
2. To delete packages that are uploaded to Predix Edge Technician Console (staged):
 - a. In the **Available Packages** section, select the package to delete, then select **Actions > Delete**.
 - b. In the **Delete** confirmation dialog, click **Delete**.

The package is deleted from Predix Edge Technician Console and no longer appears in the Available Packages list.

**Note:**

This action does not delete deployed applications.

3. To delete deployed applications:
 - a. In the **Deployed Instances** section, select the package to delete, then select **Actions > Delete**.

**Note:**

Only applications with any of the following statuses can be deleted:

- Running
- Stopped
- Error

- b. In the **Delete Application** dialog box, click **Delete**.

The application status changes to "Deleting" and it is deleted from the device. After it is deleted, it no longer appears in the **Deployed Instances** list.

Viewing Operations History for Applications and Configurations

You can view history for edge apps and configurations in Predix Edge Technician Console.

Procedure

1. In the left navigation, click the **Logs** icon.
2. In Logs, search for Predix Edge Technician Console logs:
 - a. In **Search By**, select **App- Service Name**.
 - b. For App, select **predix-edge-technician-console** and select **PETC** for the Service.
 - c. Click **Update Preview**.

The log preview displays the last 20 entries.
3. Click **Download** to download the complete log.
4. Search the Predix Edge Technician Console log for “recording_history” to view records of operations history.

You can view the history for the following operations:

- Applying configurations
- Deploying applications
- Starting applications
- Stopping running applications
- Deleting running applications
- Details about the operation, including:
 - User who performed the operation
 - Date and timestamp for when the operation was performed


Related information

[Viewing Logs \(on page xxxix\)](#)

User Management

About User Management

Predix Edge Technician Console includes user management to create, view, and delete users.

To access **User Management**, click the user icon () in the left navigation.

The **User Management** screen displays the Predix Edge Technician Console users by user name and role in a table.

User Roles

You can create users with either the Administrator or Technician roles in the Predix Edge Technician Console. The following table shows the permissions each role has to access the available functionality.


Functionality	Admin- istrator	Tech- nician
Device setup functionality includes: <ul style="list-style-type: none"> • Device enrollment • View device information • Configure network and proxy settings for the device • Host OS updates • Reboot the Predix Edge OS virtual machine • Delete enrollment settings 	X	X
Application and configuration management: <ul style="list-style-type: none"> • View the application list and the status of deployed application instances • Start, stop, and delete deployed applications • Upload, deploy, and delete applications • Apply configurations 	X	X
Logging functionality includes: <ul style="list-style-type: none"> • Searching logs • Viewing logs • Downloading logs 	X	X

Functionality	Admin- istrator	Tech- nician
User management functionality includes: <ul style="list-style-type: none"> • Create users • Update users • Delete users 	X	

Adding Users

Add new users to Predix Edge Technician Console.

Procedure

1. Sign into Predix Edge Technician Console.
2. In the left navigation, click **User Management** ()
3. In the **User Management** page, click **Add User**.
4. In the **Add User** dialog box:
 - a. Enter the information for the user:
 - **User Name** – Enter a user name for the new user.
 - **New Password** – Enter a password for the user. The user will be prompted to change their password the first time they sign into Predix Edge Technician Console.



Note:

The password must meet the following requirements:

- Be between eight and fifteen characters long
- Contain at least one uppercase letter
- Contain at least two lowercase letters
- Contain at least two numbers
- Contain at least one special character

- **Re-enter New Password** – Re-enter the password.
- b. Select the role for the new user, then click **Add**.
 - **Technician**
 - **Administrator**

**Note:**

You can assign both the technician and administrator role to a user, but functionally, it is the same as the user just having the administrator role.

You are returned to the **User Management** screen, where you see the new user listed in the table.


Related information

[About User Management \(on page xxxvi\)](#)

Deleting Users

Delete a user from Predix Edge Technician Console.

Procedure

1. Sign into Predix Edge Technician Console.
2. In the left navigation, click the **User Management** icon (.
3. In the table, select the user to delete, then select **Delete User**.
4. In the **Delete User** confirmation dialog, click **Delete** (or **Cancel** to cancel the delete operation).

