Release Notes for Cisco Industrial Network Director, Release 1.4.x

First Published: March 30, 2018
Last Updated: April 6, 2018

This release note contains the latest information about using Release 1.4.x 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.

Organization

This guide includes the following sections:

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.

Conventions	Indication
{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.

About Cisco IND

Cisco Industrial Network Director provides operations teams an easily-integrated system delivering 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) 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.

Cisco IND Features and Benefits

- Purpose-built user experience for non-IT operations personnel - Rapid adoption by operations teams for improved productivity.
- Targeted discovery of plant floor network assets customized for industrial environments – Ensures that automation devices connected to the network are not affected by discovery process.
- Automation endpoint discovery using industrial protocols, including PROFINET, CIP, BACnet/IP, and Modbus Complete automation infrastructure inventory, not solely network inventory details.
- Optimized alarm management with real-time alerting of network events and reporting of effects to automation assets – Allows for operations and plant IT team to consume network events in context of the industrial process to simplify troubleshooting issues.
- User-defined period of monitoring of Supported device metrics, traffic statistics, and network infrastructure status – Increased visibility of network health for the operations team and reduced unplanned downtime.
- Comprehensive RESTful APIs for integration with automation applications and control systems – Rapid adoption and integration with existing systems and customization by system integrators.
- Role-based access control 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.

New Features

In this release of the product, there are four primary functions supported:

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

Release 1.4.x supports the following new IND features and enhancements summarized in Table 1.

Table 1 New Features in IND 1.4.x

Feature	Description	First released	Related Documentation
Port Settings	Allows you to view and manage port settings by clicking on a Switch port on the faceplate of the switch. You can manage the following items in the Switch port window: ■ Change Port Access VLAN ■ Change Port Speed ■ Port interface: Shut down or No Shutdown options ■ Configure Port Duplex Mode	1.4.0-216	IND Online Help

Table 1 New Features in IND 1.4.x (continued)

Feature	Description	First released	Related Documentation
Share Endpoint information with Cisco ISE	Cisco IND is registered with pxGrid as a publisher and publishes information on endpoint attributes to Cisco Identity Services Engine (ISE) for the IOTASSET Dictionary. **Note**: You must register Cisco IND in Cisco ISE as a pxGrid node for the function to work. Cisco Platform Exchange Grid (pxGrid), allows multiple security products to share data and work together. This open, scalable, and IETF standards-driven platform helps you automate security to get answers and contain threats faster. Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches. Integrating pxGrid with IND allows IND to share endpoint information available in the IND inventory with ISE. Settings > pxGrid	1.4.0-216	Deploying Cisco Industrial Network Director (IND) with Cisco ISE using pxGrid Cisco pxGrid Cisco Identity Services Engine IND Online Help
BACnet Data Communications Protocol Support	Using the BACnet data communications protocol, IND can retrieve and then manage MAC addresses and configured network port information of Building Automation and Control network devices. BACnet Devices devices have a specific group icon that displays within the Topology map. Operate > Topology	1.4.0-216	IND Online Help
Configuration Backup	Allows you to backup the current device configuration into the IND Configuration Archive. You can establish both On Demand and Periodic Backups. Maintain > Configuration Archives	1.4.0-216	IND Online Help
Device Type Tags	You can define tags and then attach those tags to one or more devices on the following pages: Inventory, Device Details and Topology. You cannot delete a tag that is associated with a device. Settings > Tag	1.4.0-216	IND Online Help
Discover Topology by Group	When you create a group, it displays as an icon in the Topology map. This action occurs even in the absence of assigned assets or subgroups in the Group. Operate > Topology	1.4.0-216	IND Online Help
VLAN Overlay	Allows you to show or hide configured VLANs for devices that display. VLAN Overlay > Topology	1.4.0-216	IND Online Help
Plug and Play (PnP) CLI Config and Exec Service	New capability allows you to append additional command line interface (CLI) commands to a Device Configuration. Design > Plug and Play	1.4.0-216	IND Online Help

Table 1 New Features in IND 1.4.x (continued)

Feature	Description	First released	Related Documentation
IND Device Pack 1.4.0	Cisco Universal IOS images supported: ■ Cisco IOS Release 15.2(6)E1 ■ Cisco IOS Release 15.2(6)E0a ■ Cisco IOS Release 15.2(5)E2 ■ Cisco IOS Release 15.2(5)E1 ■ Cisco IOS Release 15.2(4)EC2(ED) ■ Cisco IOS Release 15.2(4)EA2 ■ Cisco IOS Release 15.2(4)EA1 ■ Cisco IOS Release 15.2(3)E3 ■ Cisco IOS Release 15.2(3)E2 **Note:** See Limitations and Restrictions, page 11 for image limitations. The device pack supports the following Cisco and Rockwell Automation/Allen-Bradley platforms: Cisco platforms: ■ CGS 2520 ■ IE 1000, IE 2000, IE 2000U ■ IE 3000, IE 3010 ■ IE 4000, IE 4010 ■ IE 5000 Rockwell Automation/Allen-Bradley platforms: ■ Stratix 8000/8300 Modular Managed Ethernet Switches ■ Stratix 5700 Industrial Managed Ethernet Switches ■ Stratix 5700 Industrial Ethernet Switches ■ Stratix 5410 Industrial Distribution Switches ■ Stratix 5400 Industrial Ethernet Switches ■ Stratix 2500 Lightly Managed Switches	1.4.0-216	IND Online Help

