FIELD AGENT^{TM}

USER MANUAL

EMERSON™

Contents

Warning & Caution Notes as Used in this Publication

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury to exist in this equipment or may be associated with its use.
In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Caution

Caution notices are used where equipment might be damaged if care is not taken.

Notes: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

Chapter 1: Overview

1.1 Applicable Products

Table 1:

Product Family	Catalog Number	Description	Provisioning Connection	Data Source Connection	Cloud Connection
Mini Field Agent (MFA)	ICMFA000000	Field Agent as a standalone appliance for connecting to external data sources.	Ethernet LAN	Ethernet LAN	Ethernet WAN
	ICMFA002US0 ICMFA002EU0	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning.	Ethernet LAN Wi-Fi hotspot with U.S./Canada or European country code and frequencies per catalog number	Ethernet LAN	Ethernet WAN
	ICMFA001US1 ICMFA001UM1 ICMFA001EU1 ICMFA001AU1 ICMFA001AE1	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning and optional private cellular cloud connection on AT&T®.	Ethernet LAN Wi-Fi hotspot with country codes and frequencies per catalog number	Ethernet LAN	Ethernet WAN AT&T private cellular network in various countries per catalog number
	ICMFA001US0 ICMFA001UM0 ICMFA001EU0 ICMFA001AU0 ICMFA001AE0	Field Agent as a standalone appliance for connecting to external data sources. Includes optional Wi-Fi hotspot for provisioning and optional cellular cloud connection on customer-provided network.	Ethernet LAN Wi-Fi hotspot with country codes and frequencies per catalog number	Ethernet LAN	Ethernet WAN Cellular network in various countries per catalog number using customer-provided SIM.
Embedded Field Agent (EFA)	IC695CPE400	Field Agent embedded in an Industrial Internet Control System running PACSystems*.	Ethernet WAN in Configuration Mode only	Virtual LAN through hypervisor Ethernet WAN	Ethernet WAN
Virtual Field Agent (VFA)	ICVFA000000	Field Agent as a virtual machine image.	Virtual LAN1 through hypervisor Virtual LAN2 through hypervisor	Virtual LAN1 through hypervisor Virtual LAN2 through hypervisor	Virtual WAN through hypervisor

1.2 Field Agent Architecture

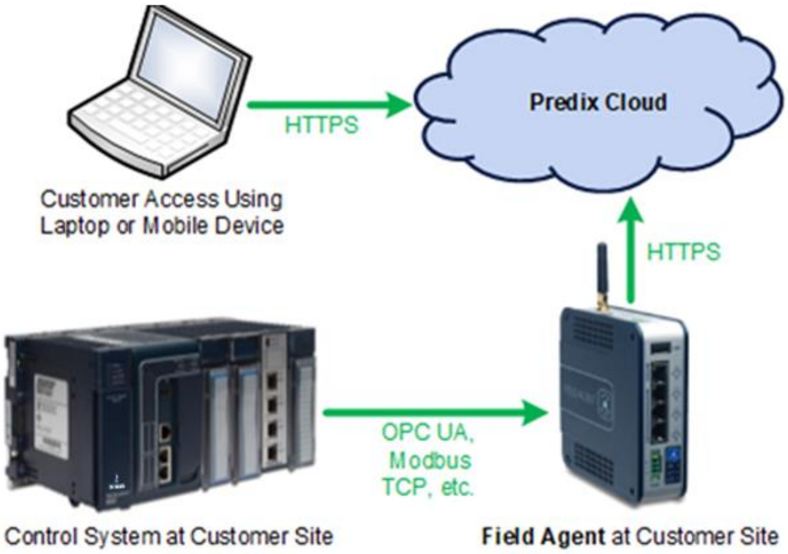
The goal of Field Agent technology is to connect industrial machines to the Predix® Cloud, so that asset owners can receive insights and optimization for their equipment. Field Agents connect and transmit this data securely. Operators can then visualize the performance of their assets and enable predictive analytics. Armed with this valuable information, operators can optimize equipment uptime. OEMs can proactively maintain and service their equipment fleet, improving operations, growing service revenues and winning new business. Asset owners can evolve past a break-fix model and implement predictive analytics to minimize unplanned downtime.

Emerson has developed a family of Field Agent devices to address the challenges of communicating equipment data. A Field Agent has two primary functions:

- Collecting and transmitting machine data securely
- A platform for running applications at the edge

Once a Field Agent is up and running, data is transferred from the plant to the cloud over encrypted channels, preserving its time stamp, quality, and fidelity. It also provides a rich domain application environment for edge processing, so logic can be executed at the most appropriate place in the architecture — locally on the machine or in the cloud.

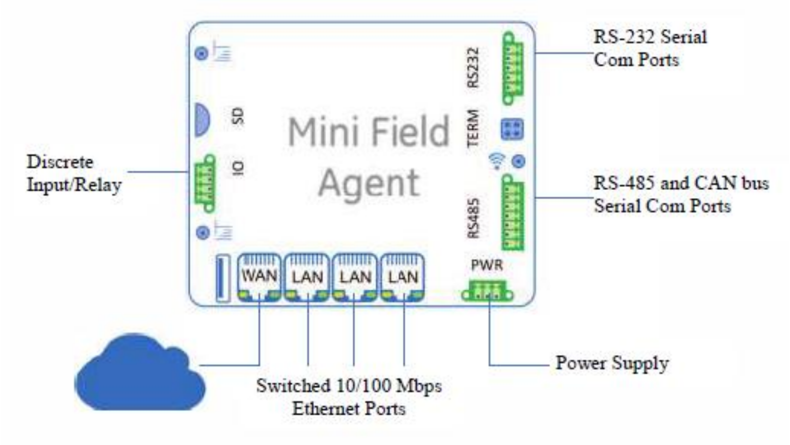
Figure 1: Field Agent Architecture



1.3 Mini Field Agent (MFA)

The Emerson Mini Field Agent^{TM} (MFA) module is a Machine to Cloud collector that securely forwards data to a Predix® Time Series Database Service. The MFA is based on the ARM architecture and designed to meet low power, harsh environment specifications for industrial use. It runs an embedded Linux® operating system and comes with Predix Machine pre-integrated and ready to enroll in Predix Edge Manager. The Field Agent ecosystem enables end users ease of developing Predix solutions using the MFA platform. The following figure depicts the typical installation of an MFA. Section 5.6, Configure the Network, provides defaults IP addresses.

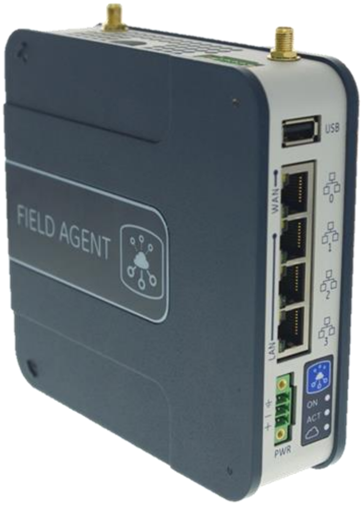
Figure 2: Mini Field Agent Connections & Ports



Features

- Predix Machine
- One Wide Area Network (WAN) Ethernet port
- Three Local Area Network (LAN) Ethernet ports with built-in switch
- RS-485 hardware interface
- RS-232 hardware interface
- CAN bus hardware interface
- One discrete input
- One relay contact
- Optional cellular modem
- Optional Wi-Fi hotspot

Figure 3: MFA Unit



1.3.1 MFA Specifications

Note: *For the latest information, refer to the webpage at https://www.emerson.com/Industrial-Automation-Controls/support.*

<table>
<tr><th>Specification</th><th colspan="3">Description</th></tr>
<tr><td>Processor</td><td colspan="3">TI AM3352 32-bit ARM processor, 800MHz</td></tr>
<tr><td rowspan="2">Memory</td><td colspan="3">512MB DDR3 RAM</td></tr>
<tr><td colspan="3">2GB on-board flash</td></tr>
<tr><td>Ambient Temperature, Humidity</td><td colspan="3">-40°C to 70°C (0°C to 70°C ATEX), 5 to 95% non-condensing
Use above 55°C requires installation in a restricted access location</td></tr>
<tr><td>Real Time Clock Battery</td><td colspan="3">Battery backup for RTC, 6 years</td></tr>
<tr><td>USB Port</td><td colspan="3">USB 2.0</td></tr>
<tr><td>SD Card Slot</td><td colspan="3">One MicroSD card slot</td></tr>
<tr><td>Wi-Fi (Optional)</td><td colspan="3">2.4GHz Wi-Fi, regional settings determined by catalog number</td></tr>
<tr><td rowspan="7">Cellular (Optional)</td><td colspan="3">LTE Cellular Modem, regional settings determined by catalog number</td></tr>
<tr><td>Region</td><td>4G LTE Bands</td><td>3G WCDMA Bands</td></tr>
<tr><td>U.S./Canada</td><td>2, 4, 5, 7, 12, 13, 25, 26</td><td>2 (1900 MHz), 5 (850 MHz)</td></tr>
<tr><td>EU</td><td>1, 3, 7, 8, 20</td><td>1 (2100 MHz), 8 (900 MHz)</td></tr>
<tr><td>Australia/New Zealand</td><td>1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, 41</td><td>1, 5, 6, 8, 9, 19</td></tr>
<tr><td>Oman</td><td>1, 3, 7, 8, 20</td><td>1 (2100 MHz), 8 (900 MHz)</td></tr>
<tr><td>UAE</td><td>1, 3, 7, 8, 20</td><td>1 (2100 MHz), 8 (900 MHz)</td></tr>
<tr><td rowspan="2">Ethernet Ports</td><td colspan="3">One unswitched Ethernet port, 10/100 Mbps</td></tr>
<tr><td colspan="3">Three switched Ethernet ports, 10/100 Mbps</td></tr>
<tr><td rowspan="3">RS-232</td><td colspan="3">One RS–232 Serial Port (pluggable screw terminal)</td></tr>
<tr><td colspan="3">Maximum cable distance is 15m</td></tr>
<tr><td colspan="3">Maximum communication rate is 115.2 kbps</td></tr>
<tr><td rowspan="3">RS-485</td><td colspan="3">One RS–485 Serial Port (pluggable screw terminal)</td></tr>
<tr><td colspan="3">Maximum cable distance: 305 m (1000 ft)</td></tr>
<tr><td colspan="3">Maximum communication rate: 115.2 kbps</td></tr>
<tr><td rowspan="3">CAN bus</td><td colspan="3">One CAN port (pluggable screw terminal)</td></tr>
<tr><td colspan="3">Maximum cable distance is 40 meters</td></tr>
<tr><td colspan="3">Maximum communication rate is 1 Mbps</td></tr>
</table>

Specification	Description
Discrete input	1 x 24 V opto-coupled / isolated input, 10 mA nominal. Minimum ON = 1.4µs Maximum OFF = 28 µs Hipot tested to 1202 Vdc (equivalent of 925 Vrms)
Relay contact	1 x Output relay, DC (Form A normally open relay contact, 30W switching power) 30 Vdc, 1A Hipot tested to 1202 Vdc (equivalent of 925 Vrms)
Operating System	Embedded Linux built using the Yocto Toolchain
Operating voltage	9 to 30 Vdc, nominal 24 Vdc
Power consumption	4 Watts (167mA@24Vdc) without cellular modem (ICMFA000000, ICMFA002xxx)
	8.4 Watts (350mA@24Vdc) with cellular modem (ICMFA001xxx)
Housing dimensions	5.53 x 5.33 x 1.55 inches (140.5 x 135.3 x 39.4 mm)
Mounting	DIN rail or panel mount
Certifications	Refer to Section 2.8, Agency Certifications and Standards.
Operational Vibration	IEC 600068-2-6 10-57Hz, 0.012"ppk displacement 57-500HZ, 2.0g acceleration
Operational Shock	IEC 60068-2-27 15g, 11ms (sine wave)
Mean Time Between Failures	ICMFA000000: 415,750 hours (47.46 years)
	ICMFA001xxx: 396,295 hours (45.24 years)
	ICMFA002xxx: 404,734 hours (46.20 years)
Security Features	On-board Trusted Platform Module
Protocols	Modbus TCP, OPC UA (built in) Other protocols can be added using Machine Adapters or the Predix Machine SDK.
3-pin power plug	Wire sizes: 22 to 16 AWG (0.34 to 1.5 mm²); Screw torque: 2 in-Ib (0.23 N-m)
	Temperature rating for copper wire: 80 °C
	Wiring to power input terminals shall be limited to 30 meters in length

1.4 Embedded Field Agent (EFA)

The Emerson Embedded Field Agent (EFA) is available on the CPE400 controller, which is part of the PACSystems* family of products. It comes with Field Agent software including Predix Machine pre-integrated and ready to enroll in Predix Edge Manager. While the EFA is essentially configured the same way as an MFA, there are different Application and Configuration templates provided for the EFA. For instance, because the EFA has more memory and a higher-performance CPU compared to the MFA, it can retain more “Store and Forward” buffered data in the event of temporary loss of communications to the cloud. Therefore, the Store and Forward configuration files for the MFA and EFA are different.

1.4.1 PACSystems IC695CPE400 RX3i Rackless CPU w/ Field Agent

The CPE400 EFA uses the EFA Port (found on the underside of the CPE400 unit) to connect to the Predix Cloud. It uses an internal virtual NIC to communicate with the controller to gather data. The CPE400 also contains a display, which is described in the EFA HW Instructions portion of this document. For more information about the CPE400 itself, refer to the PACSystems RX7i & RX3i CPU Reference Manual, GFK-2222Y or later.

1.5 Virtual Field Agent (VFA)

The Emerson Virtual Field Agent (VFA) is a Virtual Machine. It contains Predix Machine to allow streaming data to the cloud or running applications locally. It also incorporates User Interfaces for configuring networks and time synchronization, getting Field Agent Product and OS Updates, and checking status and running commands. While the VFA is essentially configured the same way as an MFA or EFA, there are different Application and Configuration templates provided for the VFA, because these templates are associated with a specific version of Predix Machine.

1.6 Revisions in this Manual

Rev	Date	Description
J	Sep 2019	• Following Emerson's acquisition of this product, changes have been made to apply appropriate branding and registration of the product with required certification agencies. No changes to material, process, form, fit or functionality.
H	Jul-2018	• VFA Release 1.3.0 • EFA Release 1.3.0 • Added Event Hub Service support.
G	Jun-2018	• MFA Release 1.3.0 • Added Predix Machine 17.2 On-demand Events. • Updated performance based on use of Tape, instead of H2, for store & forward.
F	Jul-2017	• EFA 1.1.0
E	Jun-2017	• MFA 1.1.0; Predix Machine 17.1; Added MFA cellular and Wi-Fi support.
D	Apr-2017	• Added Virtual Field Agent
C	Feb-2017	• Added Embedded Field Agent
A	Oct-2016	• MFA 1.0.1; EdgeManager updates
-	Aug-2016	• Original issue.

1.7 Related Documentation

Field Agent Manuals

Field Agent Secure Deployment Guide	GFK-3009
Field Agents Upgrade Guide	GFK-3017
Field Agents Registration Guide	GFK-3018
Field Agent Machine Adapters User Guide	GFK-3019

RX3i Manuals

PACSystems RX3i System Manual	GFK-2314
PACSystems RX3i Ethernet Network Interface Unit User's Manual	GFK-2439
PACSystems RX3i Serial Communications Modules User's Manual	GFK-2460
PACSystems RX3i DNP3 Outstation Module IC695EDS001 User's Manual	GFK-2911
PACSystems RX3i IEC 104 Server Module IC695EIS001 User's Manual	GFK-2949

PACSystems Manuals

PACSystems RX7i, RX3i and RSTi-EP CPU Reference Manual	GFK-2222
PACSystems RX7i, RX3i and RSTi-EP CPU Programmer's Reference Manual	GFK-2950
PACSystems RX7i, RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual	GFK-2224
PACSystems TCP/IP Ethernet Communications Station Manager User Manual	GFK-2225
C Programmer's Toolkit for PACSystems	GFK-2259
PAC Machine Edition Logic Developer Getting Started	GFK-1918
PAC Machine Edition Process Systems Getting Started Guide	GFK-2487
PACSystems RXi, RX3i, RX7i and RSTi-EP Controller Secure Deployment Guide	GFK-2830
PACSystems RX3i & RSTi-EP PROFINET I/O Controller Manual	GFK-2571

The most recent documentation is available on the Emerson support website https://www.emerson.com/Industrial-Automation-Controls/support.

1.8 Product Landing Pages

Product	URL
Mini Field Agent	https://www.emerson.com/Industrial-Automation-Controls/support
CPE400 with Embedded Field Agent	
Virtual Field Agent	

Chapter 2: MFA Hardware Instructions

2.1 Internal Components

⚠CAUTION

The only user-serviceable components in the Mini Field Agent are the Real Time Clock Battery and cellular SIM card.

Do not remove or alter any other components in the Mini Field Agent.

The MFA module is shipped with a battery pre-installed. The battery holder is located below the Supercap and can be replaced by opening the top cover.

To replace the battery

1. Power OFF the MFA Module.
2. Wait for 1 minute.
3. Open the top cover by loosening the four screws on the edges.
4. Use a small flat-head screw driver to gently pry out the old battery.
5. Insert the new battery.

⚠ WARNING

Replace battery only with Rayovac BR2032 or part IC690ACC001B or later. Use of another battery may present a risk of fire or explosion.

Battery may explode if mistreated. Do not recharge, disassemble, heat above 100 °C (212 °F), or incinerate.

The MFA module has an optional cellular modem. The SIM is available as a pre-installed option or may be installed by the customer. The SIM card holder is located underneath the cellular modem and can be installed by opening the top cover and removing the cellular modem.

To install a SIM Card

1. Power OFF the MFA Module.
2. Wait for 1 minute.
3. Open the top cover by loosening the four Philips-head screws along the edges.
4. Remove the cellular modem by removing the two screws, tilt the modem up and slide out of the connector.
5. Slide the SIM card holder latch toward the Open position and flip it open.
6. Slide the SIM card into the holder so that the contacts will face down when closed and with the notched end extending out of the holder.
7. Close the SIM card holder and slide the latch to the Locked position.

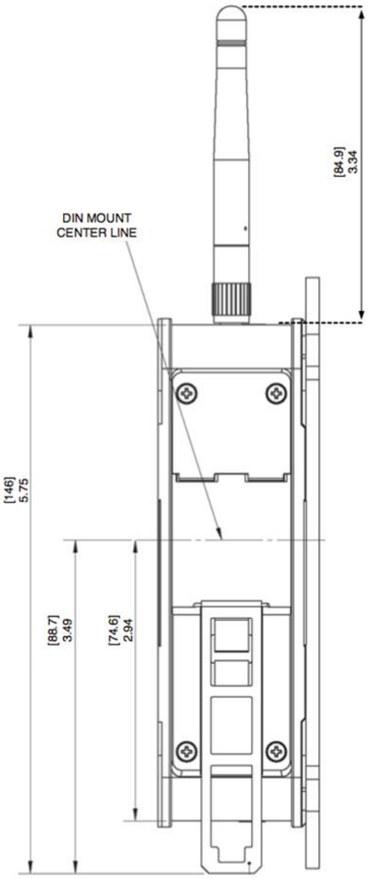
2.2 Installation

There are two different mounting options for the MFA: DIN-Rail Mount or. The ICMFAACC001 MFA Panel Mounting Kit is required to use the Panel Mount option. After mounting the MFA, connect it to the facility network using standard Ethernet cables. The LAN interface should be connected to the local area network containing one or more industrial devices. The WAN interface should be connected to a network with access to the Internet.

2.2.1 DIN-Rail Mount

The MFA comes equipped with a DIN Rail mounting clip as displayed in the following figure. For DIN Rail mounting, pull the clip down and lock it in place. Place the unit on the DIN rail, and then push the clip up to secure it. The optional panel mounting plate should not be attached because it will prevent DIN rail mounting.

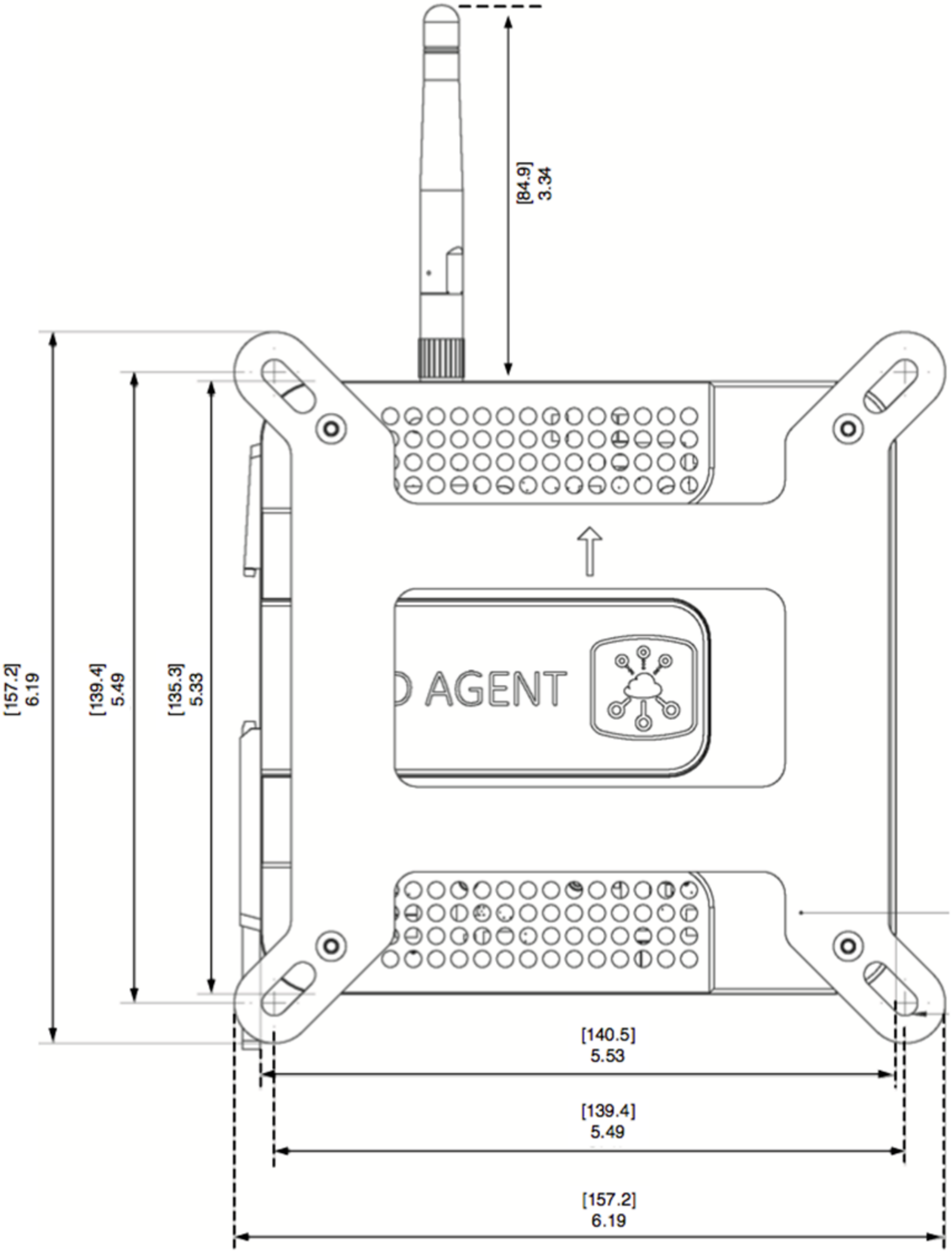
Figure 4: DIN-Rail Mounting of MFA Unit



2.2.2 Panel Mount

To panel-mount the MFA module, attach the ICMFAACC001 panel mount plate to the side of the MFA module using the four Torx M3 screws included with the mounting kit. Attach the panel mount plate in the orientation as displayed in the following figure. The screw size for each panel mount tab is recommended to not exceed M5.

