Release Notes for Cisco Industrial Network Director, Release 1.5.x

First Published: August 30, 2018
Last Updated: October 12, 2018

These release notes contains the latest information about using Release 1.5.1-4 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	Conventions used in this document.
About Cisco IND	Description of the IND application.
New Features	New features in Release 1.5.x.
IND Licenses and PIDs	Summary of supported licenses for Release 1.5.x and link to data sheet for PIDs.
System Requirements	System requirements for Release 1.5.x.
Pre-Configuration Requirements for IE Switches	Configuration required on Industrial Ethernet (IE) switches before you connect it to the IND application.
Installation Notes	Procedures for downloading software.
Important Notes	Unsupported PIDs, Supported IND Release Upgrades and Supported Cisco IOS software.
Limitations and Restrictions	Known limitations in IND.
Caveats	Open and Resolved caveats in Release 1.5.x.
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.

Cisco Systems, Inc.   www.cisco.com

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 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.

- 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

These Release Notes summarize the new features found within the four primary functions supported by IND:

- Design

- Operate (Operations)

New Features

- Maintain (Maintenance)

- Settings

Release 1.5.x supports the following new IND features and enhancements summarized in Table 1.

Note: The feature, **Configuration Restore** (Maintain > Configuration Archives) **is not** supported in this release. Please ignore all references to the feature in the Online Help or within the application itself.

Note:

Table 1   Features Supported in IND 1.5.1-4 and 1.5.0-258

Feature	Description	Related Documentation
DESIGN menu changes		
Plug and Play (PnP) CLI Config and Exec Service Enhancements	Allows you to append additional command line interface (CLI) commands to a Device Configuration. Design > Plug and Play	IND Online Help
PnP Configuration Profile Assignment Enhancements	■ Allows you to define whether a PnP Configuration Profile will be applied to the Startup or Running Configuration (toggle option). **Note:** If you apply the PnP Configuration Profile to the Running Configuration, then that Running Configuration is saved to the Startup Configuration. For this save, the credentials associated with the Access Profile, provided by the user, are applied to the PnP Configuration Profile. If the credentials in the Access Profile are incorrect, then the operation to save the PnP Configuration Profile to the Startup Configuration fails. You will see an error message on PnP inventory page. ■ PnP process supports multi-homed IND servers **Note:** Your switch must be Release 15.2(6)E2, which supports Multi-homing of servers. Design > Plug and Play	IND Online Help
OPERATE menu changes		
User interface (UI) Design Change	You can now access Device Access Profile and Discovery Profile pages through a single page, Operate > Discovery	IND Online Help
CIP Discovery Enhancements	CIP enhancements include: ■ CIP Backplane Bridged Discovery ■ CIP-enabled switches can collect vendor-specific CIP serial number and revision (major and minor revisions) ■ User can edit the CIP device name Operate > Discovery	IND Online Help

New Features

Table 1   Features Supported in IND 1.5.1-4 and 1.5.0-258

Feature	Description	Related Documentation
Device Level Ring (DLR) Discovery	DLR Supervisor modules, supported by the vendor products listed below, can be discovered by CIP. ■ Rockwell Automation/Allen Bradley Stratix 5400 DLR Supported PIDs ■ Rockwell Automation/Allen Bradley Stratix 5700 DLR Supported PIDs ■ Rockwell Automation ControlLogix Chassis DLR Supported PIDs ■ Rockwell Automation CompactLogix Chassis DLR Supported PIDs ■ Rockwell Automation ETAP DLR Supported PIDs Operate > Discovery	IND Online Help
Device Access Profile Enhancements	Device Access Profile update: ■ Discovery support for OPC United Architecture (UA) Servers. Allows retrieval of the following information for an OPC UA server: SerialNumber, RevisionCounter, Manufacturer, Model, DeviceManual, DeviceRevision, SoftwareRevision, HardwareRevision, DeviceClass, DeviceHealth ■ You can select the protocols to use for discovery in the Device Access Profile. Operate > Discovery > Device Access Profiles	IND Online Help
Inventory Enhancements	Display of devices running the OPC UA protocol and DLR. Operate > Inventory	IND Online Help
Topology Trigger	To ensure an accurate Topology view, you must initiate a Topology Discovery when one of the two tasks noted below is performed. To do so, click the **Discover Topology** button. ■ Asset Discovery Scan ■ Supported Device Move to Managed Operate > Topology	IND Online Help
VLAN Layer	Allows you to show or hide one configured VLAN. VLANs collected for all switches that are in the Licensed state in the group. Operate > Topology > Layer > VLAN	IND Online Help
SETTINGS menu changes		

