Release Notes for Cisco IC3000 Industrial Compute Gateway for Release 1.3.1

The following release notes support the Cisco IC3000. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

Revised: August 20, 2020

Contents

This publication consists of the following sections:

Image Information

Note: You must have a Cisco.com account to download the software.

Cisco IC3000 operates on the following Cisco images:

- IC3000-K9-1.3.1.SPA
- IOx version 2.3
- FND version 4.6.1

Software Downloads

The latest image file for the IC3000 can be found here:

https://software.cisco.com/download/home/286321914

Major Enhancements

The following features are included in this release.

Enhanced Factory Reset

The factory reset behavior has changed with this release. Factory reset will restore applications if the device was ordered with the application. After factory reset is executed, the device will return with the application in a running state as it came from the factory, with the default configuration on the platform.

If there was not an application shipped from the factory, then the application will not be restored. User installed applications on the device will be erased from the device by this operation.

If the device was shipped prior to release 1.3, the factory reset cannot restore the application, even if the current running image version is 1.3. This action will result in a loss of all user installed applications, and the device will not have any applications after the reload.

Enhanced Configuration Reset

The configuration reset behavior has changed with this release.

On the IC3000 Platform

When a configuration reset is executed, the system configuration and logs are erased. After the reload, the IC3000 will boot up into a default configuration with respect to the system configuration and logs.

IOx Applications

Previous behavior was to delete all the IOx applications during configuration reset. Release 1.3.1 changed this behavior to NOT delete all IOx applications. All pre-existing applications will come back to the same operational state after the configuration reset.

All activated and running applications will get notified of a platform configuration reset operation via a sentinel file at $CAF_APP_CONFIG_DIR/.iox_app_config_reset. Applications can make use of this sentinel file to reload the application configuration upon platform configuration reset operation. Then, the application is expected to delete this sentinel file.

New Reset Button Timings

The reset button action timings have changed with this release. Refer to the following table:

Action	Time Pressed and Released in Seconds
Reload	10-20
Configuration Reset	30-50
Factory Reset	60-80

Copper SFP Support

Support is now available for a new copper SFP. The GLC-TE 1000Base-T transceiver with extended temperature range support. Auto-negotiation with 1G full duplex will be the enabled capability on copper SFP.

Date, Time and Network Time Protocol (NTP) Enhancements

The user can now select the time source between manual date and time or NTP. When using NTP, the user can provide information about NTP servers manually, or get that information from a DHCP Server.

The following are options that the user can select from the Device Configuration page of the User Interface (UI):

- Manual Date and Time (User provides the information)
- Network Time Protocol (NTP)

  - Auto (DHCP Server provides the information)
  - Manual (User provides the information)

Note: Only one of the Manual or NTP options can be selected at a time.

Some of the feature caveats are:

- Time Zone can be individually selected by the customer regardless of the time source.
- Up to 5 NTP servers and 1 Preferred NTP server
- Polling interval includes max and min poll
- For NTP Authentication, the user provides the id, type, and value of the keys
- For NTP, either hostname or IP address can be used.

ExFAT Filesystem Support

A USB or SD card formatted with the following filesystems can be used:

- FAT
- FAT32
- ExFAT
- ext2
- ex3
- ex4

The system will mount the first partition if the inserted device has multiple partitions, or otherwise the single partition is mounted.

Image Verification

The operating Image is upgraded by the Local Manager or FND. The system will check the image, and if it is found corrupt, an error will be returned to the WebUI. This error will be propagated to logs as well.

DHCP Option 60

The management interface sends a DHCP option 60, also known as vendor-class-identifier, in its request. The device identification is sent as the string cisco-ic3000. Upon receiving the vendor-class-identifier, the DHCP server can take actions as required.

Enhancement on Management Interface Acquiring IP Address

To enhance usability, IDA will maintain a service which monitors the management interface every 30 seconds. If IDA detects the IP address is not available, IDA will assign the link local IP address of 169.254.128.2 to the management interface.

When the device is powered up or reloads, if a DHCP server is not available, it will set the management IP address to 169.254.128.2. After the device receives a DHCP IP address, the time it takes to fall back to LLA depends on when the DHCP lease time expires.

If the device is in managed mode, IDA will enable the device configuration page as well. Once the WebSocket connection is established, IDA will disable the device configuration page.

Note: this enhancement will only be effective when the management interface is using a DHCP configuration.