Figure 5: Panel Mounting of MFA Unit

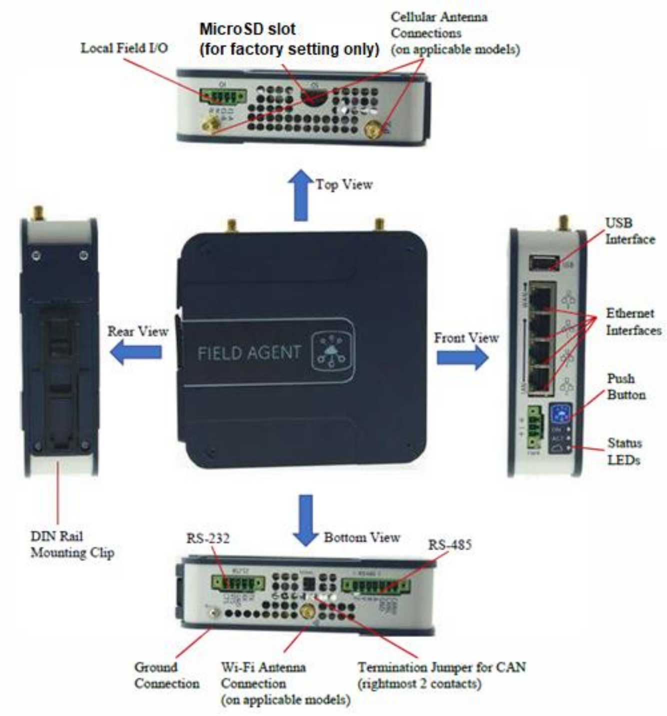


2.3 MFA Interface Details

Note: *Refer to the Mini Field Agent (MFA) Important Product Information, GFK-2997, for version-specific interface details*

Figure 6 shows the top, bottom and side views of the MFA Unit, and the connection points on each.

Figure 6: View of MFA Connection Points



2.3.1 Power Requirements

The MFA is powered by a DC Power Supply (9 to 30 Vdc, nominal 24 Vdc). Power for the MFA shall be provided by a Class II power supply marked as "double insulated", Limited Power Source (LPS), or a SELV source with a minimum 32 Vdc listed fuse with 3 A max rating. Power for the relay output and discrete input shall be provided by an isolated source.

⚠CAUTION

Reversing input power polarity might cause damage to the MFA.

The IC690PWR024 (Selectable 115/230Vac input, 24Vdc @ 5A Output) DIN-rail mountable power supply meets the power requirements of the MFA.

The ICMFAACC002 is rated for 85-264 Vac @ 47-63 Hz input and features an IEC-60320-C8 inlet plug for attachment of the AC power cord. The ICMFAACC002 may be adapted to local power by using a desktop computer-style AC power cord (with an IEC-60320 C7 connector on one end and an AC main plug suitable for the outlet provided, on the other).

⚠CAUTION

The use of the ICMFAACC002 in permanent installations shall be in accordance with the National Electric Code (NEC), the Canadian Electric Code (CEC), and/or with the authority having jurisdiction.

2.3.2 Grounding

There are two ground connections on the Mini Field Agent. One is located on the front power connector and the other is a chassis screw located on the bottom of the unit. BOTH grounds must be connected to earth ground to comply with CE performance requirements. Ground wires should be kept as short as possible and tied to a common cabinet/equipment ground point. It is recommended to use #14AWG stranded wire for the chassis ground.

2.3.3 Pin Definitions

Refer to Figure 6 for the physical location of each connector and pin.

Table 2: Pin Definitions

Connector	Function	Pin Number	Description
PWR	Power connector (9 to 30 Vdc)	1	Ground
		2	Negative Voltage
		3	Positive Voltage
IO	Normally Open relay contact output, 30 Vdc, 1 A resistive load	1	K1-A
		2	K1-B
	+24 Vdc Opto-coupled Input, 10 mA	3	IN+
		4	IN-
CAN bus	Serial	1	CAN_H
		2	CAN_L
RS-485	Serial	3	Ground
		4	A /RX
		5	B /CTS
		6	Y /TX
		7	Z /RTS
RS-232	Serial	1	TX
		2	RX
		3	GND
		4	RTS
		5	CTS

2.4 Network Configuration

Refer to Figure 6 for the physical locations of the LAN and WAN Ethernet interfaces.

The default WAN and LAN IP addresses of the Mini Field Agent are:

Table 3:

Item	WAN	LAN
IP Address	Obtain using DHCP	192.168.1.100
Subnet Mask	Obtain using DHCP	255.255.255.0
Gateway	Obtain using DHCP	Not set

WAN connects to the uppermost RJ-45 connector.

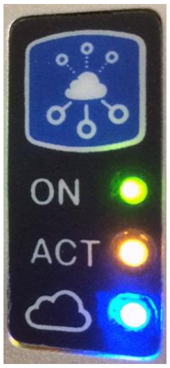
LAN connects to the three lower RJ-45 connectors and these are switched internally.

2.5 Push-Button and LEDs

The front panel of the MFA contains a blue push-button and three indicator LEDs. The LEDs exhibit different behaviors depending on whether the push-button is being depressed, or not.

In normal operation, when the push-button is not being depressed, the LEDs behave as follows.

Figure 7: MFA Front Panel



ON LED:

- Blinking green indicates Predix Machine is starting.
- Solid green indicates Predix Machine is running. The ON LED must be solid before attempting to connect to the Predix Machine Web Console over wired Ethernet or the Wi-Fi hotspot.
- Slowly fading in and out indicates the MFA is in Configuration Mode.

ACT LED:

- Blinking orange indicates that data is being received from a configured Machine Adapter.

Cloud LED:

- Blinking blue indicates Predix Machine is not connected to the Predix Cloud.
- Solid blue indicates Predix Machine is connected to the Predix Cloud.

The push-button is depressed in order to enable or disable Configuration Mode, perform a graceful reboot of the MFA, or perform a factory reset. Initiating each function depends on how long the button is held before being released. These features and the corresponding impact on the LED behavior are documented in Section, 2.6, Push-Button Operations.

Each of the four RJ-45 Ethernet connectors contains two LEDs.

- The green LED, when illuminated, indicates an Ethernet connection has been established.
- The yellow LED, when illuminated, indicates presence of packet traffic.

2.6 Push-Button Operations

- The push-button on the front of the Mini Field Agent (Figure 7) is used for the following activities based on how long the push-button is held and released. Each time interval that corresponds to an operation has a unique fast blink pattern that indicates releasing the push-button at this time will perform an operation. In between these time intervals, all LEDs blink slowly. Releasing the push-button during a time interval when all LEDs are blinking slowly or when the push-button is held for 30 or more seconds will result in no operation and the LEDs will return to their normal behavior, as described in Section 2.5, Push-Button and LEDs.

Time Interval the Push-Button is Held and Released	LED Behavior	Operation upon Release
< 5 seconds	Normal LED Behavior	None
5 – 9.9 seconds	Green ON LED fast blink	Configuration Mode
10 – 14.9 seconds	All LEDs slow blink	None
15 – 19.9 seconds	Green ON and Orange ACT LEDs fast blink	Reboot
20 – 24.9 seconds	All LEDs slow blink	None
25 – 29.9 seconds	All LEDS fast blink	Factory Reset
30+ seconds	Normal LED Behavior	None

2.6.1 Configuration Mode

If the push-button is released during the specified time interval, the Mini Field Agent will enable Configuration Mode. In Configuration Mode, a Wi-Fi hotspot is enabled that can be used to enroll the Mini Field Agent in Predix EdgeManager and read device diagnostics using an iPhone® app. While in Configuration Mode, the green ON LED fades in and out slowly. The orange ACT LED and the blue Cloud LED will both continue to operate normally according to the state of the Mini Field Agent.

Configuration Mode can be disabled by repeating the same steps taken to enable it, or by waiting one hour for Configuration Mode to automatically disable. When Configuration Mode is disabled, the LEDs will return to their normal behavior described in Section 2.5, Push-Button and LEDs. Security considerations for the Wi-Fi hotspot can be found in the Field Agents Secure Deployment Guide, GFK-3009.

Wi-Fi Hotspot Property	Value
SSID	mfa_<7-digital serial number> (e.g. mfa_td7s0sx)
Encryption Type	WPA2-PSK
Password	Printed on MFA label
Router IP Address	192.168.2.1
Router IP Subnet Mask	255.255.255.0
Number of Concurrent Client Connections	2
Client IP Address Assignment Range	192.168.2.20 - 192.168.2.21
DHCP Lease Duration	1 hour
Maximum Enabled Duration	1 hour

The GE Energy Connections Field Agent Manager iPhone app is available to Emerson Employees on the Emerson App Store. When using the Field Agent Manager iPhone app to enroll or configure a Field Agent, the wizard instructs the user to enable Configuration Mode using the push-button and connect to the Wi-Fi hotspot in the iPhone's Settings page before proceeding with enrollment.

2.6.2 Reboot

If the push-button is released during this time interval, the Mini Field Agent will perform a graceful reboot and will return to normal operation.

2.6.3 Factory Reset

If the push-button is released during this time interval, the Mini Field Agent will perform a factory reset. This operation will take several minutes, after which the Field Agent will reboot. Once the green ON LED is solid it will be possible to log into the Predix Machine Web Console and configure the Field Agent.

⚠CAUTION

On the first boot following a factory reset, Predix Machine will generate cryptographic keys used for communication. It is critical that the Mini Field Agent not be powered down during these operations to prevent key corruption. If key corruption occurs, a subsequent factory reset will be required.

Do not power cycle the Mini Field Agent on the first boot after a factory reset until the green ON LED is solid.

2.7 Field Agent Sales Catalog

2.7.1 Emerson MFA Orderable Items

Table 4: MFA Catalog Numbers

Catalog Number	Description
ICMFA000000	Mini Field Agent
ICMFA001US0	Mini Field Agent with Cellular and Wi-Fi certified for U.S./Canada
ICMFA001US1	Mini Field Agent with Cellular and Wi-Fi certified for U.S./Canada, and AT&T SIM card
ICMFA001UM0	Mini Field Agent with Cellular and Wi-Fi certified for Oman
ICMFA001UM1	Mini Field Agent with Cellular and Wi-Fi certified for Oman, and AT&T SIM card
ICMFA001EU0	Mini Field Agent with Cellular and Wi-Fi certified for European Union
ICMFA001EU1	Mini Field Agent with Cellular and Wi-Fi certified for European Union, and AT&T SIM card
ICMFA001AU0	Mini Field Agent with Cellular and Wi-Fi certified for Australia and New Zealand
ICMFA001AU1	Mini Field Agent with Cellular and Wi-Fi certified for Australia and New Zealand, and AT&T SIM card
ICMFA001AE0	Mini Field Agent with Cellular and Wi-Fi certified for UAE
ICMFA001AE1	Mini Field Agent with Cellular and Wi-Fi certified for UAE, and AT&T SIM card

2.7.2 MFA Included Items

The following item is included with all MFAs (not ordered separately).

Accessory Item	Description
Battery	Rayovac make BR2032-BA Lithium 20mm 3V 195mAh Coin Cell battery (-40°C to +85°C)

The following item is included with MFAs that support Wi-Fi (ICMFA001xxx).

Accessory Item	Description
Wi-Fi Antenna & Cable Assembly	Taoglas GW.11. A153 dipole antenna with Taoglas CAB.628IPEX MHF1 to SMA(F) RP cable.

The following item is included with MFAs that support cellular service (ICMFA001xxx).

Accessory Item	Description
Cellular Antenna & Cable Assemblies (2)	Nearson T6155AM-LTE-S LTE antennae with Taoglas CAB.618C and CAB.011 IPEX MHF1 to SMA(F) cable.

2.7.3

2.7.4 MFA Accessories

The following accessories may be ordered separately.

Table 5: MFA Accessories

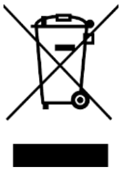
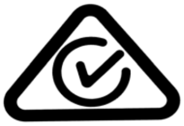
Catalog Number	Description
ICMFAACC001	Mini Field Agent Panel Mounting Kit
ICMFAACC002	24Vdc Power Supply Pre-wired with Connector
IC690PWR024	Selectable 115/230 Vac Input, 24 Vdc 5A Output, DIN Rail Mount Power Supply
ICMFAMGTM1YR	Annual Device Management Fee
ICMFADATA1GB	Annual Cellular Connectivity Fee

2.8 Agency Certifications and Standards

Refer to Mini Field Agent (MFA) Installation and Maintenance Requirements (IMR), GFK-2998, for conformance to these standards.

Note: *Markings listed below will vary based on the individual product part number. Therefore, certification and compliance to standards can only be verified by the actual marking on the product itself.*

Description	Marking	Comments
North America Safety for Information Technology Equipment North America Safety for Programmable Controller for use in Hazardous locations Class 1 Division 2 Groups ABCD Class 1 Zone 2 Gas Group IIC	c UL US LISTED	Certification by Underwriters Laboratories: UL 61010-1, UL 61010-2-201, UL 60950-1, UL 60079-0, UL 60079-15, and ISA-12.12.01-2013. CSA C22.2 No. 61010-2-201, CAN/CSA C22.2 No. 60950-1-07, CSA C22.2 No. 213 M1987, CAN/CSA-C22.2 No. 60079-0, and CAN/CSA-C22.2 No. 60079-15.
North American Radio Equipment	Contains FCCID: • TFB-TIWI-01 • N7NMC7455 Contains IC: • 5969A-TIWI101 • 2417C-MC7455	Equipment Authorization issued by Telecommunication Certification Body under authority of Federal Communications Commission (FCC) and Industry Canada (IC) for intentional transmitters
European Radio Equipment European Restriction of Hazardous Substances (RoHS)	CE	EU-Type Examination by Notified Body (#0673) to European Radio Equipment Directive 2014/53/EU Manufacturer's declaration of conformity in accordance with European RoHS Directive (2011/65/EU)
European Safety for Explosive Atmosphere Equipment Group II, Category 3, Gas Group IIC	Ex	Certification in accordance with to European ATEX Directive 2014/34/EU

Description	Marking	Comments
International Safety for Explosive Atmosphere	IECEx UL 17.0023X	Certification in accordance with the IECEx scheme and in compliance with IEC 60079-0 & IEC 60079-15
European Waste & Collection		Compliance with European WEEE Directive 2002/96/EC Amended by 2008/34/EC
Australia and New Zealand Regulatory Compliance Mark		Radiocommunications (EMC) Standard 2008 and Radiocommunications (Short Range Devices) Standard 2014, Radiocommunications (Electromagnetic Radiation – Human Exposure) Standard 2014, and AS/NZS 60950.1:2011 and AS/CA S042-2015

2.8.1 Federal Communications Commission (FCC)

The following statement is required by the Federal Communications Commission (FCC) and Industry Canada (IC):

> This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
>
> CAN ICES-3 (A)/NMB-3(A)

The Mini-Field Agent complies with Industry Canada and Federal Communications Commission RF exposure requirements when installed using the antenna as defined in section 2.7.2 of that document.

⚠CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2.9 Replacement and Spare Parts

Replacement parts may contain static-sensitive components. Emerson, therefore, ships replacement parts in anti-static bags. When handling electronics, make sure to store them in anti-static bags or boxes and wear a grounding strap.

⚠CAUTION

To prevent component damage caused by static electricity, treat all boards with static-sensitive handling techniques. Wear a wrist grounding strap when handling boards or components, but only after boards or components have been removed from potentially energized equipment and are at a normally grounded workstation.

⚠ WARNING

In addition to information provided here, always follow all wiring and safety codes that apply to your area or your type of equipment. For example, in the United States, most areas have adopted the National Electrical Code standard and specify that all wiring conform to its requirements. In other countries, different codes will apply. For maximum safety to personnel and property you must follow these codes. Failure to do so can lead to personal injury or death, property damage or destruction, or both.

2.9.1 Replacement Procedure

System troubleshooting should be at the module level. The failed module should be removed and replaced with a known good spare. The failed device should be returned to Emerson for repair. Do not attempt to repair it on site.

⚠CAUTION

To prevent equipment damage, do not remove, insert, or adjust board connections while power is applied to the equipment.

To replace the MFA

1. Lock Out Tag Out (LOTO) the equipment to isolate power sources.
2. Disconnect the incoming power plug.
3. Disconnect the Ethernet cables.
4. Remove the screws holding the MFA in place.
5. Install the new MFA by reversing steps 4 through 1.

2.9.2 Renewals and Spares

Renewals and spares (or those not under warranty) should be ordered by contacting the nearest Emerson Sales or Service Office, or an authorized Emerson Sales Representative.

Prior to ordering a replacement part:

- Identify the part (e.g. ICMFA000000-AAAA)
- Determine if the part is under warranty

While ordering, be sure to include the complete part number and revision letter. All digits are important when ordering or replacing any device. The factory may substitute newer versions based on availability and design enhancements, however, Emerson ensures backward compatibility of replacements.

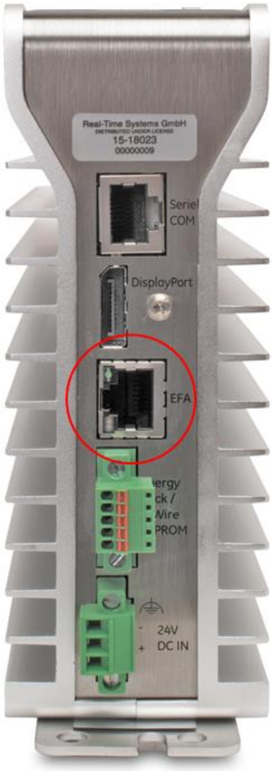
Chapter 3: EFA Hardware Instructions

Note: *The EFA will only respond to ping messages when it is in configuration mode.*

3.1 PACSystems IC695CPE400 RX3i Rackless CPU w/ Field Agent

This section describes only the hardware aspects of the CPE400 that explicitly pertain to the Field Agent functionality. For general information about the CPE400 hardware, refer to the PACSystems RX3i CPU Reference Manual, GFK-2222Y or later.

Figure 8: EFA Port on Underside of CPE400 Unit



3.1.1 CPE400 EFA -- Network Configuration

The CPE400 EFA uses the EFA Port (found on the underside of the CPE400 and circled in Figure 8) to connect to the Predix Cloud. It uses an internal virtual NIC to communicate to the controller to gather data.

The default IP Address for the EFA Cloud Port is 172.31.0.100, subnet mask 255.255.0.0. For more information on changing the IP Address, refer to Section 5.6, Configure the Network.

3.1.2 CPE400 EFA – LED, Display, and Push-Buttons

CPE400 hardware contains only one LED and a four-line display (manipulated by two push-buttons) that affect/reflect information about the EFA. The description of the display contents below covers only those items related to the Field Agent.

Field Agent Status Indicators (LEDs)

LED	LED State	Operating State
FAOK	● On Green	Field Agent Running and Connected to Cloud.
	✸ Blinking Green	Blink at 0.5 Hz: Field Agent Starting. Blink at 1 Hz: Field Agent Running.
	○ Off	Field Agent Off.

Display Navigation Push-Buttons

Push-Button	Function
DISP	Moves the cursor to the next item in the display, including moving to the next page if more than one page exists for a given level in the display hierarchy.
SEL	Executes the currently selected item in the display. This could cause the display to navigate to another location in the hierarchy, or it could cause a command to be executed if a command is currently selected. Before a command is executed, the user is given the choice to select OK or Cancel.

FA Settings Display Menu

Menu Item	Description
EFA Status	Shows the current state of the Field Agent, as follows: Off: The Field Agent is Off. Starting: The Field Agent is starting. Not Connected: The Field Agent is Running, but not connected to the cloud. Cloud Connected: The Field Agent is Running and connected to the cloud.
Network Config	Shows network interface information for the Field Agent, including IP Address, Subnet Mask, Gateway, MAC Address, and IPv6 Address. These settings are changed as described in Section 5.6, Configure the Network.
Commands Sub Menu	
Config Mode	Enter Configuration Mode, enabling access to the Web Console for one hour.
FA Reboot	This will restart the Field Agent operating system and Predix machine without affecting the controller.

Menu Item	Description
Factory Reset	This will reset the IP Address back to the default and remove Predix Enrollment information from the Field Agent. On the first boot following a factory reset, Predix Machine will generate cryptographic keys used for communication. It is Critical the Field Agent is not powered down during these operations to prevent corruption that may require another factory reset to resolve. Please wait until the EFA Status is Not Connected (FAOK LED blinking at 1Hz) before cycling power.

3.1.3 Emerson EFA Orderable Items

Table 6:

Catalog Number	Description
IC695MGMT1YR	Annual Device Management Fee

Chapter 4: VFA Instructions

This section describes the Network Configuration and VM Deployment for Virtual Field Agents.

4.1 Network Configuration

The VFA is configured with three networks; a WAN, LAN1 and LAN2. The default IP addresses are:

Table 7:

Item	WAN	LAN1	LAN2
IP Address	Obtain using DHCP	172.16.101.150	172.16.201.150
Subnet Mask	Obtain using DHCP	255.255.240.0	255.255.240.0
Network Interface	ens33	ens34	ens35

Note: *It is important that the networks above are mapped to the identified network interface. If either VMware vCenter® or VMware vSphere® Client is used to generate the Virtual Machine, then the above network interfaces should automatically be used, without the user needing to do anything special. However, if VMware Workstation Pro™ is used, it may default the network interfaces differently. In this case, after the user has generated the Virtual Machine, they should power down the Virtual Machine. Then edit the vmx file to make sure the pci slot numbers correspond to the ens numbers shown in the table above. If changes are made, make sure that there are no duplicate pci slot numbers; they may need to be changed for other hardware. For more information on changing the IP Address, refer to Section 5.6, Configure the Network.*

4.2 Configuration Mode

Configuration Mode allows access to the Web Console. Configuration Mode is always enabled on the Virtual Field Agent.

4.3 Virtual Machine Deployment

The VFA Virtual Machine is intended to be run using VMware ESXi™. There are three main files that compromise a Virtual Machine Deployment, a *. vmdk (Virtual Machine Disk Format), a *.ovf (Open Virtualization Format) and a *.mf file (Contains a security hash corresponding to the. vmdk and .ovf files).

4.4 Virtual Machine Snapshots

Note: *Once the VFA is up and working it is recommended that a snapshot be taken of the VM for backup purposes.*

4.5 Emerson VFA Orderable Items

Table 8:

Catalog Number	Description
ICVFAMGMT1YR	Annual Device Management Fee

Chapter 5: Getting Started with the Field Agent

5.1 What is the Minimum I need to do to Get Going?

This lists the minimum steps that need to be done to start using a Field Agent. The details of how to perform each step are described elsewhere in this document and are just referenced here.

1. Register the Field Agent in the Customer Portal (Refer to Section 5.2, Register the Field Agent).
2. Start the Field Agent (Refer to Section 5.4, Start the Field Agent).
3. Log into the Web Console (Refer to Section 5.5, Log into the Web Console).
4. Configure the Network (Refer to Section 5.6, Configure the Network).
5. Configure Time Synchronization (Refer to Section 5.7, Configure Time Synchronization).
6. Update the Field Agent (Refer to Section 5.8, Update the Field Agent).
7. Enroll Field Agent in Predix Cloud (Refer to Section 5.10, Enroll Field Agent in Predix Cloud). Note, even if you do not plan to stream data to the cloud, it is still required that you enroll your Field Agent.
8. If you plan to stream data to the cloud:
    a. Create Configuration (Refer to Section 6.2, Configuring Data Collection and Sending Data to the Cloud).
    b. Deploy Configuration (Refer to Section 6.1.3, Configuration Management).
9. If you plan to deploy your own applications to run on the Field Agent:
    a. Create an application. Information about how to write and deploy a custom machine adapter or data processor, including sample Predix Machine application source code, can be found by searching for “Predix Machine SDK Overview” in https://docs.predix.io.
    b. Deploy Application (Refer to Section 6.1.4, Application Management).

5.2 Register the Field Agent

Field Agents must be registered on the Customer Portal under the Assets tab. The process for registering a Field Agent, which includes the process of requesting a new EdgeManager tenancy if needed, is documented in the Field Agent Registration Guide, GFK-3018. This documentation can be found on the Landing Page for each Field Agent type referenced in Section 1.8, Product Landing Pages.