The user is deleted and you are returned to the **User Management** screen, where the user no longer appears in the table.

Logging

About Device Logging

Predix Edge Technician Console implements full journal logging to allow you to query and view logs in the console.

Logging is received from a variety of sources, such as kernel log messages, simple and structured log messages, and audit records. You can filter logs to view by date and time, as well as preset units of time, for example, the last six hours, or the last five minutes. You can also filter logs by component and process, or view only kernel messages. Additional options for viewing logs include by message priority, for example, Error or Debug.

Viewing Logs

In Predix Edge Technician Console, view the last 20 journal log entries and download the log files to view the full contents.

About this task

The preview pane in the **Logs** screen displays the last 20 journal log entries. You can apply filters to specify which logs to view.

Procedure

1. In the left navigation, click the Logs icon.
2. Apply the filters for the logs to view.

Date Range

By default, the time window for viewing logs is set to the last 24 hours. Click the calendar icon to select the date and time ranges to view. You can also select one of the pre-defined time intervals under **Presets**.

Search By

- **Component/Process** – (Optional) Enter the name of the process or component for which to display logs, for example, "NetworkManager." If you do not specify the component or process, logs for all components and processes are displayed.

You can preview logs for the following services:

- docker.service
- edge-agent-dispatcher.service
- edge-agent-gateway.service

- edge-agent-docker-init.service
- edge-agent-restapi.service
- edgeos-cfg-mnt-reload.service
- edgeos-init.service
- edgeos-machine-id-setup.service
- edgeos-data-mnt-init.service
- edgeos-data-expander.service
- edgeos-conf-reset.service
- edgeos-filesystem-expand.service
- **Show only Kernel Messages** – Typically, kernel messages are produced by the device drivers.
- **App – Service Name** – To view app service logs in PETC:
 - a. On the Logs module in PETC, under **Search by** select **App – Service Name**.
 - b. Select the app.
 - c. Select the Service Name for the app.

Additional Options

- **Message Priority** – View messages by log level, for example, Warning or Error.
Warning is the default. All logs with the specified priority and logs with higher priority are displayed. **Debug** is the lowest log level you can specify.
- **Boot Integer** – View logs for specified boot found in the journal. **1** represents the first boot found in the journal, subsequent boots are in chronological order (second boot is **2**, third boot is **3**, fourth boot is **4**, and so on). You can also enter a negative integer to view boots in reverse order, for example **-0** is the last boot recorded in the journal, **-1** is the second-to-last boot, and so on.

Output Options

Select the output options for the logs:

- **Display Timestamps in UTC** – The timestamps in the logs are displayed in the UTC time format. This is always enabled.
- **Format Output in JSON** – Formats the log as JSON.

3. Click **Update Preview**.

The last 20 log entries are displayed in the preview pane.

4. (Optional) Click **Download Log** to download the full contents for the log request.

The log is downloaded with the file name `PETC.1.log` file.

Secure Deployment Guide

Introduction

This section describes steps and considerations that end users of Predix Edge should be aware of to use the product in a safe and secure manner. As Predix Edge is an application platform and usage will vary situationally, this is not an exhaustive document, but provides guidance on some of the most important aspects of secure operation of the system.

Required Firewall Rules

A typical Predix Edge deployment involves connectivity to a variety of systems, including both assets at the customer location, and the Predix cloud environment where the corresponding Edge Manager instance is located. We recommend the application of a least-privilege based firewall policy within the installed environment to permit only required communications for typical operation. The Predix Edge virtual machine should be granted access to only those hosts required for their operation as a whitelist.

The table below lists the firewall rules required for Predix Edge. Note that only GE Digital-provided components and protocol adapters are listed, but firewall rules are required to be created only for the components used in the deployment. Additionally, either the customer or an approved third party may create custom adapters, which would likely require additional firewall rules. If this is the case, please consult with the application author to determine the requirements.