New Banner Information on Bootup

A banner informing the user to use Local Manager or FND for configuring the networking and device now appears. CLI is only for viewing configuration, settings and device and app information. The banner appears as follows:

```
Press RETURN to get started


********************************************************************************
*
*     CLI is for viewing configuration, settings and device information       *
*
*
*     Use Field Network Detector/Local Manager for configuring IC3000         *
********************************************************************************
```

Command Line Options

Following CLI commands are added to this release:

CLI Command	Status	Description/Effect

show sfp information port3/port4	New	Shows the Fiber/Copper SFP details.
		
		Note: SFP Name might not appear depending on the EEPROM programmed by the vendor.
		
		Example Output:
		
		`ic3k>`**`show sfp-information port3`**
		`SFP Type : Copper`
		`SFP Name : GLC-TE`
		`Vendor Name : CISCO`
		`Vendor OUI : 0x00 0x17 0x05`
		`Vendor PN : SP7041-TEA`
		`Vendor Rev : A1 41-TEA`
		`Vendor SN : MTC232400B3`

show golden images	New	Shows the golden image and golden application image (If the device is shipped with application).
		
		Example Output:
		
		`ic3k>`**`show golden images`**
		`GOLDEN PLAT IMAGE : IC3000-K9-1.3.1.SPA`
		`GOLDEN APPL IMAGE : CiscoCyberVision-IOx-x86-3.0.2.tar`
		
		`ic3k>`**`show golden images`**
		`GOLDEN PLAT IMAGE : IC3000-K9-1.3.1.SPA`
		`GOLDEN APPL IMAGE : No Factory installed app present`

show tech-support usb2/sdcard	Revised	Show tech support no longer prints on console. Support has been added for downloading logs to usb2.

Related Documentation

The following documentation is available:

- All of the Cisco IC3000 documentation can be found here:

  https://www.cisco.com/c/en/us/support/routers/3000-series-industrial-compute-gateways/tsd-products-support-series-home.html

- IoT Field Network Director

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html

- Cisco IOx Documentation is found here:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

- Cisco IOx Developer information is found here:

  https://developer.cisco.com/docs/iox/

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Caveats listed below are related to the IC3000 and do not include Field Network Director or IOx.

FND release notes are found here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-release-notes-list.html

IOx release notes are found here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/products-release-notes-list.html

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats

- **CSCvs22388**

  Inconsistent password validation using the Firefox browser for day 0 default password change.

  Symptoms: While logging into local manager with the default credentials, and trying to change the password using the Firefox browser, the password validation results in errors even though qualified password is used.

  Workaround: Use the Chrome browser.

- **CSCvv09921**

Symptoms: When the DHCP server is not reachable, the IC3000 management ip address will fall back to the Link Local Address 169.254.128.2. However, when the DHCP server is again reachable, there might be a big delay in getting an ip address. This is because the IC3000 exhausted sending out a series of DHCPDISCOVER. The IC3000 waits approximately 6+ minutes before sending out the next series of DHCPDISCOVER. The time required for the IC3000 to acquire an ip address depends on when DHCP server is available within this wait time.

Workaround: There is no workaround.

- **CSCvv33660**

  Console cli, show iox is not showing the correct iox version.

  Symptoms: The console cli, **show iox** is showing 1.12.0 instead of 2.3.

  Workaround: There is no workaround.

Closed Caveats

- **CSCvt65296**

  Symptoms: When bringing up an AppGroup, but hit an error, the AppGroup goes back into DEPLOYED state. Due to some Apps having already been brought up, when user goes into Manage to update the compose file, receive an error stating Make app group Down.

  Workaround: User will need to do a Down with App Destroy in order to bring all the Apps down, before going into Manage to change the compose file.

- **CSCvt96204**

  Symptoms: When the user created an AppGroup, but had not downloaded the images, and continues to create more AppGroup using the same images. Down loading images in one AppGroup will not reflected on the other created AppGroup. User will need to load them again.

  Workaround: Load the images in the first AppGroup before creating more AppGroup to avoid having to reload images.

- **CSCvv14647**

  Symptoms: When you bring up a VM and configure for iox-nat0 and brought up RUNNING. This is a valid configuration. But when a user does a Config Reset, sometimes the VM will come up DEPLOYED instead of RUNNING. The issue is that CAF have a requirement that if the management interface doesn't have an ip address at the time of restart, it will place the VM into DEPLOYED state.

  Workaround: Configure VM with iox-bridge instead of iox-nat.

- **CSCvu68015**

  Symptoms: When user create an App and use Custom in Resource Profile, the resource specified by user might not be the same as given by the system. Since there are no notification, user will see that the resources entered will not be the same as allocated.

  Workaround: There is no workaround. When both vcpu and cpu units are provided, vcpu value will take priority and cpu units adjusted accordingly.

- **CSCvu93624**

  Disable STP on svcbr_0 in /etc/network/interfaces

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.