5.3 Collect Enrollment and Configuration Information

Before enrolling and configuring a Field Agent, it is often useful to first collect all the enrollment information (URLs, Field Agent serial numbers) and configuration information (Time Series Ingestion URL, Zone ID, etc.) into a single place to reference through the process. It is recommended to fill out as much of this table as possible before proceeding and referencing it in subsequent steps.

Table 9:

Resource	Where to Find It	Value
EdgeManager URL (Certificate Enrollment URL)	Response e-mail from Field Agent Registration	
Device Name	User Selected	
Device ID	User Selected, although typically the Device Serial Number printed on the Field Agent	
Predix Machine Web Console URL	Refer to Section 5.5, Log into the Web Console. Based on Field Agent type and user-selected IP address	
Network Proxy and Port (if required)	User-specified based on target network	
Data Source IP address and Port (OPC UA Server, Modbus TCP Slave, etc.)	User- specified based on target network	
Data tag names and corresponding variable names or register addresses	User- specified based on target network	
Data subscription name(s)	User-specified based on target network. Data tags may be divided into multiple subscriptions.	
Time Series Ingestion URL	Response e-mail from Time Series database activation request	Default US-West URL: wss://gateway-predix-data-services.run.aws-usw02-pr.ice.predix.io/v1/stream/messages
Time Series Zone ID	Response e-mail from Time Series database activation request	

5.4 Start the Field Agent

After providing the Mini Field Agent or the controller with Embedded Field Agent with power, the Field Agent will begin to boot. The green ON LED (for MFA) or FAOK LED (for EFA) will begin blinking when Predix Machine is starting, which is a process that can take approximately one minute. For the MFA, the green ON LED will turn solid once Predix Machine is running. For the CPE400, the FAOK LED will blink faster once Predix Machine is running, and the Display will indicate a FA Status of "Not Connected". Once Predix Machine is running, the Web Console is accessible for configuring and enrolling the Field Agent.

For the Virtual Field Agent, power on the Virtual Machine. There is no associated LED. Instead, when the Field Agent is up you should be able to access the Web Console.

5.5 Log into the Web Console

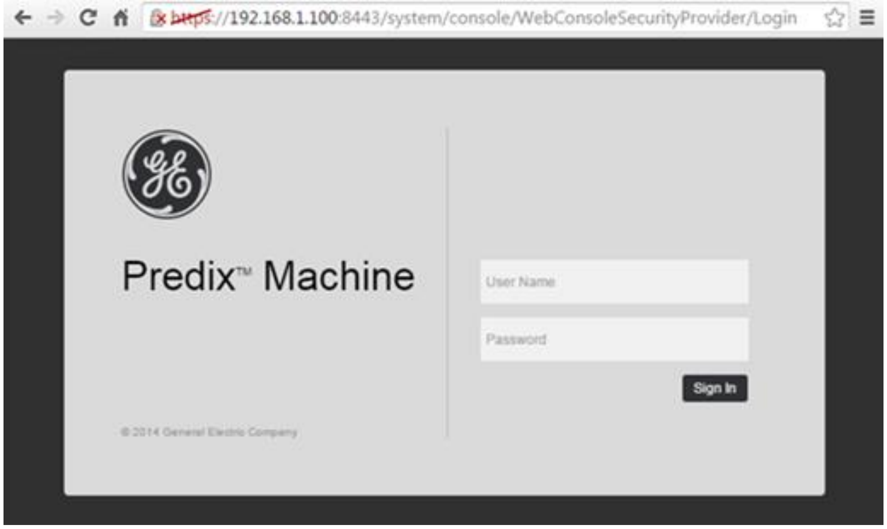
To log into the Predix Machine Web Console:

1. Connect a computer to the appropriate port on the Field Agent.
   - For an MFA, use LAN port 1, 2, or 3.
   - For an EFA use the EFA Port on the bottom of the device.
   - For a VFA, use LAN1 or LAN2
2. Configure the computer's network adapter to be an address on the Field Agent's network.
   - The MFA's default LAN IP Address is 192.168.1.100, subnet mask 255.255.255.0. Therefore, use another address on the 192.168.1.x network. For example, use 192.168.1.101 with subnet mask 255.255.255.0.
   - The EFA's default LAN IP address is 172.31.0.100, subnet mask 255.255.0.0. Therefore, use another address on the 172.31.x.x network. For example, use 172.31.0.101 with subnet mask 255.255.0.0.
   - The VFA's default LAN1 IP address is 172.16.101.150, subnet mask 255.255.240.0. The VFA's default LAN2 IP address is 172.16.201.150, subnet mask 255.255.240.0.
3. Confirm that Predix is up and running, so that the Web Console will be available.
   - For an MFA, verify that the "ON" LED is solid green.
   - For a CPE400 EFA, examine the OLED display, under "FA Settings". It should say either "Not Connected" or "Cloud Connected" if Predix is fully up and running.
   - For a VFA there is no LED to check if Predix Machine is running—just attempt to connect to the Web Console.
4. (EFA Only) Enable access to the Web Console using the process described in Section 3.1.2, CPE400 EFA – LED, Display, and Push-Buttons.
5. Browse to the Field Agent's Web Console. The Google Chrome browser is recommended for accessing the Web Console.
   - For an MFA use https://192.168.1.100:8443/system/console.
   - For an EFA use https://172.31.0.100:8443/system/console.

- For a VFA use https://172.16.101.150:8443/system/console. or https://172.16.201.150:8443/system/console.

6. Since the Web Console uses a self-signed certificate, the browser will warn that the connection is not private. When prompted, accept the connection.
7. Login using the default credentials:
   - Default User Name: Predix
   - Default Password: predix2machine

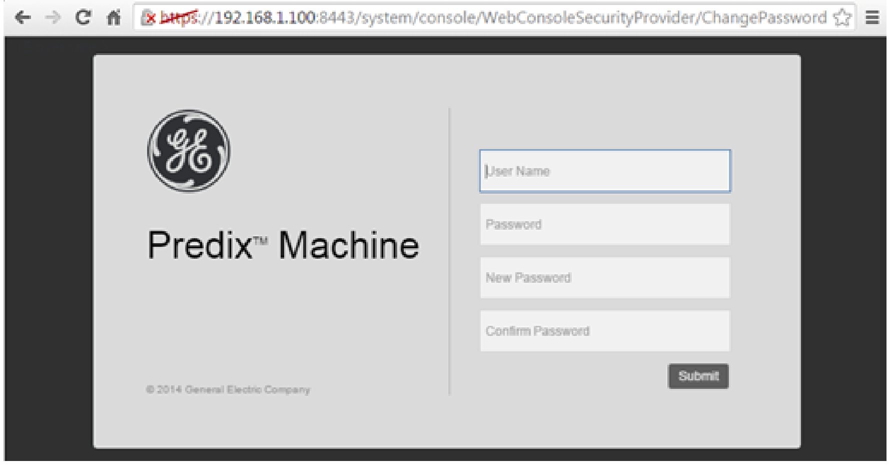
Figure 9: Predix Login Page



~~https~~://192.168.1.100:8443/system/console/WebConsoleSecurityProvider/Login

8. A prompt to change the default password displays. Complete the form to change the default password. The password complexity requirements display if the chosen password if not sufficiently complex. After changing the password, log in using the new password:

Figure 10: Predix New Password Page

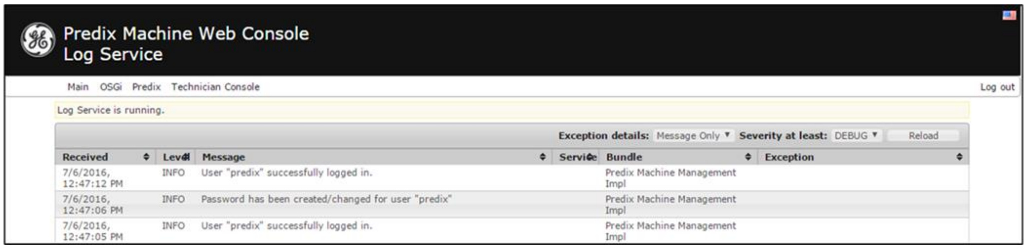


~~https~~://192.168.1.100:8443/system/console/WebConsoleSecurityProvider/ChangePassword

Note: *If the Web Console password is forgotten or lost, use the Factory Reset feature to restore all Field Agent settings, including Web Console password, to factory-default value*

9. Verify that the Log Service page displays, which indicates a successful login. Note that while the underlying Predix Machine log file logs all events in UTC (Coordinated Universal Time), all log events displayed in the OSGi Log Service are converted to and displayed in local time using the time zone of the computer running the browser used to view the Log Service

Figure 11: Predix Web Console Log Service Display



Log Service is running.

Received	Level	Message	Service	Bundle	Exception
7/6/2016, 12:47:12 PM	INFO	User "predix" successfully logged in.		Predix Machine Management Impl	
7/6/2016, 12:47:06 PM	INFO	Password has been created/changed for user "predix"		Predix Machine Management Impl	
7/6/2016, 12:47:05 PM	INFO	User "predix" successfully logged in.		Predix Machine Management Impl	

Note: *After some idle time, the Web Console will time out. Whenever this occurs, the user will need to return to the main page to log back into the console. Session timeout does not automatically redirect the console back to the login page*

5.6 Configure the Network

5.6.1 IP Addresses

The Mini Field Agent has four physical Ethernet ports, one of which is designated to be a WAN. The Embedded field agent only has one physical port, labelled either IICS Cloud Port or EFA, and it is designated to be a WAN. The following are the default settings for these networks:

Table 10:

Field Agent Type	Default WAN Setting	Default LAN1 Setting	Default LAN2 Setting
MFA	DHCP	192.168.1.100, subnet mask 255.255.255.0	N/A
EFA	172.31.0.100, subnet mask 255.255.0.0	N/A	N/A
VFA	DHCP	172.16.101.150, subnet mask 255.255.240.0	172.16.201.150, subnet mask 255.255.240.0

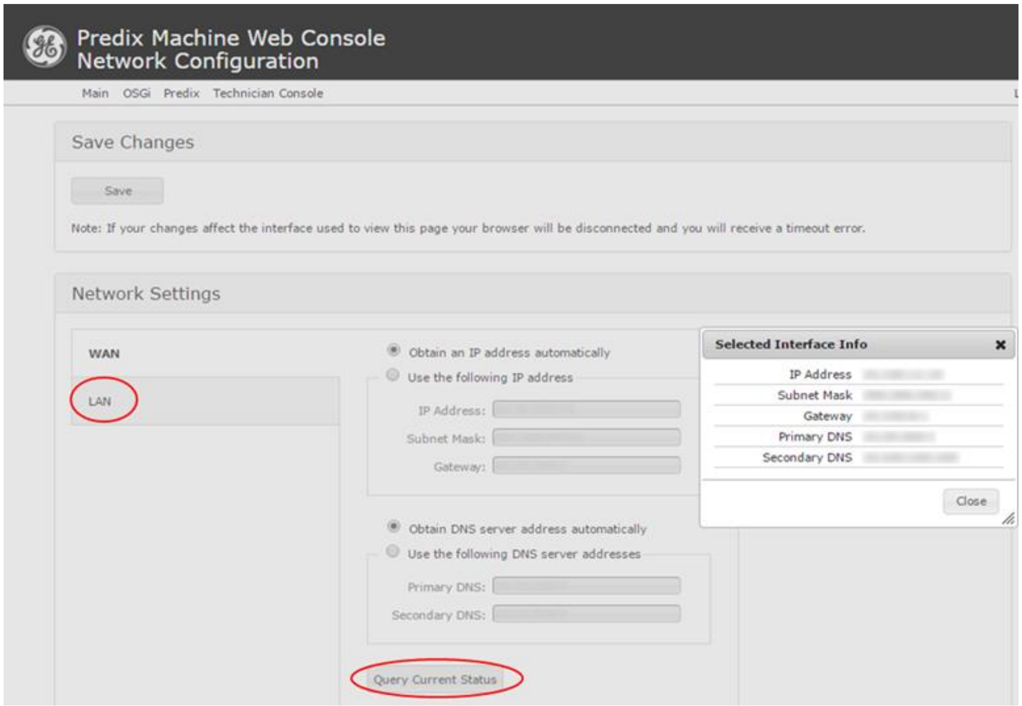
By default, the Mini Field Agent's WAN interface is set to acquire an IP address from a DHCP server on the network. The network interface settings that were automatically obtained from the DHCP server can be displayed in the Web Console.

To Identify/Change an IP Address

1. From the Web Console, navigate to the Technician Console, Network Configuration page. Note that there will be three tabs (WAN, LAN, and Cellular) for an MFA, only a single tab (WAN) for an EFA, and three tabs (WAN, LAN1, and LAN2) for a VFA.

2. To identify the DHCP assigned address for an MFA or VFA, select the WAN tab, then click the Query Current Status button.

Figure 12: Query Current Status



Predix Machine Web Console
Network Configuration

Main OSGi Predix Technician Console

Save Changes

Save

Note: If your changes affect the interface used to view this page your browser will be disconnected and you will receive a timeout error.

Network Settings

WAN

LAN

● Obtain an IP address automatically
○ Use the following IP address

IP Address: [redacted]
Subnet Mask: [redacted]
Gateway: [redacted]

● Obtain DNS server address automatically
○ Use the following DNS server addresses

Primary DNS: [redacted]
Secondary DNS: [redacted]

Query Current Status

Selected Interface Info ✖

IP Address [redacted]
Subnet Mask [redacted]
Gateway [redacted]
Primary DNS [redacted]
Secondary DNS [redacted]

Close

3. To identify a DHCP assigned address for a CPE400 EFA, use the Display on the front of the CPE400. Navigate to FA Settings, and then to Network Config.

4. To change an IP Address, select the appropriate tab (WAN or LAN). Then select the radio button Use the following IP address, enter the desired IP address and network mask, and click the Save button. When the IP Address is changed, the Web Console session will end after the Save button is pressed and a new session will need to be started by browsing to the Web Console URL using the newly chosen static IP address.

Note:

- *The DNS servers can also be configured to be obtained automatically or specified statically.*
- *The MFA supports either the WAN or the LAN using DHCP to automatically obtain an IP address – not both.*

⚠CAUTION

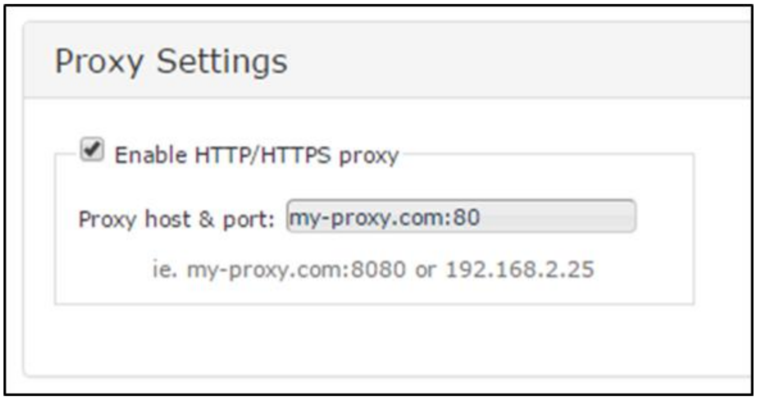
It is strongly recommended that the WAN and LAN interfaces each be configured for separate network subnets with no overlap.

5.6.2 Configure a Network Proxy

A Network Proxy is only required when your network architecture is configured to restrict access directly to the Internet. Contact your network administrator for the Network Proxy information.

If a network HTTP/HTTPS proxy server is used to route traffic from the intranet to the Internet, the network proxy must be configured in the Web Console under Technician Console, Network Configuration. To add or update a network proxy server, check the "Enable HTTP/HTTPS Proxy" check box, enter the proxy server's address and port in the form "proxy:port" in the Proxy Settings textbox, and press the Save button.

Figure 13: Set Proxy



Proxy Settings

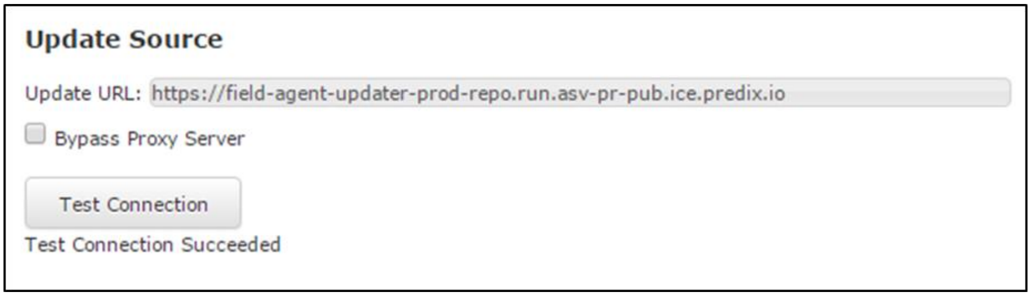
☑ Enable HTTP/HTTPS proxy

Proxy host & port: my-proxy.com:80

ie. my-proxy.com:8080 or 192.168.2.25

To verify the Field Agent can successfully use the newly configured network proxy to reach the Internet, use the Test Connection feature of the Field Agent Updater page in the Web Console under Technician Console, Field Agent Updater. Internet reachability can be tested by using either the default Update URL or any other desired URL and pressing the Test Connection button.

Figure 14: Test Connection Feature



Update Source

Update URL: https://field-agent-updater-prod-repo.run.asv-pr-pub.ice.predix.io

☐ Bypass Proxy Server

Test Connection Succeeded

If the URL is reachable, a Test Connection Succeeded message displays below the Test Connection button after the button is pressed. Otherwise, a message will appear indicating that the Test Connection attempt failed.

Note: *On the MFA, the blue Cloud LED remains blinking*

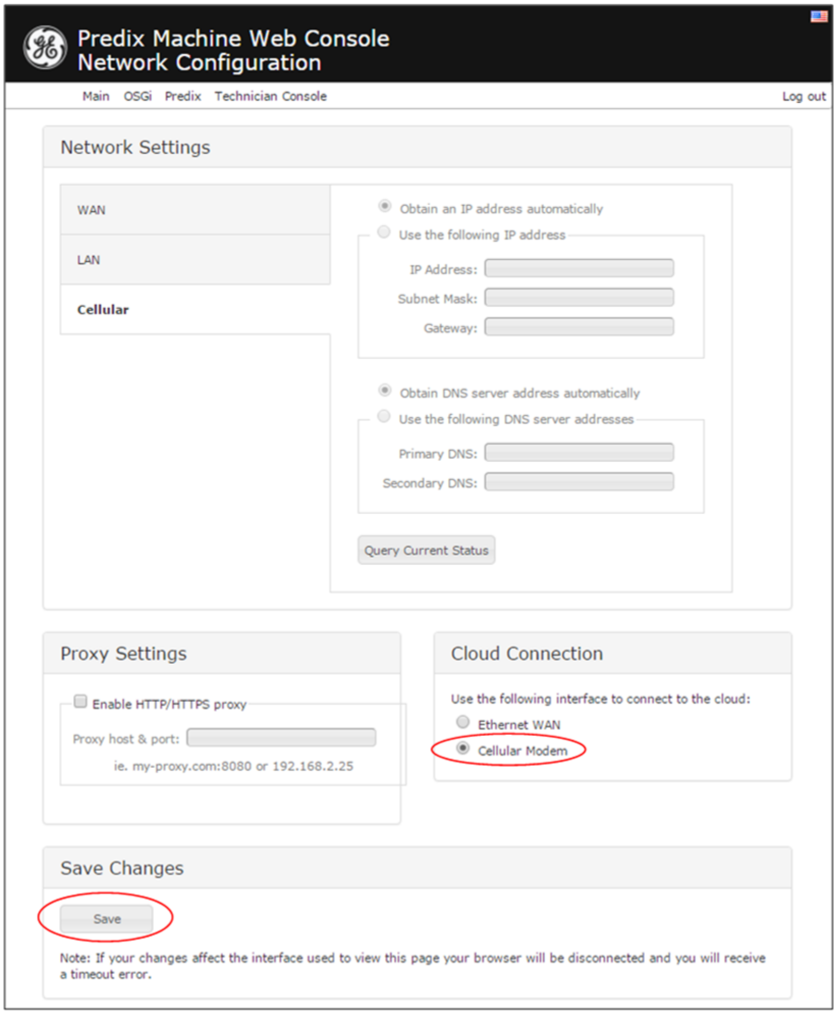
5.6.3 Configure the Cellular Network

The Mini Field Agent has an optional cellular modem. The cellular options are described in Section 0, Field Agent Sales Catalog.

Enabling the Cellular Modem

From the Web Console, navigate to the Technician Console, Network Configuration page. Select Cellular Modem for the cloud connection interface and save changes. The Mini Field Agent can connect to the cloud using either the Ethernet WAN or Cellular Modem. If both interfaces are connected, only the interface selected will be used.

Figure 15: Cellular Modem Interface Configuration



Predix Machine Web Console
Network Configuration

Network Settings

● Obtain an IP address automatically
○ Use the following IP address

IP Address:
Subnet Mask:
Gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses

Primary DNS:
Secondary DNS:

Proxy Settings

□ Enable HTTP/HTTPS proxy

Proxy host & port:
ie. my-proxy.com:8080 or 192.168.2.25

Cloud Connection

Use the following interface to connect to the cloud:
○ Ethernet WAN
● Cellular Modem

Save Changes

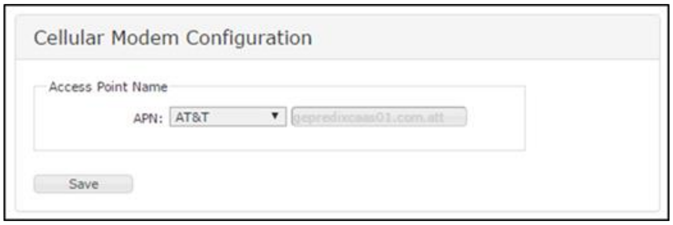
Note: If your changes affect the interface used to view this page your browser will be disconnected and you will receive a timeout error.

Configure the Access Point Name

The Access Point Name identifies the gateway for the cellular network being used and must be configured based on the installed SIM card. If the Mini Field Agent was ordered with a SIM installed, the correct APN will already be configured.

A custom APN can be set for a customer-installed SIM. From the Technician Console, Cellular page select Custom from the APN list, enter the APN specified by the cellular provider, and select Save.

Figure 16: Cellular Modem Details Configuration



Cellular Modem Configuration

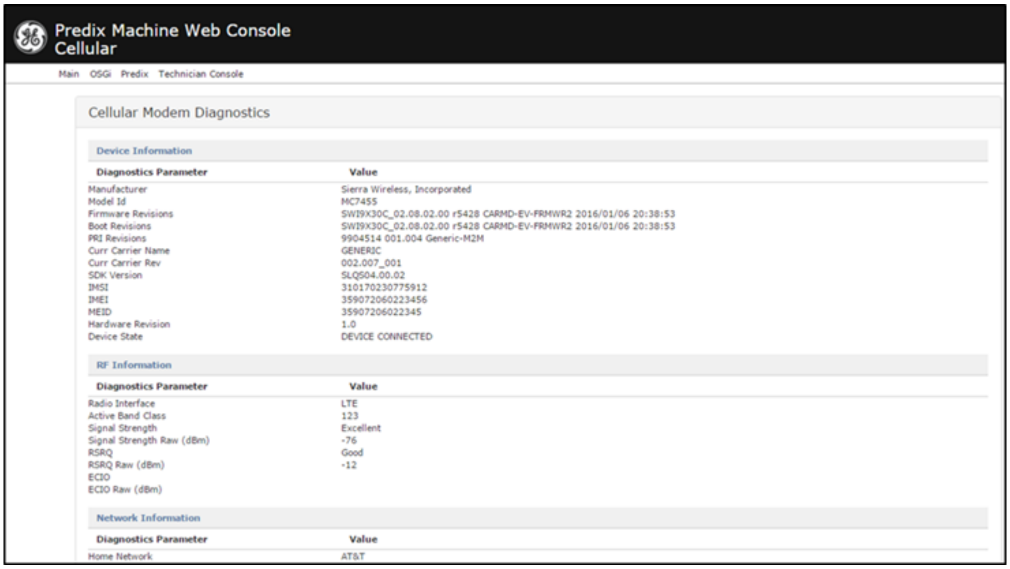
Access Point Name

APN: AT&T ▾ gepredixcaas01.com.att

View the Cellular Status

Cellular modem diagnostics including signal strength, network connectivity, usage statistics, and SIM card information are available from the Technician Console, Cellular page.

