Release Notes for Industrial Network Director, Release 1.9.x

First Published: September 30, 2020
Last Updated: January 11, 2021

These release notes contain the latest information about using Release 1.9.0 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 1.9.0 provides the following language support in addition to English: French, German, Japanese, and Spanish-Latin America.

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 1.9.0.
IND Licenses and PIDs	Summary of support licenses for Release 1.9.0 and link to data sheet for PIDs.
System Requirements	System requirements for Release 1.9.0.
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.
Caveats	Open and Resolved caveats in Release 1.9.0.
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

Note: When you upgrade from IND 1.8.x to IND 1.9.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

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

Table 1 lists new platforms and features that are managed in IND 1.9.0.

Table 1 New Features in IND 1.9.0

Feature	Description	Related Documentation
User Interface Changes	■ Group View is now found in the Main menu. ■ Role Based Access Control permission has been renamed to User Management ■ Network discovery permission is a new permission in IND 1.9, which is created upon upgrade for users who had Network permission in 1.8.	IND Online Help
Permission changes	Two new permissions are supported: ■ Discovery: Provides support for Discovery and Plug and Play	IND Online Help

Table 1 New Features in IND 1.9.0

Feature	Description	Related Documentation
New Permission Support for System Administrator	Two new permissions are supported for the System Administrator: ■ Group Based Access Control (GBAC): Allows a system administrator to restrict user access to only those devices within specific groups and sub-groups to which the user is assigned. ■ Management of Groups and Devices across groups. Changes to the IND user interface to support the two new permissions noted above are listed below: - Role-based Access Control is renamed to 'User Management'. - A new permission, 'Discovery', provides access for performing Discovery and Plug and Play (PnP) to System Administrators by default. **Only the System Administrator has the Discovery permission**. - A network administrator has Device Management permission. **Settings > Users**	IND Online Help
Create a Sub-Group Under an Existing Root Group	In the left-panel, click on Root and then click on the **Add Group** button (top, right pane). In the panel that displays, enter the Name and Description in the appropriate fields. Click **Save**. **Groups > Root > Add Group**	IND Online Help
Inventory View	Allows you to view the list of devices that a specific user can access. No other devices will display. **Operate > Inventory**	IND Online Help
Alarms View	Allows you to view the list of alarms that a user can access. **Operate > Alarms**	IND Online Help
Alarms Assignment	A user can assign alarms to users who are part of the same group. **Operate > Alarms**	IND Online Help
Delete Group Validation	Ensures that you cannot delete a group if there are any users associated with that group. An error message displays if mistakenly attempt to delete a group with users assigned to it. **Settings > Group Management**	IND Online Help

Table 1 New Features in IND 1.9.0

Feature	Description	Related Documentation
Resilient Ethernet Protocol	Resilient Ethernet Protocol (REP) is a proprietary protocol that provides an alternative to the Spanning Tree Protocol (STP) to control loops, and to handle link failures and improve convergence times. REP is supported and monitored on Cisco IE switches and Rockwell switches by IND. Cisco REP is a segment protocol and is **only supported** on Layer 2 interfaces. The following REP-related information is collected by IND: - Role of the node in a REP segment - Segment topology details ■ New Alarm Support for REP-licensed devices: – REP Segment Preempt Failed: An alarm is generated when the trigger for the segment preemption happened; however, for some reason the segment failed to preempt as expected. – REP Segment Preemption Trigger Failed: An alarm is generated when preemption on the segment is not performed because the preemption trigger failed. The failure could be due to an invalid port ID or a neighbor number. **Note:** To monitor REP devices, you **must** move the devices to the Licensed State. REP is supported on Cisco IE switches and Rockwell switches; and, IND monitors REP on both of the switch families. **Operate > Alarm Settings > Redundancy Protocols** **Operate > Inventory**	IND Online Help
REP Topology	You can view the REP segment path that connects all REP member nodes by clicking on the REP Overlay that appears at the top of the Topology display. The segment number is obtained from the device. Click the Discover Topology button to display nodes and links in the topology. Information displayed is learned from one of the following tables: CDP, LLDP or MAC address **Note:** To ensure an accurate Topology view, you must initiate a Topology Discovery when on of the two tasks noted below is performed: – Asset Discovery Scan – Supported Device Move to Licensed **Operate > Topology**	IND Online Help

Table 1 New Features in IND 1.9.0

Feature	Description	Related Documentation
IND Device Pack 1.9	■ Cisco IND Release 1.9 Cisco Universal IOS images supported: ■ Cisco IOS Release 15.2(7)E2 ■ Cisco IOS Release 15.2(7)E1a ■ Cisco IOS Release 15.2(7)E ■ 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)E2, Cisco IOS Release 15.2(5)E1, Cisco IOS Release 15.2(5)E ■ Cisco IOS Release 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 **Note:** See Limitations and Restrictions, page 14 for image limitations. The device pack supports the following Cisco and Rockwell Automation/Allen-Bradley platforms: ■ Cisco IOS platforms supported: CGS 2520, IE 2000, IE 2000U, IE 3000, IE 3010, IE 4000, IE 4010 and IE 5000 ■ Cisco IOS XE platforms supported: IE3200, IE 3300 and IE 3400	---
IND Device Pack 1.9, continued	Rockwell Automation/Allen-Bradley platforms: ■ Stratix 8000/8300 Modular Managed Ethernet Switches ■ Stratix 5800 Industrial Managed Ethernet Switches ■ Stratix 5400 and 5700 Industrial Ethernet Switches ■ Stratix 5410 Industrial Distribution Switches ■ Stratix 2500 Lightly Managed Switches	---

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 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 and transition
the device from UNLICENSED to LICENSED state in secure mode.

- 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

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

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

```
# 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 1.9.0.

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 1.9.x, 1.9 is the version number and x is the release number.

A new Device Pack must be version 1.9.0.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.9.0.

Important Notes

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

- When you upgrade to IND 1.9.0, 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 1.8.0 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.

- 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.

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
- Accessing the Bug Search Tool

Open Caveats

Table 3 Open Caveats

Caveat Number	Description
CSCvv54833	CIP Daisy Chain issue
CSCvv93349	Unable to register IND with ISE on 2.4 P13 and 2.6P7

Table 4 Platform-related Open 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 1.9.0

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.