Release Notes for Industrial Network Director, Release 1.10.x

First Published: May 14, 2021

These release notes contain the latest information about using Release 1.10.0 of the Cisco Industrial Network Director (IND) application that supports configuration and management of Industrial Ethernet switches.

The IND application provides three types of Online Help (OLH): Context-Sensitive Help, Embedded Help such as the Guided Tours, and Tooltips.

Note: IND Release 1.10.0 supports English, French, German, Japanese and Spanish Online Help.

Documentation

Note: The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Organization

These release notes include the following sections:

Conventions	Conventions used in this document
About Cisco IND	Description of the IND application.
New Platform and Features Supported	New features in IND Release 1.10.0
IND Licenses and PIDs	Summary of support licenses for Release 1.10.0 and link to data sheet for PIDs.
System Requirements	System requirements for Release 1.10.0.
Pre-Configuration Requirements for IE Switches	Configuration required on Industrial Ethernet (IE) switches before you connect them to the IND application.
Installation Notes	Procedure for downloading software.
Important Notes	Unsupported PIDs, Supported IND Release Upgrades, and Supported Cisco IOS software.
Limitations and Restrictions	Known limitations in IND.

Conventions	Conventions used in this document
Caveats	Open and Resolved caveats in Release 1.10.0.
Related Documentation	Links to the documentation associated with this release.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

About Cisco IND

Cisco Industrial Network Director provides operations teams in industrial networks an easily-integrated management system that delivers increased operator and technician productivity through streamlined network monitoring and rapid troubleshooting. IND is part of a comprehensive IoT solution from Cisco:

- Easy-to-adopt network management system purpose-built for industrial applications that leverages the full capabilities of the Cisco Industrial Ethernet product family to make the network accessible to non-IT operations personnel.

- Creates a dynamic integrated topology of automation and networking assets using industrial protocol (BACnet/IP, CIP, Modbus, PROFINET, OPC UA) discovery to provide a common framework for plant floor and plant IT personnel to monitor and troubleshoot the network and quickly recover from unplanned downtime.

- Rich APIs allow for easy integration of network information into existing industrial asset management systems and allow customers and system integrators to build dashboards customized to meet specific monitoring and accounting needs.

- Integration with existing systems and customization by system integrators.

- User Management with customizable permission mapping – Restrict system access to authorized users on a per feature basis.
- Detailed Audit trails for operational visibility of network changes, additions, and modifications – Record user actions on network devices for change management.
- Search capability integrated with major functions - Easily locate functionality and mine for information.
- Cisco Active Advisor - Free cloud-based service that provides essential network life cycle information to make sure security and product updates are current.
- Guided tours - Step-by-step guidance to maximize productivity and ease adoption.

Upgrading from IND 1.8 to IND 10.0

Note: When you upgrade from IND 1.8.x to IND 1.10.x, a Network Administrator role is automatically assigned the Discovery permission and given the new role name “Network Discovery Administrator”. Additionally:

- Upon upgrade, all of the users will be assigned to the Default Root group.
- Only devices listed under a selected group (Group Context View) and its sub-groups can be seen in the Inventory.
- Only users whose Role includes Network Setting permissions can view, update or delete groups within the group sub-tree within their authorization group.
- Only those alarms relevant to devices within a selected group (Group Context View) and its sub-groups will display on the Alarms page.

New Platform and Features Supported

The following new features are supported in IND Release 1.10.0:

- Network Monitoring of the Media Redundancy Protocol, page 4
- Network Monitoring of the Parallel Redundancy Protocol (PRP), page 4
- Manually Add Device, page 5
- Manual Update of Fields for Discover Devices, page 5

These Release Notes summarize the new features found within the four primary functions supported by IND and its user-interface:

- Design
- Operate (Operations)
- Maintain (Maintenance)
- Settings

The IND Online Help contains the related information for the following new features:

Network Monitoring of the Media Redundancy Protocol

You can perform network monitoring of the Media Redundancy Protocol (MRP). MRP is a data network protocol standardized by the International Electrotechnical Commission as IEC 62439-2. It allows rings of Ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. It is suitable to most Industrial Ethernet applications.

MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.

