



Release Notes for Cisco Industrial Network Director, Release 1.3.x

Last Updated: February 12, 2017
First Published: December 1, 2017

This release note contains the latest information about using Release 1.3.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	Conventions used in this document.
About Cisco IND	Description of the IND application.
New Features	New features in Release 1.3.x.
IND Licenses	Summary of supported licenses for Release 1.3.x.
System Requirements	System requirements for Release 1.3.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 1.3.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 .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.

About Cisco IND

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.
- Real-time 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.

New Features

- 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 1.3.x supports the following new IND features and enhancements summarized in [Table 1](#).

Table 1 New Features in IND 1.3.x

Feature	Description	First released	Related Documentation
Updated Apache FTP Server Libraries	Updated Java libraries to version 1.1.0.	1.3.1-5	---
Self-signed certificate	Each IND installation (including upgrades) generates a different self-signed certificate.	1.3.0-365	---
Cisco pxGrid Integration	<p>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.</p> <p>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.</p> <p>Settings > pxGrid</p>	1.3.0-365	<p>IND Online Help</p> <p>Cisco pxGrid</p> <p>Cisco Identity Services Engine</p>
Maintain > Software Images Page	You can upload Industrial Ethernet (IE) software images that you associate with a Plug and Play (PnP) profile. You can also delete images from this page.	1.3.0-365	IND Online Help

New Features

Table 1 New Features in IND 1.3.x (continued)

Feature	Description	First released	Related Documentation
Locate Switch - Unclaimed Devices Page	<p>The Unclaimed Devices page has a Locate button for a device in table or card view. Clicking Locate activates the Locate Switch feature to identify unclaimed devices. When Locate Switch is enabled, the switch LEDs blink alternately green and red (LEDs that are in one color blink) to provide a visual indication of the switch's location.</p> <p>Design > Plug and Play > Unclaimed Devices</p>	1.3.0-365	IND Online Help
Reduced Number of Device Categories	<p>Two Device Categories:</p> <ul style="list-style-type: none"> ■ Supported: Devices supported by Device Packs (Currently, Industrial Ethernet switches are the only Supported Device types) ■ Other: Devices such as clients that are not supported by Device Packs and are identified by their protocol such as: BACnet, CIP (user-defined), Modbus, PROFINET, SNMP, or <i>Unknown</i> <p>Note: The previously supported Device Category, <i>Client</i>, is now part of the <i>Other</i> category.</p> <p>Note: Unknown protocols display only common attributes such as ipAddress, macAddress (optional), or vendor (optional).</p>	1.3.0-365	IND Online Help
Renamed, Reduced Number of Device States	<p>Support for three Device States:</p> <ul style="list-style-type: none"> ■ Licensed: Continued support for this state. No changes. <ul style="list-style-type: none"> – A supported device which has a valid license, is actively monitored (information polling, alarms, telemetry) and has its rich information collected. ■ Unlicensed (includes former NEW and DECOMMISSIONED states) <ul style="list-style-type: none"> – No device monitoring is performed on devices in an UNLICENSED STATE. – A device in an UNLICENSED state also does not have a license associated with it. 	1.3.0-365	IND Online Help
DHCP Server	Integrated DHCP server allows for easier deployment of Industrial Switches within networks.	1.3.0-365	IND Online Help
BACnet/IP Discovery	<p>Allows discovery of BACnet/IP clients. BACnet devices are displayed under Other Devices.</p> <p>Operate > Inventory</p>	1.3.0-365	IND Online Help
Modbus/TCP Discovery	<p>Allows discovery of Modbus TCP clients. Modbus devices are displayed under Other Devices.</p> <p>Operate > Inventory</p>	1.3.0-365	IND Online Help

New Features

Table 1 New Features in IND 1.3.x (continued)

Feature	Description	First released	Related Documentation
Expanded feature set for Plug and Play (PnP) Service	<p>New features for PnP:</p> <ul style="list-style-type: none"> <li data-bbox="380 407 1036 569">■ Upload and upgrade of .tar or .bin images—Allows you to associate multiple .tar images with a single Profile and deploy that image to a device by defining the device type. Design > Plug and Play > Profiles <li data-bbox="380 600 1036 852">■ Locate Switch for Unclaimed Devices—Clicking the Locate button for a device in table or card view activates the Locate Switch feature to identify unclaimed devices. When Locate Switch is enabled, the switch LEDs blink alternately green and red (LEDs that are in one color blink) to provide a visual indication of the switch's location. Design > Plug and Play > Unclaimed Devices <li data-bbox="380 884 1036 989">■ DHCP Helper—Assigns a temporary DHCP IP address to a device so it can contact the Plug-and-Play server. Design > Plug and Play > DHCP Helper 	1.3.0-365	IND Online Help

IND Licenses

Table 1 New Features in IND 1.3.x (continued)

Feature	Description	First released	Related Documentation
IND Device Pack 1.3.0	<p>Cisco Universal IOS images supported:</p> <ul style="list-style-type: none"> ■ 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 <p>Note: See Limitations and Restrictions, page 11 for image limitations.</p> <p>The device pack supports the following Cisco and Rockwell Automation/Allen-Bradley platforms:</p> <p>Cisco platforms:</p> <ul style="list-style-type: none"> ■ CGS 2520 ■ IE 1000, IE 2000, IE 2000U <p>Note: IND only supports PROFINET clients on IE 1000.</p> <ul style="list-style-type: none"> ■ IE 3000, IE 3010 ■ IE 4000, IE 4010 ■ IE 5000 <p>Rockwell Automation/Allen-Bradley platforms:</p> <ul style="list-style-type: none"> ■ 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 	1.3.0-365	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
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.
```

Pre-Configuration Requirements for IE Switches

```
# 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:

Pre-Configuration Requirements for IE Switches

```

# Secure-mode only
# 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 server
ip http secure-server
ip http port 80
ip http secure-port 443
ip http authentication local

# 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

```

Installation Notes

```
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 1.3.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 1.3.0-365, 1.3.0 is the version number and 365 is the release number.

A new Device Pack must be version 1.3.0 and the release must be 365 or higher.

Installation Steps

For Device Pack installation steps, refer to the [Installation Guide for Cisco Industrial Network Director, Release 1.3.x](#).

Important Notes

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

Unsupported PIDs

The following IE 2000 PIDs are not supported by IND 1.1.x and are not supported by IND 1.1.0-x Device Packs:

- IE-2000-4TS-G-B-U
- IE-2000-8TC-G-B-U
- IE-2000-16TC-G-E-U

Supported Cisco IOS Software

IND 1.3.x supports the following Cisco IOS Releases:

- 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 1.2.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.

- 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

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](#)
- [Resolved Caveats, page 12](#)
- [Accessing the Bug Search Tool, page 12](#)

Open Caveats

There are no Open caveats for this release.

Resolved Caveats

The following caveats are resolved in IND release version 1.3.1-5 (bug fix only release).

Table 3 Resolved Caveats

Caveat	Headline
CSCvh16941	PnP profile: Template variables having space are not displayed correctly during Edit & Claim
CSCvh20558	PnP Profile form - example for device list is in the form of IP Address
CSCvh26253	Upgrade from 1.2 to 1.3 fails for no Other devices

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 1.3.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)

Related Documentation

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.

Related Documentation