Figure 17: View Cellular Modem via Predix Web Console



Predix Machine Web Console
Cellular
Main OSGi Predix Technician Console

Cellular Modem Diagnostics

Device Information

Diagnostics Parameter	Value
Manufacturer	Sierra Wireless, Incorporated
Model Id	MC7455
Firmware Revisions	SWI9X30C_02.08.02.00 r5428 CARMD-EV-FRMWR2 2016/01/06 20:38:53
Boot Revisions	SWI9X30C_02.08.02.00 r5428 CARMD-EV-FRMWR2 2016/01/06 20:38:53
PRI Revisions	9904514 001.004 Generic-M2M
Curr Carrier Name	GENERIC
Curr Carrier Rev	002.007_001
SDK Version	SLQS04.00.02
IMSI	310170230775912
IMEI	359072060223456
MEID	35907206022345
Hardware Revision	1.0
Device State	DEVICE CONNECTED

RF Information

Diagnostics Parameter	Value
Radio Interface	LTE
Active Band Class	123
Signal Strength	Excellent
Signal Strength Raw (dBm)	-76
RSRQ	Good
RSRQ Raw (dBm)	-12
ECIO	
ECIO Raw (dBm)	

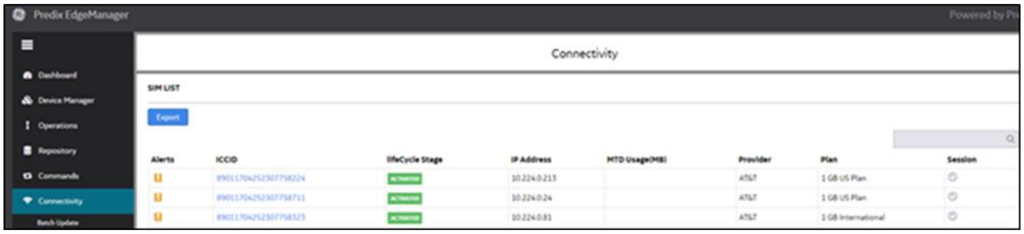
Network Information

Diagnostics Parameter	Value
Home Network	AT&T

Cellular Plan and SIM Diagnostics

Field Agents that include an AT&T SIM card (e.g. ICMFA001US1) can have their cellular data plans managed and diagnosed through EdgeManager . The EdgeManager Connectivity page shows the list of SIM ICCIDs and corresponding SIM session diagnostics, such as whether the plan is active regionally or internationally, the monthly data plan size and usage, cellular provider, whether the SIM is actively in a connected session, and the assigned IP address.

Figure 18: View Cellular Modem Subscription Details



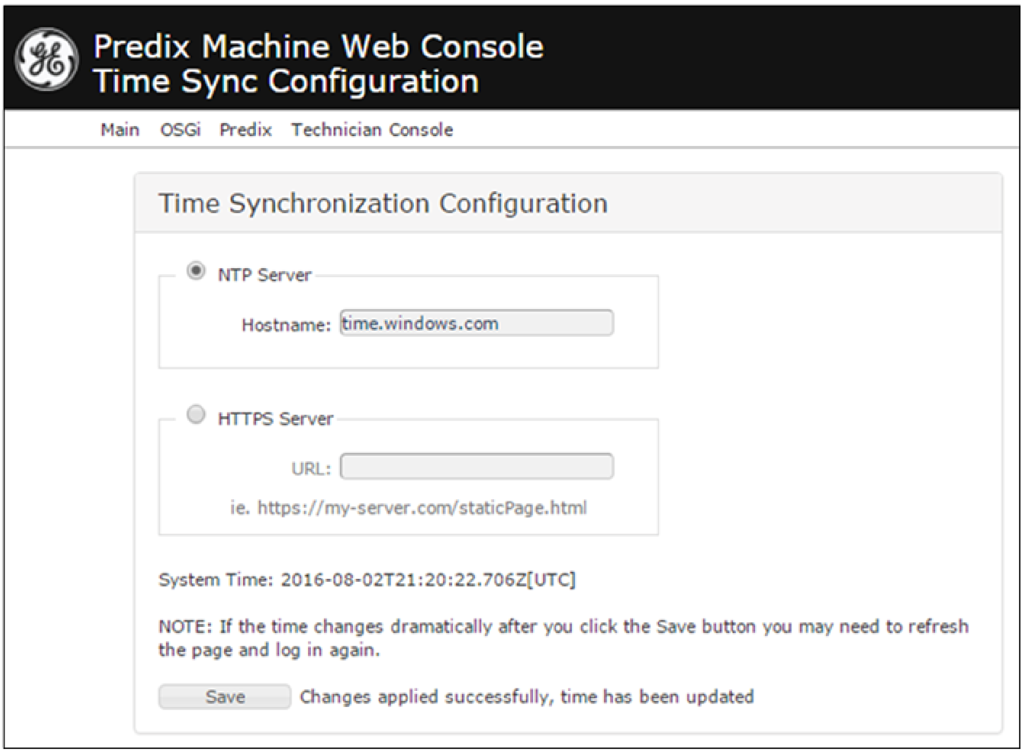
SIM LIST

Alerts	ICCID	lifeCycle Stage	IP Address	MTD Usage(MB)	Provider	Plan	Session
!	89011704252307758224	ACTIVATED	10.224.0.213		AT&T	1 GB US Plan	○
!	89011704252307758711	ACTIVATED	10.224.0.24		AT&T	1 GB US Plan	○
!	89011704252307758523	ACTIVATED	10.224.0.81		AT&T	1 GB International	○

5.7 Configure Time Synchronization

In order for industrial data time-stamping and Field Agent diagnostic information to operate reliably, it is important for the Field Agent to have an accurate time source. The Field Agent has two methods of synchronizing time – either by using a Network Time Protocol (NTP) server or by pulling time from a web page hosted by an HTTPS web server with its own reliable time source. Either method can be configured in the Web Console under Technician Console, Time Sync Configuration.

Figure 19: Configure Time Synchronization via Predix Web Console



Predix Machine Web Console
Time Sync Configuration

Time Synchronization Configuration

● NTP Server

Hostname: time.windows.com

○ HTTPS Server

URL:

ie. https://my-server.com/staticPage.html

System Time: 2016-08-02T21:20:22.706Z[UTC]

NOTE: If the time changes dramatically after you click the Save button you may need to refresh the page and log in again.

Changes applied successfully, time has been updated

Time is saved on all Field Agents in UTC (Coordinated Universal Time), as shown in the "System Time" output above the Save button on the Time Sync Configuration page. All Field Agent events (such as those recorded in the Predix Machine log file and the system journal) are therefore also represented in UTC. Any data that is ingested by a Machine Adapter and timestamped on the Field Agent will also be represented in UTC as epoch time (the number of seconds that have elapsed since January 1, 1970 at midnight UTC not counting leap seconds). This format is not changed in transit to or at rest in the Predix Time Series Database.

5.7.1 Using NTP Time Synchronization

By default, time synchronization is configured to use the time.windows.com NTP Server. If a valid network path to the Internet exists, time will be synchronized when the Field Agent boots and continuously while running. The current date and time on the Field Agent is displayed above the Save button on the Time Sync Configuration page when the page loads and can be updated by pressing the Save button or reloading the page.

Since the NTP protocol does not support passing through a network proxy, the default value of time.windows.com will only work on networks that do not require a network proxy. If a network proxy is required, a different NTP server must be configured that can be reached without passing through a network proxy.

To change the NTP server, enter the new NTP server URL in the NTP Server textbox and press the Save button. If the new server was successfully configured, a success statement will be displayed, and the updated time will be displayed. If the time and date was more than 20 minutes out of date prior to time synchronization occurring after pressing the Save button, the Web Console session may end, and an error message may be presented indicating that the session's timeout had been reached. Log back into the Web Console to verify the time was updated as expected.

5.7.2 Using HTTPS Time Synchronization

Time synchronization can also be configured to use an HTTPS web server's time by pulling it from the header of the web page it serves. To configure HTTPS time synchronization, select the HTTPS Server radio button on the Time Sync Configuration page, enter a valid HTTPS URL, and press the Save button. If a network proxy is in use, this time synchronization method will only work with HTTPS URLs that do not require a network proxy in order to reach them.

If the new HTTPS URL was successfully configured after pressing the Save button, a success statement will be displayed, and the updated time will be displayed. If the time and date was more than 20 minutes out of date prior to time synchronization occurring after pressing the Save button, the Web Console session may end and an error message may be presented indicating that the session's timeout had been reached. Log back into the Web Console to verify the time was updated as expected.

5.8 Update the Field Agent

The Mini Field Agent's operating system is a custom, embedded, Linux-based operating system called Yogurt that is built using the Yocto Project toolchain. Both the Embedded Field Agent's and the Virtual Field Agent's operating system is Ubuntu. Like many other Linux distributions, it is divided into several independently maintained and versioned software packages. Emerson and the Linux community are continuously releasing new versions of these packages to provide feature enhancements, bug fixes, and security patches.

Emerson strongly recommends that customers keep their Field Agent OS up-to-date.

In order to ensure that Linux package updates do not break the existing Predix functionality running on the Field Agent, Emerson uses a daily continuous integration process to verify that updates remain compatible with all Field Agent hardware and Predix software before they become available to installed Field Agents. Encryption and digital signatures are used to ensure that only approved package versions are installed on each Field Agent, and that the specific versions used are kept confidential.

Customers can choose one of three methods for keeping their Linux packages up-to-date. Customers must select a method while performing the one-time configuration of the Field Agent from its Field Agent Updater web page.

- Method 1: Manual Local Update Using a Local Area Network
- Method 2: Manual Cloud Update over the Internet
- Method 3: Automatic Cloud Update over the Internet

5.8.1 Access the Field Agent Updater

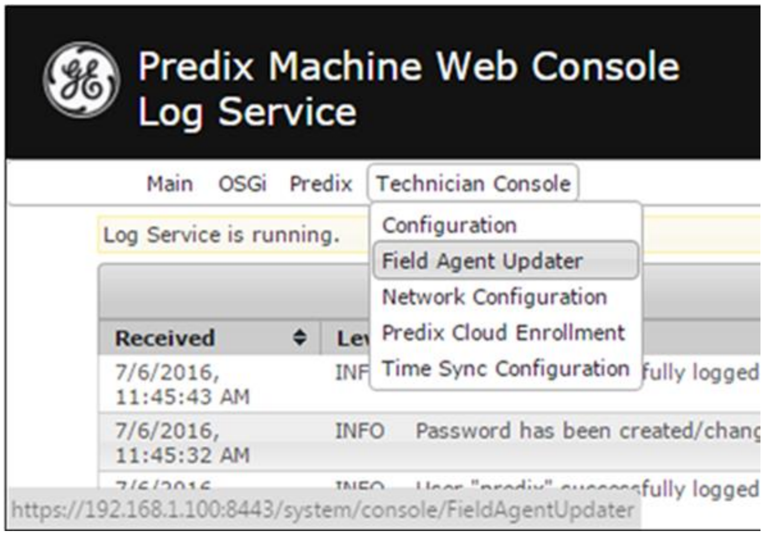
Prerequisites:

- Successfully logged into the web console
- Successfully configured the network

To access the Field Agent Updater:

1. From the Log Service page, select Technician Console, Field Agent Updater.

Figure 20: Navigate to Field Agent Updater Menu



Predix Machine Web Console
Log Service

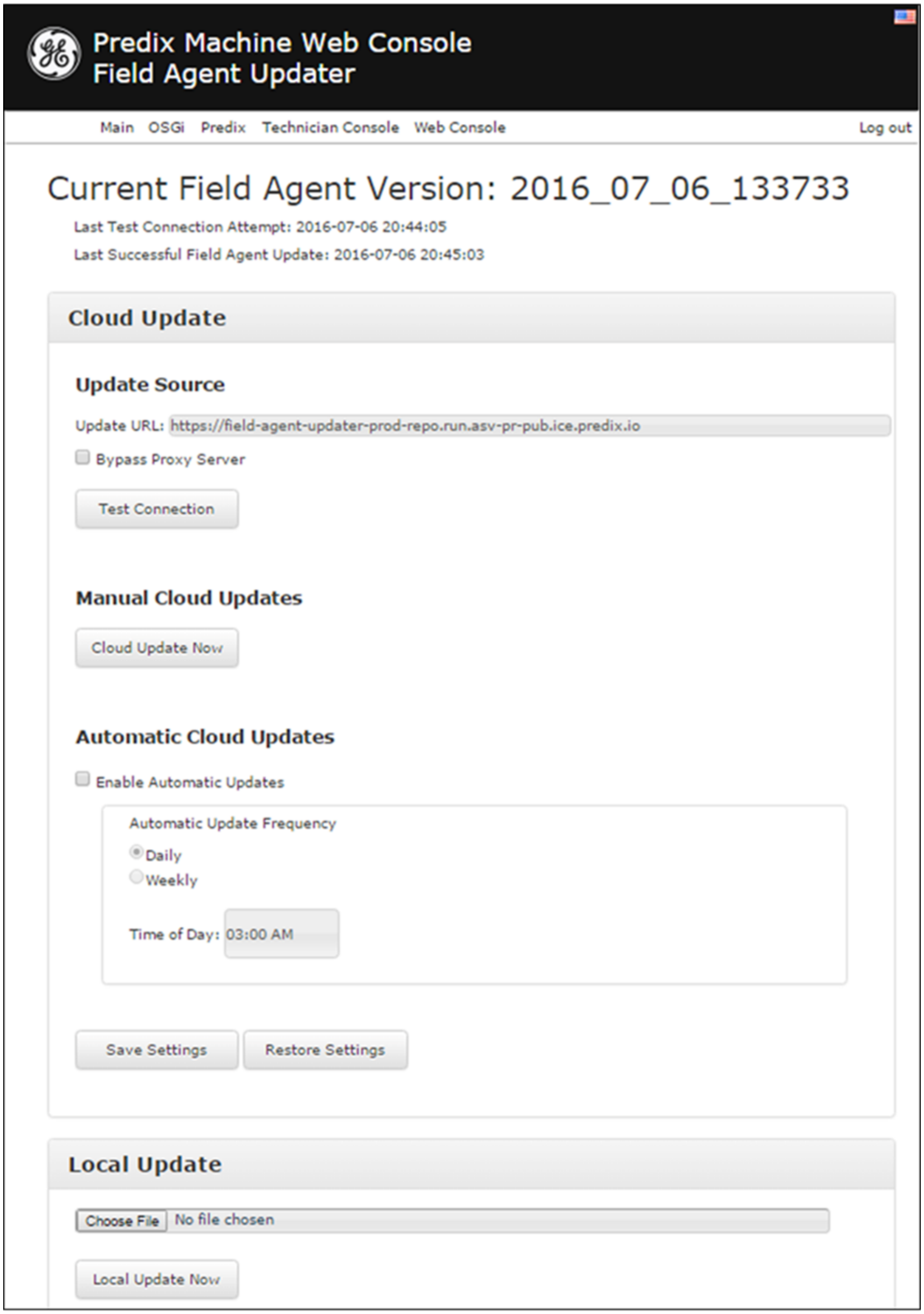
Log Service is running.

```
7/6/2016,      INF                         fully logged
11:45:43 AM
7/6/2016,      INFO   Password has been created/chang
11:45:32 AM
7/6/2016       INFO   User "predix" successfully logged
```

https://192.168.1.100:8443/system/console/FieldAgentUpdater

2. Verify that the Field Agent Updater page displays.

Figure 21: Field Agent Updater Page on Predix Web Console



Predix Machine Web Console
Field Agent Updater

Current Field Agent Version: 2016_07_06_133733

Last Test Connection Attempt: 2016-07-06 20:44:05

Last Successful Field Agent Update: 2016-07-06 20:45:03

Cloud Update

Update Source

Update URL: https://field-agent-updater-prod-repo.run.asv-pr-pub.ice.predix.io

□ Bypass Proxy Server

Manual Cloud Updates

Automatic Cloud Updates

□ Enable Automatic Updates

Automatic Update Frequency

● Daily
○ Weekly

Time of Day: 03:00 AM

Local Update

No file chosen

5.8.2 Method 1: Manual Local Update Using a Local Area Network

NOTICE

This is the recommended method for updating the Field Agent for the first time on a newly-provisioned unit. After this initial update, it is recommended to use Automatic Cloud Updates over the Internet.

It is possible to update the Field Agent while it is not connected to the Internet. Below are several reasons this may be desired:

- If the Field Agent is significantly out of date, it may not be desirable to connect it to the Internet before applying security patches.
- If one or more Field Agents are significantly out of date, it may not be desirable for each Field Agent to consume bandwidth independently updating Linux packages.
- If a specific version of the Field Agent is desired for compatibility with a customer's domain application or for any other reason, this is the easiest method for specifying the Field Agent version.
- If the Field Agent is being used in an environment without Internet connectivity, this is the only method for updating the Field Agent's Linux packages.

To manually initiate a local update using a Local Area Network connection

1. Using a computer that can be connected to the Field Agent's Local Area Network, navigate to the appropriate Firmware Image page and download the desired Field Agent package version, which ends with a .MAX file extension.

   Mini Field Agent:

   https://www.emerson.com/Industrial-Automation-Controls/support

   Embedded Field Agent:

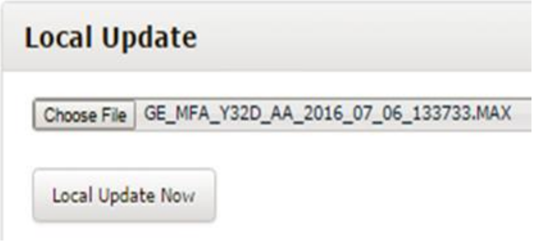
   https://www.emerson.com/Industrial-Automation-Controls/support

   Virtual Field Agent:

   https://www.emerson.com/Industrial-Automation-Controls/support

2. Access the Field Agent Updater (Section 5.8.1).
3. In the Local Update section of the Field Agent Updater, click Choose File, then browse to and select the downloaded Field Agent image (.MAX) file

Figure 22: Browse to .MAX file



Local Update

Choose File GE_MFA_Y32D_AA_2016_07_06_133733.MAX

4. Click the Local Update Now button. An Update In Progress... message displays. Wait while the update is verified and applied. The update process may take up to 20 minutes to complete.
5. Verify that the status label beneath the Local Update Now button has changed to indicate that the update succeeded.

   Verify that and that the Current Field Agent Version and Last Successful Field Agent Update labels at the top section of the Field Agent Updater page have also updated. If required, the Field Agent will reboot itself after an update. When this occurs, a timeout or error message may appear in the browser. The Predix Machine Web Console must be logged into again after the Field Agent is rebooted

5.8.3 Method 2: Manual Cloud Update over the Internet

NOTICE

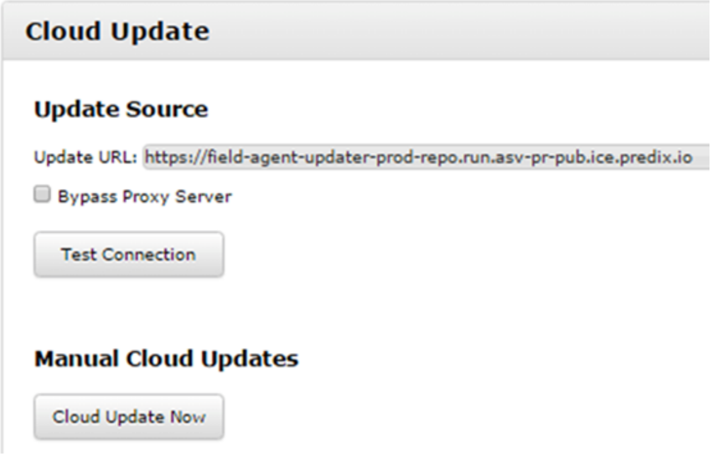
Before setting up an Automatic Cloud Update schedule using Method 3 below, it is recommended that this method be used to verify connectivity to the selected Update URL and network proxy settings.

If the Field Agent has a network path to the Internet, customers can choose to manually initiate an on-demand update of the Field Agent over the Internet. This method is also valuable for diagnosing and verifying the connection between the Field Agent and the Predix Cloud.

To manually initiate a cloud update over the Internet:

1. Access the Field Agent Updater (Section 5.8.1).
2. Under Cloud Update, the default Update URL will contain the standard location of Field Agent Update packages in the Predix Cloud. If a network proxy server is configured in the Network Configuration but the Update URL is only reachable by bypassing this proxy server, then check Bypass Proxy Server

Figure 23: Cloud Update Interface



Cloud Update

Update Source

Update URL: https://field-agent-updater-prod-repo.run.asv-pr-pub.ice.predix.io

□ Bypass Proxy Server

Manual Cloud Updates

3. Click the Test Connection button to verify the Field Agent can reach the Update URL using the current network settings
4. Under Manual Cloud Updates, click the Cloud Update Now button. A message displays to indicate that the update is in progress. Wait while the update is retrieved, verified, and installed.
5. After the update completes, verify that the status label beneath the Cloud Update Now button has changed to indicate that the update succeeded. Verify that the Current Field Agent Version and Last Successful Field Agent Update labels at the top of the Field Agent Updater page have also updated. If required, the Field Agent will reboot itself after an update. When this occurs, a timeout or error message may appear in the browser. The Predix Machine Web Console must be logged into again after the Field Agent is rebooted.

Note: *On the MFA, the blue Cloud LED remains blinking and will only turn solid after Enrollment.*

5.8.4 Method 3: Automatic Cloud Update over the Internet

NOTICE

This is the recommended long-term method for updating the Field Agent.

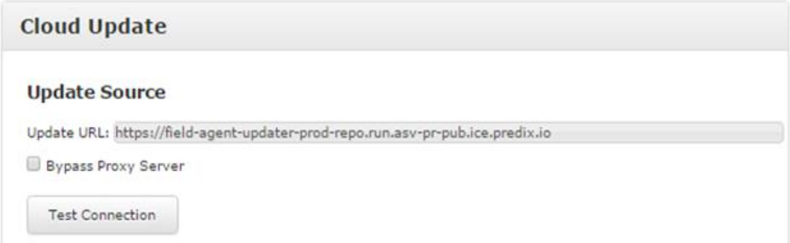
Field Agents with a network path to the Internet can be configured to update themselves automatically on a daily or weekly cadence by specifying a date and/or time for the update to occur. Customers should consider their operational processes and their network connection speed and reliability before choosing the update cadence, as the update may require a download of several megabytes of data for each Field Agent.

To configure automatic cloud updates over the Internet

1. Access the Field Agent Updater (Section 5.8.1).
2. Under Cloud Update, the default Update URL will contain the standard location of Field Agent Update packages in the Predix Cloud. If a network proxy server is configured in

the Network Configuration but the Update URL is only reachable by bypassing this proxy server, then check Bypass Proxy Server.

Figure 24: Update Source / Bypass Proxy



Cloud Update

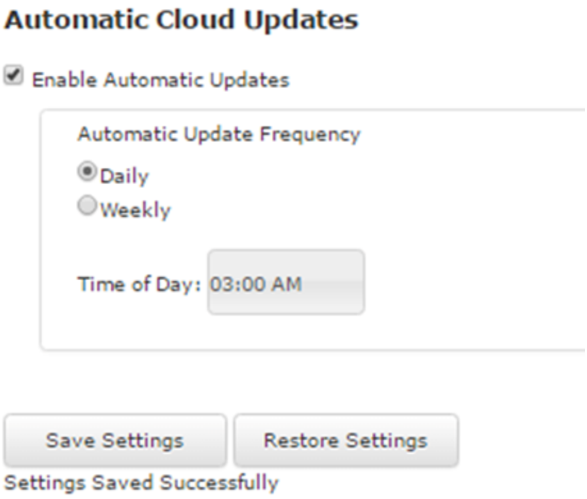
Update Source

Update URL: https://field-agent-updater-prod-repo.run.asv-pr-pub.ice.predix.io

□ Bypass Proxy Server

3. Click the Test Connection button to verify the Field Agent can reach the Update URL using the current network settings.
4. Under Automatic Cloud Updates, check Enable Automatic Updates. Select the Automatic Update Frequency, enter the Time of Day (in UTC time), then click Save Settings.