MRP provides fast convergence in a ring network topology for Industrial Automation networks. MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms and 500 ms.

IND Supports MRP monitoring only for Cisco switches and Siemens Profinet PLC/ IO devices which support MRP.

Note: Profinet PLC's and I/O devices which support MRP can be Licensed and monitored in IND.

The following MRP-related information is collected by IND:

- MRP Ring information
- MRP Port information

The following MRP Alarms are supported:

- MRP Ring Open – Processed based on device initiated SNMP Traps. Applicable only for Cisco switches playing Manager role.
- MRP Manager Change - System generated alarm to indicate Manager role change on discovered MRP Ring. This alarm will be raised during periodic and/or on-demand data collection of devices with changes in manager role.

Note: MRP Manager change alarm will be raised for devices in inventory which undergo the following role changes:

- **Current Role**: Manager ----> **New Role**: Client
- **Current Role**: Client ----> **New Role**: Manager

Supported Devices:

- IE2000, IE4000, IE4010, IE5000 and IE3x00 product family PIDs which supports MRP
- Siemens Profinet PLC/ IO devices which support MRP

Network Monitoring of the Parallel Redundancy Protocol (PRP)

Allows you to perform network monitoring of the Parallel Redundancy Protocol (PRP). PRP, as defined in the International Standard IEC 62439-3, is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks.

PRP uses a different scheme, than other redundancy protocols, where the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed, parallel networks.

IND supports PRP on devices running Cisco IOS 15.2(6) and greater releases incorporate CIP/SNMP support for PRP.

The following PRP-related information is collected by IND:

- Details of the PRP Nodes (RedBox and DAN), which includes:
  - Channel configuration and interface details,
  - Channel statistics including error counts (obtained from interface counters) for LAN-A and LAN-B ports.
  - Node table and VDAN table (only for DAN)

- Alarms in case of any faults, given there are no traps from the devices, hence alarms are raised during Periodic and On-demand refresh.

Supported devices:

- An IACS device supporting CIP Object 56 and 57 like ENT2P ControlLogix Ethernet/IP module
- Industrial Ethernet switches: IE 4000, IE 4010,IE 5000, IE2000U few PIDs,s5400, s5410 and IE3400 and IE3400H switches

Each device has predefined ports participating in PRP channel. The lower numbered Gigabit Ethernet member port is the primary port and connects to LAN-A. The higher numbered port is the secondary port and connects to LAN-B.

The following alarms are generated during periodic/on-demand refresh for PRP faults if seen:

- PRP Channel Interface Down: It is triggered when any of the ports of a PRP channel is down.
- PRP Warning Seen on LAN-A / PRP Warning Seen on LAN-B: It is raised based on an ingress warning statistic value. It indicates a potential problem with the LAN-A/LAN-B port.
- PRP Warning Count Seen on LAN-A/ PRP Warning Count Seen on LAN-B: It is triggered when an increase in ingress warning count on LAN-A/LAN-B is seen.

Note: PRP with CIP/SNMP support was first supported in Cisco IOS 15.2(6).

Manually Add Device

You can manually add endpoint devices to the IND inventory when the devices cannot be discovered **or** when devices do not return the required information such as a MAC address and IP address, or the devices cannot respond to the discovery protocol communication supported by IND.

Manually adding these devices allows the IND to support Tagging, Assigning to Group and sending asset information to ISE through the pxGrid service for the devices.

You can add a single device or use a CSV file to perform bulk addition of devices.

Users with Discovery permission can add devices by clicking the Manually Add Device menu tile on the left of the Discovery page.

Operate > Discovery

Manual Update of Fields for Discover Devices

You can manually update device information for any device when the device does not return all the relevant information during discovery or if you want to add custom values for the field.

Update is supported only for the “Name” and “Description” fields for the Discovered Devices when the protocol is MULTIPROTOCOL.

Update is supported only for Common Fields and not for Protocol-specific fields.

User with Device Management permission will be allowed to update devices.

Manually updated field values take priority over automatic updates. Specifically, a manually updated value will not be overwritten with the data fetched from the device during periodic inventory data refresh or manual data refresh. Once the user updates an attribute for a device, it will never be updated by automatic discovery until the device is deleted and rediscovered.