Table 4. Required Firewall Rules

Rule purpose	Direction	Protocol and Port
Edge device to Edge Manager	Outbound to External	HTTPS (TCP 443)
Cloud Gateway (to Predix Time-series)	Outbound to External	HTTPS/Web sockets (TCP 443)
Cloud Gateway (to Predix Event-Hub)	Inbound from Management	HTTPS (TCP 443)
PETC	Inbound from Management	HTTPS (TCP 443)
Modbus	Outbound to Control	TCP 502
OPC-UA	Outbound to Control	TCP 4840
OSI Pi	Outbound to Control	HTTPS (TCP 443)

Table 4. Required Firewall Rules (continued)

Rule purpose	Direction	Protocol and Port
EGD	Inbound and Outbound from/to Control	UDP 18246
MQTT	Outbound to Control	TCP 1883
MQTT over WebSockets	Outbound to Control	HTTPS/WebSockets (TCP 9001)
SNMP monitoring of the Edge device	Inbound from Control or External	UDP 161
NTP (if using external)	Outbound to External	UDP 123

**Note:**

- The “control” network refers to the local assets the Predix Edge device connects to; “external” is the path to the open Internet. The “management” network is ideally a local management network used for site administration functions, if available. If unavailable, please default to whatever network is considered most secure/restricted.
- EGD typically makes heavy use of multicast and broadcast traffic.
- All of the above mentioned port numbers are considered standard IANA assigned port numbers, however deployments may often use different port numbers due to operational considerations. Consult with a network engineer familiar with the site network if you are unsure.

When possible, we also recommend further restricting firewall rules for specific ports to required hosts only. For example, the Modbus rule should be further refined to allow the Edge device to communicate on port 502 to only those devices with which it is intended to communicate. In addition there are several IPS/IDS options available to restrict control network traffic via segmentation and inspection, such as [GE Digital's OpShield](#).

NTP Server Configuration

By default, the system is configured to use the following four servers for NTP:

- 0.pool.ntp.org
- 1.pool.ntp.org

- 2.pool.ntp.org
- 3.pool.ntp.org

Accurate time is required for the device to properly communicate with Edge Manager, for accurate logs, and for various other system behaviors to work as intended. If you are not able, or do not want, to use a public NTP server, please configure the device with time servers of your choosing. See [Configuring the Network Time Service \(on page xiv\)](#).

Managing Access to Predix Edge Technician Console

First logging into the Predix Edge Technician Console (PETC) is a requirement to perform device setup and enrolment. It also has an important security outcome, as until this point the device will have an insecure default username and password.

- user: admin
- password: admin

Upon first login, the user will be prompted to reset this to a new strong password. We recommend following general password hygiene practices when doing so. This includes using hard-to-guess passwords, and not reusing passwords from other accounts.

See the [instructions for the first login to PETC \(on page vi\)](#).

We also recommend each person have their own account, rather than sharing credentials for a single account among multiple people. It is also good practice to promptly disable or remove users who have departed the organization. See the [instructions for managing users within PETC \(on page xxxvi\)](#).

Device Enrolment Best Practices

The following are considerations when [adding enrolment information \(on page xxi\)](#) for a new Edge device.

- Be descriptive when selecting Device IDs and use optional fields such as Group or Description when possible. This information may assist you later in triaging issues (security or maintenance) as they arise.
- When defining a shared secret, avoid simple or reused secrets. Although this secret is used only at the time of enrolment, using unique and complex secrets will minimize the chance of an attacker being able to impersonate a device after it is added to an Edge Manager instance, but before enrolment is completed. This is particularly important when performing bulk enrolment operations via the device list import [\(on page \)](#).

Monitor Your System

Consult the PETC [instructions for using journal-based logging \(on page xxxix\)](#) or the equivalent page for collecting logs from Edge Manager (on page).

It is recommended you set up your Edge appliance to publish system statistics via SNMP. See [Configuring SNMP \(on page xv\)](#).

Predix Edge Virtual Machine Appliance

VMware ESXi and vSphere Hardening and Patch Management

The currently supported production platform for Predix Edge virtual machines is VMware vSphere/ESXi 6.5 and 6.7. As with any software platform, we recommend keeping your deployment up to date with the latest updates from VMware, in accordance with an overall vulnerability management process.