Figure 25: Configure Automatic Cloud Updates



Automatic Cloud Updates

☑ Enable Automatic Updates

Automatic Update Frequency

● Daily

○ Weekly

Time of Day: 03:00 AM

Settings Saved Successfully

Note: *The Restore Settings button reverts to the currently persisted update schedule settings.*

5. At the specified time, the Field Agent will automatically use the Update URL to locate, retrieve, validate, and install only the Linux packages containing available updates. If the Field Agent Updater page is viewed while this process is automatically occurring, the user will see an indication that an update is in progress. When the update completes, the Current Field Agent Version and Last Successful Field Agent Update labels at the top of the Field Agent Updater page are updated. If required, the Field Agent will reboot itself after an update. When this occurs, a timeout or error message may appear in the browser. The Predix Machine Web Console must be logged into again after the Field Agent is rebooted.

5.8.5 Upgrade Predix Machine If Applicable

As new versions of Predix Machine are released by Emerson, they are integrated into the various Field Agents from Emerson's Automation & Controls (A&C), validated, and released as officially supported versions. Due to resource constraints, performance optimizations, and security considerations, the default Predix Machine container is heavily customized to the profile of each A&C Field Agent. In many cases, deploying a Predix Machine container built by a customer without A&C customizations to an A&C Field Agent can cause Predix Machine to fail to run, requiring a factory reset. For this reason, A&C publishes Configuration and Application Templates that are pre-built, pre-validated Predix Machine containers on top of which customer modifications can be applied. A&C also publishes migration packages for upgrading from one major version of Predix Machine to another.

Upgrading a Field Agent from one major version of Predix Machine to another (for example, from Predix Machine 16.2 to 17.1) is a one-time activity that involves three steps:

1. Use the Field Agent Updater to update to an OS version equal to or greater than a specific OS version based on the Field Agent type.
2. Verify the starting version of Predix Machine.
3. Deploy the Predix Machine upgrade package from either:
    a. Field Agent Updater page of the Predix Machine Web Console as an offline upgrade
    b. EdgeManager as an online upgrade

The documentation guide that details the process for performing a Predix Machine upgrade on each Field Agent type is the Field Agent Upgrade Guide, GFK-3017. It can be found on the Landing Page for each Field Agent type.

5.9 Configure EdgeManager Access

EdgeManager provides a single point of entry for deploying and monitoring devices remotely. You can also administer your apps and configuration files at both a device and fleet level, which helps you keep your device software current and up to date. For the EdgeManager to perform Device and Fleet Management operations on Field Agents and connected hardware, each Field Agent must enroll with EdgeManager .

Note: *If you do not already have an EdgeManager instance, or you were not provided with one, please contact your supplier or customer support to get started.*

The Administrator logs into the EdgeManager and creates one of the following:

- Two user accounts - one with the Operator role and the other with the Technician role
- One user account with both the Operator and Technician roles

5.9.1 Create Accounts for Operator and Technician Roles

Each customer is provided their own EdgeManager space and their own User Authentication and Authorization (UAA) service that allows customers to define which users in their organization have access to EdgeManager and what operations each user can perform. Each customer is assigned at least one predefined account with the Administrator role, which can be used for adding new users and assigning permissions.

In order to enroll a Field Agent with EdgeManager , two different roles are needed. The Operator role must be assigned to the individual responsible for creating device instances in EdgeManager with the appropriate Device Name, Device ID, and Device Model according to how the Field Agents should be identified. The Technician role must be assigned to the individual responsible for performing the enrollment activity in the Web Console of each Field Agent. If desired, both of these roles can be assigned to the same individual's user account.

To create the account or accounts needed, the Administrator must log into EdgeManager , navigate to the User Manager tab, and click the Create button. After entering the new account's username, e-mail address, and initial password, the Administrator must select the roles to be assigned to this account by checking the corresponding check boxes. The roles to be assigned can be any combination of Administrator, Operator, and/or Technician. The Administrator must then press the Create button to create the account and provide the user account information including initial password to the individual assigned to the account. Upon first login, the user will be forced to change their password.

5.10 Enroll Field Agent in Predix Cloud

To administer a Field Agent, it must first be enrolled. Each Field Agent can be enrolled using EdgeManager . Additionally, the Mini Field Agent can be enrolled using the Field Agent Manager iPhone app.

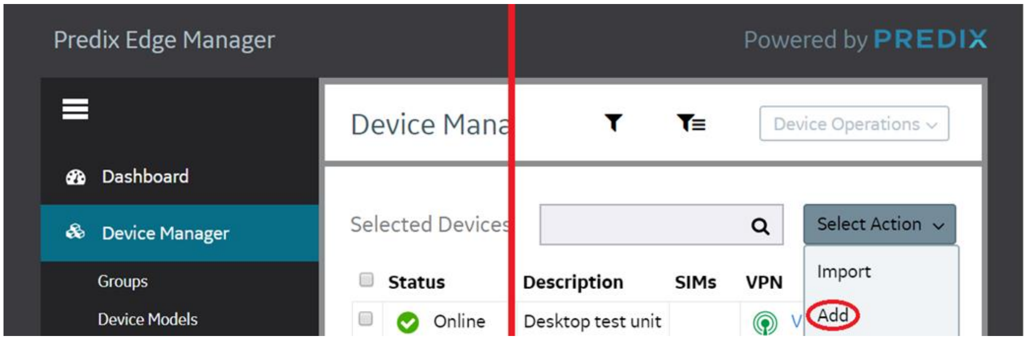
5.10.1 Enroll using EdgeManager

1. The enrollment process involves the following activities.
2. From the customer's EdgeManager URL, the Operator logs into the EdgeManager and creates a Field Agent device representation with the desired Device Name, Device ID, and assigned technician.
3. The Technician obtains enrollment information from the Operator.
4. The Technician logs into the Web Console on the Field Agent to be enrolled and navigates to the Predix Cloud Enrollment page under Technician Console, Predix Cloud Enrollment.
5. The Technician enters the enrollment information, presses the Enroll Device button, and authorizes the enrollment (which may include providing the Technician's EdgeManager Username and Password).
6. From the EdgeManager , the Operator verifies that the Field Agent is displayed as Online.

Create a Device Representation in EdgeManager

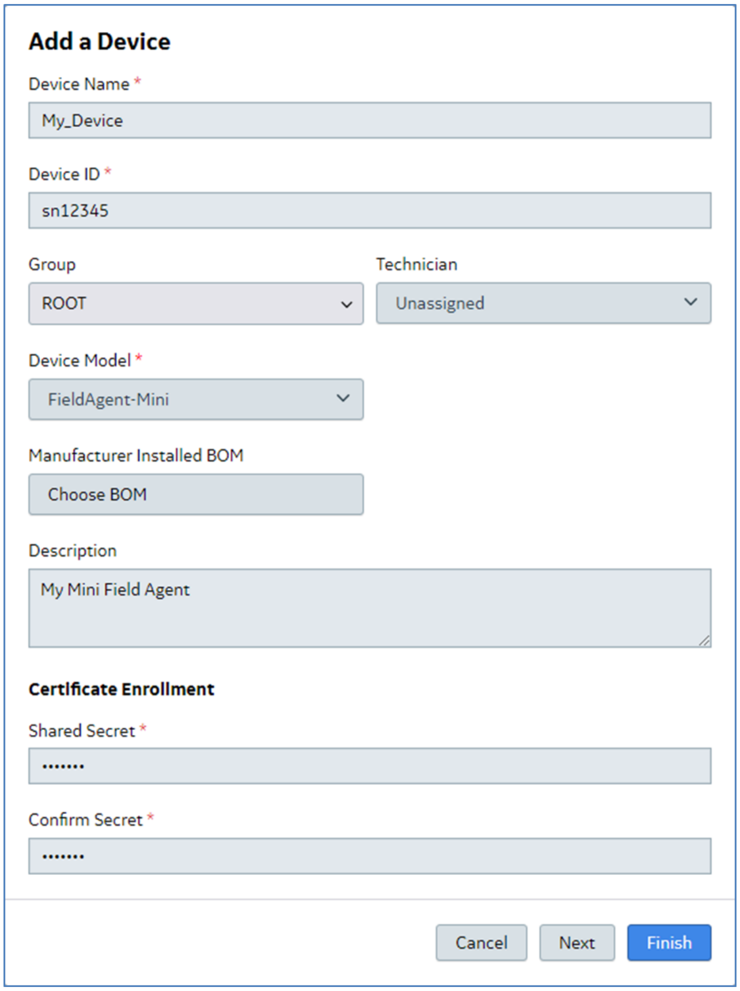
The Operator can create a device representation in EdgeManager from the Device Manager tab by selecting Add from the action's menu.

Figure 26: Add New Device in Device Manager Tab



In the new dialog that appears, fill in the device details and press the Finish button.

Figure 27: Add Device Dialog



Add a Device

Device Name *: My_Device

Device ID *: sn12345

Group: ROOT

Technician: Unassigned

Device Model *: FieldAgent-Mini

Manufacturer Installed BOM: Choose BOM

Description: My Mini Field Agent

Certificate Enrollment

Shared Secret *: •••••••

Confirm Secret *: •••••••

If it is desired that this device be a member of a group, the group can be created on the Groups page of the Device Manager tab. Then, the new group must be selected on the Add a Device page before pressing the Finish button. To select the group, use the small downward facing triangle to the right of the Group text on the Add a Device page.

The Device Name is used to list and filter the device in EdgeManager . The Device Name should be unique and descriptive and can consist of upper and lower-case characters and numbers.

The Device ID is used to enroll the device in EdgeManager . While the Device ID is typically a serial number, another option is using the MAC address of the WAN interface, which is available on the Field Agent's physical label and is auto-populated on the Predix Cloud Enrollment page in the Field Agent's Web Console. The Device ID can consist of lower-case characters and numbers. Any upper-case characters entered during device creation will be converted to lower-case.

The Device Model is the Field Agent model type. Currently, the supported Field Agent Device Models are "FieldAgent-Mini" and "FieldAgent".

(Optional) The Description is a freeform text field.

The Shared Secret is used with Certificate enrollment and is a code that will be used only for enrollment purposes on this device. Once the field agent is enrolled, the secret is no longer needed.

By clicking the Next button, optional Location information can be configured, including:

- City (string)
- State (string)
- Country (string)
- Time Zone (use the drop-down to select the closest city in the desired time zone)
- Latitude (floating point, in Degrees)
- Longitude (floating point, in Degrees)
- Elevation

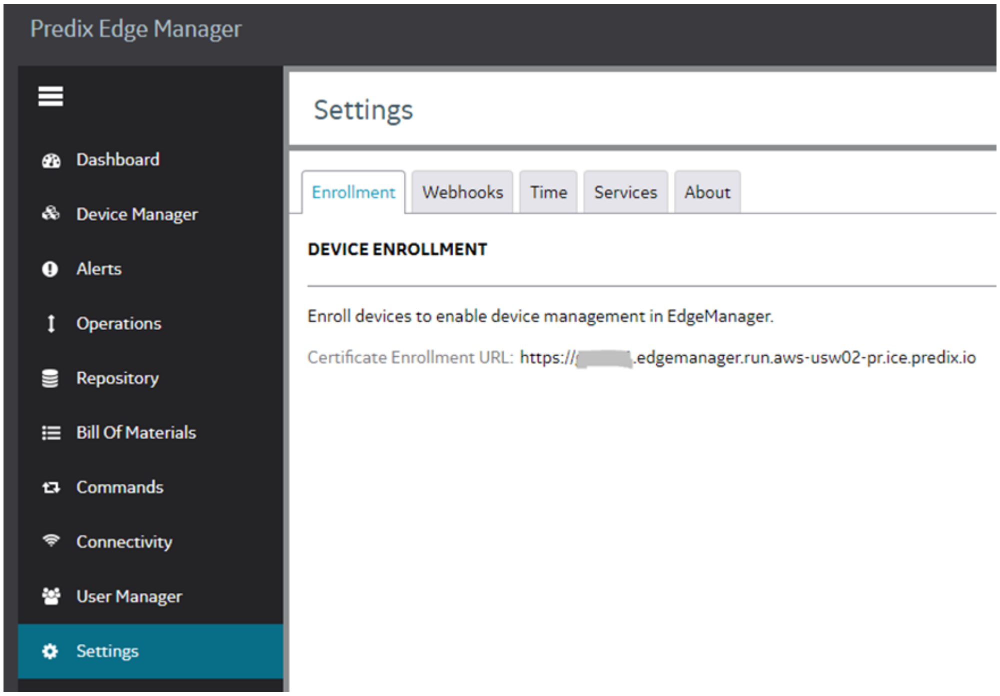
After required and desired optional fields are configured, click the Finish button to create the device representation.

Obtain Enrollment Information

The three pieces of information needed for enrollment are listed below along with where they can be found in EdgeManager .

1. Certificate Enrollment URL is available in EdgeManager on the Settings menu pick.

Figure 28: View Certificate Enrollment via Settings Tab



Settings

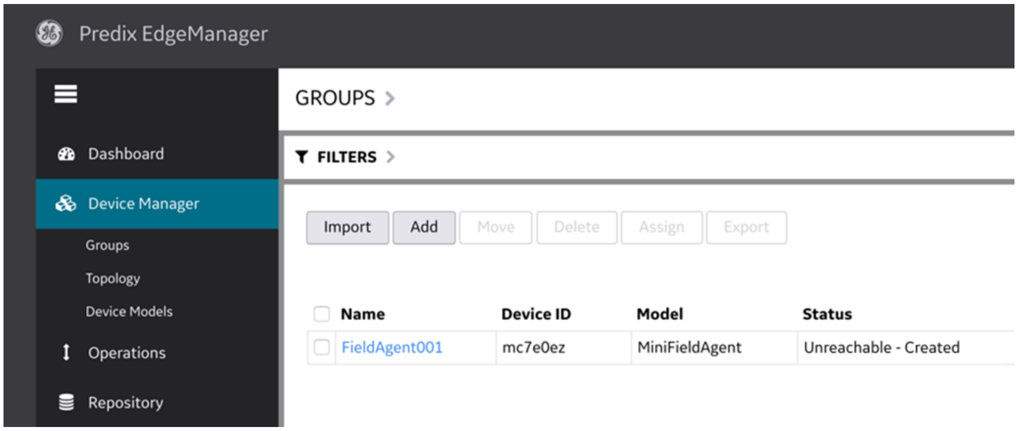
DEVICE ENROLLMENT

Enroll devices to enable device management in EdgeManager.

Certificate Enrollment URL: https://[redacted].edgemanager.run.aws-usw02-pr.ice.predix.io

2. Device ID is available in the EdgeManager Device Manager tab.

Figure 29: View Device ID via Device Manager Tab



□	Name	Device ID	Model	Status
□	FieldAgent001	mc7e0ez	MiniFieldAgent	Unreachable - Created

3. Shared Secret is remembered by the user from when it was entered in Figure 27 above.

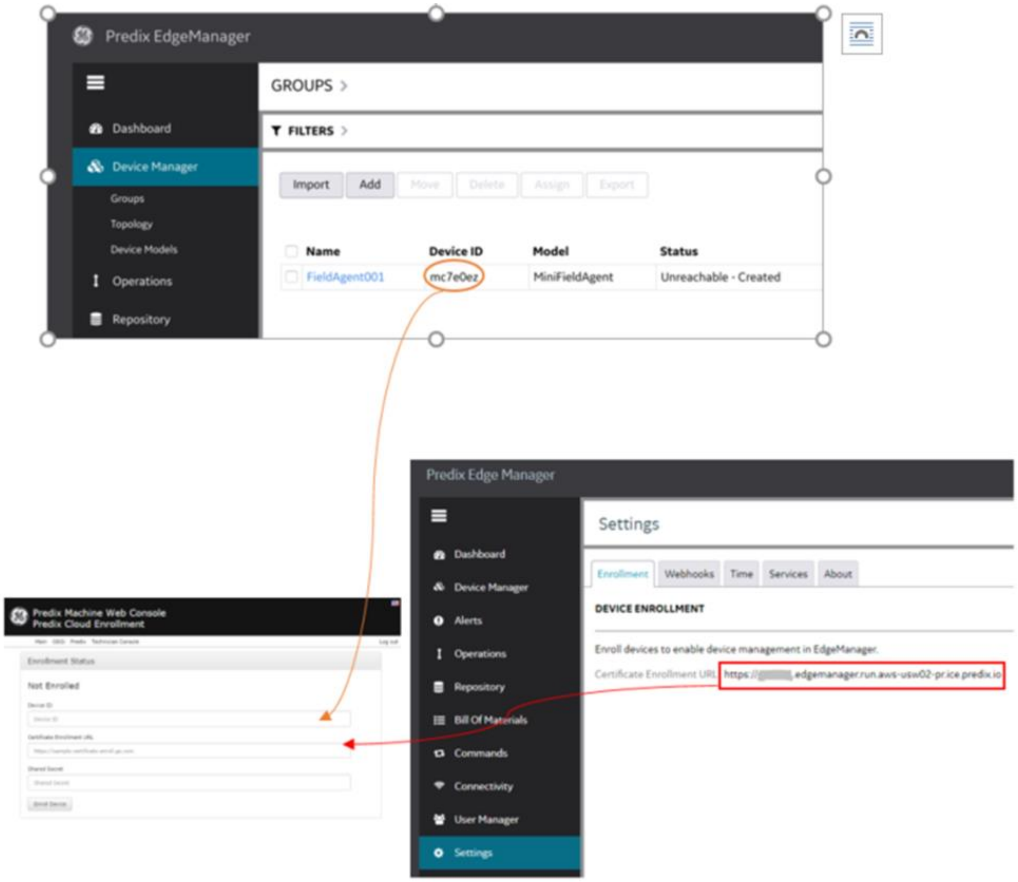
Follow the steps defined in Section5.5, Log into the Web Console, for the Field Agent being enrolled, and navigate to the Predix Cloud Enrollment page under Technician Console, Predix Cloud Enrollment.

Enter Enrollment Information and Trigger Enrollment

Enter the enrollment information into the Predix Cloud Enrollment page. If the Technician is using a computer that has network access to both the Field Agent LAN (e.g. via wired Ethernet) and the Internet (e.g. via wireless Ethernet), then the Technician can copy this information from

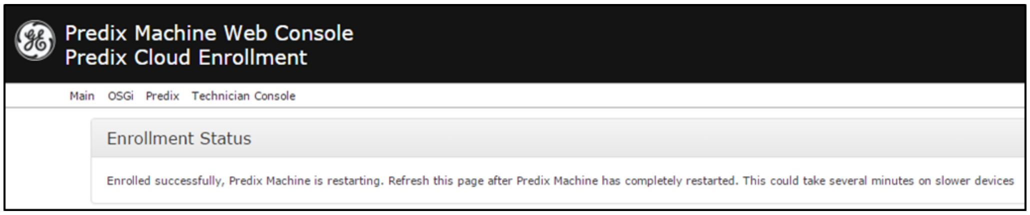
EdgeManager and paste it into the Predix Cloud Enrollment page. The following is an example of where information is copied from EdgeManager into the Predix Cloud Enrollment page.

Figure 30: Copy Info to Cloud Example



After pressing the Enroll Device button, the Enroll Device button will become grayed out while the Field Agent generates a certificate and sends the corresponding Certificate Signing Request (CSR) to the Predix Cloud to be signed and for enrollment to complete. This process can take up to 30 seconds to complete before an enrollment success message is displayed. After certificate enrollment is complete, Predix Machine will restart itself before it appears in EdgeManager as Online.

Figure 31: Enrollment Status Confirmation


Predix Machine Web Console
Predix Cloud Enrollment

Main OSGi Predix Technician Console

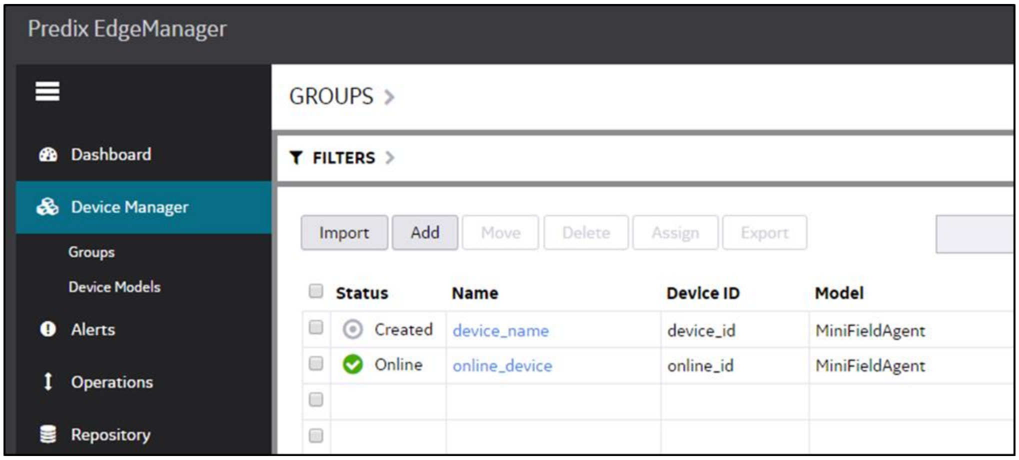
Enrollment Status

Enrolled successfully, Predix Machine is restarting. Refresh this page after Predix Machine has completely restarted. This could take several minutes on slower devices

Verify the Field Agent is Online in EdgeManager

Within one minute of completing the enrollment process, the Technician should notice an indication that the Field Agent is connected to the Predix Cloud. The Operator should verify that the Field Agent is listed as Online under the Status column of the EdgeManager 's Device Manager.

Figure 32: Device Online Status Indicated



□	Status	Name	Device ID	Model
□	○ Created	device_name	device_id	MiniFieldAgent
□	✓ Online	online_device	online_id	MiniFieldAgent
□				
□				

Chapter 6: Using the Field Agent

6.1 Device Management

6.1.1 Field Agent Status

Using EdgeManager - Field Agent Health Status and Resource Usage

The Device Manager in EdgeManager displays several health indications for each Field Agent including reachability, processor utilization, memory utilization, and disk utilization. In the Devices page of the Device Manager, the Status column shows the reachability of each Field Agent. The meanings of each status are displayed in the following table.

Status	Meaning
Created	The Field Agent has not yet been enrolled
Offline	The Field Agent is enrolled but is currently not connected to EdgeManager
Online	The Field Agent is enrolled and currently connected to EdgeManager

By clicking the Device Name hyperlink on the Devices page, additional health information specific to the Field Agent can be seen on the Summary tab. Under the Health Status section, the reachability status is repeated along with a date and time of the communication with the Field Agent. Under the Resource Usage section, the processor utilization, memory utilization, and disk utilization percentages are shown. If the Field Agent is not currently Online, the Resource Usage values shown represent the values sent from the Field Agent when it was last Online.