Table 1 **Features Supported in IND 1.5.1–4 and 1.5.0–258**

Feature	Description	Related Documentation

pxGrid Enhancements	■ pxGrid support for CIP Chassis
	
	■ IND support has expanded to include forwarding of the following pxGrid information to a Cisco ISE:
	
	  – CIP Chassis: Forwarding of IP and MAC addresses of each port of a communication module within a CIP chassis to a Cisco ISE.
	
	  – Re-registration (every 5 minutes): Forwarding of periodic re-registration requests by pxGrid clients managed by IND to the Cisco ISE (server) in order to notify that the pxGrid client is active
	
	■ New pxGrid statistics reported in IND:
	
	  – pxGrid Sync Status – Display the current pxGrid sync status (IN-SYNC/OUT-OF-SYNC/DISABLED) via REST-API
	
	  – Last pxGrid Sync Status probe time: Last time that IND received a request for Sync status. indicates whether of nor ISE is probing IND every 10 minutes as expected.
	
	■ New Bulk requests:
	
	  – Last Bulk Request Time – Indicates last time that IND sent all assets as part of a Bulk request response
	
	  – Number of assets shared by Last Bulk request
	
	■ Asset updates:
	
	  – Last Update asset: Provides information on the asset in the Last Update
	
	  – Last Update operation: Provides Operation type (ADD/DELETE/UPDATE) of the last update sent from IND to ISE
	
	  – Last Update time – Indicates the Last time the Asset Update was sent
	
	Note: IND must be registered in Cisco Identity Services Engine (ISE) to support these pxGrid enhancements.
	
	Note: Endpoint information from IND is shared with Cisco Identity Services Engine (ISE) by integrating pxGrid in the IND application.
	
	Settings > pxGrid
		IND Online Help
		
		Deploying Cisco Industrial Network Director with ISE using pxGrid

Table 1   Features Supported in IND 1.5.1-4 and 1.5.0-258

Feature	Description	Related Documentation
IND Device Pack 1.5.1	Cisco Universal IOS images supported: ■ Cisco IOS Release 15.2(6)E2 ■ 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 12 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	IND Online Help

IND Licenses and PIDs

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 and PIDs for ordering purposes, 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:

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
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 1.5.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 1.5.1-4, 1.5.1 is the version number and 4 is the release number.

A new Device Pack must be version 1.5.1 and the release must be 4 or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.5.x.

Important Notes

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

Supported Cisco IOS Software

IND 1.5.1-4 supports the following Cisco IOS Releases:

- Cisco IOS Release 15.2(6)E2A
- Cisco IOS Release 15.2(6)E2
- 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 form 1.5.0 to 1.5.1

- Upgrade from 1.4.x to 1.5.1

- Upgrade from 1.4.x to 1.5.0

- 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 1.4 to IND 1.5, 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 12

- Accessing the Bug Search Tool, page 13

Open Caveats

Table 4 displays open caveats that may affect the functionality of IND 1.5.

Table 3   IND Open Caveats

Bug ID	Headline
CSCvm47069	When group name is changed, in Inventory page, the contents of the group is no longer seen
CSCvm64016	Groups filter is disabled after move to licensed
CSCvm64024	With Selected button not working for System generated alarm category

Table 4 displays open or closed caveats for some IE switches that may affect the functionality of IND 1.5.

Table 4   Platform-related caveats

Bug ID	Headline
CSCvj28967	Device Manager Images and IOx tab fail to load frequently

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 1.5.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

Related Documentation