We recommend following the steps in the [VMware hardening guides](#).

Production and Development VM Images

Two variants of the virtual machine image are available: production and development. Only the production image should ever be used in production/deployment scenarios.

There are several features that differ between the two images that are optimized for security (for production) or ease of use (for development).

Though not an exhaustive list, some important differences include:

- Production images require all Predix Edge applications to contain a valid signature, whereas development images do not enforce application signatures, allowing potentially malicious applications to be run.
- Production images have SSH disabled, whereas development images allow logging into the system with the insecure account (user: root/password: root) in addition to the developer RSA key pair.

Predix Edge Gateway 3002

Default Network Settings

As described in the product overview (*on page*), this device is equipped with two ethernet ports. Please note the default settings for each port, LAN1 is PoE and defaults to a static IP of 192.168.100.2, and LAN2 is DHCP by default. The Predix Edge Technician Console (PETC) is available only via LAN1.

The intended use of each port can be described in terms of LAN and WAN, Purdue Levels, etc., but the idea is that LAN1 is placed on the more restrictive network to segregate access to PETC as much as is possible.

Outbound traffic will be routed to the appropriate outbound physical port, but should also be taken into consideration when creating firewall/IDS/ACL rules.

Physical Security

Note that physical access to a Predix Edge Gateway may allow an attacker to bypass some or all security controls. Please ensure that the environment the device operates in is sufficiently secured from intruders, as is appropriate to the situation.

Unsupported IO Devices

Note: The following hardware IO are not supported:

- Bluetooth
- ZigBee
- WiFi
- CANBus
- MicroSD storage
- USB peripherals, including mass storage devices

Edge Agent for Ubuntu

Edge Agent for Ubuntu has considerable flexibility as compared to the Predix Edge Gateway 3002 and the VM Appliance. With this flexibility are additional responsibilities for maintaining a secure system. A comprehensive guide to these are beyond the scope that can be covered here, however, the following are some key points to consider.

**Note:**

To install Edge Agent for Ubuntu, see [Installation](#) (*on page*).

Differences From Other Edge Devices

- The Predix Edge Technician Console (PETC) is not supported on Ubuntu, and as such, advice related to PETC is not applicable to this system. This also means the internal API that drives PETC is not present.
- SNMP is not installed as a dependency of Edge Agent for Ubuntu. It is recommended that another performance monitoring solution be added.
- Edge Agent for Ubuntu does not benefit from any of the log management improvements added to Edge OS through journald and syslog. It is recommended to add a log streaming/management capability to the system, either through Edge Manager Custom Commands (with System Builder Commands), or some other third-party tool.
- There is no hard distinction between Production and Development images as there is for the VM. Code signing is enabled by default, but can be disabled for development purposes by editing `/etc/edge-agent/agent-data.json` and changing `"enforce_signing":true` to `false`. It is highly recommended that code signing be left on in any production setting. Refer to the Application Signing (*on page*) instructions for more information on getting an Edge Application signed by GE Digital.

Restricting Access to Docker the Edge Agent User

Access to `eauser`, the user that the Edge Agent runs as, should be highly restricted. This is because `eauser` is highly privileged (effectively root). Similarly any user with access to running docker should be understood to be highly privileged as this will allow the user to not just impact the availability/integrity of Edge applications, but of the system as a whole.

It is recommend as much of your device administration as possible be performed through Edge Manager, and only using CLI level access to Edge Agent as a last resort to minimize this risk. This goes hand in hand with having good user management practices in general, to avoid unintended access to support/admin accounts.

Building a Minimal System

Edge Agent for Ubuntu will install a minimal set of dependencies, and is able to remotely deploy additional software via `apt`. However it is good practice to reduce the amount of software installed to the system in general. Each additional software package brings not just its own set of risks to the system, but also those inherited from its full dependency tree. In particular, caution should be exercised when adding new network listening code, or anything that elevates privileges.

There is often a wide variety of tools on Linux for any given job. Selecting the right one can be hard, but when in doubt, favor software that is well vetted, minimal to the required task, and still actively supported by the vendor.

