Release Notes for Cisco Industrial Network Director, Release 1.6.x

First Published: 2018-12-26
Last Updated: 2019-02-08

These release notes contains the latest information about using Release 1.6.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 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)

- Maintain (Maintenance)
- Settings

Release 1.6.x supports the following new IND features and enhancements summarized in Table 1.

Table 1 Features Supported in IND 1.6.0-438 and later

Feature	Description	Related Documentation
IND Installer Enhancement	The IND install process now allows you to select from two installation options based on the available storage available on your Microsoft Windows Operating System (OS): ■ Regular Profile: Choose this option when your Windows OS system **does** meet the minimum system requirements specified in the Installation Guide for Cisco Industrial Network Director, Release 1.6.x ■ Micro Profile: Choose this option when your Windows OS system **does not** meet system requirements noted in the Installation Guide for Cisco Industrial Network Director, Release 1.6.x Maintain > Software Images	Installation Guide for Cisco Industrial Network Director, Release 1.6.x
OPERATE menu changes		
User interface (UI) Design Change	New message for a CIP device such as a Discovered Bridge Device lets you know when to move the device to a licensed state: Move this device to licensed state to enable the following features: - DLR Monitoring - Discover downstream devices using CIP Routing. Operate > Inventory	IND Online Help
Upgrade or Downgrade a Cisco IOS software image on an IE switch.	After selecting the desired Cisco IOS software, you can initiate an upgrade or downgrade by selecting the Upgrade icon and confirming your software and IE switch (including IE 1000) selection in subsequent pages that display. Operate > Inventory > Device > Details **Note:** You can also perform this software image install on the Maintain > Software Images page.	IND Online Help

Table 1 Features Supported in IND 1.6.0-438 and later

Feature	Description	Related Documentation
Device Level Ring (DLR) Supervisor Monitoring	Allows you to monitor the DLR status of the Supervisor Module and Ring Nodes. To initiate this DLR monitoring capability, IND allows you to assign licenses to the Supervisor nodes (Stratix and non-Stratix nodes listed below). ■ 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 > Inventory	IND Online Help
DLR Topology Discovery	You can view the DLR ring path that connects all DLR member nodes by clicking on the badge that appears at the top of the Topology display. It does not show the link details. (Nodes and links shown in the topology represent information learned through either the CDP, LLDP or MAC address table.) The Ring number is obtained by the device. Click the **Discover Topology** button. Nodes and links shown in the topology represent information learned through either the CDP, LLDP or MAC address table. **Note:** To ensure an accurate Topology view, you must initiate a Topology Discovery when one of the two tasks noted below is performed. ■ Asset Discovery Scan ■ Supported Device Move to Licensed Operate > Topology	IND Online Help
MAINTAIN menu changes		
Configuration Restore	For Cisco IOS IE devices, feature allows you restore a backed up Startup Configuration of a switch to the Startup Configuration. Device reload occurs. For IE1000 devices, feature allows you restore a backed up Running Configuration of a switch. After a successful restore, the Running Configuration is saved to the Startup Configuration of a switch. Maintain > Configuration Archives	IND Online Help
SETTINGS menu changes		

Table 1 Features Supported in IND 1.6.0-438 and later

Feature	Description	Related Documentation
External Authentication	Allows you to select the authentication mode for authenticating and authorizing IND users. A remote user is only granted access when both authentication and authorization are successful. Settings > Users > External Authentication	IND Online Help
New Page: Security Settings	A new page, Security Settings, allows.you to set the SSL Security Level (TLSv1.2, by default) for SSL communications such as Plug-n-Play (PnP) and Web UI services. **Note:** For non-SSL communications, the settings are: Strong (default setting) or Weak. **Note:** When PnP provisioning is running on IE switches running 15.2(4)EA*x,* the setting will remain set at "Certificate-Install_success state" since devices with this software version only use TLSv1.0 SSL. To proceed with PnP provisioning on an IE switch running 15.2(4)EA*x* software, you can change the Security Level in Security Settings page to 'weak' which will enable TLSv1.0, TLSv1.1 and TLSv1.2 SSL versions for SSL communications. Settings > System Settings > Security Settings	IND Online Help
Access to two Cisco Identity Services Engine (ISE) systems provides High Availability for Cisco Platform Exchange Grid (pxGrid)	Cisco pxGrid (Platform Exchange Grid) 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. IND can connect up to two Cisco ISE systems, each of which is selected from an available server pool, in a round robin fashion, to provide high-availability to pxGrid. Each of the ISE controllers has a different IP and hostname. Each of these IP and host names must be configured within IND pxGrid settings. **Note:** IND must be registered in Cisco Identity Services Engine (ISE) as a pxGrid node. **Note:** Endpoint information from IND is shared with Cisco Identity Services Engine (ISE) by integrating pxGrid in the IND application. Settings > Policy Servers	IND Online Help Deploying Cisco Industrial Network Director with ISE using pxGrid
RADIUS Server Protocol Support	IND allows you to select a single RADIUS server or multiple RADIUS servers. Settings > Policy Servers	IND Online Help