Operate > Discovery

System Requirements

Table 1 System Requirements

Desktop Requirements	Minimum Requirements
Windows Operating System (OS)	Windows 7 Enterprise or Professional with Service Pack 2 Windows 10 Windows 2012 R2 Server
Browser	Chrome: Version 50.0.2661.75, 53.0.2785.116 or above Firefox: 55.0.3, 57.04, 63.0.3 or above
CPU	Quad-Core 1.8 GHz
RAM	8 GB
Storage	50 GB

Pre-Configuration Requirements for IE Switches

The following information describes the CLI configuration required for IND to discover a Supported Device.

- For IE switches running Cisco IOS, refer to Prerequisite Configuration Required for ALL IE Switches Running Cisco IOS.
- For IE1000 switches, refer to Configuration Required for Discovery and Management of Cisco IOS.

Prerequisite Configuration Required for ALL IE Switches Running Cisco IOS

The following information describes the CLI configuration required for the system to discover a Licensed device and to transition the device from an Unlicensed to Licensed State.

This section also describes the Device Manager configuration required on IE 1000 switches.

Note: A local account is not needed on the device if TACACS is available.

Configuration Required for Discovery and Management of Cisco IOS

You can find configuration information for this feature in the IND 1.10 OLH under the heading *Device Prerequisite Configuration*.

Follow these steps to configure the switch so that IND can discover the device and transition from UNLICENSED to LICENSED state.

1. Enter global configuration mode:

   configure terminal

2. Configure SNMP to allow the system to successfully discover the device:

   snmp-server community *read-community* **ro**

read-community must match the SNMPv2 read string defined in the system Access Profile that is attached to the Discovery Profile. the default read community string is “public”.

3. Enter the following command to allow the system to discover a Licensed Device and transition the device from a UNLICENSED to LICENSED state with SNMPv3. The group that you create and the mode are used to associate with the SNMPv3 user that you configure in the next step. Based on the mode that you choose for the group. you can configured the authentication privacy protocols and passwords for the user.

   ```
   snmp-server group group_name v3 mode
   ```

   where *mode* is one of the following:

   priv: Enables Data Encryption Standard (DES) packet encryption

   auth: Enables the Message Digest (MD5) and the Secure Hash Algorithm (SHA) packet authentication

   noauth: Enables the noAuthNoPriv security level. This is the default if no-keyword is specified.

4. Add a new user to the SNMP group:

   ```
   snmp-server user user_name group_name v3 [auth authentication_type authentication_password [priv privacy_type privacy_password]
   ```

   Note: Passwords for **auth** or **priv** should not exceed 64 characters.

   — **auth**: Specifies an authentication level setting session that can be either the HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password sting *auth_password*. Supported privacy_type values are: **{aes | 128 | des}**

   — **priv**: Configured a private (**priv**) encryption algorithm and password string *privacy-password*

5. Configure the following for the system to successfully transition the device from UNLICENSED to LICENSED state.This should match the device access username and password specified in the system Access Profile.

   ```
   username username privilege 15 password 0 password
   ```

6. Enter the following commands to configure authentication, authorization and accounting (AAA):

   ```
   aaa new-model

   aaa authentication login default local

   aaa authorization exec default local
   ```

7. Configure the Secure Shell (SSH) server:

   ```
   ip ssh version 2
   ```

8. Configure the HTTP/HTTPS server:

   ```
   ip http server

   ip http secure-server

   ip http authentication aaa login-authentication default
   ```

9. Configure the number of Telnet sessions (times) and a Telnet password for the line or lines:

   ```
   line vty 0 15

   login authentication default

   transport input all

   transport output all
   ```

10. Return to privileged EXEC mode:

    end

Device Manager Configuration Required for Discovery and Management of IE 1000 Switches

1. Login to the IE 1000 Device Manager.
2. Leave the username field blank and enter **cisco** as password.
3. Choose **Admin** > **Users**.
4. Create Device Access User and use the same in Access Profile on IND.
5. Configure SNMP community string for Read Only (ro):

   a. Choose **Configure** > **SNMP**. Click **OK** in the pop-up windows to confirm enabling SNMP.

   b. Check the check box to enable SNMP Mode globally. Click **Submit**

6. Select Community Strings tab. Add a *public* Community String read only access. (By default, this is a Read Only (ro) string)

   For SNMPv3:

   a. Select the Users tab and add an snmpv3 user with name, security level, authentication protocol, authentication password, privacy protocol, and privacy password. Click **OK**.

   b. Select the Group tab, select the created user, and specify the group name. Click **OK**.