It is also worth recommending that any software that does not need access to the root system could instead be turned into an Edge Application. This allows the application to benefit from all of the security boundaries built into the Edge Application framework, such as chroot, apparmor, seccomp, and code signing.

Monitoring for Updates

Unlike other Edge platforms, the onus is on the user to maintaining an up-to-date system. It is important to stay informed of not just security updates from GE Digital, but also Ubuntu, and any other third-party software you add to the system.

It is recommended to subscribe to receive the latest [security updates](#) directly from Ubuntu.

Additional Resources For Ubuntu Security

- Ubuntu provides a cross version matrix of [security features](#). Each feature comes with an explanation and information for digging deeper into that topic, which is useful for designing an approach to various aspects of the system, such as filesystem encryption or configuring a firewall.
- The United Kingdom's National Cyber Security Centre (NCSC) has released a [hardening guide for Ubuntu](#) that covers topics in greater depth.

Other Platforms

Predix Embedded System Developers or Custom Devices

The Predix Edge stack is available to be licensed, integrated, and modified to fit the use case of other businesses. If you are using such a device, please consult with the producer of that custom device, as this information may be incorrect or incomplete.

VMware Fusion and Workstation

VMware Fusion and Workstation are excellent choices for a convenient, laptop friendly development solution for developing Predix Edge applications. However, they are not suitable for real-world production use, and as such, are not in scope of this document.

Raspberry Pi

The Raspberry Pi image provided by GE Digital is infrequently updated and not suitable for use as a production system. The image is intended to be used only for prototyping, learning, and demonstration purposes.

Troubleshooting

Troubleshoot Predix Edge Technician Console

The following are general issues you may experience when using Predix Edge Technician Console.

Device Appears Offline in Edge Manager After Enrolling in Predix Edge Technician Console

If you successfully enroll the device in Predix Edge Technician Console, and the device still displays a status of “offline” in Edge Manager after a few minutes, verify the following:

- In the Predix Edge Technician Console **Device Status** page, verify the UTC time displayed is correct. If the UTC time displayed for the device is not the correct current time, check the [NTP settings \(on page xiv\)](#).
- [Check your proxy settings \(on page xi\)](#).
- Check the network connectivity from the device. If there is not network connectivity, the device correctly displays an “offline” status.

Cannot Connect to Predix Edge Technician Console

If you cannot connect to Predix Edge Technician Console, check the following:

Verify that Predix Edge OS is Running

To run, Predix Edge Technician Console must be able to communicate with Predix Edge OS.

Verify the IP Address

If you are using the dynamic host configuration protocol (DHCP), the assigned IP address of Edge OS may change periodically, or when the device is restarted. Verify you are using the current assigned IP address to reach Predix Edge Technician Console. If you are using the development image of Predix Edge, you can check the IP address you should use by logging into Predix Edge OS, and entering the following at the command line:

```
ifconfig
```

The currently assigned IP address is returned.

If you are using the production version of Predix Edge, use the nmap option to find the IP address.

|

Error enrolling: Invalid device

When you enter the device information in the **Enroll Device** dialog box, and click **Enroll**, you receive the following error:

```
Error enrolling: Invalid device
```

Cause

The device ID you entered does not match the information entered when the device was added to Predix Edge Manager.

Solution

Contact the admin or operator to verify the correct device ID.

Error enrolling: Unauthorized device

When you enter the device information in the **Enroll Device** dialog box, and click **Enroll**, you receive the following error:

```
Error enrolling: Unauthorized device
```

Cause

The shared secret you entered does not match the shared secret that was entered when the device was added to Predix Edge Manager.

Solution

Contact the admin or operator to verify the correct shared secret.

Error enrolling: Failed to connect to Edge Manager

When you enter the device information in the **Enroll Device** dialog box, and click **Enroll**, you receive the following error:

```
Error enrolling: Failed to connect to Edge Manager
```

Cause

The certificate enrollment URL you entered for the device is incorrect.

Solution

Verify you are using the correct certificate enrollment URL:

1. Sign into Predix Edge Manager.
2. In the left navigation pane, click **Settings**.
3. Copy the **Certificate Enrollment URL**.
4. Paste the certificate enrollment URL into the **Enroll Device** dialog box.