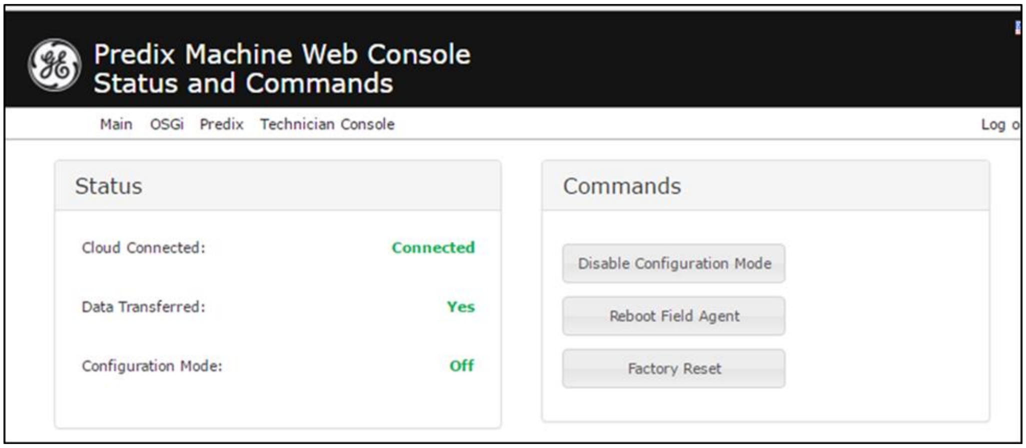
Using Web Console – Status Information

From the Web Console, navigate to the Technician Console, Status and Commands page. On this page, the following information is displayed, depending upon which Field Agent is deployed:

Status	Meaning	MFA	EFA	VFA
Cloud Connected	The Field Agent is enrolled and currently connected to EdgeManager .	Shown	Shown	Shown
Data Transferred	A Machine Adapter in the Field Agent has read data and has sent this data to the Hoover Spillway. (The Hoover Spillway normally then sends this data to a Time Serves DB in the cloud.)	Shown	Shown	Shown

Status	Meaning	MFA	EFA	VFA
Configuration Mode	MFA: The Wi-Fi hotspot is on. EFA & VFA: The Web Console is accessible.	Not Shown	Shown	Not Shown, because it is always in Configuration Mode.

Figure 33: Status & Commands Web Page (Predix Web Console)



Status

Cloud Connected: Connected

Data Transferred: Yes

Configuration Mode: Off

6.1.2 Field Agent Commands

Using EdgeManager - Supported Field Agent Commands

EdgeManager can be used to send commands to one or more Field Agents. The list of available commands is extensible, but the core list of commands supported on all A&C Field Agents and meanings are listed below. Additional information on Commands, including how to add and delete Custom Commands, can be found by searching for "Commands Overview" in https://docs.predix.io. Note that built-in commands not included in the list below may not be supported by A&C Field Agents. For example, the commands "HTTP Tunnel: Enable" and "HTTP Tunnel: Disable" and all Application Container commands are not supported.

Command	Meaning	Predix Machine		
		16.2	17.1	17.2
Predix Machine: Get Available Logs	Retrieves a list of available log files that can be downloaded from the Field Agent to EdgeManager , which is then accessible in the user's browser. The individual log files can be specified to be downloaded from the "Predix Machine: Get Log" command.	No	Yes	Yes
Predix Machine: Get Log	Downloads a specified log file from the Field Agent to EdgeManager , which is then accessible in the user's browser. The specified log file defaults to the Predix Machine log file (machine.log), but can be parameterized using the output of the "Predix Machine: Get Available Logs" command.	Yes, without parameters	Yes	Yes

Command	Meaning	Predix Machine		
		16.2	17.1	17.2
Predix Machine: Get IP Address	Retrieves the list of network interfaces on the Field Agent and the IP addresses for each interface.	No	Yes	Yes
Predix Machine: Refresh	Restarts the OSGi™ bundles while leaving the rest of the Predix Machine container running.	Yes	Yes	Yes
Predix Machine: Restart	Restarts the entire Predix Machine container including all bundles.	Yes	Yes	Yes
Predix Machine: Set Polling Interval	Updates the rate at which Predix Machine contacts the Predix Cloud to report status and retrieve operations to run.	Yes	Yes	Yes
Predix Connectivity: Set VPN Log Verbosity	Sets the logging level of the VPN service.	No	No	Yes
Predix Connectivity: Start VPN Management	Opens a Virtual Private Network connection between the Field Agent and Edge Manager.	No	No	Yes
Predix Connectivity: Stop VPN Management	Closes and removes the Virtual Private Network connection between the Field Agent and Edge Manager.	No	No	Yes
Predix Machine: Upload Configurations	Uploads the Predix Machine configuration directory from the Field Agent to the EdgeManager Repository. The configuration can then be downloaded from the EdgeManager Repository to a connected computer.	Yes	Yes	Yes
Technician Console: Disable	Disables the Web Console, closing TCP port 8443 on the LAN	Yes	Yes	Yes
Technician Console: Enable	Enables the Web Console, opening TCP port 8443 on the LAN	Yes	Yes	Yes

Using the Device Manager in EdgeManager , commands can be sent to one Field Agent at a time or to several Field Agents or groups of Field Agent at a time. Commands can also be scheduled to occur immediately for Online Field Agents, or scheduled to occur at any future date and time for Online or Offline Field Agents. If a command is scheduled to occur immediately for an Offline Field Agent, or at a date or time that the Field Agent becomes Offline, then the command will be executed the next time the Field Agent connects and becomes Online. The specific instructions to send commands from Device Manager to Field Agents can be found by searching for “Executing Commands” in https://docs.predix.io.

Each Field Agent maintains a history of each command run against it and the corresponding command status. This history can be seen by navigating to the device page for the Field Agent and selecting the Commands tab. Command operation failures on Online Field Agents can be diagnosed either by reading the error entry in the Log Service of the Field Agent’s Predix Machine Web Console or by reading the error entry in the Predix Machine log file retrieved using the “Predix Machine: Get Log” command.

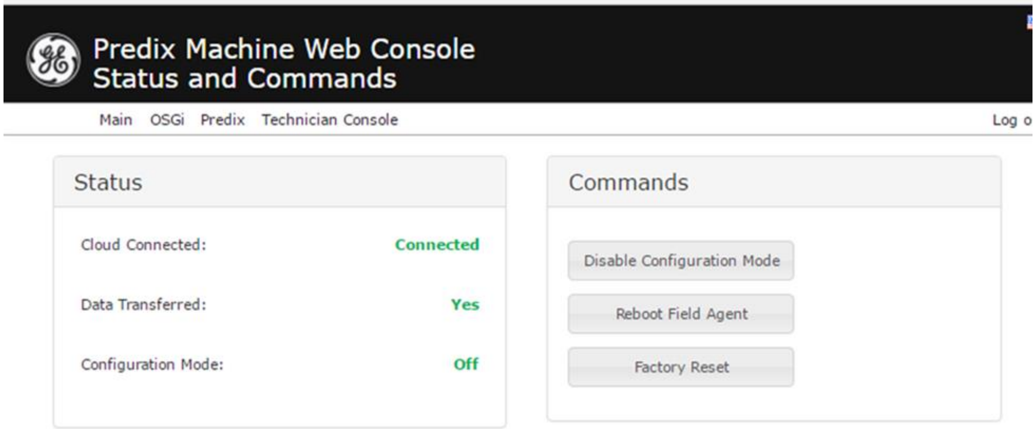
Using Web Console – Sending Commands

From the Web Console, navigate to the Technician Console, Status and Commands page. On this page, the operator can perform the following commands, depending upon which Field Agent are being used:

Table 11:

Command	Meaning	MFA	EFA	VFA
Disable Configuration Mode	MFA: Disables the Wi-Fi hotspot. EFA & VFA: Disables access to the Web Console.	Not Available	Available	N/A
Reboot Field Agent	Reboots the Field Agent. Note: For a CPE400 it does NOT reboot the controller—it only reboots the Field Agent.	Available	Available	Available
Factory Reset	Resets the Field Agent to the Factory Configuration	Not Available	Available	Not Available

Figure 34: Status & Commands Web Page (Predix Web Console)



Cloud Connected: Connected
Data Transferred: Yes
Configuration Mode: Off

When Might a Factory Reset be Required?

A factory reset may be required in the following scenarios:

- Reset the IP address to default
- Reset the Predix Machine Web Console username or password to default
- There is a desire to re-enroll the Field Agent in EdgeManager .
- There is a desire to restore the Predix Machine installation to the factory image.
- The “ON” or “FA OK” LED does not turn solid after five minutes on boot up indicating Predix Machine failed to run.

Since the factory reset operation deletes the existing Predix Machine content and restores Predix Machine to a pristine copy, any custom configuration or application modifications will be lost. It is highly recommended that production configuration and application modifications be stored in the EdgeManager Repository so they can be easily re-deployed after a factory reset.

6.1.3 Configuration Management

Many Predix Machine bundles use configuration files to specify their behavior. These configuration files can be managed both from EdgeManager across multiple Field Agents and from the Predix Machine Web Console for an individual Field Agent. In both cases, a default set of configuration and application files must be obtained as a starting place for making modifications and additions. The default collection of configuration files is referred to as the Configuration Template. Configuration Templates for the various Field Agent types can be found below.

Mini Field Agent Predix Machine configuration files can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

Embedded Field Agent Predix Machine configuration files can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

Virtual Field Agent Predix Machine configuration files can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

EdgeManager Configuration Management

Note: *Not all configuration files that ship with Predix Machine will be applied when deployed from EdgeManager . For example, the identity configuration file is unique to each Field Agent, and is therefore left unaffected on the Field Agent even if a new identity configuration file is deployed from EdgeManager .*

Below is a list of Predix Machine configuration files that are not applied to the Field Agent by default. This list can be found in the configuration/install/install.sh script inside the Configuration Template.

- com.ge.dspmicro.predixcloud.identity.config
- com.ge.dspmicro.device.techconsole.config
- org.apache.http.proxyconfigurator-0.config
- com.ge.dspmicro.storeforward-taskstatus.config

The following files are not applied when the Field Agent is running Predix Machine 17.1 or earlier. These files are applied in Predix Machine 17.2 and later:

- com.ge.dspmicro.storeforward-0.config
- com.ge.dspmicro.storeforward-1.config
- com.ge.dspmicro.storeforward-2.config
- com.ge.dspmicro.storeforward-3.config

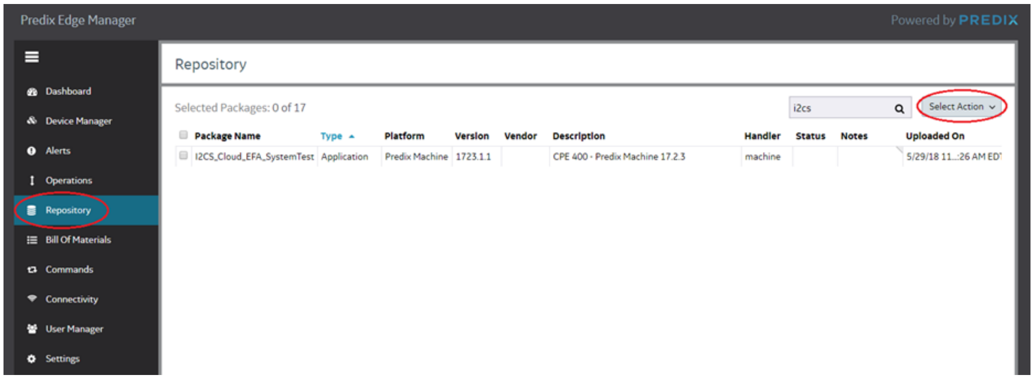
Instructions for modifying configuration files to send Modbus TCP or OPC UA data from a connected industrial device to the Predix Time Series Database can be found in Section 6.2, Configuring Data Collection and Sending Data to the Cloud. For additional information on configuring other machine adapters (i.e. EGD, Ethernet IP, OSI-PI), refer to the Field Agent Machine Adapters User Guide, GFK-3019 in Field Agent Manuals.

To make a group of configuration files available in EdgeManager to deploy to one or more Field Agents, the entire outer “configuration” directory must be compressed into a zip file such that decompression will result in a “configuration” directory with all contents contained within. Refer to the sub-section Compression Utilities below for more information.

The configuration zip file must then be uploaded to EdgeManager in the Repository tab. Here are the steps to upload your zip file:

1. Go to your EdgeManager instance.
2. Go to “Repository” in the navigation panel and click on “Select Action” > “Upload”.

Figure 35: EdgeManager Repository Page

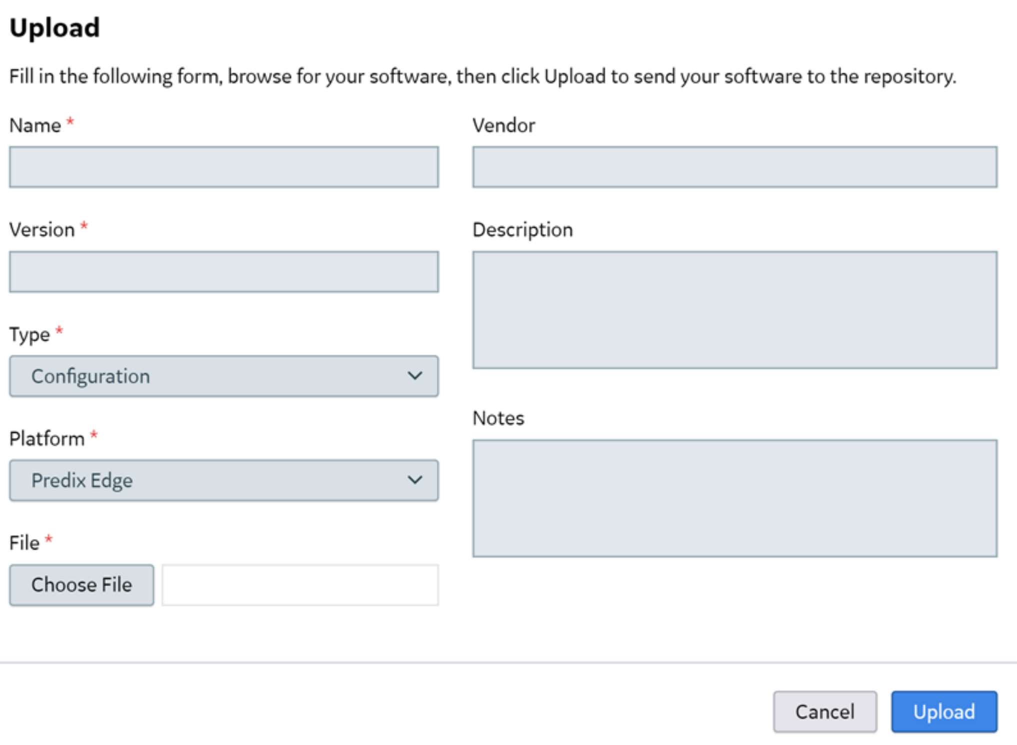


Selected Packages: 0 of 17

□	Package Name	Type ▲	Platform	Version	Vendor	Description	Handler	Status	Notes	Uploaded On
□	I2CS_Cloud_EFA_SystemTest	Application	Predix Machine	1723.1.1		CPE 400 - Predix Machine 17.2.3	machine			5/29/18 11..:26 AM EDT

3. A dialog box will pop up; fill out the information, as follows:
   a. Name – fill out the name for your repository.
   b. Version – fill out the version of this file. Note that if you use the same name for the package for multiple versions, the package will get grouped together automatically.
   c. Type – select the appropriate type for the package.
      – Select “Configuration” if you are uploading the zipped configuration folder.
      – Platform – choose “Predix Machine”.
      – File – select the zipped folder from the template.

Figure 36: EdgeManager Upload package



Upload

Fill in the following form, browse for your software, then click Upload to send your software to the repository.

Name *

Version *

Type *
Configuration

Platform *
Predix Edge

File *

Vendor

Description

Notes

4. Press “Upload”.
5. Repeat steps 3-4 for the other zipped folders. Ensure that they both uploaded successfully by checking the “Repository” page.

Once a Configuration is uploaded to the EdgeManager Repository, it can be deployed to one or more Field Agents from the Device Manager or Operations pages. Here are the steps:

1. Go to the Device Manager on the navigation bar.
2. Add one or more Field Agents or groups of Field Agents to the Selected Items list.
3. Click the “Device Operations” dropdown button and press the “Deploy Configuration” button.
4. Select the Configuration to deploy and press the Schedule button.
5. Select the date and time for the update to occur and press the Submit button. If a Configuration deployment is scheduled to occur immediately for an Offline Field Agent, or at a date or time that the Field Agent becomes Offline, then the Configuration will be deployed the next time the Field Agent connects and becomes Online.

Each Field Agent maintains a history of each Configuration deployment performed including the deployment status. This history can be seen by navigating to the device page for the Field Agent and selecting the Configuration tab. Configuration deployment failures for Online Field Agents can be diagnosed by reading the Execution Logs that can be downloaded for each deployment. Additional error messages may be logged to the Predix Machine log file which can be read from the OSGi Log Service in the Field Agent’s Predix Machine Web Console or by downloading the Predix Machine log file using the Predix Machine: Get Log command.

Compression Utilities

Most compression utilities that support the zip format will create zip files that are compatible with the Field Agent. When creating a zip archive, always use the default compression-level settings and do not include extra file attributes.

Note: *Some compression utilities always include extra file attributes with no setting to disable this behavior. These utilities may create zip files that are incompatible with the MFA.*

The following are recommended methods for creating zip files using built-in functionality on each platform.

Windows®:

Windows Explorer includes a built-in file compression utility. To create a zip file:

1. Open Windows Explorer.
2. Browse to and right-click on the "configuration" directory you wish to compress.
3. Select the "Send to" > "Compressed (zipped) folder" menu item.

macOS™:

The macOS Finder® can be used to create a zip file compatible with the EFA. To create a zip file using the Finder:

1. Switch to the Finder.
2. Browse to and right-click on the "configuration" folder you wish to compress.
3. Select the "Compress '<folder name>'" menu item.

Note: *The "Compress" feature found in the macOS Finder creates zip files that are incompatible with the MFA. Some third-party applications from the Apple App Store® may also create zip files incompatible with the MFA.*

The macOS Terminal can be used to create a zip file compatible with all Field Agents. To create a zip file using the Terminal:

1. Open the Terminal application (in /Applications/Utilities).
2. Change to the directory containing the configuration directory. If you drag a folder from the Finder and drop it on the Terminal window, the path to that folder will be added at the cursor location.
3. Use the following command: zip -r -X <archive_name>.zip <directory name> (replace <archive_name> with the name for the zip file and <directory name> with the name of the directory). If your file name contains spaces, you will need to surround the entire file name (including the .zip) with quotes ("").

Note: *If you are not comfortable using the Terminal, the following third-party utilities have been verified to create zip files compatible with the MFA when using their default settings:*

- *StuffIt™ 16 (*http://my.smithmicro.com/stuffit-deluxe-mac.html)
- *WinZip® (*http://www.winzip.com/mac/en/index.html*)*

Both utilities can be found in the Apple App Store or purchased directly from their manufacturer.

Linux:

A compatible zip file can be created from the shell. To create a zip file:

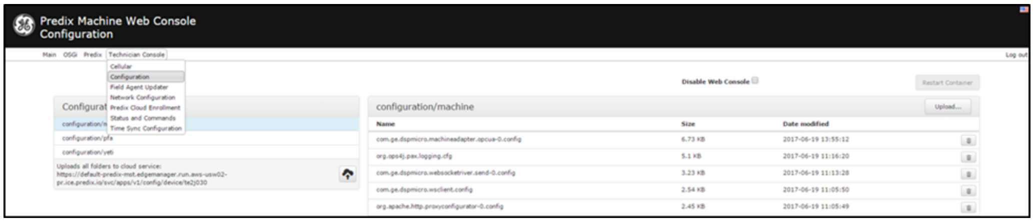
1. Open the shell of your choice.
2. Change to the directory containing the configuration directory.
3. Use the following command: zip -r -X <archive name>.zip <directory name> (replace <archive_name> with the name for the zip file and <directory name> with the name of the directory). If your file name contains spaces, you will need to surround the entire file name (including the .zip) with quotes (“”).

Predix Machine Web Console Configuration Management

Once the Configuration and Application Template files have been deployed to a Field Agent from the EdgeManager Repository, two additional Predix Machine Web Console services are enabled that simplify the process of adjusting the configuration of an individual Field Agent. These services can be used to prototype configuration adjustments for an application before it is packaged into a configuration zip file, uploaded to the EdgeManager Repository, and deployed to one or more Field Agents.

The Technician Console, Configuration page provides a way to delete existing configuration files and upload new configuration files.

Figure 37: Predix Console Configuration Page



configuration/m
configuration/pfa
configuration/yeti

Uploads all folders to cloud service:
https://default-predix-mst.edgemanager.run.aws-usw02-pr.ice.predix.io/svc/apps/v1/config/device/te2j030

Disable Web Console □

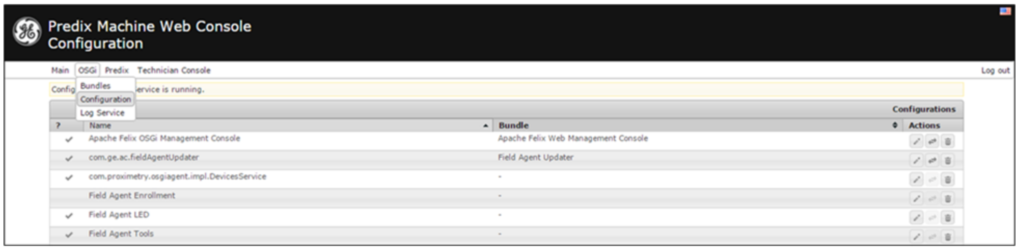
configuration/machine

Name	Size	Date modified
com.ge.dspmicro.machineadapter.opcua-0.config	6.73 KB	2017-06-19 13:55:12
org.ops4j.pax.logging.cfg	5.1 KB	2017-06-19 11:16:20
com.ge.dspmicro.websocketriver.send-0.config	3.23 KB	2017-06-19 11:13:28
com.ge.dspmicro.wsclient.config	2.54 KB	2017-06-19 11:05:50
org.apache.http.proxyconfigurator-0.config	2.45 KB	2017-06-19 11:05:49

Note: *Depending on the configuration file that is modified, restarting the Predix Machine container may be required. This can be performed by pressing the Restart Container button in the upper right-hand corner, or by sending the “Container: Restart” command from EdgeManager .*

The OSGi, Configuration page allows for fine tune adjustments of parameters within most of the available configuration files

Figure 38: Use OGSi Config Page to Adjust Parameters



Predix Machine Web Console
Configuration

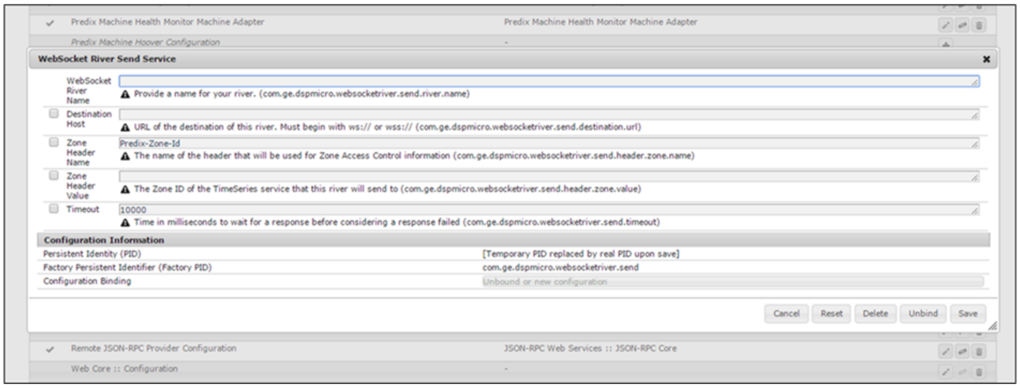
Config ...ervice is running.

Configurations

?	Name	Bundle	Actions
✓	Apache Felix OSGi Management Console	Apache Felix Web Management Console	
✓	com.ge.ac.fieldAgentUpdater	Field Agent Updater	
✓	com.proximetry.osgiagent.impl.DevicesService	-	
	Field Agent Enrollment	-	
✓	Field Agent LED	-	
✓	Field Agent Tools	-	

To adjust any of the parameters in a given configuration file, click the row corresponding to the bundle to be updated, edit the parameters, and press the Save button.