7. Choose **Admin** > **Access Management**.

   a. Check the check box to enable either SSH or Telnet. (This option determines how the IE1000 communicates with IND)

   b. Click **Submit**.

Bootstrap Configuration for IE Switches

Still relevant? Any updates?

The system pushes the following configuration when you move the device to the Licensed state in the system:

Note: In the configuration script below, the {certificate key length} is obtained from the device access profile.

```
# Secure-mode only
# If the device has a self-signed certificate with RSA key pair length <{certificate-key-length}.The
certificate key length is obtained from the device access profile.\ (or) if the device does not have a
self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR
modulus <{certificate-key-length}>
crypto pki trustpoint IND_HTTP_CERT_KEYPAIR
enrollment selfsigned
subject-name OU=”IOT”
rsakeypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable

# If AAA is not enabled on the device
ip http authentication local
#Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
#Insecure mode only
ip http server
ip http port {regular-mode-access-port}

# Configure WSMA
# The system uses WSMA for management
wsma agent exec
profile exec
# Secure-mode only
wsma profile listener exec
transport https path /wsma/exec
# Insecure mode only
wsma profile listener exec
transport http path /wsma/exec

# SNMP configuration
# Trap destination. The system supports both v2c and v3
snmp-server host <ind-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp-server host {ind-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162

# Bootstrap configuration for SNMPv3
# The system needs the following configuration to be able to query bridge-mib with SNMPv3
security in IOS devices.
# This bridge-mib is required by inventory service to get MAC-Table from SNMP when the
system moves device from new to managed state.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
# Enable RFC2233 compliant for linkDown and linkUp trap
snmp-server trap link ietf

# Enable traps supported by the system
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rep
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps alarms informational
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
# Configure SNMP to retain ifindex across reboots
snmp ifmib ifindex persist

# Enable dual-power supply
# Not applicable for S5410, IE5K, CGS2K, IE3010
power-supply dual

# Enable SD card alarm
# Not applicable for S8000,CGS2K,IE2000U,IE3010,IE3K,IE3200,IE3300,IE34000 and S5800
alarm facility sd-card enable
alarm facility sd-card notifies
# Turn on notifies for selected facility alarms
```

```
alarm facility temperature primary notifies
alarm facility temperature secondary notifies
# Following not application for CGS2K, IE3010
alarm facility power-supply notifies
no alarm facility power-supply disable
```

Bootstrap Configuration for IE 1000 Switches

Still relevant?

```
# Traps for IE1K
snmp.config.trap_source.add coldStart
snmp.config.trap_source.add warmStart
snmp.config.trap_source.add linkDown
snmp.config.trap_source.add linkUp
snmp.config.trap_source.add topologyChange
snmp.config.trap_source.add authenticationFailure
snmp.config.trap_source.add entConfigChange
snmp.config.trap_source.add fallingAlarm
snmp.config.trap_source.add risingAlarm
snmp.config.trap_source.add newRoot
# Trap destination
snmp.config.trap_receiver.add <ind-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp.config.trap_receiver.add {ind-ip-address} version 3 {snmpv3_mode} {snmpv3_username}
udp-port 30162
```

Installation Notes

IND Application Installation

The installation procedure for IND is described in the Installation Guide for Industrial Network Director for Release 1.10.0.

Device Pack Installation

Installation Requirements

IND Device Packs can only be installed with an IND application that has a matching *version* number, and the *release number* **must be** the same or greater than the IND release number.

For example, in release 1.10.x, 1.10 is the version number and x is the release number.

A new Device Pack must be version 1.10.0.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.10.0.

Important Notes

Please note the following information about Windows OS, Cisco IOS software and PID support on IND.