IND Licenses

The Cisco Industrial Network Director is licensed on a per-device, term subscription basis and supports two licensing models. For details on the supported IND licenses, refer to the:

Cisco Industrial Network Director Data Sheet

System Requirements

Table 2 System Requirements

Desktop Requirements	Minimum Requirement
Windows Operating System (OS)	Windows 7 Enterprise or Professional with Service Pack 2 Windows 10 Windows 2012 R2 Server Windows 2016 Server (64-bit version) **Note:** When using Windows 2016 Server, you may not be able to select the **Uninstall** option from the Windows Start program window. If this occurs, do the following: - Log out of Windows 2016 and then log in again. - If you do not see the **Uninstall** option in the Windows menu, then **Restart** the PC.
Browser	Chrome: Version 50.0.2661.102 or later Firefox: Version 46.01 or later
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 and transition the device from UNLICENSED to LICENSED state in secure mode.

- For IE switches running Cisco IOS, refer to Requirements for ALL IE Switches Running Cisco IOS
- For IE1000 switches, refer to Device Manager Configuration Required for Discovery and Management of IE 1000 Switches

Requirements for ALL IE Switches Running Cisco IOS

- Configuration Required for Discovery and Management of Cisco IOS

Configuration Required for Discovery and Management of Cisco IOS

```
# The following SNMP configuration is required to be configured on the device for the system to
successfully discover it:
# The <read-community> must match the SNMP V2 Read string defined in the system Access
Profile which is attached to the Discovery Profile.
snmp-server community <read-community> RO
# Default read community string is "public"

# Device Prerequisite Configuration for SNMPv3
# The following configuration is required for the system to discover a Supported device and
 transition the device from UNLICENSED to LICENSED state with SNMPv3:

snmp-server group <group_name> v3 <mode>
# Supported mode values are [priv, auth, noauth]

# Supported authentication_type values are [sha, md5]
```

```
# Supported privacy_type values are [aes 128, des]
# The group created with mode will be used by the below CLI command for associating the
SNMPv3 user with that mode.
# According the mode chosen, user can configure the authentication, privacy protocols and
passwords.
snmp-server user <user_name> <group_name> v3 [auth <authentication_type>
<authentication_password> [priv <privacy_type> <privacy_password>]]

# The following configuration is required to be configured on the device for the system
to successfully transition the device from UNLICENSED to LICENSED state.
# This should match the device access username & password specified in the system Access
Profile
username <username> privilege 15 password 0 <password>

# Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local

# Configure SSH server
ip ssh version 2

# Configure HTTP/HTTPs server
ip http server
ip http secure-server
ip http authentication aaa login-authentication default

# Configure VTY
line vty 0 15
login authentication default
transport input all
transport output all
```

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

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

```
# Secure-mode only
# If the device has a self-signed certificate with RSA key pair length < 1024 bits \ (or) if the device
does not have a self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR
modulus 1024
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
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

```
# 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 1.4.x.

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 1.4.0-216, 1.4.0 is the version number and 216 is the release number.

A new Device Pack must be version 1.4.0 and the release must be 216 or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.4.x.

Important Notes

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

Supported Cisco IOS Software

IND 1.4.0-216 supports the following Cisco IOS Releases:

- Cisco IOS Release 15.2(6)E1
- Cisco IOS Release 15.2(6)E0a
- Cisco IOS Release 15.2(5)E1
- Cisco IOS Release 15.2(5)E
- Cisco IOS 15.2(4)EC2(ED)
- Cisco IOS Release 15.2(4)EA5
- Cisco IOS Release 15.2(4)EA2
- Cisco IOS Release 15.2(4)EA1
- Cisco IOS Release 15.2(3)E3
- Cisco IOS Release 15.2(3)E2
- Release 1.6 for Industrial Ethernet 1000

Supported IND Release Upgrades

You can perform the following IND upgrades:

- Upgrade from 1.3.1 to 1.4.0
- Upgrade from 1.3.0 to 1.3.1
- Upgrade from 1.2.x to 1.3.0
- Upgrade from 1.1.x to 1.2.0
- Upgrade from 1.0.x to 1.2.0

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.

- After you upgrade from IND 1.3 to IND 1.4, you must re-register with the pxGrid Service.
- Import of PnP profile from IND 1.3 to IND 1.4 is not supported.
- PnP process is supported only on single-homed (Single IP) IND servers for Cisco IOS Release 15.2(6)E1.
- PnP process fails intermittently in Cisco IOS Release 15.2(6)E0a.
- A PnP Service Error 1410 occurs in Cisco IOS Release 15.2(6)E0a due to AAA command not working (CSCvg64039).
- A crash occurs on IE 2000 and Stratix 5700 devices with IOS 15.2(6)E0a if the PnP process is enabled using DHCP option 43 (CSCvg72151).

Caveats

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

- Open Caveats, page 11
- Accessing the Bug Search Tool, page 11

Open Caveats

Table 3 displays open caveats for some IE switches that may affect the functionality of IND 1.4.

Table 3 Platform-related caveats

Bug ID	Headline
CSCvi33467	PnP: PnP Error 1410 with Euphrates image [Release 15.2(6)E0a].
CSCvi55460	Cannot SSH to the device after the PnP commissioning with Cauvery Image. [15.2(4)EA5, All IE switches].
CSCvi66102	MRP Mode changes to Client upon Rebooting the device [Release 15.2(6)E1].
CSCvi69546	Tar upgrade from Cauvery or Danube to Winter [Release 15.2(6)E1] is failing for IE3000 or s8000.

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 1.4.x at:

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

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

http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html