Figure 39: Edit/Save Parameters



✓	Predix Machine Health Monitor Machine Adapter	Predix Machine Health Monitor Machine Adapter
	Predix Machine Hoover Configuration	-

WebSocket River Send Service

	WebSocket River Name	 Provide a name for your river. (com.ge.dspmicro.websocketriver.send.river.name)
□	Destination Host	 URL of the destination of this river. Must begin with ws:// or wss:// (com.ge.dspmicro.websocketriver.send.destination.url)
□	Zone Header Name	Predix-Zone-Id The name of the header that will be used for Zone Access Control information (com.ge.dspmicro.websocketriver.send.header.zone.name)
□	Zone Header Value	 The Zone ID of the TimeSeries service that this river will send to (com.ge.dspmicro.websocketriver.send.header.zone.value)
□	Timeout	10000 Time in milliseconds to wait for a response before considering a response failed (com.ge.dspmicro.websocketriver.send.timeout)

Configuration Information

Persistent Identity (PID)	[Temporary PID replaced by real PID upon save]
Factory Persistent Identifier (Factory PID)	com.ge.dspmicro.websocketriver.send
Configuration Binding	Unbound or new configuration

✓	Remote JSON-RPC Provider Configuration	JSON-RPC Web Services :: JSON-RPC Core
	Web Core :: Configuration	-

6.1.4 Application Management

In addition to configuring existing Predix Machine OSGi bundles to perform activities like sending Time Series data to the Predix Cloud, Field Agents can have their application capabilities expanded by adding and running new applications. These application bundles can be managed both from EdgeManager for multiple Field Agents and from the Predix Machine Web Console for an individual Field Agent. In both cases, a default set of application bundles must be obtained as a starting place for making additions. The default collection of application files is referred to as the Application Template. Application Templates for the various Field Agent types can be found below.

Mini Field Agent Predix Machine application bundles can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

Embedded Field Agent Predix Machine application bundles can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

Virtual Field Agent Predix Machine application bundles can be obtained from the following location:

https://www.emerson.com/Industrial-Automation-Controls/support

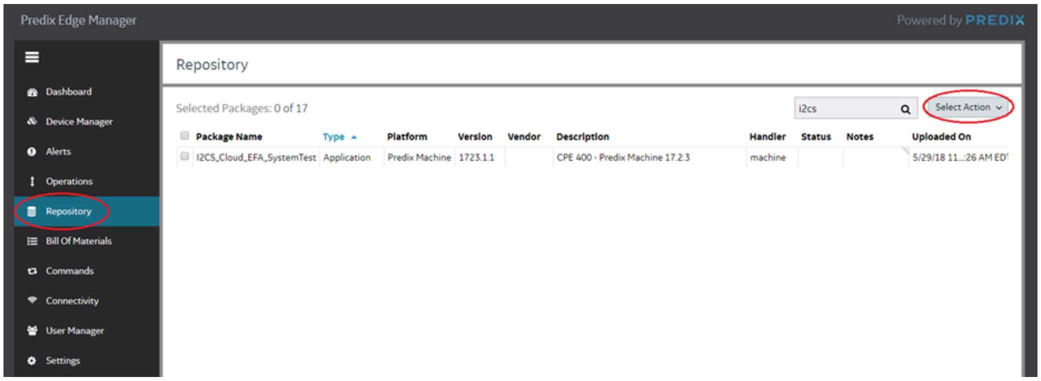
EdgeManager Application Management

In order to make a group of application bundles available in EdgeManager to deploy to one or more Field Agents, the entire outer "machine" directory must be compressed into a zip file such that decompression will result in a "machine" directory with all contents contained within. Refer to the sub-section Compression Utilities in Section 6.1.3 for more information.

The machine zip file must then be uploaded to EdgeManager in the Repository tab. Here are the steps to upload your zip file:

1. Go to your EdgeManager instance.
2. Go to "Repository" in the navigation panel and click on "Select Action" > "Upload".

Figure 40: EdgeManager Repository Page



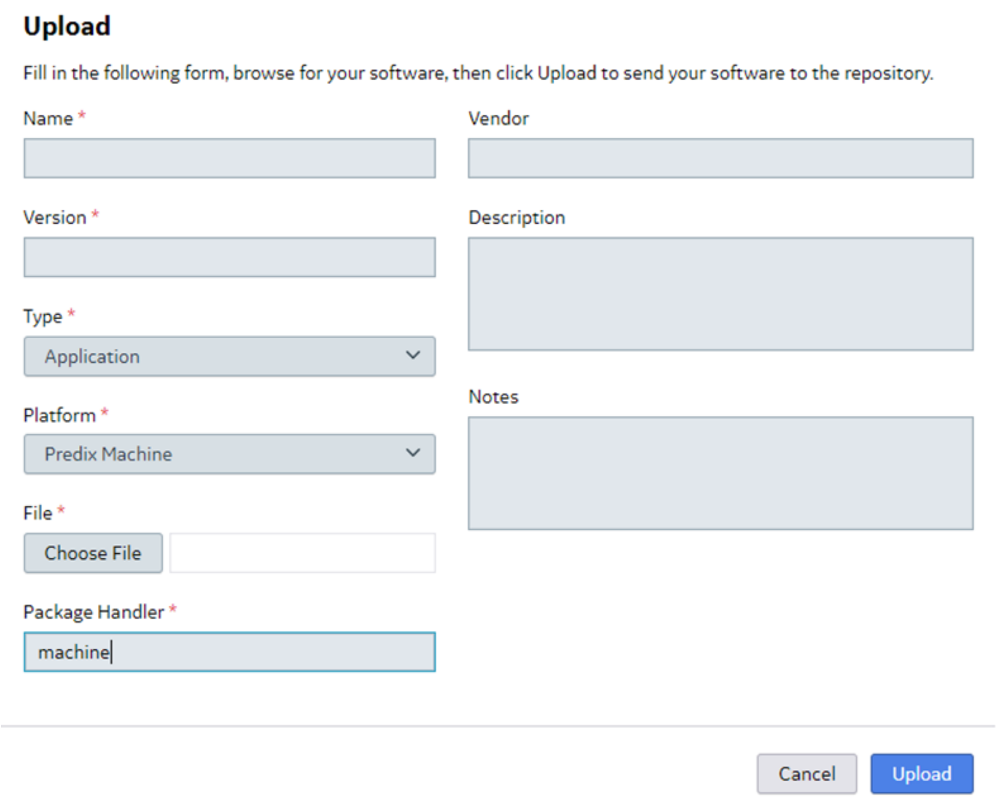
Repository

Selected Packages: 0 of 17

□	Package Name	Type	Platform	Version	Vendor	Description	Handler	Status	Notes	Uploaded On
□	I2CS_Cloud_EFA_SystemTest	Application	Predix Machine	1723.1.1		CPE 400 - Predix Machine 17.2.3	machine			5/29/18 11...26 AM EDT

3. A dialog box will pop up; fill out the information, as follows:
   a. Name – fill out the name for your repository.
   b. Version – fill out the version of this file. Note that if you use the same name for the package for multiple versions, the package will get grouped together automatically.
   c. Type – select the appropriate type for the package.
      – Select "Application" if you are uploading the zipped configuration folder.
   d. Platform – choose "Predix Machine".
   e. File – select the zipped folder from the template.
   f. Package Handler – "machine"

Figure 41: EdgeManager Upload package



Upload

Fill in the following form, browse for your software, then click Upload to send your software to the repository.

Type *: Application

Platform *: Predix Machine

Package Handler *: machine

4. Press "Upload".
5. Repeat steps 3-4 for the other zipped folders. Ensure that they both uploaded successfully by checking the "Repository" page.

Once an application is uploaded to the EdgeManager Repository, it can be deployed to one or more Field Agents from the Device Manager or Operations pages. Here are the steps:

1. Go to the Device Manager on the navigation bar.
2. Add one or more Field Agents or groups of Field Agents to the Selected Items list.
3. Click the "Device Operations" dropdown button and press the "Deploy Software" button.
4. Select the Application to deploy and press the Schedule button.
5. Select the date and time for the update to occur and press the Submit button. If an Application deployment is scheduled to occur immediately for an Offline Field Agent, or at a date or time that the Field Agent becomes Offline, then the Application will be deployed the next time the Field Agent connects and becomes Online.

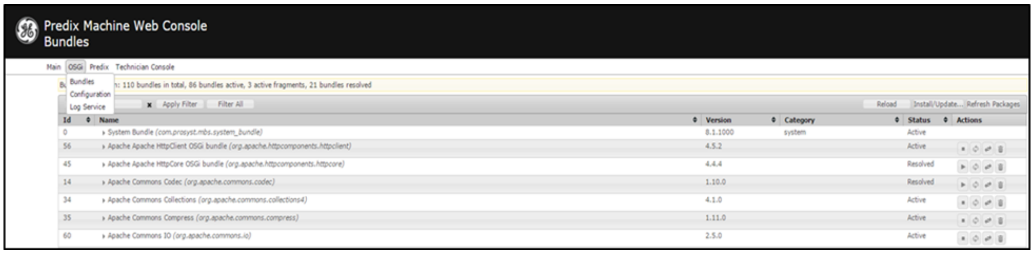
Each Field Agent maintains a history of each Application deployment performed including the deployment status. This history can be seen by navigating to the device page for the Field Agent and selecting the Software tab. Application deployment failures for Online Field Agents can be diagnosed by reading the Execution Logs that can be downloaded for each deployment. Additional error messages may be logged to the Predix Machine log file which can be read from the OSGi Log Service in the Field Agent's Predix Machine Web Console or by downloading the Predix Machine log file using the Predix Machine: Get Log command.

Predix Machine Web Console Application Management

Once the Configuration and Application Templates files have been deployed to a Field Agent from the EdgeManager Repository, one additional Predix Machine Web Console service is enabled that simplifies the process of adding or removing application bundles on an individual Field Agent. This service can be used to develop and debug new application bundles before they are packaged into a machine zip file, uploaded to the EdgeManager Repository, and deployed to one or more Field Agents.

The OSGi, Bundles page allows individual application bundles to be installed, updated, removed, stopped, and started.

Figure 42: Use Bundles Page to Control Applications



Bu[...]n: 110 bundles in total, 86 bundles active, 3 active fragments, 21 bundles resolved

Id	Name	Version	Category	Status	Actions
0	System Bundle (com.prosyst.mbs.system_bundle)	8.1.1000	system	Active	
56	Apache Apache HttpClient OSGi bundle (org.apache.httpcomponents.httpclient)	4.5.2		Active	■ ⟳ ✎ 🗑
45	Apache Apache HttpCore OSGi bundle (org.apache.httpcomponents.httpcore)	4.4.4		Resolved	▶ ⟳ ✎ 🗑
14	Apache Commons Codec (org.apache.commons.codec)	1.10.0		Resolved	▶ ⟳ ✎ 🗑
34	Apache Commons Collections (org.apache.commons.collections4)	4.1.0		Active	■ ⟳ ✎ 🗑
35	Apache Commons Compress (org.apache.commons.compress)	1.11.0		Active	■ ⟳ ✎ 🗑
60	Apache Commons IO (org.apache.commons.io)	2.5.0		Active	■ ⟳ ✎ 🗑

To install or update an application bundle, click the “Install/Update…” button in the upper right-hand corner to open the “Upload/Install Bundles” dialog. Click the “Choose File” button, browse to the JAR file of the application bundle, and click the “Open” button. If the bundle should be started immediately, check the “Start Bundle” check box. If the list of available packages should be refreshed automatically when the bundle is installed or updated, click the “Refresh Packages” check box. Click the “Install or Update” button to perform the installation.

To delete an application bundle, click the trash can button to the far right of the bundle row.

To stop an application bundle, click the stop sign button to the far right of the bundle row. When an application bundle is stopped, the stop sign button is replaced with a start sign button. To start the application bundle, click the start sign button.

6.1.5 How to Open Ports on a Field Agent

Some applications and Machine Adapters may require opening one or more of the user or registered TCP or UDP ports (starting at port number 1024). If a Machine Adapter requires connecting to a server on another device, a port does not need to be opened in this Field Agent’s firewall since outgoing client requests are permitted by default. For example, the OPC UA Machine Adapter acts as a client that connects to an external OPC UA server, so the default firewall does not need to be modified in this case. However, if an application or Machine Adapter requires listening on a port for incoming network traffic, the firewall needs to be modified to permit incoming traffic on this port. For example, the EGD Machine Adapter requires UDP port 18246 to be opened in the Field Agent’s firewall.

Currently, the MFA and VFA support opening additional ports through the firewall on Local Area Network (LAN) interfaces. The EFA also supports opening additional ports, but since there is no dedicated LAN interface on the EFA, the ports are opened on the WAN interface. Opening ports on the EFA WAN is intended for use cases involving an EFA connected to a LAN from which data is being collected. Whenever EFA WAN ports are opened, it is the responsibility of the customer to set up and configure proper routers and firewalls between the LAN and the Internet to limit outgoing traffic to only what is required for the EFA to communicate with the EdgeManager and the Time Series database.

Refer to the Field Agent Machine Adapters User Guide, GFK-3019, for the list of required ports to be opened for each supported Machine Adapter. Refer to the Field Agents Secure Deployment Guide, GFK-3009, for the cybersecurity considerations of opening non-default ports on the Field Agent's firewall. Beginning with MFA release 1.3.0, the EGD UDP port is open by default.

To open ports, the user edits the port's configuration file, deploys the new file, and activates it.

The Ports Configuration File

The ports configuration file (com.ge.ac.fieldagent.network.ports.cfg) is available as part of the Configuration template associated with a Field Agent. For a link to this template, refer to Section 6.1.3, Configuration Management. In this configuration file there is a line for TCP ports and a line for UDP ports. The following example shows opening up TCP ports 8080 and 8081 and UDP ports 7937 and 18246.

```
com.ge.ac.fieldagent.network.ports.open.lan.tcp="8080,8081"

com.ge.ac.fieldagent.network.ports.open.lan.udp="7937,18246"
```

Once the com.ge.ac.fieldagent.network.ports.cfg file is edited as required for this job, it must be deployed. For instructions on deploying a configuration, refer to Section 6.1.3, Configuration Management.

Activating the Ports Configuration

Once the ports configuration file has been deployed, it must be activated. Currently there are several possible ways in which this file can be activated. In a future release the Configuration Templates will be upgraded so that deploying the template will make sure that the ports configuration file is activated. However, with current releases, one of the following must be done:

1. Press Save on the Network Configuration page in the Web Console (even if no changes are made) OR
2. Reboot the Field Agent OR
3. On an MFA or EFA, enable or disable Configuration Mode.

6.2 Configuring Data Collection and Sending Data to the Cloud

The primary use cases for a Field Agent are to read data from a connected control system or other industrial device and either make the data available to a locally running application and/or to send the data to the Predix Cloud. This section of the User's Guide describes how to configure the data collection, and how to configure sending data to the cloud. Currently the two data collection protocols that come with Field Agents are OPC UA and Modbus TCP. Information about how to write a custom machine adapter or data processor, including sample Predix Machine application source code, can be found by searching for "Predix Machine SDK Overview" in https://docs.predix.io. Information about how to deploy a configuration or application can be found in Section 6.1.3, Configuration Management, and Section 6.1.4, Application Management.

6.2.1 Determine the Data Source and Data to Consume

The first step in configuring the data collection is to identify which data should be consumed from which data source. Once a data source is chosen, then you need to know its IP Address and Port. There are practical limitations on the number of data tags that can be configured for a given protocol based on the available processor, memory, and disk storage resources on a given Field Agent platform. Recommendations for maximum configured data tags can be found in Section 6.2.5, Guidelines for Maximum Configured Variables.

After the data source IP address and port is determined, it is recommended to use a separate software application to verify connectivity to the data source and determine the data tag names and types to be consumed. Free tools like UaExpert for OPC UA and Modbus Poll for Modbus TCP can be downloaded and configured to view the available data tags in a data source. Note that some OPC UA Servers limit the total number of subscriptions, the total number of variables/subscription and sometimes even the total number of variables allowed to be exposed over OPC UA. Also, be aware that UaExpert uses two subscriptions even if you are only monitoring one variable. Therefore, after you have checked your data, make sure you disconnect from the OPC UA Server in UaExpert so you do not use sessions needed for your Field Agent.

6.2.2 Field Agent Configuration Tool

A Field Agent Configuration Tool is available that simplifies the process of creating configuration files to read data from either an OPC UA Server or Modbus Slave, and streaming data to a Time Series Database. A copy of this tool and its associated User's Guide can be found at the following URL:

https://www.emerson.com/Industrial-Automation-Controls/support

6.2.3 Configure the Field Agent Data Source

This section and the next describe how to manually configure a Field Agent. If the Field Agent Configuration Tool works for your use case, you will not need to do the steps described in these sections.

Download the default Field Agent configuration files appropriate for your Field Agent Hardware form factor, using the links in Section 6.1.3, Configuration Management. Download the configuration files to a computer where they will be edited with a normal text editor such as Notepad++. The configuration files are inside the configuration/machine directory.

You will note a zero at the end of the OPC UA and Modbus configuration (.config) and XML files. This zero refers to the first instance of this type data source. If you require a single Field Agent to read data from two different OPC UA Servers, then make a copy of both the configuration and XML files and replace the zero with a one in the file name of the copies. By deploying two sets of configuration files, then two instances of the data collection program will be created, even though only a single program file (also known as a JAR file or OSGi bundle) is part of the Application files downloaded to the Field Agent.

Configure an OPC UA Data Source

The steps to configure the OPC UA Machine Adapter are:

1. Open the file com.ge.dspmicro.machineadapter.opcua-0.config for editing.
2. Edit line 52 to specify the path to the OPC UA configuration XML file, which by default will be:
    - com.ge.dspmicro.machineadapter.opcua.configFile="configuration/machine/com.ge.dspmicro.machineadapter. opcua-0.xml"
3. If the OPC UA Server you are connecting to uses authentication or encryption, edit line 68 to specify the appropriate Security Mode. If a username and password is used for authentication, edit lines 118 and 121 respectively. The plaintext password will be encrypted, removed from line 121, and added to line 124 in its encrypted form. If certificates are used for authentication, they must be installed into security/machinegateway_truststore.jks as part of the configuration package's install/install.sh script.
4. Save and close com.ge.dspmicro.machineadapter.opcua-0.config.
5. Open the file com.ge.dspmicro.machineadapter.opcua-0.xml for editing.
6. Edit the ServerUri and AppUri XML elements to configure the IP address and port number of the OPC UA server:
    - For MFA, edit the ServerUri and AppUri XML elements to replace localhost with the IP address of the OPC UA server, and replace port 4841 with the port of the OPC UA server.
    - For EFA on CPE400, the ServerUri and AppUri XML elements default to using localControllerHost and port 4840 for connecting to the OPC UA server through an internal interface. localControllerHost is a hostname assigned to the internal virtual NIC to communicate with the controller.

7. Edit the data contained within the DataNodeConfigs and DataSubscriptionConfigs elements to specify the following:
    - Each DataNode element represents an OPC UA variable. Configure only the variables to be collected.
        - The StringId element contains the variable name as exposed in the OPC UA server with the namespace index number before the colon and the variable name after the colon.
        - The Name element contains the tag name as it will appear in the Predix Cloud. The name should be unique amongst all of the variables from any Field Agent that will be going to this same Time Series Database.
    - Each DataSubscriptionConfig represents a group of OPC UA variables to be read and published to the Predix Cloud at a given interval.
        - The Name element represents the name of the subscription, which is used in Section 0,

- Configure Sending Data to the Predix Cloud.
- The PublishingInterval is the rate in milliseconds at which the subscription is set up for getting data from the OPC UA Server. The OPC UA Server will send data at this rate, assuming that the value of the variables has changed since the last publishing interval. Whenever changed data is received in Predix Machine, it will immediately be forwarded on to the Predix Cloud, given that the data is configured to go to the cloud and a DataChangeFilter does not restrict it.
- The TimestampOrigin specifies which time stamp is preferred for the data. The possible values are:

  a. Source: Prefer the time stamp from the data source. If the time stamp from the data source is not available, the OPC UA Server time stamp will be used instead.

  b. Server: Prefer the time stamp from the OPC UA Server. If the time stamp from the OPC UA Server is not available, the data source time stamp will be used instead.

  c. Adapter: Prefer the time stamp from the Field Agent. Source and Server fall back to using the Field Agent time if both data source and OPC UA Server time stamps are unavailable. All time stamps made by the OPC UA Machine Adapter will be in UTC (Coordinated Universal Time).
- Each DataNode element corresponds to a DataNode defined in the DataNodeConfigs element.
- A DataChangeFilter can be optionally applied to each DataNode or to the DataSubscriptionConfig as a whole to specify the conditions under which each OPC UA variable is recognized as changed and sent on.

8. Save and close com.ge.dspmicro.machineadapter.opcua-0.xml

Note: *Additional information on configuring the OPC UA Machine Adapter, including settings for each configuration item, can be found by searching for "OPC-UA Machine Adapter" in https://docs.predix.io.*

Configure a Modbus TCP Data Source

The steps to configure the Modbus Machine Adapter are:

1. Open the file com.ge.dspmicro.machineadapter.modbus-0.xml for editing.
2. Edit the data contained within the dataNodeConfigs and dataSubscriptionConfigs elements to specify the following:

   a. Each channel element corresponds to a Modbus Slave Server from which this program will read values.

   - The protocol should be set to TCP_IP.
   - The tcpIpAddress should be set to the IP Address of the Modbus Slave Server:
     - For MFA, replace 127.0.0.1 with the IP address of the Modbus Slave Server.

    - For EFA on CPE400, the tcpIpAddress element defaults to using localControllerHost for connecting to the Modbus Slave Server through an internal interface. localControllerHost is a hostname assigned to the internal virtual NIC to communicate with the controller.

  - The tcpIpPort will most likely be set to 502, which is the reserved port for Modbus communications.
  - regBaseAddress is an optional parameter whose value is either 0 (the default) or 1. This controls whether the Machine Adapter uses zero or one-based addressing for the registers. If set to 1, the Machine Adapter will subtract one from each register address configured for this Slave Server.
  - bitBaseAddress is an optional parameter whose value is either 0 (the default) or 1. This controls the whether the Machine Adapter uses zero or one-based addressing for bit offsets within a register.
  - defaultModbusByteOrder is an optional parameter whose value is either true (the default) or false. This controls whether the byte order is interpreted as the default Modbus byte ordering (big endian) or the Intel byte ordering (little endian).
  - first16BitLow is an optional parameter whose value is either true (the default) or false. This controls whether the Machine Adapter interprets the first 16 bits of a 32-bit data type to be the low or high word of the 32-bit value.
  - first32BitLow is an optional parameter whose value is either true (the default) or false. This controls whether the Machine Adapter interprets the first 32 bits of a 64-bit data type to be the low or high double word of the 64-bit value.
  - mostSigBit is an optional parameter whose value is either true or false (the default). This controls whether the Machine Adapter should use Modicon bit ordering which reverses the bit order.

b. The unit corresponds to a Modbus Slave Address, also known as the Slave ID.

c. Modbus registers.

  - The name element contains the tag name as it will appear in the Predix Cloud. The name should be unique amongst all of the variables from any Field Agent that will be going to this same Time Series Database.
  - The datatype element possible values are: BOOLEAN, BYTE, SHORT (2-byte integer), INTEGER (4-byte integer), LONG (8-byte integer), FLOAT (4-byte real), DOUBLE (8-byte real) and STRING.
  - The address is the register or coil number to be read.
  - The registerType attribute’s possible values are: HOLDING, INPUT, COIL and DISCRETE.
  - The description attribute is optional and can be set to any text description that gives a human-readable summary of the register’s purpose.
  - The count attribute is only valid for STRING data types, and indicates the number of registers used to hold the string.

- The bitIndex attribute is only valid for BOOLEAN data types of HOLDING and INPUT registers, and indicates the bit offset within the register to interpret as a Boolean value. When bitBaseAddress="0", the valid values are 0-15 inclusive. When bitBaseAddress="1", the valid values are 1-16 inclusive.

d. Each dataSubscriptionConfig represents a group of Modbus registers to be read and published to the Predix Cloud at a given interval.

    - The name attribute represents the name of the subscription, which is used in Section 0,

- Configure Sending Data to the Predix Cloud.
- The documentation for the remaining attributes can be found in the link below.
- Each node Name element corresponds to a name defined for a register, in the dataNodeConfigs section of the xml file.