Table 1 Features Supported in IND 1.6.0-438 and later

Feature	Description	Related Documentation
Simple and Advanced Toggle Switch for Policy Server	■ Simple option allows you to define the following for servers: Protocol, Host Name, IP address, Description, AAA Settings (Reset Shared or Secret Option) ■ Advanced option includes all Simple options plus additional AAA settings (Retries, Timeout, Authentication Port). Settings > Policy Servers	IND Online Help
IND Device Pack 1.6	Cisco Releases 1.6 and 1.7 (Industrial Ethernet 1000 only) Cisco Universal IOS images supported: ■ 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 Cisco Universal IOS XE images supported: ■ Cisco IOS 16.10 XE **Note:** See Limitations and Restrictions, page 11 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, IE 3400 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 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)
Browser	Chrome: Version 50.0.2661.75, 53.0.2785.116 Firefox: 55.0.3, 57.0.4, 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.

Note: In all configuration examples below, a Hashtag (#) precedes all comment text.

- 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 device must be pre-configured for either SNMPv2 or SNMPv3 in order for the system to successfully
discover it:

#Device Prerequisite Configuration for SNMPv2

    snmp-server community <read-community> RO

#Device Prerequisite Configuration for SNMPv3
# Supported mode values are [priv, auth, noauth]
# Supported authentication_type values are [sha,md5]
# Supported privacy_type values are [aes 128, des]

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

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

#The device must be pre-configured for either Telnet/HTTP or SSH/HTTPs for the system to successfully
transition the device from UNLICENSED to LICENSED state.

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,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 1.6.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 1.6.x, 1.6 is the version number and x is the release number.

A new Device Pack must be version 1.6.x and the release must x value or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.6.x.

Important Notes

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

Supported IND Release Upgrades

You can perform the following IND upgrades:

- Upgrade from 1.5.x to 1.6.x
- 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.

- pxGrid service needs to be registered again after the upgrade from 1.5 to 1.6 if Cisco ISE servers are in HA mode.
- PnP process is supported only on single-homed (Single IP) IND servers for Cisco IOS Release 15.2(6)E1.
- A PnP Service Error 1410 occurs in Cisco IOS Release 15.2(6)E0a due to AAA command not working (CSCvg64039)
- IE 5000: Horizontal Stacking is not supported. Stacked devices can be discovered on IND but cannot be licensed.

- IE2000/IE3000: Image upgrade is not supported without a SD Card through IND. For a successful image upgrade from IND, currently running images of Cisco IOS should be set to SD Flash on these product families. Device manager can be used to upgrade software images for devices with no SD Card.

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 12

Open Caveats

Table 3 displays open caveats for IND 1.6

Table 4 displays open caveats for Industrial Ethernet switches that may affect the functionality of IND 1.6.

Table 3 IND 1.6 Open Caveats

Bug ID	Headline
CSCvn26802	Tasks are not completing in some rare scenarios

Table 4 Platform-related Open Caveats

Bug ID	Headline
CSCvm36711	IE1000 devices do not return hostname in PnP work response.
CSCvn65113	SNMP Engine ID to be unique ID per device, currently all 16.x releases display 800000090300000000000000.
CSCvn75300	PnP: AAA authorization failed with (15.2(4)) image.

Resolved Caveats

Table 5 IND 1.6.1 Resolved Caveats

Bug ID	Headline
CSCvo06289	Cannot save the Access Profile with SSH enabled in JA, DE and ES-XL.
CSCvm90058	Duplicate mac address for unknown 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 1.6.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