- If you upgrade from 1.8 to 1.10, you must re-upload the IND pxGrid certificate to ISE.

  Self-signed Certificates are issued on MacOS by restricting the life of self-signed certificate to 398 days.

  All the system Self-Signed Certificates are regenerated upon upgrade to meet the new security requirements for TLS server certificates in iOS 13 and macOS 10.15.

Supported IND Release Upgrades

You can perform the following IND upgrades:

- Upgrade from 1.9.0 to 1.10.0.
- Upgrade from 1.8.0 to 1.9.0
- Upgrade from 1.7.1 to 1.8.0
- Upgrade from 1.7.0 to 1.8.0
- Upgrade from 1.6.1 to 1.8.0
- Upgrade from 1.6.1 to 1.8.0
- Upgrade from 1.6.0 to 1.8.0
- Upgrade from 1.6.x to 1.7.x

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT IND. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the software.

- IND upgrades managed devices in groups of six (6). This approach is by design to ensure server resources are not overloaded.
- Make sure that the Windows server running IND is not abruptly shutdown as this might lead to a loss of files needed for IND to function.
- State transition for the devices newly discovered running a Cisco IOS Release lower than 15.2(7)E1a cannot be moved from the Unlicensed state to Licensed State in the secure mode. Metrics collection for the devices already managed by IND running a Cisco IOS Release lower that 15.2(7)E1a would fail due to self-signed certificate expiry in the secure mode. Telnet should work without any issues on a switch that is running a software version lower than 15.2(7)E1a.
- If your switch is running, Cisco IOS Release 15.2(4) software, a weak cipher **must be** used for secure communication to the device. Weak Ciphers are disabled by default on IND. To enable, go to Settings > System Settings > Security Settings.
- Device Image upgrade in IND: An image upgrade **will not** be supported for devices with low memory and no SD flash support, if the device is managed on IND in secure mode. Please use Device Manager to upgrade the image.
- SNMPv3 protocol doesn't work in device IE3x00 running with 16.10.1
- PnP process is supported only on single-homed (Single IP) IND servers for Cisco IOS Release 15.2(6)E1.

  Note: A PnP Service Error 1410 occurs in Cisco IOS Release 15.2(6)E0a due to the AAA command not working. (CSCvg64039). Caveat currently marked Unreproducible in CDETs. **Note**: This issue is resolved in software releases greater than Cisco IOS 15.2(6)E0a.

- IE 5000: Horizontal Stacking is not supported. Stacked devices can be discovered on IND but cannot be licensed.
- IOS devices should have sufficient space in flash directory for upgrading the devices from IND using software image upgrade. For low memory devices, use the removable SD flash memory card.
- PRP or MRP capable devices discovered in previous versions of IND will not support PRP or MRP after upgrading to IND 1.10. The device must be re-discovered on IND 1.10 to enable PRP or MRP support.

Caveats

This section presents open and resolved caveats in this release and information on using the Bug Search Tool to view details on those caveats. Section topics are:

- Open Caveats
- Resolved Caveats
- Accessing the Bug Search Tool

Open Caveats

Table 2 Open Caveats

Caveat Number	Description
CSCvq23714	IE1k PnP fails with CA signed certificate.
CSCvy03179	Self-signed cert failure in IE1K 1.8.1.

Resolved Caveats

Table 3 Resolved Platform Related Caveats

Caveat Number	Description
CSCvv10572	Unable to register IND with ISE on 2.4 P13

Accessing the Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, use the following URL: https://tools.cisco.com/bugsearch/search

To search using a specific bug ID, use the following URL: https://tools.cisco.com/bugsearch/bug/*<BUGID>*

Related Documentation

Installation Guide for Industrial Network Director Application for Release 1.10.0

Find documentation for the Cisco Industrial Ethernet Switches at: (select the link for the relevant switch to access user guide on the page below):

- Cisco Industrial Ethernet 1000 Series Switches
- Cisco Industrial Ethernet 4000 Series Switches
- Cisco Industrial Ethernet 4010 Series Switches
- Cisco Industrial Ethernet 5000 Series Switches

No combinations are authorized or intended under this document.