3. Save and close com.ge.dspmicro.machineadapter.modbus-0.xml.

Note: *All time stamps made by the Modbus Machine Adapter will be in UTC (Coordinated Universal Time).*

Additional information on configuring the Modbus Machine Adapter, including options for each configuration item, can be found by searching for "Modbus Machine Adapter" in https://docs.predix.io.

6.2.4 Configure Sending Data to the Predix Cloud

Predix Machine uses the Hoover Spillway and Data River bundles to select available data and forward it to a data destination such as a Time Series Database. The Hoover Spillway must be configured to specify which of the available Machine Adapter data subscriptions should be consumed, and sent to which Data River. To send the data to a Time Series Database, the WebSocket River can be used. The WebSocket River must be configured to specify which Time Series Database instance the data should be sent to. This is done by specifying a Zone ID, which is unique to each EdgeManager tenancy.

The steps to configure the Hoover Spillway and WebSocket River are:

1. Open the file com.ge.dspmicro.hoover.spillway-0.config for editing.
2. Edit line 60 to set com.ge.dspmicro.hoover.spillway.dataSubscriptions to include only the data subscription names defined in Section 6.2.3, Configure the Field Agent Data Source.

Note: *When Predix Machine first starts, an error message may be logged for each configured subscription stating that the subscription could not be found. This is because the Hoover Spillway can load prior to Machine Adapters and will look for its configured subscriptions before the subscriptions are available from configured Machine Adapters. Once the subscriptions are available from the Machine Adapter(s), Hoover Spillway automatically re-attempts to connect to the configured subscriptions.*

3. Verify the Hoover Spillway is configured to send the subscription data to the WebSocket River. The “WS Sender Service” name comes from the WebSocket River name that was configured in the com.ge.dspmicro.websocketriver.send-0.config file.
   - com.ge.dspmicro.hoover.spillway.destination=”WS Sender Service”
4. Verify the Hoover Spillway is configured to enable the Store and Forward service, which buffers data while the connection to the Predix Cloud is broken. If the Store and Forward service is not desired, this variable should be set to two double quotes (“”).
   - com.ge.dspmicro.hoover.spillway.storeforward="DefaultStoreForward"
5. Save and close com.ge.dspmicro.hoover.spillway-0.config.
6. Open com.ge.dspmicro.websocketriver.send-0.config for editing.
7. Verify line 54 is set to include the URL of the Time Series Database.
   - com. ge.dspmicro.websocketriver.send.destination.url="wss://gateway-predix-data-services.run.aws-usw02-pr.ice.predix.io/v1/stream/messages"
8. Edit line 60 to include the Zone ID of the Time Series Database (provided upon activation of Time Series Service).
   - com.ge.dspmicro.websocketriver.send.header.zone.value="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Note: *It is not recommended to disable Gzip compression for data sent to Predix Time Series Database. Disabling Gzip compression will require additional upstream bandwidth and may decrease maximum number of published variables.*

9. Save and close com.ge.dspmicro.websocketriver.send-0.config.

Note:

1. *All Machine Adapter timestamps are sent to and stored in the Predix Time Series Database as epoch time (the number of seconds that have elapsed since January 1, 1970 at midnight UTC not counting leap seconds).*
2. *Additional information on configuring the Hoover Spillway can be found by searching for "Configuring the Hoover Service" in https://docs.predix.io.*
3. *Additional information on configuring the WebSocket River can be found by searching for "Configuring the WebSocket River" in https://docs.predix.io.*
4. *Additional information on the Predix Time Series Database can be found by searching for "Time Series Service Setup" in https://docs.predix.io.*

6.2.5 Guidelines for Maximum Configured Variables

All variables read from the Server by a Machine Adapter are published. The OPC UA Machine Adapter supports OPC UA Subscription functionality, which can be used to limit the variables published to those that have either changed or changed more than a specified amount since the last subscription interval. Other protocols do not include this functionality; Machine Adapters for these protocols will publish all variables configured to be read each interval.

Variables of type LREAL (OPC UA type Double) are supported for both OPC UA and Modbus TCP Machine Adapters; one LREAL may be configured and published in the place of two 4-byte or smaller variables. This formula may be used to calculate the effective number of 4-byte or smaller variables when also configuring and publishing LREAL variables:

(# of 4-Byte or smaller variables) + (# of LREAL variables * 2) = Effective Variable Count

When using multiple Subscriptions, the maximum number of configured variables and the maximum number of published variables is cumulative across all Subscriptions on a given Field Agent. When using different Publish Interval settings for different subscriptions, the fastest Publish Interval in use should be used to determine the maximum numbers of configured and published variables.

Using the OPC UA Machine Adapter without Store and Forward

Note: *Using the OPC UA Machine Adapter without Store and Forward is not currently supported on the EFA or VFA.*

When Store and Forward is disabled, the OPC UA Machine Adapter limits for the Mini Field Agent platform are displayed in the following table.

Supported Configurations for OPC UA Machine Adapter with Store and Forward Disabled on MFA

Table 12:

Publish Interval (ms)	Configured 4-Byte Variables	Max Published
500	600	300
1,000	1,200	600
60,000	2,500	2,500

Note:

1. *For ICMFA000000-AAxx only, multiply the values in the above table by 0.83 to calculate the OPC UA Machine Adapter limits when Store and Forward is disabled.*
2. *Some OPC UA Servers may negotiate a different interval at the time of the connection if the configured PublishInterval does not match its available subscription intervals. It is recommended to confirm that the OPC UA Server to which the Mini Field Agent is connected can serve data at the requested interval.*
3. *The minimum supported OPC UA Machine Adapter PublishInterval on the Mini Field Agent is 500ms when running Predix Machine 17.1.2 or later.*

Using Store and Forward with the OPC UA Machine Adapter

This section applies to Field Agents running Predix Machine 17.1 and earlier. Beginning with Predix Machine 17.2, performance improvements eliminate the performance reduction when Store and Forward is enabled. Use the data in the previous section, instead of the data in this section.

When Store and Forward is enabled, the OPC UA Machine Adapter limits for each Field Agent platform are displayed in the following table.

OPC UA Machine Adapter with Store and Forward Enabled (Predix Machine 17.1 and earlier)

Table 13:

PublishInterval (ms)	MFA		EFA		VFA
	Configured 4-Byte Variables	Max Published	Configured 4-Byte Variables	Max Published	Configured and Published 4-Byte Variables
500-999	225	75	500	500	4,000
1000-1999	450	150	1,000	1,000	20,000 Given Network Bandwidth: Upstream = 40 MB/sec Downstream = 21 MB/sec
2000-2999	450	300			
	900	150			
≥3000	450	450			
	1,200	150			

Note:

1. *For ICMFA000000-AAxx only, multiply the MFA values in the above table by 0.66 to calculate the OPC UA Machine Adapter limits when Store and Forward is enabled.*
2. *Note: Some OPC UA Servers may negotiate a different interval at the time of the connection if the configured PublishInterval does not match its available subscription intervals. It is recommended to confirm that the OPC UA Server to which the Mini Field Agent is connected can serve data at the requested interval.*
3. *Note: The minimum supported OPC UA Machine Adapter PublishInterval on the Field Agent is 500ms when running Predix Machine 17.1.2 or later.*

Using the Modbus TCP Machine Adapter

The Modbus TCP Machine Adapter limits for each Field Agent platform are displayed in the following tables.

Modbus TCP Machine Adapter on Predix Machine 17.1 and earlier

Table 14:

Update Interval (ms)	MFA Max Configured and Published 4-Byte Variables	EFA Max Configured and Published 4-Byte Variables
1,000-1,999	100	100
2,000-2,999	200	200
3,000-3,999	300	300
4,000-4,999	400	400
5,000- 59,999	500	500
60,000	2,500	2,500

Modbus TCP Machine Adapter on Predix Machine 17.2 and later

Table 15:

Update Interval (ms)	MFA Max Configured and Published 4-Byte Variables
1,000	300
60,000	2,500

Note:

1. *All variables read from the Server by a Machine Adapter are published. Since Modbus TCP Server does not feature a Subscription capability like that found in other automation protocols (such as OPC UA Server), the Modbus TCP Machine Adapter will publish all variables configured to be read each update interval.*
2. *Note: For ICMFA000000-AAxx field agents, use the values in the Predix Machine 17.1 table, even if running a newer Predix Machine.*

Using Store and Forward When Internet Connectivity is Disrupted and Restored

Field Agents Running Predix Machine 17.2 or Later

When Internet connectivity has been disrupted:

- At a publish rate of 100 4-Byte variables every second, the Mini Field Agent can store data for four hours.
- At a publish rate of 100 4-Byte variables every minute, the Mini Field Agent can store data for 10 days.

When the Store and Forward database becomes full, the Field Agent will stop storing new data until Internet connectivity has been restored and enough records have been forwarded to allow room for new records to be added. Stored data values are forwarded in chronological order.

Field Agents Running Predix Machine 17.1 or Earlier

At a publish rate of 100 4-Byte Variables every second, the Mini Field Agent can store data for one hour when Internet connectivity has been disrupted. At maximum load, the Embedded Field Agent can store data for 24 hours when Internet connectivity has been disrupted. When the StoreForward database becomes full, the Field Agent will stop storing new data until Internet connectivity is restored and 60% of the stored data has been forwarded to the Predix Time Series Database. Stored data values are forwarded in chronological order.

Note: *Because the processes that store and forward data values run asynchronously, new data values must be stored to the StoreForward database before being forwarded to the Predix Time Series Database. When Internet connectivity is restored after the StoreForward database has reached maximum capacity, 60% of the stored data must be forwarded to the Predix Time Series Database before new data values will be stored in the StoreForward database. The time required to forward this stored data depends on the available upload bandwidth.*

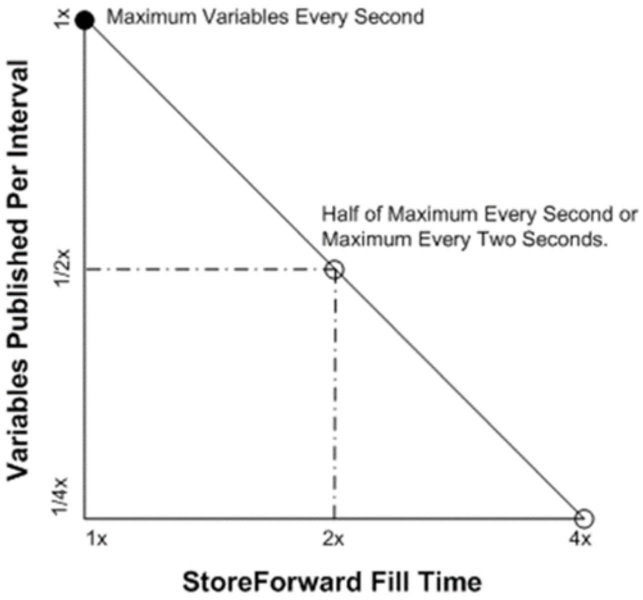
General Information

Note: *On the MFA, the StoreForward database is not retained when power is lost or when restarted.*

The StoreForward database is a buffer that has a maximum size, a fill rate, and an empty rate.

- The maximum size of the StoreForward database is fixed on the Field Agent and cannot be adjusted.
- The fill rate of the StoreForward database can be adjusted by either changing the number of variables published, changing the publication interval of the configured variables, or both. The fill rate is determined by the fastest publication interval in use and the number of variables published.
  - The maximum time that it takes to fill the StoreForward database increases inversely based on the fill rate of the database. The following illustrates the relationship between variables published and fill rate:

Figure 43: Effect of Variables Published Per Interval on StoreForward Fill Time



- The maximum time that it takes to fill the StoreForward database is limited to twelve hours on MFAs running Predix Machine 17.1 and earlier, 10 days on MFAs running Predix Machine 17.2 and later, and 72 hours (three days) on the EFA.

- The maximum empty rate of the StoreForward database is fixed on the Field Agent and cannot be adjusted. The empty rate is influenced by network bandwidth and latency to the Time Series Database endpoint.

6.2.6 Reconfigure the Field Agent

After completing the local changes to Configure the Field Agent Data Source and

Configure Sending Data to the Predix Cloud, complete one of the two methods for updating the configuration on the Field Agent to reflect these local changes.

- First Time Configuration
- Reconfiguration for Production Environment

First Time Configuration

When first-time configuration changes are being made to multiple Field Agents, it is easiest to attempt and debug new configuration changes on a single Field Agent using the Predix Machine Web Console's Configuration pages using the instructions in the sub-section Predix Machine Web Console Configuration Management in Section 6.1.3. In order to use this method, EdgeManager must be used once to deploy the default configuration and applications as described in Section 6.1.3, Configuration Management and Section 6.1.4, Application Management.

The Predix Machine Web Console's Log Service should be checked to verify no unexpected errors are occurring. If a Machine Adapter is misconfigured, the OSGi Log Service should have warning or error entries contained within it describing the issue. Note that while the underlying Predix Machine log file logs all events in UTC (Coordinated Universal Time), all log events displayed in the OSGi Log Service are converted to and displayed in local time using the time zone of the computer running the browser used to view the Log Service. If the Field Agent is connected to EdgeManager , the error could also be diagnosed by obtaining the Predix Machine log from EdgeManager by executing the Predix Machine: Get Log command and reading the log file for warnings and errors. On Field Agents running Predix Machine 17.x, the Predix Machine: Get Available Logs command can be used to retrieve a list of all logs on the Field Agent. The Predix Machine: Get Log command can then be used to retrieve any log file returned in the list from the Predix Machine: Get Available Logs command. Note that all log files generated and retrieved from Predix Machine will include timestamps in UTC.

On the MFA, the orange ACT (activity) LED is a visual indication that a configured Machine Adapter is successfully retrieving data from a data source. The activity LED will blink at a fixed rate of once per second while data is being read from a configured Machine Adapter. Additionally, the Status and Commands page in the Predix Machine Web Console shows this indication.

Once it is confirmed that the Machine Adapter is successfully retrieving data from the configured data source, there are several ways of verifying the data is being sent to the Predix Time Series Database. The Predix Tool Kit be used to verify the raw data is populated in a given Time Series Database.

Reconfiguration for Production Environment

After debugging the configuration files, they can be packaged into a configuration zip file, stored in the EdgeManager Repository as a new configuration, and deployed to one or more Field Agents using the instructions in EdgeManager Configuration Management in Section 6.1.3. This is the recommended reconfiguration method for production environments since a record of the deployment is kept in EdgeManager , along with the specific revision of configuration. The identity and enrollment information for each Field Agent will be retained, even when deploying the same configuration zip file to all Field Agents.

6.3 Predix Machine On-Demand Events

The Predix Machine On-Demand Events feature allows users to notify a Field Agent, over a VPN tunnel, to synchronize with Edge Manager. It is available on Field Agents running Predix Machine 17.2.3 or later. This feature allows the Field Agent to be notified of the presence of an EdgeManager command or package deployment that requires service. Upon receipt of the notification, the Field Agent will query EdgeManager for the command or package and then process it. This allows the polling interval to be set to a very long time, thus minimizing the Internet traffic between the Field Agent and EdgeManager due to polling. The polling interval is configured in the com.ge.dspmicro.cloud.gateway.config file.

The On-Demand Events feature is enabled by starting the Predix VPN Service. This service is started from EdgeManager by sending the Start VPN Management command to the field agent. When the service starts, it creates an encrypted VPN connection between the Field Agent and Edge Manager. From this point, EdgeManager notifications will be sent to the Field Agent through the VPN connection. No other network traffic uses the VPN.

If it is desired to stop the Predix VPN Service, it can be stopped from EdgeManager by sending the Stop VPN Management command to the field agent.

6.3.1 Use of On-Demand Events

Use the following process to make use of On-Demand Events:

1. Choose a Field Agent that will receive On-Demand Events.
2. In Edge Manager, start the VPN service with that Field Agent. The VPN service will not start immediately. At the end of the polling interval, the Field Agent will retrieve the command, start the VPN service, and report the completion status to Edge Manager.
3. Configure the Field Agent's polling interval to a long value—for example, 1 day.
4. In Edge Manager, deploy a package or execute a command on the device. This will queue the operation until the Field Agent polls EdgeManager for the next thing to do.
5. Using a separate Internet-connected computer, send an event to Predix's On-Demand Event API endpoint. The endpoint will reply with an Event ID that can be used to check the status of the event.

   After the event is received by Edge Manager, it will send a message over the VPN connection to the Field Agent, telling it to poll Edge Manager. The Field Agent will poll Edge Manager, perform the operation that was queued-up in step 4, and report completion status to Edge Manager.
6. Optionally, using the separate Internet-connected computer, send GET requests to the On-Demand Event API endpoint to retrieve the status of the event. Repeat periodically until the event completes.
7. Repeat steps 4 through 6 for each package or command.

In the case where a package deployment or a command execution is queued in Edge Manager, but step 5 is not done, the queued item will be retrieved at the end of the polling interval by the Field Agent.

6.4 Event Hub

Event Hub is a publish-subscribe service offered with Predix that can ingest streaming data from anywhere and send it to the Predix Cloud for processing. The Event Hub River Service provides an asynchronous fault tolerant method of communication between the Field Agent and Predix Cloud. For more information on Event Hub, go to: https://docs.predix.io/en-US/content/service/data_management/event_hub/event-hub-service-overview and https://docs.predix.io/en-US/content/service/edge_software_and_services/machine/event-hub-river-service.

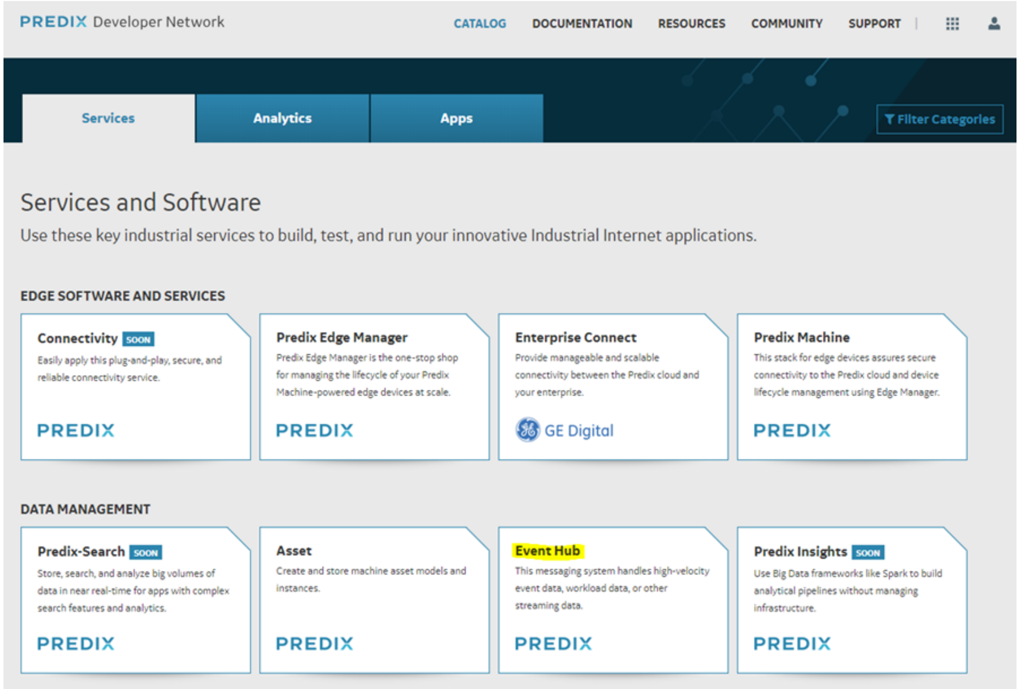
This will walk you through how to:

1. Create an Event Hub Service in Predix Cloud, Section 6.4.1
2. Configure Event Hub River Service on your Field Agent, Section 6.4.2

6.4.1 Create an Event Hub Service in Predix Cloud

1. Create an Event Hub Service in Predix.
2. Go back to https://www.predix.io/ and click on "Catalog" > "Services".
3. Click to log in on the top right and you should be brought back to the Catalog Services page.
4. Find "Event Hub" under the "Services" tab and click on it.

Figure 44: Services and Software Menu



Services and Software

Use these key industrial services to build, test, and run your innovative Industrial Internet applications.

EDGE SOFTWARE AND SERVICES

Connectivity SOON
Easily apply this plug-and-play, secure, and reliable connectivity service.
PREDIX

Predix Edge Manager
Predix Edge Manager is the one-stop shop for managing the lifecycle of your Predix Machine-powered edge devices at scale.
PREDIX

Enterprise Connect
Provide manageable and scalable connectivity between the Predix cloud and your enterprise.
GE Digital

Predix Machine
This stack for edge devices assures secure connectivity to the Predix cloud and device lifecycle management using Edge Manager.
PREDIX

DATA MANAGEMENT

Predix-Search SOON
Store, search, and analyze big volumes of data in near real-time for apps with complex search features and analytics.
PREDIX

Asset
Create and store machine asset models and instances.
PREDIX

Event Hub
This messaging system handles high-velocity event data, workload data, or other streaming data.
PREDIX

Predix Insights SOON
Use Big Data frameworks like Spark to build analytical pipelines without managing infrastructure.
PREDIX

Note: *the UAA in your dashboard should match your EdgeManager UAA url.*

1. *Click on the "Client Management" tab.*
2. *Click on "Switch to Services View".*
3. *Click on the name of your Event Hub service.*
4. *Copy the "Service Instance Id". You will need this for your EdgeManager configuration.*
5. *Under "Authorized Clients", type in the client that you want to authorize this for and click "Submit". Note: the client should be your EdgeManager client.*
6. *Click on the "Switch to Clients View".*
7. *Find the client that you just added for "Authorized Clients" from two steps ago and click on it.*
8. *Note that your event hub service should appear under the "Authorized Services" section.*

Connecting Event Hub to Edge Manager

1. Go to your EdgeManager instance and log in.
2. Go to "Settings" and click on the "Services" tab.
3. Fill in the information for service instance.

- Service Instance Name - should match the service instance name that you gave your event hub service.
- Instance Id - the "Service Instance Id" that you copied in previous steps.
- Service URL -event-hub-aws-usw02.data-services.predix.io
- Scopes - add the following 3 scopes and replace the ${instance_id} with your instance id.

    predix-event-hub.zones.${instance_id}.user

    predix-event-hub.zones.${instance_id}.grpc.publish

    predix-event-hub.zones.${instance_id}.wss.publish

4. Click "Save".

6.4.2 Configure Event Hub River Service on your Field Agent

1. Modify the required fields in the EventHubRiver config file (com.ge.dspmicro.eventhubriver.send-0.config)
    - Modify the friendly and unique name of the Event Hub River adding the desired name
    - Add the URL of the Event Hub endpoint

      wss://event-hub-aws-usw02.data-services.predix.io/v1/stream/messages
    - Add the Zone Id for the EventHub service from EdgeManager
        - Log in to the EdgeManager
        - Settings, Select the Event Hub Service name, Record the Instance ID (same as Event Hub Zone ID)
    - Modify the data format if required (EDGEDATA (default) or PDATAVALUE)
2. Modify the Spillway file (com.ge.dspmicro.hoover.spillway-0.config)
    - Update the Destination Data River name to match the destination name in the EventHubRiver config file:

      Example: com.ge.dspmicro.hoover.spillway.destination="Event Hub Sender Service"
3. Create a Subscriber
    - Create a client for Event Hub in the UAA Dashboard
        - Log in to the UAA Dashboard with the UAA URL and Client Secret
        - On the Client Management tab, click Create Client
        - Enter a Client ID and Client Secret for your Subscriber
        - Under Authorized Services, add your Event Hub instance
        - Under Scopes, add the following:

          predix-event-hub.zones.{instance_id}.user

          predix-event-hub.zones.{instance_id}.grpc.publish

          predix-event-hub.zones.{instance_id}.wss.publish predix-event-hub.zones.{instance_id}.gprc.subscribe

- Add the same entries under Authorities
- Save
- In the Choose Service box, add the Event Hub instance name
- Submit

Technical Support & Contact Information

Home link: http://www.emerson.com/industrial-automation-controls

Knowledge Base: https://www.emerson.com/industrial-automation-controls/support

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.

EMERSON™