Also check to verify the proxy settings are entered and correct in the **Device Setup > Network** settings.

Error enrolling: Device with ID <ID> attempted enrollment, but...

When you enter the device information in the **Enroll Device** dialog box, and click **Enroll**, you receive the following error:

```
Error enrolling: Device with ID <ID> attempted enrollment, but it has already been online
```

Cause

The device has already been enrolled and had its identity established with the cloud.

Solution

You do not need to enroll this device.

Failed to enroll device <device_id>; reason: Forbidden

When you enter the device information in the **Enroll Device** dialog box, and click **Enroll**, you receive the following error:

```
Failed to enroll device <device_id>; reason: Forbidden
```

Cause

This can happen when the system time is not working correctly (for example, NTP servers are not available).

Solution

- Update the NTP servers in Predix Edge Technician Console.
- On the **Device Status** page, verify the time appearing in the **Current Time** field is correct.

Predix Edge Technician Console Release Notes

Predix Edge Technician Console Release Notes 2.5.0

These are the new features and known and resolved issues for the 2.5.0 release of the Predix Edge Technician Console (PETC 1.2).

Enhancements

Maximum Transmission Unit (MTU) Configuration

The ability to set a value for MTU has been added to the setup of Network Adapters within the Predix Edge Technician Console (PETC). MTU configuration is available in both DHCP and Static modes; the default value is 1500 bytes.

Predix Edge Technician Console Release Notes 2.4.0

These are the new features and known and resolved issues for the 2.4.0 release of Predix Edge Technician Console (PETC 1.2).

Known Issues

Timestamp Not Updated After OS Upgrade

After upgrading Predix Edge OS via Predix Edge Manager, the **Last Updated** timestamp in PETC will not be updated. Within Edge Manager you can verify a device's currently installed version in the field **OS Version** (Select **Device Manager > Devices** and then the device name to see the **Summary** page).

Successful Factory Reset Returns Failure Message

After performing a factory reset via PETC, an error message will pop up indicating the operation **Failed to reset device**; however, the factory reset will have been successful.

Predix Edge Technician Console Release Notes 2.3.0

These are the new features and known and resolved issues for the 2.3.0 release of Predix Edge Technician Console (PETC 1.2).

New Features

Predix Edge Technician Console (PETC) will ship as part of the Predix Edge images with the following new capabilities:

- Support for Dell Edge Gateway 3002 device:
 - The following conventions are recommended for network adapter configuration: LAN1 is intended for LAN use; LAN2 is intended for WAN use. It is recommended to configure the gateway for LAN2 (intended for WAN) only; do not configure the gateway for LAN1 (intended for LAN).
 - PETC will be accessible on static IP address 192.168.100.2 on LAN1 only.
- Configure SNMPv3 settings.
- Reset the device.
- Configure secondary DNS setting.
- Disable network interface.
- View polling interval.
- View MAC Address for each network adapter.

Input Validation for NTP Configuration

User input validation of the NTP configuration and additional details in the PETC UI about the NTP configuration:

- Maximum of 10 addresses allowed in the NTP setting.
- The user's session may be invalidated and the user logged out if the NTP server time differs by more than 5 minutes.

Known Issues

This release contains the following known issues:

Reset Password Page Re-direct

Users might be re-directed to the reset password page instead of the login page when they reset their user password.

Workaround: Open PETC again in a new tab and navigate to https://<EDGE_IP>

NTP Error Tooltip

When an invalid NTP address is set in the NTP configurations, there is an error tooltip. That error tooltip might cover other modals in the UI (e.g., save/reset modals).

Firefox Log Out

When a user tries to log out of PETC in Firefox, it fails.

Workaround: Use Google Chrome, or clear cookies in Firefox.

Password Reset

You cannot reset your password via the PETC UI. To reset a user's password, a PETC admin user should delete the user and re-create it.

Simultaneous Operations

PETC does not support concurrent administrative requests. Doing an operation which modifies the state of Predix Edge should be performed from only one browser at a time. Otherwise, the results are unpredictable. Examples of such operations include a host update and applying a configuration to an application.

Predix Edge Technician Console Release Notes 2.2.0

These are the new features and known and resolved issues for the 2.2.0 release of Predix Edge Technician Console (PETC 1.2).

New Features

This release contains the following new features:

Input Validation for NTP Configuration

User input validation of the NTP configuration and additional details in the PETC UI about the NTP configuration:

- Maximum of 10 addresses allowed in the NTP setting.
- The user's session may be invalidated and the user logged out if the NTP server time differs by more than 5 minutes.

Support for Underscores

Support has been added for underscores in application/service names/IDs.

Disallowed Actions for System Containers Disabled

Actions that are not allowed on system containers are now disabled when a system container is selected.

Defect Fixes

This release contains the following defect fixes:

Accessibility of User Management Module

The user management module should always be accessible for PETC Admin users.

Duplicate Services

Remove duplicate services in the Logs module.

Certificate Issue

Fixed certificate issue that may prevent you from connecting to multiple Predix Edge consoles on the same browser. With this fix, you may have to manually refresh the PETC browser tab the first time after a Host OS upgrade.

Known Issues

This release contains the following known issues:

Firefox Log Out

When a user tries to log out of PETC in Firefox, it fails.

Workaround: Use Google Chrome, or clear cookies in Firefox.

Password Reset

You cannot reset your password via the PETC UI. To reset a user's password, a PETC admin user should delete the user and re-create it.

Update Host OS

If you are not redirected to the PETC login page within five minutes of applying a host OS update in PETC from Predix Edge 2.0.x, please refresh your browser.

Simultaneous Operations

PETC does not support concurrent administrative requests. Doing an operation which modifies the state of Predix Edge should be performed from only one browser at a time. Otherwise, the results are unpredictable. Examples of such operations include a host update and applying a configuration to an application.

Predix Edge Technician Console Release Notes 2.1.0

These are the new features and known and resolved issues for the 2.1.0 release of Predix Edge Technician Console.

New Features

This release contains the following new features:

Edge application management

Manage edge applications in Predix Edge Technician Console, including the ability to:

- Upload and deploy applications
- Start, stop, and delete applications running on the device
- View the status of applications, and drill down into a details view to also view the status of the application's containers and services
- Query for edge application service logs

See [Applications Manager Page \(on page xxvii\)](#)

Configuration Management

Manage configurations in Predix Edge Technician Console, including the ability to upload and apply configurations to edge apps running on the device.

See [Applying Configurations \(on page xxxi\)](#) and [Uploading Packages \(on page xxix\)](#)

Reduced footprint

The Predix Edge Technician Console footprint has been reduced by over 90%.

Configurable Settings

Configurable settings from within PETC include host OS update file upload size limit, max aggregate staging space for multi-container app file uploads, user session timeout, and device model name.

View history

You can now view the history audit trail of user operations in Predix Edge Technician Console app logs.

Perform remote operations

You can now perform the following operations from Predix Edge Technician Console:

- Reboot Edge

See [Rebooting the Predix Edge OS VM \(on page xviii\)](#)

- Delete enrollment information from the device

Raspberry Pi 3+

Support for Predix Edge Technician Console is now available on Raspberry Pi 3+.

Known Issues

This release contains the following known issues:

NTP Settings

If a user configures NTP settings via PETC, the user session may be invalidated and logged out if NTP server time differs by more than five minutes.

Password Reset

Users cannot reset their password via PETC UI. To reset a user's password, a PETC admin user should delete the user and re-create it.

Update Host OS

If you are not redirected to the PETC login page within five minutes of applying a host OS update in PETC from Predix Edge 2.0.x, please refresh your browser.

Application IDs

When deploying an application to PETC's Application Manager, please do not include any underscores (_) in the application ID.

Log Retrieval

When selecting an application service to retrieve logs, duplicate services may be listed in the dropdown menu. Please disregard this as these duplicates will yield the same result.

Simultaneous Operations

PETC supports consecutive requests. Multiple simultaneous operations on applications are not supported.